Artin-Schreier extensions of normal bases

David Thomson, Colin Weir

Artin-Schreier extensions of normal bases

David Thomson[1] and Colin Weir[2]

[1] School of Mathematics and Statistics, Carleton University, 1125 Colonel By Dr., Ottawa, Ontario, Canada, K1S 5B6.
dthomson@math.carleton.ca

[2] Department of Mathematics, Simon Fraser University, 8888 University Dr., Burnaby, British Columbia, Canada, V5A 1S6.
colin_weir@sfu.ca

Abstract. This manuscript deals with extending a normal basis 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.
MSC 2010 Classification: 12E30, 12E20, 11T30, 12Y05
Keywords: Finite fields, normal bases, complexity, Artin-Schreier extensions.

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 α 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*) $\{1, \alpha, \ldots, \alpha^{n-1}\}$.

Of course, multiple forms of 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 [10, 11], for example. Reducing the complexity of multiplication using a normal basis representation is an active area of study whereby normal bases with few non-zero structure constants (entries in the multiplication tables) are sought after; lower bounds and constructions can be found in [1, 2, 9], 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. We conclude and comment on some natural generalizations of this work in Section 6.

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 $\alpha^{q^i}\alpha^{q^j} = \sum_{k=0}^{n-1} t_{ij,k}\alpha^{q^k}$. 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 [6], and the details on arithmetic using normal bases can be found in Sections 5.2-3, 11.1 and 16.7.4-5 of [8].

It was shown in [9] 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 studied in [9] and fully characterized in [3].

Theorem 1. [3] *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 α 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 γ.*

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 γ be a primitive r-th root of unity in $\mathbb{F}_q^{nt}$. Furthermore, let κ 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, 2] *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 these 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 normal bases for certain field extensions from others; the first is via a product construction and the second is via a projection mapping. These are outlined respectively in the two theorems below.

Theorem 5. [8, 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. [8, Theorem 5.3.14] *Let* α *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 [7] provides the minimum complexity normal basis of $\mathbb{F}_{2^\ell}$ 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. [4, 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* σ *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. [4, 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* α *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* α *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* α *is a normal element, then* $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) \neq 0$*.*

2. For $\alpha \in \mathbb{F}_q$, $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = 0$ if and only if $\alpha = \beta^q - \beta$ for some $\beta \in \mathbb{F}_q$.

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_α 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_α 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 β 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 α. 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 γ^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 ith 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, square is preformed in $\mathcal{O}(\log n)$ n-bit word XORs; 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 α 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

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

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:

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

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 ith 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 [2].

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.

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_0th 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

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

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 ℓ_k. If $j - i \equiv n/2 \pmod{n}$ (if $j = 0$), then $t_{j-i,k-i} = 1$ for all k, and $\sum_{\ell=0}^{n-1} \alpha^{q^\ell} + \sum_{0 \leq k < n, k \neq n/2} \sum_{\ell=0}^{n-1} t_{k\ell}\alpha^{q^\ell}$. As $k \neq n/2$ varies, $t_{kl} = 1$ for distinct values of $\ell \neq 0$; hence $\sum_{\ell=0}^{n-1} \alpha^{q^\ell} + \sum_{0 \leq k < n, k \neq n/2} \sum_{\ell=0}^{n-1} t_{k\ell}\alpha^{q^\ell} = \alpha$. 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. For brevity, we omit the proof from this extended abstract. □

Following [7], 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, whereas optimal normal bases have complexity $4n - 1$. The total number of non-zeroes across all multiplication tables is $2nc_N$. Hence, the expected total number of non-zeroes for a random normal bases is $4n^3$, and optimal normal bases have less than $4n^2$ non-zeroes. In comparison, Artin-Schreier extensions of Type I and Type II optimal normal bases have less than $10n^2$ and $12n^2$ non-zeroes across all multiplication tables 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

The accompanying website `http://www.math.carleton.ca/~daniel/hff/` to [8, Section 2.1] contains the normal basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ of lowest complexity by exhaustive search for $n \leq 39$ and by the methods of Section 2 for $n \geq 40$.

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.

n	c_N	nnz_AS	$\frac{\text{nnz\_AS}}{n}$	n	c_N	nnz_AS	$\frac{\text{nnz\_AS}}{n}$	n	c_N	nnz_AS	$\frac{\text{nnz\_AS}}{n}$
4	7	29	7.25	26	51	3301	126.96	48	425	14041	**292.52**
6	11	77	12.83	28	55	2189	78.18	50	99	15349	306.98
8	21	137	**17.13**	30	59	3805	126.83	52	103	7805	150.10
10	19	245	24.50	32	361	7361	**230.03**	54	209	23245	430.46
12	23	365	30.42	34	243	7381	**217.09**	56	399	7673	**137.02**
14	27	705	50.36	36	71	3133	87.03	58	115	9749	168.09
16	85	905	**56.56**	38	207	11997	315.71	60	119	10445	174.08
18	35	869	48.28	40	189	6665	**166.63**	62	351	42397	683.82
20	63	941	**47.05**	42	135	10921	260.02	64	1829	61865	**966.64**
22	63	1325	**60.22**	44	147	7549	171.57	66	131	12677	192.08
24	105	1369	**57.04**	46	135	6077	**132.11**	68	567	42413	623.72

Table 1. Complexity c_N of a normal basis versus non-zeroes (nnz_AS) of Artin-Schreier multiplication tables for even $n = 4, \ldots, 68$.

We explain Table 1 here. The heading nnz_AS is the number of non-zeroes in the multiplication tables of the Artin-Schreier extension basis. The following column is normalized by the degree for comparison with the complexity of the best-known normal bases c_N. Bold entries indicate when the normalized value is less than the best-known complexity of a normal basis for this degree.

6 Conclusions

In this paper we study bases of quadratic extensions of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ by extending normal bases with roots of Artin-Schreier polynomials. These extended bases permit efficient squaring, taking advantage of their underlying normal bases. They also permit efficient multiplication: for 12 even-degree extensions $4 \leq n \leq 64$, our bases have less non-zero entries in their multiplication tables than the normal basis with the minimum-known complexity. Moreover, the number of non-zero terms in the multiplication tables of the Artin-Schreier extension basis depends only on the form of the multiplication table of the normal basis and hence require little storage.

From this work there are a number of natural directions for further investigation. We observe that Artin-Schreier theory holds identically over finite fields of any characteristic, and also for prime power extension degrees. We also observe that we could use the above 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. For all of these directions, one may expect that the larger non-normal extension will cause the arithmetic of the extended basis to resemble that of a power basis and less so 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. Our initial investigations support this observation, though we are optimistic that the additional cost of exponentiation can be kept manageable.

Acknowledgement. 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. 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.
3. S. Gao and H. W. Lenstra, Optimal normal bases, *Designs, Codes and Cryptography*, **2** (1992), 315-323.
4. S. Lang, *Algebra (3rd ed.)*, Graduate Texts in Mathematics **211**, Springer (2002).
5. R. Lidl and H. Niederreiter, *Finite Fields (2nd ed.)*, Cambridge University Press, Cambridge, UK. (1997).
6. 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).
7. 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.
8. G. L. Mullen and D. Panario, *Handbook of Finite Fields*, CRC Press, Boca Raton, FL. (2013).
9. 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.
10. Y. Nawaz and G. Gong, The WG Stream Cipher, ECRYPT Stream Cipher Project Report 2005/033. Available at `http://www.ecrypt.eu.org/stream`.
11. 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.