On finite field arithmetic in characteristic 2

Tony Ezome, Mohamadou Sall

ON FINITE FIELD ARITHMETIC IN CHARACTERISTIC 2

TONY EZOME AND MOHAMADOU SALL

ABSTRACT. We are interested in extending normal bases of $\mathbf{F}_{2^n}/\mathbf{F}_2$ to bases of $\mathbf{F}_{2^{nd}}/\mathbf{F}_2$ which allow fast arithmetic in $\mathbf{F}_{2^{nd}}$. This question has been recently studied by Thomson and Weir in case d is equal to 2. We construct efficient extended bases in case d is equal to 3 and 4. We also give conditions under which Thomson-Weir construction can be combined with ours.

.

1. INTRODUCTION

Representing elements of a finite field extension $\mathbf{F}_{q^m}/\mathbf{F}_q$ by using normal bases is adequate when doing arithmetic in $\mathbf{F}_{q^m}$. The main computational advantage of these bases is that they allow fast exponentiation by q, this corresponds simply to a cyclic shift of coordinates. When computing arbitrary products in $\mathbf{F}_{q^m}$, Gao, von zur Gathen, Panario and Shoup [5] showed that fast multiplication methods such as FFT can be adapted to normal bases of $\mathbf{F}_{q^m}/\mathbf{F}_q$ constructed from Gauss periods over $\mathbf{F}_q$. On the other hand, Couveignes and Lercier [3] constructed an FFT-like multiplication algorithm with normal bases of $\mathbf{F}_{q^m}/\mathbf{F}_q$ obtained from elliptic curves over $\mathbf{F}_q$. But the existence of these efficient normal bases puts constraints on the sizes of m and q. If there is no efficient normal bases of $\mathbf{F}_{q^m}/\mathbf{F}_q$ for some m and q, one may hope that m has a proper divisor n such that $\mathbf{F}_{q^n}/\mathbf{F}_q$ admits an efficient normal basis $\mathcal{N} = (\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}})$. Set $m = nd$. Then any basis $B = (\beta_j)_{0\leq j\leq d-1}$ of $\mathbf{F}_{q^m}/\mathbf{F}_{q^n}$ obviously induces a basis $\Theta = (\alpha^{q^i}\beta_j)_{i,j}$ of $\mathbf{F}_{q^m}/\mathbf{F}_q$. This is not a normal basis, since the q-Frobenius automorphism does not act on B. We call such a basis as Θ an *extension of* $\mathcal{N}$ *with degree* d. In this paper, we construct bases of $\mathbf{F}_{q^m}/\mathbf{F}_q$ by extending normal bases of $\mathbf{F}_{q^n}/\mathbf{F}_q$ and we show that arithmetic operations in $\mathbf{F}_{q^m}$ may be efficiently computed (at least in some cases) by using these extended bases. Let us recall one of the basics of complexity theory in our context. Assume that Γ is a straight-line program which computes the coordinates of the product $x \times y$ in an arbitrary basis $\mathcal{B}$ of $\mathbf{F}_{q^m}/\mathbf{F}_q$ from the ones of x and y by using additions, subtractions, multiplications of a register by a constant, and additions, subtractions, multiplications between two registers. Then the *complexity* of Γ is the total number of such operations. The complexity of $\mathcal{B}$ is defined to be the minimal possible complexity of a straight-line program computing the coordinates of $x \times y$ from the ones of x and y. In addition, we introduce the following terminology.

Definition 1. *Let $\mathcal{N} = (\alpha^{q^i})_{0\leq i\leq n-1}$ be a normal basis of $\mathbf{F}_{q^n}/\mathbf{F}_q$ (this means that $\mathcal{N}$ is a basis of $\mathbf{F}_{q^n}/\mathbf{F}_q$ generated by the normal element α).*

Research supported by Simons Foundation, Inria International Lab LIRIMA, and ICTP.

1. The multiplication table of $\mathcal{N}$ is defined to be the matrix $T = (t_{i,j})_{0\leq i,j\leq n-1}$ given by

$$\alpha\alpha^{q^i} = \sum_{j=0}^{n-1} t_{i,j}\alpha^{q^j},\ i = 0, 1 \ldots, n-1. \tag{1}$$

2. The weight of $\mathcal{N}$, denoted by $w(\mathcal{N})$, is defined to be the total number of non-zero entries $t_{i,j}$.
3. The density of $\mathcal{N}$, denoted by $d(\mathcal{N})$, is equal to $n \times w(\mathcal{N})$.
4. For $i, j, k, l \in \{0, \ldots, n-1\}$, the products $t_{i,j}t_{k,l}$ are called the cross-products of the multiplication table of $\mathcal{N}$.
5. Let $\mathcal{B} = (b_i)_{0\leq i\leq m-1}$ be an arbitrary basis of $\mathbf{F}_{q^m}/\mathbf{F}_q$. For $i, j \in \{0, 1 \ldots, m-1\}$, set

$$b_i b_j = \sum_{k=0}^{m-1} t_{i,j}^k b_k. \tag{2}$$

(i) The multiplication tables of $\mathcal{B}$ are defined to be the matrices $(T_0, T_1, \ldots, T_{m-1})$, where

$$T_k = (t_{i,j}^k)_{0\leq i,j\leq m-1} \tag{3}$$

is defined from equation (2).

(ii) The density of $\mathcal{B}$, denoted by $d(\mathcal{B})$, is defined to be the total number of non-zero entries $t_{i,j}^k$ for $i, j, k \in \{0, \ldots, m-1\}$.

Addition and substraction of two elements

$$X = \sum_{0\leq k\leq m-1} x_k b_k \text{ and } Y = \sum_{0\leq k\leq m-1} y_k b_k \text{ in } \mathbf{F}_{q^m}$$

expressed in an arbitrary basis $\mathcal{B} = (b_k)_{0\leq k\leq m-1}$ of $\mathbf{F}_{q^m}/\mathbf{F}_q$ are performed componentwise and easy to implement. But multiplication may be more difficult. Set $Z = X \times Y$, and denote by $\sum_{0\leq k\leq m-1} z_k b_k$ the decomposition of Z in $\mathcal{B}$. The coefficients z_k are obtained from the multiplication tables $(T_k)_{0\leq k\leq m-1}$ of $\mathcal{B}$ as follows:

$$z_k = XT_k{}^tY. \tag{4}$$

So the number of operations required to implement multiplication in $\mathbf{F}_{q^m}$ from the multiplication tables of $\mathcal{B}$ depends on the density of $\mathcal{B}$. This means that normal bases having low weight have good complexity. On the other hand, there are quasi-linear time algorithms (for instance the one described in [3]) which output the coordinates of $X \times Y$ in a normal basis $\mathcal{N}$ from the ones of X and Y without using the multiplication table of $\mathcal{N}$. But if the known normal bases of $\mathbf{F}_{q^m}/\mathbf{F}_q$ have bad complexity, one may turn to extensions of normal bases of intermediate fields. This means that we first look for suitable subfields $\mathbf{K}$ of $\mathbf{F}_{q^m}$ containing $\mathbf{F}_q$ such that there exists an efficient normal basis $\mathcal{N}$ of $\mathbf{K}/\mathbf{F}_q$, and then we extend $\mathcal{N}$ to a basis of $\mathbf{F}_{q^m}/\mathbf{F}_q$. In [11] the authors constructed extended bases in characteristic 2 by using Artin-Schreier theory. So they focused on the case when the degree is equal to 2. In the present paper we construct extended bases whose degree is equal to 3 and 4 by using Kummer theory and Artin-Schreier-Witt theory. We also give conditions under which Thomson-Weir construction can be combined with ours. When the original normal basis $\mathcal{N}$ has subquadratic weight and subquadratic complexity, we show that all the resulting extended bases have subquadratic complexity.

Plan. In Section 2 we present quadratic Artin-Schreier extended bases and degree 4 Artin-Schreier-Witt extended bases. In Section 3 we describe degree 3 Kummer extended bases. Section 4 is devoted to extended bases in the context of towers of field extensions obtained from Artin-Schreier and Kummer theories.

Notation: Throughout this paper $\mathbf{K}$ denotes a field with characteristic $p > 0$, and $\overline{\mathbf{K}}$ is an algebraic closure of $\mathbf{K}$.

2. Extended bases whose degree is a power of 2

In this section we recall general results concerning cyclic extensions of $\mathbf{K}$ whose degree is a p-power, and we specify the case when $\mathbf{K}$ is a finite field with characteristic 2.

2.1. **Artin-Schreier extended bases in characteristic** 2**.** It is proved in [[6], Chapter VI, Theorem 6.4] that any degree p cyclic extension of $\mathbf{K}$ is generated by a root of a polynomial of the form

$$X^p - X - \alpha,$$

where $\alpha \in \mathbf{K}$ lies outside of the set $\{x^p - x \,|x \in \mathbf{K}\}$. Irreducible polynomials of this type are useful both for constructing efficient normal bases and for extending them. For instance in [[4], Theorem 1] the authors constructed a normal basis of $\mathbf{K}[X]/(X^p - X - \alpha)$ over $\mathbf{K}$ with low weight and quasi-linear complexity. On the other hand, *degree p Artin-Schreier extended bases* defined below are constructed from irreducible polynomials of the form $X^p - X - \alpha$.

Definition 2. *Let p be a prime number and q a power of p. Let $\mathcal{N} = (\alpha^{q^i})_{0\leq i\leq n-1}$ be a normal basis of $\mathbf{F}_{q^n}/\mathbf{F}_q$. Denote by $\overline{\mathbf{F}_q}$ an algebraic closure of $\mathbf{F}_q$ containing $\mathbf{F}_{q^n}$. A degree p Artin-Schreier extension of $\mathcal{N}$ (also Artin-Schreier extended basis) is a basis $\mathcal{A}$ of $\mathbf{F}_{q^{np}}/\mathbf{F}_q$ for which there exists β in $\overline{\mathbf{F}_q}$ outside of $\mathbf{F}_{q^n}$ such that $\beta^p - \beta = \alpha$ and $\mathcal{A} = (\alpha^{q^i}\beta^j)_{i,j}$.*

It is shown that any normal basis $\mathcal{N} = (\alpha, \alpha^2, \dots, \alpha^{2^{n-1}})$ of $\mathbf{F}_{2^n}/\mathbf{F}_2$ admits an Artin-Schreier extension. Indeed, assume that the polynomial $f(X) = X^2 + X + \alpha$ is reducible over $\mathbf{F}_{2^n}$. Then the additive form of Hilbert's Theorem 90 ensures that $\mathrm{Tr}_{\mathbf{F}_{2^n}/\mathbf{F}_2}(\alpha) = 0$. But this is impossible since α is a normal element of $\mathbf{F}_{2^n}/\mathbf{F}_2$. Hence any β in $\mathbf{F}_{2^{2n}}$ satisfying

$$\beta^2 + \beta = \alpha$$

defines a quadratic Artin-Schreier extension $\mathcal{A} = \mathcal{N} \cup \beta\mathcal{N}$ of $\mathcal{N}$. The following statement describes squaring in $\mathbf{F}_{2^{2n}}$, it also gives the complexity and density of $\mathcal{A}$.

Proposition 1. *Let $\mathcal{N} = (\alpha, \alpha^2, \dots, \alpha^{2^{n-1}})$ be a normal basis of $\mathbf{F}_{2^n}/\mathbf{F}_2$ and β an element in $\mathbf{F}_{2^{2n}}$ such that $\mathcal{A} = \mathcal{N} \cup \beta\mathcal{N}$ is a degree 2 Artin-Schreier extension of $\mathcal{N}$.*

1. Squaring in $\mathbf{F}_{2^{2n}}$ is given by

$$(C + \beta D)^2 = (C_> + E) + \beta D_>,$$

where $C_>$ and $D_>$ stand for right-cyclic shifts of the coordinate vectors of C and D, and

$$E = {}^tD_> \times T$$

is a vector-matrix multiplication between the transpose of $D_>$ and the multiplication table of $\mathcal{N}$.

2. The complexity of $\mathcal{A}$ consists in at most:
   (a) 3 multiplications and 4 additions between elements lying in $\mathbf{F}_{2^n}$;
   (b) 1 vector-matrix multiplication between a vector of $\mathbf{F}_{2^n}/\mathbf{F}_2$ and the multiplication table of $\mathcal{N}$.

3. If $\mathcal{N}$ has subquadratic complexity and subquadratic weight, then $\mathcal{A}$ has also subquadratic complexity.

4. Let $w(\mathcal{N})$ be the weight of $\mathcal{N}$. For $(i,\delta) \in \{0,\ldots,n-1\} \times \{0,1\}$, set $\mathfrak{a}_{i+\delta n} = \alpha^{2^i}\beta^\delta$ so that $\mathcal{A} = (\mathfrak{a}_k)_{0\leq k\leq 2n-1}$.
   (a) For $0 \leq k \leq n-1$, the number of non-zero entries in the k-th multiplication table of $\mathcal{A}$, is equal to

$$w(\mathcal{N}) + \sum_{0\leq i,j\leq n-1} \varphi(\sum_{r=0}^{n-1} t_{j-i,r-i}t_{r,k}),$$

   where subscripts are taken modulo n, $(t_{i,j})_{0\leq i,j\leq n-1}$ is the multiplication table of $\mathcal{N}$, and φ is the unique ring homomorphism from $\mathbf{F}_2$ into $\mathbb{Z}$.
   (b) The k-th multiplication table of $\mathcal{A}$, for $n \leq k \leq 2n-1$, has $3w(\mathcal{N})$ non-zero entries.

The density of $\mathcal{A}$ is given by

$$d(\mathcal{A}) = 4d(\mathcal{N}) + \sum_{0\leq k\leq n-1}\sum_{0\leq i,j\leq n-1} \varphi(\sum_{0\leq r\leq n-1} t_{j-i,r-i}t_{r,k}).$$

Proof. 1. This is [[11], Proposition 3.7]. Let $C = \sum_{i=0}^{n-1} c_i\alpha^{2^i}$ and $D = \sum_{i=0}^{n-1} d_i\alpha^{2^i}$ be the linear combinations of C and D with respect to $\mathcal{N}$. We have

$$\begin{aligned}(C+\beta D)^2 &= \textstyle\sum_{i=0}^{n-1} c_{i-1}\alpha^{2^i} + \beta^2 \sum_{i=0}^{n-1} d_{i-1}\alpha^{2^i}\\ &= \textstyle\sum_{i=0}^{n-1} c_{i-1}\alpha^{2^i} + (\beta+\alpha) \sum_{i=0}^{n-1} d_{i-1}\alpha^{2^i}\\ &= \Big(\textstyle\sum_{i=0}^{n-1} c_{i-1}\alpha^{2^i} + \sum_{i=0}^{n-1} d_{i-1}\alpha\alpha^{2^i}\Big) + \beta \sum_{i=0}^{n-1} d_{i-1}\alpha^{2^i}.\end{aligned}$$

So

$$(C+\beta D)^2 = \Big(\sum_{i=0}^{n-1} c_{i-1}\alpha^{2^i} + \sum_{i=0}^{n-1} d_{i-1}\sum_{k=0}^{n-1} t_{i,k}\alpha^{2^k}\Big) + \beta\sum_{i=0}^{n-1} d_{i-1}\alpha^{2^i},$$

where subscripts are taken modulo n and $(t_{i,k})_{i,k}$ stands for the multiplication table of $\mathcal{N}$. The term $\sum_{i=0}^{n-1} d_{i-1}\sum_{k=0}^{n-1} t_{i,k}\alpha^{2^k}$ corresponds to a vector-matrix multiplication between the transpose of the right-cyclic shift of the coordinate vector of D and the multiplication table of $\mathcal{N}$. Assume that $\mathcal{N}$ has subquadratic weight in n. This means that its multiplication table is a sparse matrix with $o(n^2)$ non-zero entries. So the computation of the above vector-matrix multiplication needs $o(n^2)$ operations in $\mathbf{F}_2$. Since a cyclic shift of coordinates of a vector in $\mathbf{F}_{2^n}$ over $\mathbf{F}_2$ runs in time $O(n)$, we conclude that squaring in $\mathbf{F}_{2^{2n}}$ has subquadratic running time.

2. Let $C = C_0 + \beta C_1$ and $D = D_0 + \beta D_1$ be two elements of $\mathbf{F}_{2^{2n}}$ expressed in $\mathcal{A}$. A Karatsuba-like multiplication algorithm gives

$$\begin{aligned}C \times D &= \beta^2 C_1D_1 + \beta\Big((C_1+C_0)(D_1+D_0) + C_1D_1 + C_0D_0\Big) + C_0D_0\\ &= (\beta^2+\beta)C_1D_1 + \beta\Big((C_1+C_0)(D_1+D_0) + C_0D_0\Big) + C_0D_0.\end{aligned} \tag{5}$$

Since $\beta^2+\beta=\alpha$, we have

$$C \times D = C_0D_0 + \alpha C_1D_1 + \beta\Big((C_1+C_0)(D_1+D_0) + C_0D_0\Big). \tag{6}$$

So the product $C \times D$ consists in 3 multiplications and 4 additions between elements in $\mathbf{F}_{2^n}$, and a vector-matrix multiplication which corresponds to the term $\alpha C_1 D_1$ in equation (6).

3. We described the computation of the vector-matrix multiplication $\alpha C_1 D_1$ in the first item of the present proof. Thus if $\mathcal{N}$ has subquadratic weight and subquadratic complexity, then a multiplication in $\mathbf{F}_{2^n}$ needs $o(n^2)$ operations in $\mathbf{F}_2$, as well as a vector-matrix multiplication. Since sum of two vectors in $\mathbf{F}_{2^n}$ over $\mathbf{F}_2$ can be computed in time $O(n)$, we conclude that the product $C \times D$ needs $o(n^2)$ operations in $\mathbf{F}_2$.
4. For $(i,\delta) \in \{0,\ldots,n-1\} \times \{0,1\}$, we set $\mathfrak{a}_{i+\delta n} = \alpha^{2^i}\beta^\delta$ so that $\mathcal{A} = (\mathfrak{a}_k)_{0\le k\le 2n-1}$. Hence, the multiplication tables T_k of $\mathcal{A}$ are given by the block matrix

$$\left(\begin{array}{c|c} (\alpha^{2^i}\alpha^{2^j})_{0\le i,j\le n-1} & (\beta\alpha^{2^i}\alpha^{2^j})_{0\le i,j\le n-1} \\ \hline (\beta\alpha^{2^i}\alpha^{2^j})_{0\le i,j\le n-1} & ((\alpha+\beta)\alpha^{2^i}\alpha^{2^j})_{0\le i,j\le n-1} \end{array}\right)$$

   (a) For $0 \le k \le n-1$, the components of the matrix T_k come from the blocks $(\alpha^{2^i}\alpha^{2^j})_{0\le i,j\le n-1}$ and $((\alpha+\beta)\alpha^{2^i}\alpha^{2^j})_{0\le i,j\le n-1}$. On the other hand, the multiplication table $T=(t_{r,s})_{0\le r,s\le n-1}$ of $\mathcal{N}$ is given by

$$\alpha\alpha^{2^r} = \sum_{s=0}^{n-1} t_{r,s}\alpha^{2^s},\ 0 \le r \le n-1.$$

   Since

$$\alpha^{2^i}\alpha^{2^j} = \sum_{r=0}^{n-1} t_{i,j}^r \alpha^{2^r},$$

   it follows that $t_{i,j}^r = t_{j-i,r-i}$. So

$$\alpha\alpha^{2^i}\alpha^{2^j} = \alpha\sum_{r=0}^{n-1} t_{j-i,r-i}\alpha^{2^r} = \sum_{r=0}^{n-1} t_{j-i,r-i}\sum_{k=0}^{n-1} t_{r,k}\alpha^{2^k}, \tag{7}$$

   where subscripts are taken modulo n. The number of non-zero entries in the matrix T_k coming from $\alpha\alpha^{2^i}\alpha^{2^j}$ is given by the coefficient of α^{2^k} in the linear combination (7). This number is equal to

$$\varphi(\sum_{r=0}^{n-1} t_{j-i,r-i}t_{r,k}),$$

   where φ is the unique ring homomorphism from $\mathbf{F}_2$ into $\mathbb{Z}$. Hence the total number of non-zero entries in T_k is equal to

$$w(\mathcal{N}) + \sum_{0\le i,j\le n-1} \varphi(\sum_{r=0}^{n-1} t_{j-i,l-i}t_{r,k}).$$

(b) For $n \leq k \leq 2n-1$, the components of T_k come from the blocks $(\beta\alpha^{2^i}\alpha^{2^j})_{0\leq i,j\leq n-1}$ and $((\beta+\alpha)\alpha^{2^i}\alpha^{2^j})_{0\leq i,j\leq n-1}$. So the number of non-zero entries in T_k is equal to $3w(\mathcal{N})$.

$\square$

2.2. **Background on Witt vectors.** Witt described in [12] cyclic field extensions whose degree is a power of the characteristic of the base field. Theorem 1 below is one of the main results of [12]. Let A be a commutative ring with unit element, and S a (possibly infinite) subset of the natural numbers $\mathbb{N}$. The structure of commutative ring with unit on the cartesian product A^S is easily verified, addition and multiplication are performed componentwise. There may be other ring structures on A^S, for instance the one from the theory of Witt vectors (see [9] or [10]). We let p be a prime number and ϕ the unique ring-homomorphism from the integers into A. For any n in $\mathbb{Z}$, we write again n instead of $\phi(n)$. We start with the assumption that p is invertible in A. Then the set of Witt vectors with components in A denoted by $W(A)$ is the set of sequences $\mathbf{x} = (x_k)_{k\in\mathbb{N}}$ of elements of A which admit *sequences of ghost components* $(x^{(k)})_{k\in\mathbb{N}}$ defined by

$$x^{(k)} := x_0^{p^k} + px_1^{p^{k-1}} + \ldots + p^k x_k, \tag{8}$$

On the other hand, it is easily seen that

$$x_0 = x^{(0)},\ \ x_1 = \frac{1}{p}\Big(x^{(1)} - x_0^p\Big) \ \text{ and } \ x_k = \frac{1}{p^k}\Big(x^{(k)} - \sum_{0\leq d\leq k-1} p^d x_d^{p^{k-d}}\Big) \ \text{ for any } \ k \geq 1. \tag{9}$$

So components of a Witt vector are recursively computed from its ghost components and vice versa. We deduce that the map

$$\begin{array}{rcl} \varphi : W(A) & \longrightarrow & A^{\mathbb{N}} \\ \mathbf{x} = (x_k)_{k\in\mathbb{N}} & \longmapsto & (x^{(k)})_{k\in\mathbb{N}} \end{array}$$

is a bijection. From the structure of product ring on $A^{\mathbb{N}}$, we obtain a structure of commutative ring with unit on $W(A)$ whose composition laws are given by

$$\mathbf{x} + \mathbf{y} = \varphi^{-1}((x^{(k)})_k + (y^{(k)})_k) \quad \text{and} \quad \mathbf{x} \times \mathbf{y} = \varphi^{-1}((x^{(k)})_k \times (y^{(k)})_k).$$

Actually the components of the sum and product of two Witt vectors $\mathbf{x}$ and $\mathbf{y}$ may be computed from polynomial equations involving the components of $\mathbf{x}$ and $\mathbf{y}$, for a more detailed exposition of this fact see [12], [9] or [10]. It is shown that there exists a unique sequence $S_0, S_1, \ldots, S_n, \ldots$ of polynomials in $\mathbb{Z}[X_0, X_1, \ldots, X_n, \ldots; Y_0, Y_1, \ldots, Y_n, \ldots,]$ (resp. a unique sequence $P_0, P_1, \ldots, P_n, \ldots$) so that for $\mathbf{x}$ and $\mathbf{y}$ in $W(A)$ we have

$$(\mathbf{x}+\mathbf{y})_k = S_k(\mathbf{x},\mathbf{y}) \quad \text{and} \quad (\mathbf{x}\times\mathbf{y})_k = P_k(\mathbf{x},\mathbf{y}). \tag{10}$$

In both cases, the first two polynomials S_0 and S_1(resp. P_0 and P_1) can be easily computed:

$$\begin{array}{l} S_0(\mathbf{x},\mathbf{y}) = x_0 + y_0, \quad S_1(\mathbf{x},\mathbf{y}) = x_1 + y_1 + \frac{1}{p}\sum_{k=1}^{p-1} \left(\begin{array}{c} p \\ k \end{array}\right) x_0^k y_0^{p-k}, \\ P_0(\mathbf{x},\mathbf{y}) = x_0 y_0, \quad P_1(\mathbf{x},\mathbf{y}) = x_1 y_0^p + y_1 x_0^p + p x_1 y_1. \end{array} \tag{11}$$

In case A is an arbitrary commutative ring with unit (even if p is not invertible), it is shown that $W(A)$ is also a commutative ring with unit, the laws being defined from the polynomials S_k and P_k in equation (10) (see [[9], Chapter II, §6] or [[10], Section 1.1]). Since the polynomials S_k and P_k only involve variables X_k and Y_k whose index are $\leq k$, we deduce that for any positive integer r the set $W_r(A)$ of truncated Witt vectors $(x_0, x_1, \ldots, x_{r-1})$ with length r and components in A form a commutative ring with unit. In case A is a field with characteristic p, the group-homomorphism

$$\begin{array}{rccc} \wp: & A & \longrightarrow & A \\ & x & \mapsto & x^p - x. \end{array}$$

induces a group-homomorphism from $W_r(A)$ into itself that we call $\wp$ also. The following theorem generalizes Artin-Schreier Theorem.

Theorem 1. *Let K be a field with characteristic $p > 0$, and $r \geq 1$ an integer.*

1. Let $x = (x_0, x_1, \ldots, x_{r-1})$ be a truncated Witt vector with components in K.
   (a) The equation

$$\wp(\xi) = x \tag{12}$$

   either has no root in $W_r(K)$, or it has a root in $W_r(K)$. In the later case, all its p^r roots lie in $W_r(K)$.
   (b) If equation (12) has no root in $W_r(K)$, then $K(\wp^{-1}(x))$ is a cyclic extension of K with degree dividing p^r. The degree $[K(\wp^{-1}(x)) : K]$ is equal to p^r if and only if $x_0 \notin \wp(K)$.

2. If L/K is a cyclic extension with degree p^r, then there exists x in $W_r(K)$ such that $L = K(\wp^{-1}(x))$ and $x_0 \notin \wp(K)$.

Proof. See [12], [[6], Page 331] or [[10], Section 2.1.1]. □

2.3. **Artin-Schreier-Witt extended bases in characteristic 2.** We first introduce the following terminology.

Definition 3. *Let p be a prime number and q a power of p. Let $\mathcal{N} = (\alpha^{q^i})_{0 \leq i \leq n-1}$ be a normal basis of $\mathbf{F}_{q^n}/\mathbf{F}_q$. Denote by $\overline{\mathbf{F}}_q$ an algebraic closure of $\mathbf{F}_q$ containing $\mathbf{F}_{q^n}$. Let $(\beta_1, \ldots, \beta_r) \in W_r(\overline{\mathbf{F}}_q)$ be a truncated Witt vector outside of $W_r(\mathbf{F}_{q^n})$ such that*

$$(\beta_1^p, \ldots, \beta_r^p) - (\beta_1, \ldots, \beta_r) = (\alpha, x_1 \ldots, x_{r-1})$$

where $x_1, \ldots, x_{r-1}$ are arbitrary elements in $\mathbf{F}_{q^n}$. Set $\mathcal{W}_1 = \mathcal{N} \cup \beta_1\mathcal{N} \cup \ldots \cup \beta_1^{p-1}\mathcal{N}$ and

$$\mathcal{W}_i = \mathcal{W}_{i-1} \cup \beta_i \mathcal{W}_{i-1} \cup \ldots \cup \beta_i^{p-1}\mathcal{W}_{i-1}, \text{ for any } i \in \{2, \ldots, r\}$$

so that $\mathcal{W}_i$ is a basis of $\mathbf{F}_{q^{np^i}}/\mathbf{F}_{q^n}$. Such a basis $\mathcal{W}_i$ is called a degree p^i Artin-Schreier-Witt extension of $\mathcal{N}$ (also Artin-Schreier-Witt extended basis).

In this section, we focus on the case when the lenght of the truncated Witt vectors and the characteristic of the base field are equal to 2. Given two truncated Witt vectors $\mathbf{x} = (x_0, x_1)$ and $\mathbf{y} = (y_0, y_1)$ in $W_2(\overline{\mathbf{F}}_{2^n})$, we know from equation (11) that

$$\mathbf{x} + \mathbf{y} = (x_0 + y_0, x_1 + y_1 + x_0 y_0). \tag{13}$$

Theorem 1 tells us that constructing degree 4 Artin-Schreier-Witt extensions is related to solving equations of the form $\wp(\xi) = x$ in $W_2(\overline{\mathbf{F}}_{2^n})$. Let $\mathcal{N} = (\alpha, \alpha^2, \ldots, \alpha^{2^{n-1}})$ be a normal basis of $\mathbf{F}_{2^n}/\mathbf{F}_2$. Assume that (β_0, β_1) is a truncated Witt vector in $W_2(\overline{\mathbf{F}}_{2^n})$ such that

$$(\beta_0^2, \beta_1^2) + (\beta_0, \beta_1) = (\alpha, \alpha). \tag{14}$$

Set $(s_0, s_1) = (\beta_0^2, \beta_1^2) + (\beta_0, \beta_1)$. From equation (13), we obtain

$$s_0 = \beta_0^2 + \beta_0 \text{ and } s_1 = \beta_1^2 + \beta_1 + \beta_0^3.$$

By setting $(s_0', s_1') = (s_0, s_1) + (\alpha, \alpha)$, we find

$$s_0' = \beta_0^2 + \beta_0 + \alpha \text{ and } s_1' = \beta_1^2 + \beta_1 + \beta_0^3 + \alpha + \alpha\beta_0^2 + \alpha\beta_0.$$

Hence equation (14) yields

$$\beta_0^2 = \beta_0 + \alpha \text{ and } \beta_1^2 = \beta_1 + \beta_0(1 + \alpha) + \alpha^2.$$

Squaring in $\mathbf{F}_{2^{4n}}$ and the complexity of a degree 4 Artin-Schreier-Witt extension of $\mathcal{N}$ are described in the following statement.

Proposition 2. *Let p be a prime number and q a p-power. Let $\mathcal{N} = (\alpha, \alpha^p, \ldots, \alpha^{p^{n-1}})$ be a normal basis of $\mathbf{F}_{p^n}/\mathbf{F}_p$.*

1. *$\mathcal{N}$ admits an Artin-Schreier-Witt extension with degree q.*
2. *Assume $p = 2$ and $q = 4$. Denote by $\overline{\mathbf{F}}_{2^n}$ an algebraic closure of $\mathbf{F}_2$ containing $\mathbf{F}_{2^n}$. Let (β_0, β_1) be a truncated Witt vector in $W_2(\overline{\mathbf{F}}_2)$ outside of $W_2(\mathbf{F}_{2^n})$ and such that*

$$(\beta_0^2, \beta_1^2) + (\beta_0, \beta_1) = (\alpha, \alpha). \tag{14}$$

Denote by $\mathcal{W} = (\mathcal{N} \cup \beta_0\mathcal{N}) \cup \beta_1(\mathcal{N} \cup \beta_0\mathcal{N})$ the corresponding degree 4 Artin-Schreier-Witt extension of $\mathcal{N}$.

(a) If $\gamma = A + \beta_0 B + \beta_1(C + \beta_0 D)$ is an element of $\mathbf{F}_{2^{4n}}$ expressed in $\mathcal{W}$, then

$$\gamma^2 = \Bigg[A_> + \alpha B_> + \alpha^2 C_> + (\alpha^3 + \alpha^2 + \alpha)D_> + \beta_0\Big(B_> + (1+\alpha)C_> + D_>\Big)\Bigg] + \beta_1\Bigg[C_> + \alpha D_> + \beta_0 D_>\Bigg],$$

where $A_>, B_>, C_>$ and $D_>$ stand for right-cyclic shifts of the coordinate vectors of A, B, C and D.

(b) The complexity of $\mathcal{W}$ consists in at most:
   - *9 multiplications and 33 additions between elements lying in $\mathbf{F}_{2^n}$;*
   - *9 vector-matrix multiplications between a vector of $\mathbf{F}_{2^n}$ and the multiplication table of $\mathcal{N}$.*

3. *If $\mathcal{N}$ has subquadratic complexity and subquadratic weight, then $\mathcal{W}$ has also subquadratic complexity.*

Proof. 1. One shows that α lies outside of $\{x^p - x \mid x \in \mathbf{F}_{p^n}\}$ by using Hilbert's Theorem 90 as in the beginning of Section 2.1. Let $r \geq 1$ be an integer such that $q = p^r$. Let $x = (\alpha, x_1, x_2, \ldots, x_{r-1})$ be a truncated Witt vector with components in $\mathbf{F}_{p^n}$. By Theorem 1, we conclude that $\mathbf{F}_{p^n}(\wp^{-1}(x))$ is a degree q cyclic extension of $\mathbf{F}_{p^n}$.

2. (a) We have

$$\Big(A + \beta_0 B + \beta_1(C + \beta_0 D)\Big)^2 = A_> + \beta_0^2 B_> + \beta_1^2(C_> + \beta_0^2 D_>),$$

where $A_>$, $B_>$, $C_>$ and $D_>$ stand for right-cyclic shifts of the coordinate vectors of A, B, C and D. We saw that equation (14) implies

$$\beta_0^2 = \beta_0 + \alpha \;\text{ and }\; \beta_1^2 = \beta_1 + \beta_0(1+\alpha) + \alpha^2.$$

So

$$\begin{aligned}\beta_1^2(C_> + \beta_0^2 D_>) = &\Big[\alpha^2 C_> + (\alpha^3+\alpha^2+\alpha)D_> + \beta_0\Big((1+\alpha)C_> + D_>\Big)\Big] \\ &+\; \beta_1\Big[C_> + \alpha D_> + \beta_0 D_>\Big].\end{aligned}$$

Hence

$$\begin{aligned}\Big(A + \beta_0 B + \beta_1(C + \beta_0 D)\Big)^2 \;=\; &\Bigg[A_> + \alpha B_> + \alpha^2 C_> \\ +\; (\alpha^3+\alpha^2+\alpha)D_> + \beta_0\Big(B_> + (1+\alpha)C_> + D_>\Big)\Bigg] \;+\; &\beta_1\Bigg[C_> + \alpha D_> + \beta_0 D_>\Bigg].\end{aligned}$$

From the study made in the proof of Proposition 1, we dedude that the terms $P(\alpha)X$ (for $P(\alpha)$ a non-constant polynomial in $\mathbf{F}_2[\alpha]$ with degree ≤ 3 and X a vector in $\mathbf{F}_{2^n}$) correspond to sums of vectors of the form $\alpha^i X$ with $1 \leq i \leq 3$. Each such vector $\alpha^i X$ corresponds to i vector-matrix multiplications between vectors in $\mathbf{F}_{2^n}$ and the multiplication table of $\mathcal{N}$.

(b) From a Karatsuba-like multiplication method, the product of two elements

$$X_1 = (A_1 + \beta_0 B_1) + \beta_1(C_1 + \beta_0 D_1) \;\text{ and }\; X_2 = (A_2 + \beta_0 B_2) + \beta_1(C_2 + \beta_0 D_2) \;\text{ in }\; \mathbf{F}_{2^{4n}}$$

is given by

$$\begin{aligned}X_1 \times X_2 \;=\; &\beta_1^2(C_1 + \beta_0 D_1)(C_2 + \beta_0 D_2) \\ &+\beta_1\Big[(A_1 + \beta_0 B_1 + C_1 + \beta_0 D_1)(A_2 + \beta_0 B_2 + C_2 + \beta_0 D_2) \\ &+(A_1 + \beta_0 B_1)(A_2 + \beta_0 B_2) + (C_1 + \beta_0 D_1)(C_2 + \beta_0 D_2)\Big] \\ &+(A_1 + \beta_0 B_1)(A_2 + \beta_0 B_2),\end{aligned}$$

that is

$$X_1 \times X_2 \;=\; \beta_1^2\Bigg[\beta_0^2 D_1 D_2 + \beta_0\Big((C_1 + D_1)(C_2 + D_2) + C_1 C_2 + D_1 D_2\Big) + C_1 C_2\Bigg]$$

$$
\begin{aligned}
&+ \quad \beta_1\Big[\beta_0^2(B_1+D_1)(B_2+D_2)+\beta_0\Big((A_1+B_1+C_1+D_1)(A_2+B_2+C_2+D_2)\\
&+ \quad (A_1+C_1)(A_2+C_2)+(B_1+D_1)(B_2+D_2)\Big)+(A_1+C_1)(A_2+C_2)\\
&+ \quad \beta_0^2B_1B_2+\beta_0\Big((A_1+B_1)(A_2+B_2)+A_1A_2+B_1B_2\Big)+A_1A_2+\beta_0^2D_1D_2\\
&+ \quad \beta_0\Big((C_1+D_1)(C_2+D_2)+C_1C_2+D_1D_2\Big)+C_1C_2\Big]+\beta_0^2B_1B_2\\
&+ \quad \beta_0\Big((A_1+B_1)(A_2+B_2)+A_1A_2+B_1B_2\Big)+A_1A_2.
\end{aligned}
$$

Since $\beta_0^2=\beta_0+\alpha$ and $\beta_1^2=\beta_1+\beta_0(\alpha+1)+\alpha^2$, we have

$$
\begin{aligned}
X_1\times X_2 \quad &= \quad \Big[A_1A_2+\alpha B_1B_2+\alpha^2C_1C_2\\
&+ \quad (\alpha^3+\alpha^2+\alpha)D_1D_2+(\alpha^2+\alpha)\Big((C_1+D_1)(C_2+D_2)+C_1C_2+D_1D_2\Big)\\
&+ \quad \beta_0\Big(A_1A_2+(\alpha+1)C_1C_2+D_1D_2+(A_1+B_1)(A_2+B_2)\\
&+ \quad (\alpha^2+\alpha+1)\Big((C_1+D_1)(C_2+D_2)+C_1C_2+D_1D_2\Big)\Big]\\
&+ \quad \beta_1\Big[A_1A_2+\alpha B_1B_2+C_1C_2+\alpha D_1D_2+(A_1+C_1)(A_2+C_2)\\
&+ \quad \alpha(B_1+D_1)(B_2+D_2)+\beta_0\Big(A_1A_2+C_1C_2+(A_1+B_1)(A_2+B_2)+(A_1+C_1)(A_2+C_2)\\
&+ \quad (C_1+D_1)(C_2+D_2)+(A_1+B_1+C_1+D_1)(A_2+B_2+C_2+D_2)\Big)\Big].
\end{aligned}
$$

For $1\leq i\leq 3$ and X a vector in $\mathbf{F}_{2^n}$, α^iX corresponds to i vector-matrix multiplications between vectors in $\mathbf{F}_{2^n}$ and the multiplication table of $\mathcal{N}$. So the computation of $X_1\times X_2$ consists in:

- 9 multiplications and 33 additions between elements lying in $\mathbf{F}_{2^n}$;
- 9 vector-matrix multiplications between a vector of $\mathbf{F}_{2^n}$ and the multiplication table of $\mathcal{N}$.

3. The same argument as in the proof of Proposition 1 shows that a normal basis with subquadratic weight and subquadratic complexity yields Artin-Schreier-Witt extended bases with subquadratic complexity.

□

The density of the degree 4 Artin-Schreier-Witt extended basis

$$\mathcal{W}=(\mathcal{N}\cup\beta_0\mathcal{N})\cup\beta_1(\mathcal{N}\cup\beta_0\mathcal{N})$$

described in Proposition 2 is given by Lemma 1 below. For $(i,\delta,\lambda)\in\{0,\ldots,n-1\}\times\{0,1\}\times\{0,1\}$, we set $\mathrm{w}_{i+\delta n+\lambda n}=\alpha^{2^i}\beta_0^\delta\beta_1^\lambda$ so that $\mathcal{W}=(\mathrm{w}_\ell)_{0\leq\ell\leq 4n-1}$.

Lemma 1. *With the above notation, let $w(\mathcal{N})$ be the weight of the normal basis $\mathcal{N}$.*

1. *For $0 \le \ell \le n-1$, the number of non-zero entries in the ℓ-th multiplication table of $\mathcal{W}$, is equal to*

$$\begin{aligned}
& w(\mathcal{N}) + \textstyle\sum_{0\le i,j\le n-1} \varphi(\sum_{r=0}^{n-1} t_{j-i,r-i} t_{r,\ell}) \\
+ \quad & \textstyle\sum_{0\le i,j\le n-1} \varphi\left(\sum_{r=0}^{n-1} \sum_{s=0}^{n-1} t_{j-i,r-i} t_{r,s} t_{s,\ell} \right) \\
+ \quad & 2\textstyle\sum_{0\le i,j\le n-1} \varphi\left(\sum_{r=0}^{n-1} \sum_{s=0}^{n-1} t_{j-i,r-i} t_{r,s} t_{s,\ell} + \sum_{r=0}^{n-1} t_{j-i,r-i} t_{r,\ell} \right), \\
+ \quad & \textstyle\sum_{0\le i,j\le n-1} \varphi\left(\sum_{r=0}^{n-1} \sum_{s=0}^{n-1} \sum_{k=0}^{n-1} t_{j-i,r-i} t_{r,s} t_{s,k} t_{k,\ell} \right. \\
+ \quad & \left. \textstyle\sum_{r=0}^{n-1} \sum_{s=0}^{n-1} t_{j-i,r-i} t_{r,s} t_{s,\ell} + \sum_{s=0}^{n-1} t_{j-i,r-i} t_{r,\ell} \right),
\end{aligned}$$

   where subscripts are taken modulo n, $(t_{i,j})_{0\le i,j\le n-1}$ is the multiplication table of $\mathcal{N}$, and φ is the unique ring homomorphism from $\mathbf{F}_2$ into $\mathbb{Z}$.
2. *For $n \le \ell \le 2n-1$, the number of non-zero entries in the ℓ-th multiplication table of $\mathcal{W}$, is equal to*

$$\begin{aligned}
& 4w(\mathcal{N}) + \textstyle\sum_{0\le i,j\le n-1} \varphi\left(\sum_{r=0}^{n-1} t_{j-i,r-i} t_{r,\ell} + t_{j-i,\ell-i} \right) \\
+ \quad & 2\textstyle\sum_{0\le i,j\le n-1} \varphi\left(\sum_{r=0}^{n-1} \sum_{s=0}^{n-1} t_{j-i,r-i} t_{r,s} t_{s,\ell} + \sum_{r=0}^{n-1} t_{j-i,r-i} t_{r,\ell} + t_{j-i,\ell-i} \right).
\end{aligned}$$

3. *For $2n \le \ell \le 3n-1$, the number of non-zero entries in the ℓ-th multiplication table of $\mathcal{W}$, is equal to*

$$3w(\mathcal{N}) + 3 \sum_{0\le i,j\le n-1} \sum_{r=0}^{n-1} \varphi(t_{j-i,r-i} t_{r,\ell}).$$

4. *The ℓ-th multiplication table of $\mathcal{W}$, for $3n \le \ell \le 4n-1$, has $9w(\mathcal{N})$ non-zeros entries.*

Proof. The entries of the multiplication tables T_ℓ of $\mathcal{W}$ are given by the block matrix

$$\left(\begin{array}{c|c|c|c}
(\alpha^{2^i}\alpha^{2^j})_{0\le i,j\le n-1} & (\beta_0\alpha^{2^i}\alpha^{2^j})_{0\le i,j\le n-1} & (\beta_1\alpha^{2^i}\alpha^{2^j})_{0\le i,j\le n-1} & (\beta_0\beta_1\alpha^{2^i}\alpha^{2^j})_{0\le i,j\le n-1} \\ \hline
(\beta_0\alpha^{2^i}\alpha^{2^j})_{0\le i,j\le n-1} & (\beta_0^2\alpha^{2^i}\alpha^{2^j})_{0\le i,j\le n-1} & (\beta_0\beta_1\alpha^{2^i}\alpha^{2^j})_{0\le i,j\le n-1} & (\beta_0^2\beta_1\alpha^{2^i}\alpha^{2^j})_{0\le i,j\le n-1} \\ \hline
(\beta_1\alpha^{2^i}\alpha^{2^j})_{0\le i,j\le n-1} & (\beta_0\beta_1\alpha^{2^i}\alpha^{2^j})_{0\le i,j\le n-1} & (\beta_1^2\alpha^{2^i}\alpha^{2^j})_{0\le i,j\le n-1} & (\beta_0\beta_1^2\alpha^{2^i}\alpha^{2^j})_{0\le i,j\le n-1} \\ \hline
(\beta_0\beta_1\alpha^{2^i}\alpha^{2^j})_{0\le i,j\le n-1} & (\beta_0^2\beta_1\alpha^{2^i}\alpha^{2^j})_{0\le i,j\le n-1} & (\beta_0\beta_1^2\alpha^{2^i}\alpha^{2^j})_{0\le i,j\le n-1} & (\beta_0^2\beta_1^2\alpha^{2^i}\alpha^{2^j})_{0\le i,j\le n-1}
\end{array}\right)$$

Recall that equation (14) yields $\beta_0^2 = \beta_0 + \alpha$ and $\beta_1^2 = \beta_1 + \beta_0(\alpha+1) + \alpha^2$. Hence:

1. For $0 \le \ell \le n-1$, the components of the matrix T_ℓ come from 1 block $(\alpha^{2^i}\alpha^{2^j})_{0\le i,j\le n-1}$, 1 block $(\beta_0^2\alpha^{2^i}\alpha^{2^j})_{0\le i,j\le n-1}$, 1 block $(\beta_1^2\alpha^{2^i}\alpha^{2^j})_{0\le i,j\le n-1}$, 2 blocks $(\beta_0\beta_1^2\alpha^{2^i}\alpha^{2^j})_{0\le i,j\le n-1}$ and 1 block $(\beta_0^2\beta_1^2\alpha^{2^i}\alpha^{2^j})_{0\le i,j\le n-1}$. These correspond to 1 block $(\alpha^{2^i}\alpha^{2^j})_{0\le i,j\le n-1}$, 1 block $(\alpha\alpha^{2^i}\alpha^{2^j})_{0\le i,j\le n-1}$, 1 block $(\alpha^2\alpha^{2^i}\alpha^{2^j})_{0\le i,j\le n-1}$, 2 blocks $((\alpha^2+\alpha)\alpha^{2^i}\alpha^{2^j})_{0\le i,j\le n-1}$ and 1 block $((\alpha^3+\alpha^2+\alpha)\alpha^{2^i}\alpha^{2^j})_{0\le i,j\le n-1}$. From the study made in the proof of Proposition 1 (see equation (7)), we know that

$$\alpha^{2^i}\alpha^{2^j} = \sum_{\ell=0}^{n-1} t_{j-i,\ell-i}\alpha^{2^\ell},$$

where subscripts are taken modulo n and $(t_{i,j})_{0\le i,j\le n-1}$ is the multiplication table of $\mathcal{N}$. So

$$\alpha\alpha^{2^i}\alpha^{2^j} = \sum_{\ell=0}^{n-1}\left(\sum_{r=0}^{n-1} t_{j-i,r-i}t_{r,\ell}\right)\alpha^{2^\ell}, \quad \alpha^2\alpha^{2^i}\alpha^{2^j} = \sum_{\ell=0}^{n-1}\left(\sum_{s=0}^{n-1}\sum_{r=0}^{n-1} t_{j-i,r-i}t_{r,s}t_{s,\ell}\right)\alpha^{2^\ell},$$

and

$$\alpha^3\alpha^{2^i}\alpha^{2^j} = \sum_{\ell=0}^{n-1}\sum_{k=0}^{n-1}\sum_{s=0}^{n-1}\sum_{r=0}^{n-1} t_{j-i,r-i}t_{r,s}t_{s,k}t_{k,\ell}\alpha^{2^\ell}.$$

We conclude that the number of non-zero entries in T_ℓ is equal to

$$\begin{aligned}
& w(\mathcal{N}) + \textstyle\sum_{0\le i,j\le n-1} \varphi(\sum_{r=0}^{n-1} t_{j-i,r-i}t_{r,\ell}) \\
+ \quad & \textstyle\sum_{0\le i,j\le n-1} \varphi\left(\sum_{r=0}^{n-1} \sum_{s=0}^{n-1} t_{j-i,r-i}t_{r,s}t_{s,\ell} \right) \\
+ \quad & 2\textstyle\sum_{0\le i,j\le n-1} \varphi\left(\sum_{r=0}^{n-1} \sum_{s=0}^{n-1} t_{j-i,r-i}t_{r,s}t_{s,\ell} + \sum_{r=0}^{n-1} t_{j-i,r-i}t_{r,\ell} \right), \\
+ \quad & \textstyle\sum_{0\le i,j\le n-1} \varphi\left(\sum_{r=0}^{n-1} \sum_{s=0}^{n-1} \sum_{k=0}^{n-1} t_{j-i,r-i}t_{r,s}t_{s,k}t_{k,\ell} \right. \\
+ \quad & \left. \textstyle\sum_{r=0}^{n-1} \sum_{s=0}^{n-1} t_{j-i,r-i}t_{r,s}t_{s,\ell} + \sum_{s=0}^{n-1} t_{j-i,r-i}t_{r,\ell} \right),
\end{aligned}$$

where φ is the unique ring homomorphism from $\mathbf{F}_2$ into $\mathbb{Z}$.

2. For $n \le \ell \le 2n-1$, the components of the matrix T_ℓ come from 2 blocks $(\beta_0\alpha^{2^i}\alpha^{2^j})_{0\le i,j\le n-1}$, 1 block $(\beta_0^2\alpha^{2^i}\alpha^{2^j})_{0\le i,j\le n-1}$, 1 block $(\beta_1^2\alpha^{2^i}\alpha^{2^j})_{0\le i,j\le n-1}$, 2 blocks $(\beta_0\beta_1^2\alpha^{2^i}\alpha^{2^j})_{0\le i,j\le n-1}$ and 1 block $(\beta_0^2\beta_1^2\alpha^{2^i}\alpha^{2^j})_{0\le i,j\le n-1}$. These correspond to 4 blocks $(\beta_0\alpha^{2^i}\alpha^{2^j})_{0\le i,j\le n-1}$, 1 block $((\alpha+1)\beta_0\alpha^{2^i}\alpha^{2^j})_{0\le i,j\le n-1}$ and 2 blocks $((\alpha^2+\alpha+1)\beta_0\alpha^{2^i}\alpha^{2^j})_{0\le i,j\le n-1}$. So the number of non-zero entries in T_ℓ is equal to

$$\begin{aligned}
& 4w(\mathcal{N}) + \textstyle\sum_{0\le i,j\le n-1} \varphi\left(\sum_{r=0}^{n-1} t_{j-i,r-i}t_{r,\ell} + t_{j-i,\ell-i} \right) \\
+ \quad & 2\textstyle\sum_{0\le i,j\le n-1} \varphi\left(\sum_{r=0}^{n-1} \sum_{s=0}^{n-1} t_{j-i,r-i}t_{r,s}t_{s,\ell} + \sum_{r=0}^{n-1} t_{j-i,r-i}t_{r,\ell} + t_{j-i,\ell-i} \right).
\end{aligned}$$

3. For $2n \le \ell \le 3n-1$, the components of the matrix T_ℓ come from 2 blocks $(\beta_1\alpha^{2^i}\alpha^{2^j})_{0\le i,j\le n-1}$, 2 blocks $(\beta_0^2\beta_1\alpha^{2^i}\alpha^{2^j})_{0\le i,j\le n-1}$, 1 block $(\beta_1^2\alpha^{2^i}\alpha^{2^j})_{0\le i,j\le n-1}$, and 1 block $(\beta_0^2\beta_1^2\alpha^{2^i}\alpha^{2^j})_{0\le i,j\le n-1}$. These correspond to 3 blocks $(\beta_1\alpha^{2^i}\alpha^{2^j})_{0\le i,j\le n-1}$, 3 blocks $(\beta_1\alpha\alpha^{2^i}\alpha^{2^j})_{0\le i,j\le n-1}$. So the number of non-zero entries in T_ℓ is equal to

$$3w(\mathcal{N}) + 3\sum_{0\le i,j\le n-1} \varphi(\sum_{r=0}^{n-1} t_{j-i,r-i}t_{r,\ell}).$$

4. For $3n \le \ell \le 4n-1$, the components of the matrix T_ℓ come from 4 blocks $(\beta_0\beta_1\alpha^{2^i}\alpha^{2^j})_{0\le i,j\le n-1}$, 2 blocks $(\beta_0^2\beta_1\alpha^{2^i}\alpha^{2^j})_{0\le i,j\le n-1}$, 2 blocks $(\beta_0\beta_1^2\alpha^{2^i}\alpha^{2^j})_{0\le i,j\le n-1}$ and 1 block $(\beta_0^2\beta_1^2\alpha^{2^i}\alpha^{2^j})_{0\le i,j\le n-1}$. This means that we have 9 blocks $(\beta_0\beta_1\alpha^{2^i}\alpha^{2^j})_{0\le i,j\le n-1}$. So the number of non-zero entries in T_ℓ is equal to $9w(\mathcal{N})$.

□

3. KUMMER EXTENDED BASES WITH DEGREE PRIME TO 2

Cyclic extensions of $\mathbf{K}$ with degree prime to p are described by Kummer theory. Indeed, let $n \ge 2$ be a prime to p integer such that $\mathbf{K}$ contains a primitive n-root of unity. It is proved [[6], Chapter VI, Theorem 6.2] that every degree n cyclic extension $\mathbf{L}$ of $\mathbf{K}$ is generated by a radical. This means that there exists a non-zero element a in $\mathbf{K}$ whose class in $\mathbf{K}^*/\mathbf{K}^{*n}$ has order n and such that $\mathbf{L}$ is isomorphic to $\mathbf{K}[X]/(X^n - a)$. However, irreducible polynomials of the form $X^n - a$ may also be used for extending normal bases.

Definition 4. *Let p be a prime number and q a power of p. Let $\mathcal{N} = (\alpha^{q^i})_{0\leq i\leq n-1}$ be a normal basis of $\mathbf{F}_{q^n}/\mathbf{F}_q$. Denote by $\overline{\mathbf{F}}_q$ an algebraic closure of $\mathbf{F}_q$ containing $\mathbf{F}_{q^n}$. Assume that $\mathbf{F}_{q^n}$ possesses a primitive d-th root of unity. A degree d Kummer extension (also Kummer extended basis) of $\mathcal{N}$ is a basis $\mathcal{K}$ of $\mathbf{F}_{q^{nd}}/\mathbf{F}_q$ for which there exists $\beta \in \overline{\mathbf{F}}_q$ outside of $\mathbf{F}_{q^n}$ such that $\beta^d - \alpha = 0$ and $\mathcal{K} = (\alpha^{q^i}\beta^j)_{i,j}$.*

In this section, we are interested in degree 3 Kummer extensions of normal bases of $\mathbf{F}_{2^n}/\mathbf{F}_2$.

3.1. **Complexity of degree 3 Kummer extended bases in characteristic 2.** In general, a normal basis $\{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$ of $\mathbf{F}_{q^n}/\mathbf{F}_q$ is said to be *primitive* if α generates the multiplicative group $\mathbf{F}_{q^n}^*$. So any primitive normal basis of $\mathbf{F}_{q^n}/\mathbf{F}_q$ admits a degree d Kummer extension, provided that d divides $q^n - 1$. Lenstra and Schoof [7] showed that for any prime power q and positive integer n, there is a primitive normal basis of $\mathbf{F}_{q^n}$ over $\mathbf{F}_q$. The following proposition describes degree 3 Kummer extensions of primitive normal bases of $\mathbf{F}_{2^n}/\mathbf{F}_2$.

Proposition 3. *Let n be a positive integer such that 3 divides $2^n - 1$. Assume that $\mathcal{N} = (\alpha^{2^i})_{1\leq i\leq n-1}$ is a primitive normal basis $\mathbf{F}_{2^n}/\mathbf{F}_2$. Then:*

1. *There exists β in $\mathbf{F}_{2^{3n}}$ such that $\mathcal{K} = \mathcal{N} \cup \beta\mathcal{N} \cup \beta^2\mathcal{N}$ is a degree 3 Kummer extension of $\mathcal{N}$.*
2. *If $\gamma = C + \beta D + \beta^2 E$ is an element of $\mathbf{F}_{2^{3n}}$ expressed in $\mathcal{K}$, then squaring is given by*
$$\gamma^2 = C_> + \beta G + \beta^2 D_>,$$
where $C_>$ and $D_>$ stand for right-cyclic shifts of the coordinate vectors of C and D; and
$$G = {}^tE_> \times T$$
is a vector-matrix multiplication between the transpose of the right-cyclic shift of the coordinate vector of E and the multiplication table of $\mathcal{N}$.
3. *The complexity of $\mathcal{K}$ consists in at most:*
   (a) 6 multiplications and 15 additions between elements of $\mathbf{F}_{2^n}$,
   (b) 2 vector-matrix multiplications between vectors in $\mathbf{F}_{2^n}$ and the multiplication table of $\mathcal{N}$.
4. *If $\mathcal{N}$ has subquadratic complexity and subquadratic weight in n, then $\mathcal{K}$ has also subquadratic complexity in n.*

Proof. 1. Since α generates $\mathbf{F}_{2^n}^*$, the polynomial $x^3 - \alpha$ is irreducible over $\mathbf{F}_{2^n}$. The result follows from [[6], Chapter VI, Theorem 6.2].

2. Let $C = \sum_{i=0}^{n-1} c_i\alpha^{2^i}$, $D = \sum_{i=0}^{n-1} d_i\alpha^{2^i}$ and $E = \sum_{i=0}^{n-1} e_i\alpha^{2^i}$ be the linear combinations of C, D and E with respect to $\mathcal{N}$. We have
$$\begin{aligned}(C + \beta D + \beta^2 E)^2 &= \textstyle\sum_{i=0}^{n-1} c_{i-1}\alpha^{2^i} + \beta^2 \sum_{i=0}^{n-1} d_{i-1}\alpha^{2^i} + \beta^4 \sum_{i=0}^{n-1} e_{i-1}\alpha^{2^i} \\ &= \textstyle\sum_{i=0}^{n-1} c_{i-1}\alpha^{2^i} + \beta \sum_{i=0}^{n-1} e_{i-1} \sum_{k=0}^{n-1} t_{ik}\alpha^{2^k} + \beta^2 \sum_{i=0}^{n-1} d_{i-1}\alpha^{2^i}.\end{aligned}$$

where subscripts are taken modulo n and $(t_{ik})_{i,k}$ stands for the multiplication table of $\mathcal{N}$. So

$$(C+\beta D+\beta^2 E)^2 = C_> + \beta({}^tE_> \times T) + \beta^2 D_>,$$

where $C_>, D_>$ and $E_>$ stand for right-cyclic shifts of the coordinate vectors of C, D, E, and

$${}^tE_> \times T$$

is a vector-matrix multiplication between the transpose of $E_>$ and the multiplication table of $\mathcal{N}$.

3. Let $C = C_0 + \beta C_1 + \beta^2 C_2$ and $D = D_0 + \beta D_1 + \beta^2 D_2$ be two elements of $\mathbf{F}_{2^{3n}}$ expressed in $\mathcal{K}$. A Karatsuba-like multiplication algorithm gives

$$\begin{aligned} C\times D &= \beta^4 C_2D_2 + \beta^2\Big((C_2+\beta C_1+C_0)(D_2+\beta D_1+D_0) + C_2D_2 + (\beta C_1+C_0)(\beta D_1+D_0)\Big) \\ &\quad +(\beta C_1+C_0)(\beta D_1+D_0). \end{aligned}$$

So

$$\begin{aligned} C\times D &= \beta^4 C_2D_2 + \beta^2\Bigg(\beta\Big((C_0+C_1+C_2)(D_0+D_1+D_2) + (C_0+C_2)(D_0+D_2) \\ &\quad +(C_0+C_1)(D_0+D_1) + C_0D_0\Big) + C_2D_2 + (C_0+C_2)(D_0+D_2) + C_0D_0\Bigg) \\ &\quad +\beta^2 C_1D_1 + \beta\Big((C_0+C_1)(D_0+D_1) + C_1D_1 + C_0D_0\Big) + C_0D_0. \end{aligned}$$

Since $\beta^3 = \alpha$, we have

$$\begin{aligned} C\times D &= C_0D_0 + \alpha\Big(C_0D_0 + (C_0+C_1)(D_0+D_1) + (C_0+C_2)(D_0+D_2) \\ &\quad +(C_0+C_1+C_2)(D_0+D_1+D_2)\Big) \\ &\quad +\beta(C_0D_0 + C_1D_1 + \alpha C_2D_2 + (C_0+C_1)(D_0+D_1)) \\ &\quad +\beta^2\Big(C_0D_0 + C_1D_1 + C_2D_2 + (C_0+C_2)(D_0+D_2)\Big) \end{aligned} \tag{15}$$

So the product $C \times D$ consists in:

(a) 6 products and 15 additions between elements lying in the field $\mathbf{F}_{2^n}$;

(b) 2 vector-matrix multiplications between vectors in $\mathbf{F}_2^n$ and the multiplication table of $\mathcal{N}$. These correpond to the computation of the terms $\alpha C_2 D_2$ and

$$\alpha\Big(C_0D_0 + (C_0+C_1)(D_0+D_1) + (C_0+C_2)(D_0+D_2) + (C_0+C_1+C_2)(D_0+D_1+D_2)\Big).$$

4. The same argument as in the proof of Proposition 1 shows that a normal basis with subquadratic weight and subquadratic complexity in n yields Kummer extended bases with subquadratic complexity in n.

□

3.2. **Density.** We just described squaring and multiplication in $\mathbf{F}_{2^{3n}}$ with respect to a Kummer extension $\mathcal{K} = \mathcal{N} \cup \beta\mathcal{N} \cup \beta^2\mathcal{N}$ of a primitive normal basis

$$\mathcal{N} = \{\alpha, \alpha^2, \ldots, \alpha^{2^{n-1}}\}$$

of $\mathbf{F}_{2^n}/\mathbf{F}_2$. In this section we are interested in multiplication tables of $\mathcal{K}$. These are $3n \times 3n$ matrices with entries in $\mathbf{F}_2$. For $(i,\delta) \in \{0,\ldots,n-1\} \times \{0,1,2\}$, we set $\kappa_{i+\delta n} = \alpha^{2^i}\beta^\delta$ so that $\mathcal{K} = (\kappa_\ell)_{0\le\ell\le 3n-1}$.

Lemma 2. *With the above notation, let $w(\mathcal{N})$ be the weight of the normal basis $\mathcal{N}$.*

1. *For $0 \leq \ell \leq n-1$, the number of non-zero entries in the ℓ-th multiplication table of $\mathcal{K}$, is equal to*
$$w(\mathcal{N}) + 2 \sum_{0\leq i,j\leq n-1} \varphi(\sum_{r=0}^{n-1} t_{j-i,\ell-i} t_{r,\ell}),$$
where subscripts are taken modulo n, $(t_{i,j})_{0\leq i,j\leq n-1}$ is the multiplication table of $\mathcal{N}$, and φ is the unique ring homomorphism from $\mathbf{F}_2$ into $\mathbb{Z}$.
2. *For $n \leq \ell \leq 2n-1$, the number of non-zero entries in the ℓ-th multiplication table of $\mathcal{K}$, is equal to*
$$2w(\mathcal{N}) + \sum_{0\leq i,j\leq n-1} \varphi(\sum_{r=0}^{n-1} t_{j-i,\ell-i} t_{r,\ell}).$$
3. *The ℓ-th multiplication table of $\mathcal{K}$, for $2n \leq \ell \leq 3n-1$, has $3w(\mathcal{N})$ non-zeros entries.*

The density of $\mathcal{K}$ is given by
$$d(\mathcal{K}) = 6d(\mathcal{N}) + 3 \sum_{0\leq \ell\leq n-1} \sum_{0\leq i,j\leq n-1} \varphi(\sum_{0\leq r\leq n-1} t_{j-i,r-i} t_{r,\ell}).$$

Proof. The multiplication tables T_ℓ of $\mathcal{K}$ are given by the block matrix
$$\left(\begin{array}{c|c|c}
(\alpha^{2^i}\alpha^{2^j})_{0\leq i,j\leq n-1} & (\beta\alpha^{2^i}\alpha^{2^j})_{0\leq i,j\leq n-1} & (\beta^2\alpha^{2^i}\alpha^{2^j})_{0\leq i,j\leq n-1} \\
\hline
(\beta\alpha^{2^i}\alpha^{2^j})_{0\leq i,j\leq n-1} & (\beta^2\alpha^{2^i}\alpha^{2^j})_{0\leq i,j\leq n-1} & (\alpha\alpha^{2^i}\alpha^{2^j})_{0\leq i,j\leq n-1} \\
\hline
(\beta^2\alpha^{2^i}\alpha^{2^j})_{0\leq i,j\leq n-1} & (\alpha\alpha^{2^j}\alpha_j)_{0\leq i,j\leq n-1} & (\beta\alpha\alpha^{2^i}\alpha^{2^j})_{0\leq i,j\leq n-1}
\end{array}\right)$$

1. For $0 \leq \ell \leq n-1$, the components of the matrix T_ℓ come from 1 block $(\alpha^{2^i}\alpha^{2^j})_{0\leq i,j\leq n-1}$ and 2 blocks $(\alpha\alpha^{2^i}\alpha^{2^j})_{0\leq i,j\leq n-1}$. Using the same argument as in the proof of Proposition 1, we conclude that the total number of non-zero entries in T_ℓ is equal to
$$w(\mathcal{N}) + 2 \sum_{0\leq i,j\leq n-1} \varphi(\sum_{r=0}^{n-1} t_{j-i,r-i} t_{r,\ell}),$$
where subscripts are taken modulo n, $(t_{i,j})_{0\leq i,j\leq n-1}$ is the multiplication table of $\mathcal{N}$, and φ is the unique ring homomorphism from $\mathbf{F}_2$ into $\mathbb{Z}$.
2. For $n \leq \ell \leq 2n-1$, the components of the matrix T_ℓ come from 2 blocks $(\beta\alpha_i\alpha_j)_{0\leq i,j\leq n-1}$ and 1 block $(\beta\alpha\alpha_i\alpha_j)_{0\leq i,j\leq n-1}$. So the total number of non-zero entries in T_k is equal to
$$2w(\mathcal{N}) + \sum_{0\leq i,j\leq n-1} \varphi(\sum_{r=0}^{n-1} t_{j-i,r-i} t_{r,\ell}).$$

TABLE 1. Sums of cross-products of the multiplication table of the best known normal bases of $\mathbf{F}_{2^n}/\mathbf{F}_2$, for even integers $2 \leq n \leq 14$

n	Modulus	Normal elements	$\sum_{0\leq\ell\leq n-1}\sum_{0\leq i,j\leq n-1}\varphi(\sum_{0\leq r\leq n-1} t_{j-i,r-i}t_{r,\ell})$
2	$1+x+x^2$	x	5
4	$1+x+x^4$	x^3	25
6	$1+x+x^6$	$x^3+x^4+x^5$	101
8	$1+x+x^3+x^4+x^8$	x^6+x^7	233
10	$1+x^3+x^{10}$	$x^3+x^5+x^7+x^9$	181
12	$1+x^3+x^{12}$	$x^2+x^3+x^4+x^5$ $+x^6+x^7+x^8+x^9$	265
14	$1+x^5+x^{14}$	$x^5+x^6+x^7+x^9$ $+x^{12}+x^{13}$	677

TABLE 2. Sums of cross-products of the multiplication table of the best known normal bases of $\mathbf{F}_{2^n}/\mathbf{F}_2$, for even integers $16 \leq n \leq 26$

n	Modulus	Normal elements	$\sum_{0\leq\ell\leq n-1}\sum_{0\leq i,j\leq n-1}\varphi(\sum_{0\leq r\leq n-1} t_{j-i,r-i}t_{r,\ell})$
16	$1+x^3+x^{16}+x^{16}$	$x^6+x^8+x^9+x^{11}+x^{12}$ $+x^{13}+x^{14}+x^{15}$	1921
18	$1+x^3+x^{18}$	$x^4+x^5+x^7+x^8+x^9$ $+x^{11}+x^{15}+x^{16}+x^{17}$	613
20	$1+x^3+x^{20}$	$x^3+x^8+x^{11}+x^{15}+x^{16}$ $+x^{17}+x^{18}+x^{19}$	1625
22	$1+x+x^{22}$	$x^8+x^{11}+x^{12}$ $+x^{19}+x^{20}+x^{21}$	2005
24	$1+x+x^3+x^4+x^{24}$	$x^5+x^6+x^{10}+x^{16}$ $+x^{17}+x^{18}+x^{19}+x^{23}$	3961
26	$1+x+x^3+x^4+x^{26}$	$x^5+x^{10}+x^{12}+x^{15}+x^{16}$ $+x^{19}+x^{20}+x^{21}+x^{22}$ $+x^{23}+x^{25}$	2501

3. For $2n \leq \ell \leq 3n-1$, the components of the matrix T_ℓ come from 3 blocks $(\beta^2\alpha_i\alpha_j)_{0\leq i,j\leq n-1}$. So the total number of non-zero entries in T_ℓ is equal to $3w(\mathcal{N})$.

□

We computed the sums

$$\sum_{\ell=0}^{n-1}\sum_{0\leq i,j\leq n-1}\varphi(\sum_{r=0}^{n-1} t_{j-i,r-i}t_{r,\ell})$$

of cross-products of the multiplication table of the best known normal bases of $\mathbf{F}_{2^n}/\mathbf{F}_2$ for even integers $2 \leq n \leq 26$. The results are provided by tables 1 and 2. These sums are useful when computing densities of Kummer extended bases from formula given in Lemma 2. To design the tables we used [[8], Section 2.2] and the website accompanying it which is available at https://people.math.carleton.ca/ daniel/hff/.

4. Towers of extensions

It is clear that extended bases obtained by iterating Artin-Schreier theory corresponds to extended bases constructed from Artin-Schreier-Witt theory. In this section, we study extended bases in the context of towers of field extensions constructed from Kummer theory. We are also interested in towers combining Artin-Schreier and Kummer theories. Indeed any primitive normal basis of $\mathbf{F}_{2^n}/\mathbf{F}_2$ admits a Kummer extension of degree d, provided d divides 2^n-1. A question is whether the Kummer extended basis itself admits a Kummer extension or an Artin-Schreier extension.

Lemma 3. *Let $\mathcal{N}=(\alpha,\alpha^2,\dots,\alpha^{2^{n-1}})$ be a normal basis of $\mathbf{F}_{2^n}/\mathbf{F}_2$.*

1. *There exists β in $\mathbf{F}_{2^{2n}}$ such that $\mathcal{A}=\mathcal{N}\cup\beta\mathcal{N}$ is an Artin-Schreier extension of $\mathcal{N}$.*
   - (a) *The polynomial $X^2+X+\beta$ is irreducible over $\mathbf{F}_{2^{2n}}$ if and only if n is odd (if that is the case one says that $\mathcal{N}$ admits a degree 4 Artin-Schreier-Witt extension, or a biquadratic Artin-Schreier extension).*
   - (b) *Assume that 3 divides $2^{2n}-1$. Then the polynomial $X^3+\beta$ is irreducible over $\mathbf{F}_{2^{2n}}$ if and only if the class of β generates $\mathbf{F}_{2^{2n}}^*/\mathbf{F}_{2^{2n}}^{*3}$ (if that is the case one says that the Artin-Schreier extension $\mathcal{A}$ admits a degree 3 Kummer extension).*
2. *Assume that 3 divides 2^n-1 and that β is an element in $\mathbf{F}_{2^{3n}}$ such that $\mathcal{K}=\mathcal{N}\cup\beta\mathcal{N}\cup\beta^2\mathcal{N}$ is a degree 3 Kummer extension of $\mathcal{N}$. Then:*
   - (a) *The polynomial $X^2+X+\beta$ is always reducible over $\mathbf{F}_{2^{3n}}$ (one says that the Kummer extension $\mathcal{K}$ admits no Artin-Schreier extension).*
   - (b) *If $\mathcal{N}$ is a primitive normal basis, and if the 3-adic valuation satisfies*
   $$v_3\Big(\frac{2^{3n}-1}{2^n-1}\Big)=1,$$
   then the polynomial $X^3+\beta$ is irreducible over $\mathbf{F}_{2^{3n}}$ (in that case one says that $\mathcal{N}$ admits a bicubic Kummer extension).

Proof. 1. This is [[11], Lemma 3.4].
   - (a) This assertion corresponds [[11], Lemma 5.1].
   - (b) The assertion follows from [[6], Chapter VI, Theorem 6.2] or [[2], A V.84].

2. (a) The characteristic polynomial of β over $\mathbf{F}_{2^n}$ is $X^3-\alpha\in\mathbf{F}_{2^n}[X]$. So $\mathrm{Tr}_{\mathbf{F}_{2^{3n}}/\mathbf{F}_{2^n}}(\beta)=0$. We have
   $$\mathrm{Tr}_{\mathbf{F}_{2^{3n}}/\mathbf{F}_2}(\beta)=\mathrm{Tr}_{\mathbf{F}_{2^n}/\mathbf{F}_2}(\mathrm{Tr}_{\mathbf{F}_{2^{3n}}/\mathbf{F}_{2^n}}(\beta))=0.$$
   From [[6], Chapter VI, Theorem 6.3], there exists γ in $\mathbf{F}_{2^{3n}}$ such that $\beta=\gamma^2+\gamma$. So $X^2+X+\beta$ is a reducible polynomial over $\mathbf{F}_{2^{3n}}$.

   (b) We know that $\beta^3=\alpha$. So β has order $3(2^n-1)$ in $\mathbf{F}_{2^{3n}}^*$ because 3 divides 2^n-1 and α generates $\mathbf{F}_{2^n}^*$. Let δ be a generator of $\mathbf{F}_{2^{3n}}^*$. Then there exists an integer $r\geq 1$ which is prime to $2^{3n}-1$ such that
   $$\beta=\delta^{\frac{r(2^{3n}-1)}{3(2^n-1)}}.$$

Since $v_3\left(\frac{2^{3n}-1}{2^n-1}\right) = 1$ and r is prime to 3, we have

$$v_3\left(\frac{r(2^{3n}-1)}{3(2^n-1)}\right) = 0.$$

So β is not a cube in $\mathbf{F}_{2^{3n}}$. We conclude that $\mathbf{F}_{2^{3n}}(\beta)$ is a degree 3 cyclic extension of $\mathbf{F}_{2^{3n}}$ by [[6], Chapter VI, Theorem 6.2] or [[2], A V.84].

□

5. Conclusion

This paper presents bases of $\mathbf{F}_{2^{nd}}/\mathbf{F}_2$ constructed by extending normal bases of $\mathbf{F}_{2^n}/\mathbf{F}_2$ from Artin-Schreier theory and Kummer theory respectively. In case d is equal to 2, 3 and 4, we explain how squaring in $\mathbf{F}_{2^{nd}}$ can be efficiently computed from the extended bases. We also explain how a Karatsuba-like multiplication algorithm may be used to efficiently compute the product of two elements in $\mathbf{F}_{2^{nd}}$. Then we specify conditions under which Artin-Schreier and Kummer theories may be combined in order to extend normal bases of $\mathbf{F}_{2^n}/\mathbf{F}_2$.

From the study made in Sections 2 and 3, we can actually determine properties of Kummer extensions of an Artin-Schreier extended basis. Indeed let $\mathcal{N} = (\alpha, \alpha^2, \ldots, \alpha^{2^{n-1}})$ be a normal basis of $\mathbf{F}_{2^n}/\mathbf{F}_2$ and

$$\mathcal{A} = \mathcal{N} \cup \beta\mathcal{N}$$

an Artin-Schreier extension of $\mathcal{N}$. Assume that 3 divides $2^{2n}-1$. Assume that β is not a cube in $\mathbf{F}_{2^{2n}}$. Let γ be an element of $\mathbf{F}_{2^{6n}}$ such that

$$\mathcal{KA} = \mathcal{A} \cup \gamma\mathcal{A} \cup \gamma^2\mathcal{A}$$

is a degree 3 Kummer extension of $\mathcal{A}$ (see Lemma 3 $1.(b)$). Multiplications in $\mathbf{F}_{2^{6n}}$ with respect to $\mathcal{K}$ is described from Propositions 1 and 3. On the one hand, squaring an element

$$X = (A+\beta B) + \gamma(C+\beta D) + \gamma^2(E+\beta F) \in \mathbf{F}_{2^{6n}}$$

is given by

$$\begin{aligned} X^2 = \;& (A+\beta B)^2 + \gamma^2(C+\beta D)^2 + \gamma^4(E+\beta F)^2 \\ = \;& \Big((A_> + {}^tB_> \times T) + \beta B_>\Big) + \gamma\Big({}^tF_> \times T + \beta(E_> + F_> + {}^tF_> \times T)\Big) \\ + \;& \gamma^2\Big((C_> + {}^tD_> \times T) + \beta D_>\Big), \end{aligned}$$

where $A_>, B_>, C_>, D_>, E_>$, $F_>$ stand for right-cyclic shifts of the coordinate vectors of A, B, C, D, E, F, and

$${}^tX \times T$$

is a vector-matrix multiplication between the transpose of X and the multiplication table of $\mathcal{N}$. On the other hand, the product of two distinct elements

$X_1 = (A_1+\beta B_1)+\gamma(C_1+\beta D_1)+\gamma^2(E_1+\beta F_1)$ and $X_2 = (A_2+\beta B_2)+\gamma(C_2+\beta D_2)+\gamma^2(E_2+\beta F_2)$

is given by

$$\begin{aligned}
X_1 \times X_2 &= (A_1+\beta B_1)(A_2+\beta B_2)\\
&+ \alpha\Bigg((A_1+\beta B_1)(A_2+\beta B_2)+\Big((A_1+\beta B_1)+(C_1+\beta D_1)\Big)\Big((A_2+\beta B_2)+(C_2+\beta D_2)\Big)\\
&+ \Big((A_1+\beta B_1)+(E_1+\beta F_1)\Big)\Big((A_2+\beta B_2)+(E_2+\beta F_2)\Big)\\
&+ \Big((A_1+\beta B_1)+(C_1+\beta D_1)+(E_1+\beta F_1)\Big)\Big((A_2+\beta B_2)+(C_2+\beta D_2)+(E_2+\beta F_2)\Big)\Bigg)\\
&+ +\beta\Bigg((A_1+\beta B_1)(A_2+\beta B_2)+(C_1+\beta D_1)(C_2+\beta D_2)\alpha(E_1+\beta F_1)(E_2+\beta F_2)\\
&+ \Big((A_1+\beta B_1)+(C_1+\beta D_1)\Big)\Big((A_2+\beta B_2)+(C_2+\beta D_2)\Big)\Bigg)\\
&+ \beta^2\Bigg((A_1+\beta B_1)(A_2+\beta B_2)+(C_1+\beta D_1)(C_2+\beta D_2)(E_1+\beta F_1)(E_2+\beta F_2)\\
&+ \Big((A_1+\beta B_1)+(E_1+\beta F_1)\Big)+\Big((A_2+\beta B_2)+(E_2+\beta F_2)\Big)\Bigg).
\end{aligned}$$

Moreover, the density of $\mathcal{KA}$ is computed from the following block matrix

$$\left(\begin{array}{c|c|c|c|c|c}
(\alpha^{2^i}\alpha^{2^j}) & (\beta\alpha^{2^i}\alpha^{2^j}) & (\gamma\alpha^{2^i}\alpha^{2^j}) & (\gamma\beta\alpha^{2^i}\alpha^{2^j}) & (\gamma^2\alpha^{2^i}\alpha^{2^j}) & (\gamma^2\beta\alpha^{2^i}\alpha^{2^j}) \\ \hline
(\beta\alpha^{2^i}\alpha^{2^j}) & (\beta^2\alpha^{2^i}\alpha^{2^j}) & (\gamma\beta\alpha^{2^i}\alpha^{2^j}) & (\gamma\beta^2\alpha^{2^i}\alpha^{2^j}) & (\gamma^2\beta\alpha^{2^i}\alpha^{2^j}) & (\gamma^2\beta^2\alpha^{2^i}\alpha^{2^j}) \\ \hline
(\gamma\alpha^{2^i}\alpha^{2^j}) & (\gamma\beta\alpha^{2^i}\alpha^{2^j}) & (\gamma^2\alpha^{2^i}\alpha^{2^j}) & (\gamma^2\beta\alpha^{2^i}\alpha^{2^j}) & (\beta\alpha^{2^i}\alpha^{2^j}) & (\beta^2\alpha^{2^i}\alpha^{2^j}) \\ \hline
(\gamma\beta\alpha^{2^i}\alpha^{2^j}) & (\gamma\beta^2\alpha^{2^i}\alpha^{2^j}) & (\gamma^2\beta\alpha^{2^i}\alpha^{2^j}) & (\gamma^2\beta^2\alpha^{2^i}\alpha^{2^j}) & (\beta^2\alpha^{2^i}\alpha^{2^j}) & (\beta^3\alpha^{2^i}\alpha^{2^j}) \\ \hline
(\gamma^2\alpha^{2^i}\alpha^{2^j}) & (\gamma^2\beta\alpha^{2^i}\alpha^{2^j}) & (\beta\alpha^{2^i}\alpha^{2^j}) & (\beta^2\alpha^{2^i}\alpha^{2^j}) & (\gamma\beta\alpha^{2^i}\alpha^{2^j}) & (\gamma\beta^2\alpha^{2^i}\alpha^{2^j}) \\ \hline
(\gamma^2\beta\alpha^{2^i}\alpha^{2^j}) & (\gamma^2\beta^2\alpha^{2^i}\alpha^{2^j}) & (\beta^2\alpha^{2^i}\alpha^{2^j}) & (\beta^3\alpha\alpha^{2^i}\alpha^{2^j}) & (\gamma\beta^2\alpha^{2^i}\alpha^{2^j}) & (\gamma\beta^3\alpha\alpha^{2^i}\alpha^{2^j})
\end{array}\right)$$

If the original normal basis $\mathcal{N}$ has quasi-linear complexity $O(n\log n|\log\log n|)$ and linear weight $O(n)$, then $\mathcal{A}$ has also quasi-linear complexity and its density is quadratic by Proposition 1. From argument analogous to the one used in the proof of Proposition 2, we deduce that $\mathcal{KA}$ has quasi-linear complexity. Obviously, degree d Kummer extensions of an Artin-Schreier extension of a normal basis $\mathcal{N}$ of $\mathbf{F}_{2^n}/\mathbf{F}_2$ are useful when doing arithmetic in $\mathbf{F}_{2^{2nd}}$ provided that d is not too large. In order to fully take advantage of properties of the original normal basis, we are only authorized to construct Kummer extended bases with low degrees.

We know (from equation (4)) that the complexity of a multiplication algorithm using multiplication tables of a basis $\mathcal{B}$ depends on the density of $\mathcal{B}$. So density is an important criterion when selecting efficient extended bases. Since polynomials of the form $X^3 + \alpha$ are sparser than the ones of the form $X^2 + X + \alpha$, we guess that there are many cases for which extended bases constructed from Kummer theory have better densities than the ones from Artin-Schreier theory. We used Magma [1] to construct Table 3 which confirm our guess by comparing the densities of the best known Kummer extended bases to the densities of the best known Artin-Schreier extended bases and the densities of the best known normal bases of $\mathbf{F}_{2^m}/\mathbf{F}_2$ in case $6 \leq m \leq 78$. We observe that (when they exist) Kummer extended bases have better densities than both others, except in cases $m \in \{18, 24\}$ for which the densities of Kummer extended bases lie between the densities of both others.

Acknowledgments. The work reported in this paper is supported by Simons Foundation via PREMA project, and the Inria International Lab LIRIMA via the Associate team FAST. The first author acknowledges the International Centre for Theoretical Physics (ICTP) for their hospitality within the framework of Associate Scheme. The authors would like to thank Jean-Marc Couveignes for his comments on early version of this work. We also thank the anonymous referee for various comments that were helpful for the improvement of the exposition.

References

[1] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[2] N. Bourbaki. *Éléments de mathématique. I: Les structures fondamentales de l'analyse. Fascicule XI. Livre II: Algèbre. Chapitre 4: Polynomes et fractions rationnelles. Chapitre 5: Corps commutatifs*. Deuxième édition. Actualités Scientifiques et Industrielles, No. 1102. Hermann, Paris, 1959.

[3] Jean-Marc Couveignes and Reynald Lercier. Elliptic periods for finite fields. *Finite Fields Appl.*, 15(1):1–22, 2009.

[4] Tony Ezome and Mohamadou Sall. Normal bases from 1-dimensional algebraic groups. *J. Symbolic Comput.*, 2019. https://doi.org/10.1016/j.jsc.2019.07.002.

[5] Shuhong Gao, Joachim von zur Gathen, Daniel Panario, and V. Shoup. Algorithms for exponentiation in finite fields. *J. Symbolic Comput.*, pages 879–889, 2000.

[6] Serge Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.

[7] H. W. Lenstra and R. J. Schoof. Primitive normal bases for finite fields. *Math. Comp.*, 48(177):217–231, 1987.

TABLE 3. Best known densities $d(\mathcal{K})$ of Kummer extended bases, versus best known densities $d(\mathcal{A})$ of Artin-Schreier extended bases and best known densities $d(\mathcal{N})$ of normal bases of $\mathbf{F}_{2^m}/\mathbf{F}_2$, for integers $6 \leq m \leq 78$ which are multiple of 6. All these bases are computed from the best known normal elements given in tables 1 and 2. Bold entries indicate that Kummer extended bases are better than both others. Minus symbol indicates that there is no normal element in tables 1 or 2 which generates a normal basis admiting a degree 3 Kummer extension. Blanc indicates that data are not available in the literature.

m	$d(\mathcal{N})$	$d(\mathcal{A})$	$d(\mathcal{K})$
6	66	77	**51**
12	276	365	-
18	630	869	699
24	2520	1369	1707
30	1770	3805	-
36	2556	3133	-
42	5670	10921	**4299**
48	20400	14041	**13923**
54	11286	23245	-
60	7140	10445	-
66	8646	12677	-
72	25704		-
78	18018		**15459**

[8] G. L. Mullen and D. Panario. *Handbook of Finite Fields*. CRC Press, 2013.
[9] J.P. Serre. *Corps locaux*. Actualités scientifiques et industrielles. Hermann, 1980.
[10] Lara Thomas. *Arithmétique des extensions d'Artin-Schreier-Witt*. PhD thesis, Université Toulouse II Le Mirail, 2005.
[11] David Thomson and Colin Weir. Artin-schreier extension of normal bases. *Finite Fields Appl.*, 53:267–286, 2018.
[12] Ernst Witt. Zyklische körper und algebren der charateristik p vom grad p^n structur diskret bewerteter perfekter körper mit vollkommenem restklassenkörper der characteristik p^n. *Journal für die reine undwandte Mathematik*, 176:126–140, 1936.