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

Gauss Periods as Constructions of Low Complexity Normal Bases

M. Christopoulou · T. Garefalakis · D. Panario · D. Thomson

February 16, 2011

Abstract Optimal normal bases are special cases of the so-called Gauss periods (Disquisitiones Arithmeticae, Articles 343-366); in particular, optimal normal bases are Gauss periods of type $(n,1)$ for any characteristic and type $(n,2)$ for characteristic 2. We present the multiplication tables and complexities of Gauss periods of type (n,t) for all n and $t = 3,4,5$ over any finite field and give a slightly weaker result for Gauss periods of type $(n,6)$. In addition, we give some general results on the so-called cyclotomic numbers, which are intimately related to the structure of Gauss periods.

We also present the general form of a normal basis obtained by the trace of any normal basis in a finite extension field. Then, as an application of the trace construction, we give upper bounds on the complexity of the trace of a Gauss period of type $(n,3)$.

Mathematics Subject Classification (2000) 11T99; 11T22, 12E20

Keywords Cyclotomic numbers · Gauss periods · Finite fields · Normal bases

1 Introduction

Let q be a power of a prime p and let $\mathbb{F}_q$ be the finite field with q elements. For any element $\alpha \in \mathbb{F}_{q^n}$, the *conjugates* of α are given by α^{q^i}, $i = 0,1,\ldots,n-1$. We denote the ith conjugate of α as $\alpha_i = \alpha^{q^i}$, $i = 0,1,\ldots,n-1$. The element α is a *normal element* when α and its conjugates form a basis for $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. In this case we call the basis $N = \{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}$ a *normal basis*.

For the normal basis N there is an associated matrix $T_\alpha = (t_{ij})$ given by the relations

$$\alpha\alpha_i = \sum_{j=0}^{n-1} t_{ij}\alpha_j.$$

M. Christopoulou · T. Garefalakis
Department of Mathematics, University of Crete, Knoussou Ave. 71409 Heraklion, Crete, Greece
E-mail: {mchris,theo}@math.uoc.gr

D. Panario · D. Thomson
School of Mathematics and Statistics, Carleton University, 1125 Colonel By Dr., Ottawa ON, Canada, K1S 5B6
E-mail: {daniel,dthomson}@math.carleton.ca

The number of nonzero entries in T_α is called the *complexity* (also sometimes called the density) of the basis N [16].

Using a normal basis yields efficient exponentiation, as qth powers of elements are given by a cyclic bit-shift of the corresponding coordinate vector. Massey and Omura [14] patented an efficient hardware multiplier for normal bases over $\mathbb{F}_2$ and modifications of this can be found [12,17,18,20], for example. Normal bases have also been implemented efficiently in software, see, for example, [4,6,8].

The hardware and time complexity of multiplication using normal bases depends on the structure of the normal basis used, particularly on the complexity of the normal basis. Mullin et al. [16] prove that the complexity of any normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ is at least $2n-1$. Normal bases which achieve this lower bound are called *optimal* normal bases. Mullin et al. give two constructions of optimal normal bases, named Type I and Type II optimal normal bases, and conjecture that there are no other optimal normal bases. Gao and Lenstra [7] later prove this claim.

Optimal normal bases exist but not in every finite extension field, thus in the absence of optimal normal bases it is desirable to know the normal basis with the least complexity. Young and Panario [23] show that the dual basis of a Type I optimal normal basis over $\mathbb{F}_2$ has complexity $3n-3$ and conjecture that no basis exists with complexity up to $3n$ except in extensions which already contain an optimal normal basis. Wan and Zhou [21] show that the complexity of the dual bases of Type I optimal normal bases over $\mathbb{F}_q$, q odd, is $3n-2$ and extend Young and Panario's conjecture for odd q. Masuda, et al. [15] exhaustively search finite fields $\mathbb{F}_{2^n}$, $n \leq 39$, for normal bases and present a table including the number of normal bases, minimum and maximum complexities, the average and variance of the complexities. They use their data and constructions from the literature to create a table of the lowest known complexity of a normal basis for all extensions of $\mathbb{F}_2$ with degree $n \leq 512$.

The constructions of optimal normal bases due to Mullin, et al. [16] are special cases of *Gauss periods*. Gauss periods were introduced by Gauss [11, Articles 343-366], and were used in determining ruler-and-compass constructions of regular polygons. Gauss periods can be considered over any Galois extension of fields, but in this paper we only consider the finite field case. Gauss periods as normal bases were introduced by Ash, Blake and Vanstone [2] as a generalization of the optimal normal bases.

Definition 1.1 *Let $r = tn+1$ be a prime not dividing q. Furthermore, let κ be the unique subgroup of order t in $\mathbb{Z}_r^*$. Also, let β be a primitive rth root of unity in $\mathbb{F}_{q^{tn}}$. The elements α_i, $i = 0,1,\ldots,n-1$, are given by*

$$\alpha_i = \sum_{a \in \kappa_i} \beta^a,$$

where $\kappa_i = \{a \cdot q^i : a \in \kappa\} \subseteq \mathbb{Z}_r^*$. The elements $\alpha_0, \alpha_1, \ldots, \alpha_{n-1}$ are called the Gauss periods *of type (n,t) over $\mathbb{F}_q$.*

It is easy to show that Gauss periods are elements of $\mathbb{F}_{q^n}$. The following theorem gives conditions under which Gauss periods define normal elements.

Theorem 1.2 [6,22] *Let $\alpha \in \mathbb{F}_{q^n}$ be a Gauss period of type (n,t) as defined in Definition 1.1. The following are equivalent:*

- *The set $N = \left\{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\right\}$ forms a normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.*
- *If e is the order of q modulo r, then $\gcd(nt/e, n) = 1$.*
- *The (disjoint) union of $\kappa_0, \kappa_1, \ldots, \kappa_{n-1}$ is $\mathbb{Z}_r^*$. Equivalently, $\mathbb{Z}_r^* = \langle q, \kappa \rangle$.*

Gauss periods of type $(n,1)$, for any q, and type $(n,2)$, for $q=2$, define the optimal normal bases given by Mullin et al. [16]. For any value of t and prime power q, von zur Gathen and Pappalardi [9] show under the generalized Riemann hypothesis that there are infinitely many n such that there exists a normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ generated by Gauss periods of type (n,t).

Gauss periods were experimentally shown to have high order by Gao, von zur Gathen and Panario [5]. This was later shown by von zur Gathen and Shparlinski [10] for certain Gauss periods and these results were extended by Ahmadi, Shparlinski and Voloch [1]. Gauss periods also have applications in cryptography and coding theory, see, for example, [5, 19].

Suppose $\alpha_0, \alpha_1, \ldots, \alpha_{n-1}$ are Gauss periods forming a normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, we follow the form of the multiplication table of normal bases due to Gauss periods presented by Gao et al. [6]. First we define the *cyclotomic numbers* $t_{ij} = |(1+\kappa_i) \bigcap \kappa_j|$. Also, let $j_0 < n$ be the unique index such that $-1 \in \kappa_{j_0}$. If t is even, then $j_0 = 0$, and if t is odd, then $j_0 = n/2$. Finally, define

$$\delta_j = \begin{cases} 0 & \text{if } j \neq j_0 \\ 1 & \text{if } j = j_0. \end{cases}$$

Then the form of the multiplication table T_α is

$$\alpha\alpha_i = \delta_i t + \sum_{j=0}^{n-1} t_{ij}\alpha_j. \tag{1}$$

An explicit determination of the multiplication table T_α depends therefore on studying the cyclotomic numbers t_{ij}.

The structure of the paper is as follows: in Section 2 we give some general results on cyclotomic numbers and their relation to Gauss periods. We also give a technical lemma which is used extensively in Section 3. In Section 3 we present the multiplication tables of Gauss periods of type $(n,3)$, $(n,4)$ and $(n,5)$. In addition, we give the complexity of a type $(n,6)$ Gauss period over any characteristic. Although it is possible to give other Gauss periods of type (n,t), $t > 5$, there is a substantial problem when t grows. For large n and t, there are Gauss periods whose multiplication tables do not follow a simply prescribed pattern. Gauss periods of type $(n,3)$ have simple structure since t is small. Gauss periods of type $(n,4)$ have a slightly different structure because t is even. Type $(n,5)$ Gauss periods begin to show some of the additional structure of the multiplication tables of Gauss periods have, yet still have t small enough that the multiplication tables follow a simply prescribed pattern. We give a multiplication table of a Gauss period that does not follow this pattern at the end of Section 3. In Section 4.1 we give the multiplication table of the trace of any normal basis. Section 4.2 contains an application of the results of Section 4.1 to Gauss periods of type $(n,3)$, given in Section 3.1, for any finite field. Also, in Section 4.3 we take this opportunity to correct some small typos and inconsistencies in our paper [3]. We finish with some conclusions and future work in Section 5.

We remark that in this paper we consider only Gauss periods which construct normal bases (and thus, satisfy the conditions of Theorem 1.2).

2 General results on Gauss periods

First, we notice that the cyclotomic numbers are symmetric when t is even.

Proposition 2.1 *Let $n \in \mathbb{N}$, $n > 2$, and let $r = tn+1$ be an odd prime with t even. Let ω be a primitive t-th root of unity in $\mathbb{F}_r$ and $\kappa = \langle \omega \rangle$. Then $t_{jh} = t_{hj}$ for all $0 \leq j,h \leq n-1$.*

PROOF. It is enough to show that $t_{jh} \leq t_{hj}$. Let $t = 2x$ and suppose $y \in (1+\kappa_j) \bigcap \kappa_h$, then $y = 1+q^j\omega^i = q^h\omega^k$ for $0 \leq i,k \leq t-1$. Then

$$\begin{aligned} q^h\omega^k - 1 = q^j\omega^i &\Leftrightarrow q^h\omega^k + \omega^x = q^j\omega^i \Leftrightarrow \omega^x(q^h\omega^{k-x}+1) = q^j\omega^i \\ &\Leftrightarrow q^h\omega^{k-x} + 1 = q^j\omega^{i-x}. \end{aligned}$$

This provides an injective map from $(1+\kappa_j)\bigcap\kappa_h$ to $(1+\kappa_h)\bigcap\kappa_j$ defined by mapping $1+q^j\omega^i$ to $q^j\omega^{i-x}$. ∎

We briefly recall that a normal basis is *self-dual* if and only if its multiplication table is symmetric [13]. Therefore, by Equation (1), we can check that the multiplication table is self dual if t is even and the characteristic divides t. This result appears in [6], where the authors give a formula for the dual basis of the multiplication table of a Gauss period of any type. For $q = 2$, different forms of this result appear in [2,13].

We observe that row $n-j$ of the multiplication table is a cyclic left shift of row j of the multiplication table by j positions, for any $0 < j < n/2$. Since, for $0 < j < n/2$, the jth row of the multiplication table depends only on t_{jh}, $h = 0,1,\ldots,n-1$, we conclude the following proposition on cyclotomic numbers.

Proposition 2.2 *Let $n \in \mathbb{N}$, $n > 2$, and let $r = tn+1$ be an odd prime. Let ω be a primitive t-th root of unity in $\mathbb{F}_r$ and $\kappa = \langle \omega \rangle$. Then $t_{j,j+h} = t_{n-j,h}$ for all $0 < j < n/2$.*

PROOF. It is enough to show that $t_{j,j+h} \leq t_{n-j,h}$. Suppose $x \in (1+\kappa_j)\bigcap\kappa_{j+h}$. Then $x = 1+q^j\omega^u = q^{j+h}\omega^v$. Multiplying both sides by q^{n-j} yields $q^{n-j}+q^n\omega^u = q^{n+h}\omega^v$. We note that q^n is a t-th root of unity in $\mathbb{F}_r^*$, and therefore $q^{n-j}+\omega^U = q^h\omega^V$, for some U,V. Finally, multiplying both sides by ω^{-U} gives $\omega^{-U}q^{n-j}+1 = q^h\omega^{V-U}$. Substituting $j = n-j'$ and $h = h'+j'$, for some j',h', yields the reverse inequality. ∎

Remark 1 *We note that $t_{jh} > 1$ is the same as $|(1+\kappa_j)\bigcap\kappa_h| > 1$. In this case, it is enough to show that if $x,y \in \kappa_j$ then $1+x, 1+y \in \kappa_h$. In other words, we require x,y, $x \neq y$ such that $x/y \in \kappa$ and $(1+x)/(1+y) \in \kappa$.*

Now, we provide a technical lemma which is used in the derivations of the multiplication tables which appear in this section.

Lemma 2.3 *Let $n,t \in \mathbb{N}$, $n,t > 1$, and $r = nt+1$ be an odd prime. Let ω be a primitive t-th root of unity in $\mathbb{F}_r$, and let κ be the subgroup of $\mathbb{F}_r^*$ of order t. Then there are $(t-1)(t-2)/2$ distinct subsets $\{x,y\} \subset \mathbb{F}_r\backslash\{0,-1\}$, such that $x \neq y$ $\frac{x}{y} \in \kappa$ and $\frac{1+x}{1+y} \in \kappa$, given by $S_{i,j} = \{x_{i,j}, y_{i,j}\}$, where*

$$x_{i,j} = \frac{\omega^j - 1}{1-\omega^{i+j}},\ y_{i,j} = \omega^i x_{i,j}, \qquad 1 \leq i \leq t-1,\ 1 \leq j \leq t-1,\ i+j < t.$$

Furthermore, $S_{t-2j,j} \subseteq \kappa$, $1 \leq j \leq \frac{t-1}{2}$.

PROOF. Let $x,y \in \mathbb{F}_r\backslash\{0,-1\}$, $x \neq y$. Then $x/y \in \kappa$ and $(1+x)/(1+y) \in \kappa$ if and only if $y = \omega^i x$ and $1+x = \omega^j(1+y)$, for some $1 \leq i,j \leq t-1$. It follows that $1+x = \omega^j + \omega^{i+j}x$.

Since $j \not\equiv 0 \pmod{t}$, we have $i+j \not\equiv 0 \pmod{t}$, which is equivalent to $i+j \neq t$. So the sets that satisfy the given conditions are $S_{i,j} = \{x_{i,j}, y_{i,j}\}$ with

$$x_{i,j} = \frac{\omega^j - 1}{1-\omega^{i+j}}, \;\; y_{i,j} = \omega^i x_{i,j}, \;\; 1 \leq i \leq t-1, \;\; 1 \leq j \leq t-1, \;\; i+j \neq t. \tag{2}$$

To identify which of those sets coincide, note that $S_{i_1,j_1} = S_{i_2,j_2}$ if and only if

$$x_{i_1,j_1} = x_{i_2,j_2}, \quad y_{i_1,j_1} = y_{i_2,j_2}, \tag{3}$$

or

$$x_{i_1,j_1} = y_{i_2,j_2}, \quad x_{i_2,j_2} = y_{i_1,j_1}. \tag{4}$$

If Equation (3) holds then

$$y_{i_1,j_1} = \omega^{i_1} x_{i_1,j_1} = \omega^{i_1} x_{i_2,j_2} = \omega^{i_1-i_2} y_{i_2,j_2},$$

which implies that $i_1 = i_2$. Considering Equation (2) and letting $i_1 = i_2 = i$, we get $(\omega^{j_1} - 1)(1-\omega^{i+j_2}) = (\omega^{j_2}-1)(1-\omega^{i+j_1})$, and thus $(\omega^{j_1} - \omega^{j_2})(\omega^i - 1) = 0$. Since $1 \leq i \leq t-1$, $\omega^i \neq 1$ and we conclude that $j_1 = j_2$.

If Equation (4) holds then

$$y_{i_1,j_1} = \omega^{i_1} x_{i_1,j_1} = \omega^{i_1} y_{i_2,j_2} = \omega^{i_1+i_2} x_{i_2,j_2},$$

which implies that $i_1 + i_2 = t$. Equation (2) becomes $\frac{\omega^{j_1}-1}{1-\omega^{i_1+j_1}} = \omega^{i_2} \frac{\omega^{j_2}-1}{1-\omega^{i_2+j_2}}$, and so $(\omega^{j_1+j_2} - 1)(\omega^{i_1} - 1) = 0$. Again, $\omega^{i_1} \neq 1$, therefore $j_1 + j_2 = t$. It follows that $S_{i_1,j_1} = S_{i_2,j_2}$ if and only if $i_2 = t - i_1$ and $j_2 = t - j_1$, in which case Equation (4) holds.

One way to reject duplicates is to restrict the range of values of i and j, as described in the statement of the lemma. In particular, to ensure there is no double-counting of elements we require $i + j < t$. For the last statement, note that for $i = t - 2j$, we have

$$x_{t-2j,j} = \frac{\omega^j - 1}{1-\omega^{-j}} = \omega^j,$$

and $y_{t-2j,j} = \omega^{t-2j} x_{t-2j,j} = \omega^{-j}$, so that $S_{t-2j,j} = \{\omega^j, \omega^{-j}\} \subseteq \kappa$. ∎

We note that $\mathrm{Tr}(\alpha) = \mathrm{Tr}_{q^n/q}(\alpha) = -1$. Indeed,

$$\begin{aligned}\mathrm{Tr}_{q^n/q}(\alpha) &= \sum_{i=0}^{n-1} \left(\sum_{a \in \kappa} \beta^a \right)^{q^i} = \sum_{i=0}^{n-1} \sum_{a \in \kappa} \beta^{aq^i} = \sum_{i=0}^{n-1} \sum_{a \in \kappa_i} \beta^a \\ &= \sum_{i=1}^{r-1} \beta^i = \beta + \beta^2 + \cdots + \beta^{r-1} = -1.\end{aligned}$$

In the following section we use an equivalent form of the rows of the multiplication table. We have

$$\sum_{j=0}^{n-1} t_{ij} \alpha_j = \sum_{j=0}^{n-1} (t_{ij} - \delta_i t) \alpha_j + \sum_{j=0}^{n-1} \delta_i t \alpha_j,$$

where the last sum is $\delta_i t \cdot \mathrm{Tr}(\alpha) = -\delta_i t$. Thus,

$$\alpha \alpha_i = \sum_{j=0}^{n-1} (t_{ij} - \delta_i t) \alpha_j. \tag{5}$$

3 Multiplication tables of Gauss periods of small type

In this section, we give the general structure of the multiplication tables of Gauss periods of type $(n,3)$, $(n,4)$ and $(n,5)$. We also give the complexity of a Gauss period of type $(n,6)$ over any characteristic.

3.1 Gauss periods of type $(n,3)$

In this section, we present the multiplication table of Gauss periods of type $(n,3)$ for all characteristics. A direct application of Lemma 2.3 gives the following lemma.

Lemma 3.1 *Let $n \in \mathbb{N}$, $n > 3$ and let $r = 3n+1$ be a prime. Let ω be a primitive 3rd root of unity in $\mathbb{F}_r$ and let $\kappa = \langle \omega \rangle$. There is one subset $S = \{x, y\} \subset \mathbb{F}_r \backslash \{0, -1\}$ such that $x \neq y$, $\frac{x}{y} \in \kappa$ and $\frac{1+x}{1+y} \in \kappa$. In particular, $S = \{\omega, \omega^2\} \subset \kappa$.*

Theorem 3.2 *Let q be a power of an odd prime $p > 3$, and let α be a Gauss period of type $(n,3)$ generating the normal basis $\{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}$ of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Then, the complexity of the multiplication table T_α generated by α is $4n-4$. Furthermore, the first row of T_α has 2 nonzero terms, the $n/2$ row of T_α has n nonzero terms and every other row has exactly 3 nonzero terms.*

PROOF. Let $r = 3n+1$ be a prime, and let $\kappa = \{1, \omega, \omega^2\}$, where ω is a primitive 3rd root of unity in $\mathbb{Z}_r^*$. Observe that n is even since $3n+1$ is an odd prime. Also, let β be a primitive rth root of unity in $\mathbb{F}_{q^n}$. The elements α_i, $i = 0, 1, \ldots, n-1$ are given by

$$\alpha_i = \sum_{a \in \kappa_i} \beta^a,$$

where $\kappa_i = \{a \cdot q^i : a \in \kappa\} \subseteq \mathbb{Z}_r^*$.

To examine the multiplication table generated by α, we require the expression of the products $\alpha\alpha_j$ in terms of the basis elements $\alpha, \alpha_1, \ldots, \alpha_{n-1}$. Thus, we consider Equation (5) with $t = 3$. We then examine the cyclotomic numbers t_{jh} to determine the number of nonzero entries in each row.

Case 1: $j = 0$
Since all the κ_h, $h = 0, 1, \ldots, n-1$, form a partition of $\mathbb{Z}_r^*$ we have that $\sum_{h=0}^{n-1} t_{0h} = 3$, so to show that there are two nonzero terms it is enough to show that $t_{0h} = 2$ for some $h = 0, 1, \ldots, n-1$. Lemma 3.1 gives that there are exactly 2 elements $x, y \in \kappa$ such that $1+x, 1+y \in \kappa_h$ for some $h = 0, 1, \ldots, n-1$. Thus, $t_{0h} = 2$ and the first row contains only one other nonzero entry, equal to 1.

Case 2: $j = n/2$
We prove that the $n/2$ row has n nonzero elements. Since $\delta_{n/2} = 1$ we have

$$\alpha\alpha_{n/2} = \sum_{h=0}^{n-1} \left(t_{n/2,h} - 3\delta_{n/2}\right) \alpha_h = \sum_{h=0}^{n-1} \left(t_{n/2,h} - 3\right) \alpha_h.$$

It is enough to show that $t_{n/2,h} \neq 3$ for all $h = 0, 1, \ldots, n-1$. Suppose $t_{n/2,h} = 3$ for some h. Thus $1 + \kappa_{n/2} = \kappa_h$ and since $-1 \in \kappa_{n/2}$ we have $0 \in 1 + \kappa_{n/2}$, contradicting $\kappa_h \subseteq \mathbb{Z}_r^*$.

Case 3: $j \neq 0, n/2$
Last, we prove that each of the remaining $n-2$ rows has exactly 3 distinct nonzero terms, all equal to 1. Let $m \neq 0, n/2$, and consider the mth row of the multiplication table:

$$\alpha\alpha_m = \sum_{h=0}^{n-1} t_{mh}\alpha_h.$$

Since the cosets $\kappa_h, h = 0,1,\ldots,n-1$, form a partition of $\mathbb{Z}_r^*$ we have that $\sum_{h=0}^{n-1} t_{mh} = 3$. We show that each of these values of t_{mh} are equal to 1.

Suppose, to the contrary, that $t_{mh} > 1$ for some $h = 0,1,\ldots,n-1$, that is

$$t_{mh} = |(1+\kappa_m) \bigcap \kappa_h| \geq 2.$$

Thus, there are at least two distinct elements $x, y \in \kappa_m$ such that $1+x, 1+y \in \kappa_h$. Since $m \neq n/2$ we know $x \neq -1$ and $y \neq -1$ and from Lemma 3.1 we have $x = \omega, y = \omega^2$ for some primitive 3rd root of unity ω. Thus, $x, y \in \kappa_0$ which contradicts the choice of m. ∎

We present similar statements for the characteristic 2 and 3 cases, and note the differences to $p > 3$ case in the proofs of each characteristic.

Theorem 3.3 *Let q be a power of 3 and let α be a Gauss period of type $(n,3)$ generating the normal basis $\{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}$ of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Then, the complexity of the multiplication table T_α generated by α is $3n-2$. Furthermore, the first row of T_α has exactly 2 nonzero terms, the $n/2$ row of T_α has exactly 2 nonzero terms and every other row has exactly 3 nonzero terms.*

PROOF. The proof follows Theorem 3.2 except in the $n/2$ row. Since the characteristic is 3 the expression for the $n/2$ row becomes

$$\alpha\alpha_{n/2} = \sum_{h=0}^{n-1} t_{n/2,h}\alpha_h,$$

where $t_{n/2,h} = |(1+\kappa_{n/2}) \bigcap \kappa_h|$. Since $0 \in 1+\kappa_{n/2}$ and the $\kappa_h, h = 0,1,\ldots,n-1$, partition $\mathbb{Z}_r^*$, we have that $\sum_{h=0}^{n-1} t_{n/2,h} = 2$. Also, $t_{n/2,h} < 2$ for all h by Lemma 3.1, therefore the $n/2$ row contains exactly 2 nonzero entries. ∎

Theorem 3.4 *Let q be a power of 2 and let α be a Gauss period of type $(n,3)$ generating the normal basis $\{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}$ of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Then, the complexity of the multiplication table T_α generated by α is $4n-7$. Furthermore, the first row of T_α has exactly 1 nonzero term, the $n/2$ row of T_α has exactly $n-2$ nonzero terms and every other row has exactly 3 nonzero terms.*

PROOF. The proof follows that of Theorem 3.2 except for the first row and the $n/2$ row. When q is a power of 2, the expression for the first row can be computed as in Theorem 3.2. We have $t_{0h} = 2$ for some h and thus the term $t_{0h}\alpha_h$ vanishes in the derivation of the first row of T_α.

The $n/2$ row becomes

$$\alpha\alpha_{n/2} = \sum_{h=0}^{n-1} (t_{n/2,h}+1)\alpha_h,$$

where $t_{n/2,h} = |(1+\kappa_{n/2}) \bigcap \kappa_h|$. Since $0 \in 1+\kappa_{n/2}$ and the κ_h, $h = 0,1,\ldots,n-1$, partition $\mathbb{Z}_r^*$, we have that $\sum_{h=0}^{n-1} t_{n/2,h} = 2$. Also, $t_{n/2,h} < 2$ for all h by Lemma 3.1, thus, there are only 2 values for which $t_{n/2,h}+1 = 0$, proving the claim. ∎

We remark that the complexity of Gauss periods of type (n,t) over $\mathbb{F}_2$ where t is a prime, twice a prime, four times a prime or a power of 2 is given in [2]. Thus, our result for $q = 2$ is not new and our contribution in this case is to present explicitly the rows of the multiplication table.

3.2 Gauss periods of type $(n,4)$

In this section, we follow a similar process as in Section 3.1.

Lemma 3.5 *Let $n \in \mathbb{N}$, $n > 2$, and $r = 4n+1$ be an odd prime. Let ω be a primitive 4th root of unity in $\mathbb{F}_r$ and $\kappa = \langle \omega \rangle$. There are three distinct subsets $\{x,y\} \subset \mathbb{F}_r \backslash \{0,-1\}$ such that $x \neq y$, $\frac{x}{y} \in \kappa$ and $\frac{1+x}{1+y} \in \kappa$. These sets are disjoint and exactly one is a subset of κ.*

PROOF. By Lemma 2.3 there are three subsets satisfying the conditions of the lemma

$$S_{i,j} = \{x_{i,j}, y_{i,j}\}, (i,j) \in I = \{(1,1),(1,2),(2,1)\}.$$

If two of these sets have an element in common, say $\{x,y\}$ and $\{x,z\}$ with $y \neq z$, then the set $\{y,z\}$ also belongs to the collection. It follows that there exist distinct pairs of indices $(i_1,j_1),(i_2,j_2) \in I$ such that $x_{i_1,j_1} = x_{i_2,j_2}$ or $x_{i_1,j_1} = y_{i_2,j_2}$. This is equivalent to

$$(\omega^{j_1}-1)(\omega^{i_2+j_2}-1) = (\omega^{j_2}-1)(\omega^{i_1+j_1}-1), \tag{6}$$

or

$$(\omega^{j_1}-1)(\omega^{i_2+j_2}-1) = \omega^{i_2}(\omega^{j_2}-1)(\omega^{i_1+j_1}-1). \tag{7}$$

Furthermore, $S_{2,1} = \{\omega, \omega^3\} \subset \kappa$ and so we need only check $S_{1,1}$ and $S_{1,2}$.

First, we notice that Equation (6) is invalid since if $i_1 = i_2$ then $j_1 = j_2$ and similarly, if $j_1 = j_2$ then $i_1 = i_2$.

If $(i_1,j_1) = (1,1)$ and $(i_2,j_2) = (1,2)$, Equation (7) becomes

$$(\omega-1)(\omega^3-1) = \omega(\omega^2-1)^2.$$

Since $\omega^2 = -1$ we have $(\omega-1)(-\omega-1) = 4\omega$ and thus $2\omega = 1$. Thus, $r = 5$, contradicting $n > 1$.

Interchanging (i_1,j_1) and (i_2,j_2) gives

$$(\omega^2-1)^2 = \omega(\omega-1)(\omega^3-1).$$

Expanding gives $2\omega = 4$, thus $\omega = 2$ and $-1 = 4$, or $r = 5$, contradicting $n > 1$. ∎

Theorem 3.6 *Let q be a power of an odd prime $p > 4$, and let α be a Gauss period of type $(n,4)$ generating the normal basis $\{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}$ of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Then, the complexity of the multiplication table T_α generated by α is $5n-6$. Furthermore, the first row of T_α has n nonzero terms, 2 rows of T_α have exactly 3 nonzero terms and every other row of T_α has exactly 4 nonzero terms.*

PROOF. The jth row of the multiplication table of the basis generated by α is of the following form:

$$\alpha\alpha_j = \sum_{h=0}^{n-1} (t_{jh} - 4\delta_j)\alpha_h,$$

where $\delta_j = 0$ if $j \neq 0$ and $\delta_j = 1$ if $j = 0$.

First, we observe that $t_{jh} < 3$ for all $0 \leq j,h \leq n-1$ because otherwise there are three distinct elements $x,y,z \in \mathbb{F}_r \backslash \{0,-1\}$, such that $x,y,z \in \kappa_j$ and $1+x, 1+y, 1+z \in \kappa_h$. This would imply that the sets $\{x,y\}$ and $\{x,z\}$ that satisfy the conditions of Lemma 3.5 are distinct but not disjoint, a contradiction.

Next, we observe that the case where $t_{jh_1} = t_{jh_2} = 2$ is invalid. That is, that no two subsets $S_{i,j}$ given in Lemma 3.5 may coincide with the same row of the multiplication table. Since $S_{2,1} \subseteq \kappa$ we need only check $S_{1,1}$ and $S_{1,2}$. Suppose, by way of contradiction, that $x_{11} = q^j\omega^i$ and $x_{12} = q^j\omega^k$ for fixed j with $0 \leq i,k \leq 3$ and $i \neq k$. Isolating for q^j gives

$$\omega^{-i}\frac{1-\omega}{\omega^2-1} = \omega^{-k}\frac{1-\omega^2}{\omega^3-1}.$$

Canceling terms gives $\omega^{-i} = 2\omega^{-k}$ since ω is a root of x^2+1. Thus 2 is a 4th root of unity and so $16 \equiv 1 \pmod{r}$, yielding $r = 3$ or $r = 5$, a contradiction when $n > 1$.

Now, we give the number of nonzero entries in each row of the multiplication table:

Case 1: $j = 0$

The first row of the multiplication table is

$$\alpha\alpha_0 = \sum_{h=0}^{n-1} (t_{0h} - 4)\alpha_h.$$

Since $-1 \in \kappa_0$, we know that $\sum_{h=0}^{n-1} t_{0h} = 3$. Furthermore, by Lemma 3.5, we know that $t_{0h} = 2$, for some $h = 0,1,\ldots,n-1$. Thus, there are exactly n nonzero entries in the $j = 0$ row.

Case 2: $j \neq 0$

The $j \neq 0$ row of the multiplication table is

$$\alpha\alpha_j = \sum_{h=0}^{n-1} t_{jh}\alpha_h.$$

By Lemma 3.5 we have precisely 2 entries, $t_{jh} = 2$ and $t_{j'h'} = 2$, where $j \neq j'$ and every other nonzero term is equal to 1. Since $\sum_{h=0}^{n-1} t_{jh} = 4$, for $j = 1,2,\ldots,n-1$, there are exactly 2 rows, row j and row j', with 3 nonzero terms and $n-3$ rows with 4 nonzero terms.

Thus, the complexity of the multiplication table of the basis generated by α, where α is a type $(n,4)$ Gauss period over $\mathbb{F}_q$ is $n + 4(n-3) + 2\cdot 3 = 5n - 12 + 6 = 5n - 6$. ∎

We also state analogous theorems to Theorem 3.6 for characteristics 2 and 3. For the characteristic 3 case, the difference in the proof occurs only in the $j = 0$ row, where the term $t_{0h} = 1$ causes one additional cancelation.

Theorem 3.7 *Let q be a power of 3, and let α be a Gauss period of type $(n,4)$ generating the normal basis $\{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}$ of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Then, the complexity of the multiplication table T_α generated by α is $5n-7$. Furthermore, the first row of T_α has $n-1$ nonzero terms, 2 rows of T_α have exactly 3 nonzero terms and every other row of T_α has exactly 4 nonzero terms.*

We remark that the difference in the proof of the characteristic 2 case occurs in the $j = 0$ row, where the $t_{0h} = 2$ term yields an additional cancelation, and the two rows containing terms $t_{jh} = 2$.

Theorem 3.8 *Let q be a power of 2, and let α be a Gauss period of type $(n,4)$ generating the normal basis $\{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}$ of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Then, the complexity of the multiplication table T_α generated by α is $4n-7$. Furthermore, the first row of T_α has 1 nonzero term, 2 rows of T_α have 2 nonzero terms and the remaining rows of T_α have 4 nonzero terms.*

As before, we remark that the complexity given in Theorem 3.8 is not a new result for $q = 2$ and has appeared in [2]. The additional contribution of this work is to explicitly give the rows of the multiplication table.

3.3 Gauss periods of type $(n,5)$

We note that obtaining the multiplication tables of Gauss periods of type $(n,5)$ and $(n,6)$ is similar to the previous cases. In order to save space, in the following two sections, we present only the results with a brief sketch of the proofs. We also indicate any differences with the previous cases.

In this section, we note that the methods for determining the cyclotomic numbers are the same as those seen in Section 3.2, but the multiplication tables of type $(n,5)$ Gauss periods more closely resemble those of Section 3.1 since the type t is odd. We begin with the statement of the lemma.

Lemma 3.9 *Let $n \in \mathbb{N}$, $n > 2$, and $r = 5n+1$ be an odd prime. Let ω be a primitive 5th root of unity in $\mathbb{F}_r$, and $\kappa = \langle \omega \rangle$. There are 6 distinct subsets $\{x,y\} \subset \mathbb{F}_r \backslash \{0,-1\}$ such that $x \neq y$, $\frac{x}{y} \in \kappa$ and $\frac{1+x}{1+y} \in \kappa$, and these sets are disjoint. Furthermore, exactly two of these subsets are subsets of κ.*

By Lemma 2.3 with $t = 5$, there are 6 distinct subsets satisfying the statement of the lemma:

$$S_{i,j} = \{x_{i,j}, y_{i,j}\}, \qquad (i,j) \in I = \{(1,1),(1,2),(1,3),(2,1),(2,2),(3,1)\}.$$

The procedure for determining that the subsets $S_{i,j}$ are disjoint are identical to that in the proof of Lemma 3.5.

We now present the form of the multiplication table of a normal basis obtained by Gauss periods of type $(n,5)$ over $\mathbb{F}_q$, where q is a power of an odd prime $p \neq 5$.

Theorem 3.10 *Let q be a power of an odd prime $p \neq 5$. Furthermore, let α be a Gauss period of type $(n,5)$, $n > 6$, generating the normal basis $\{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}$ of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Then, the complexity of the multiplication table T_α generated by α is $6n-11$. Furthermore, the first row of T_α has exactly 3 nonzero terms, the $n/2$ row of T_α has exactly n nonzero terms, exactly 4 rows of T_α have 4 nonzero terms and the remaining rows of T_α have exactly 5 nonzero terms.*

We start with the observation that $t_{jh} < 3$ for $0 \leq j,h \leq n-1$, $j \neq n/2$. Indeed, if $t_{jh} \geq 3$, then there exist three distinct elements $x,y,z \in \mathbb{F}_r \backslash \{0,-1\}$, such that $x,y,z \in \kappa_j$ and $1+x, 1+y, 1+z \in \kappa_h$. This would imply that the sets $\{x,y\}$ and $\{x,z\}$ that satisfy the conditions of Lemma 3.9 are distinct but not disjoint, a contradiction.

Next, we observe that the case where $t_{jh_1} = t_{jh_2} = 2$ is invalid for a fixed j. That is, that no two subsets $S_{i,j}$ given in Lemma 3.9 may coincide with the same row of the multiplication table. This requires checking the subsets $S_{1,1}, S_{1,3}, S_{2,1}$ and $S_{2,2}$ pairwise.

Finally, we break the analysis of the multiplication table into rows with different forms: the row $j = 0$, the row $j = n/2$ and all other rows. The method is identical to the proof of Theorem 3.6.

Now, we give similar statements for the characteristic 2 and 5 cases.

Theorem 3.11 *Let q be a power of 2, and let α be a Gauss period of type $(n,5)$ generating the normal basis $\{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}$ of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Then, the complexity of the multiplication table T_α generated by α is $6n-21$. Furthermore, the first row of T_α has exactly 1 nonzero term, the $n/2$ row of T_α has exactly $n-4$ nonzero terms, 4 rows of T_α have exactly 3 nonzero terms and the remaining rows of T_α have exactly 5 nonzero terms.*

As before, we remark that the complexity given in Theorem 3.11 is not a new result for $q = 2$, and has appeared in [2]. The additional contribution of this work is to explicitly give the rows of the multiplication table.

Theorem 3.12 *Let q be a power of 5, and let α be a Gauss period of type $(n,5)$ generating the normal basis $\{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}$ of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Then, the complexity of the multiplication table T_α generated by α is $5n-7$. Furthermore, the first row of T_α has exactly 3 nonzero terms, the $n/2$ row of T_α has exactly 4 nonzero terms, 4 other rows of T_α have exactly 4 nonzero terms and the remaining rows of T_α have exactly 5 nonzero terms.*

3.4 Gauss periods of type $(n,6)$

In this section we present the complexities of the multiplication tables of Gauss periods of type $(n,6)$. As in Section 3.3, we present only the results with brief sketches of the proofs.

Lemma 3.13 *Let $n \in \mathbb{N}, n > 2$, and $r = 6n+1$ be an odd prime. Let ω be a primitive 6th root of unity in $\mathbb{F}_r$ and $\kappa = \langle \omega \rangle$. There are 10 distinct subsets $\{x,y\} \subset \mathbb{F}_r \backslash \{0,-1\}$ such that $x \neq y$, $\frac{x}{y} \in \kappa$ and $\frac{1+x}{1+y} \in \kappa$. These sets are disjoint and exactly two of these are subsets of κ.*

By Lemma 2.3 there are 10 distinct such subsets $S_{i,j} = \{x_{i,j}, y_{i,j}\}$, where

$$x_{i,j} = \frac{\omega^j - 1}{1 - \omega^{i+j}}, \quad y_{i,j} = \omega^i x_{i,j},$$

such that

$$(i,j) \in I = \{(1,1),(1,2),(1,3),(1,4),(2,1),(2,2),(2,3),(3,1),(3,2),(4,1)\}.$$

We must show, as in Lemma 3.5 and Lemma 3.9, that all the sets $S_{i,j}$, $(i,j) \in I$ are disjoint for distinct pairs of indices. The method is identical to that in the proof of Lemma 3.5 and left to the reader.

Remark 2 *Consider the following multiplication table of a type (10,6) Gauss period over* $\mathbb{F}_7$

$$\begin{bmatrix} 3 & 1 & 3 & 1 & 1 & 1 & 1 & 1 & 1 & 2 \\ 0 & 1 & 0 & 2 & 0 & 1 & 1 & 1 & 0 & 0 \\ 2 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 2 \\ 0 & 2 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 2 & 2 & 0 \\ 1 & 0 & 2 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \end{bmatrix}.$$

In the third row of this table we observe two 2*s, in contrast to our findings in the* $t = 4$ *and* $t = 5$ *cases. This yields a further complication in the multiplication table, and so for* $t = 6$ *we provide only the complexity of the multiplication table and not a complete row-by-row analysis of the multiplication table. In principle, conditions where two* 2*s occur on the same row can be computed, but the number of cases becomes extremely large as there are* 28 *pairs of elements to check.*

We present the complexity of a normal basis due to a Gauss period of type $(n,6)$ for any characteristic. We give only the complexities of the bases and not a row-by-row analysis.

Theorem 3.14 *Let* q *be a power of a prime* p*, and let* α *be a Gauss period of type* $(n,6)$ *generating the normal basis* $\{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}$ *of* $\mathbb{F}_{q^n}$ *over* $\mathbb{F}_q$*. Then, the complexity of the multiplication table* T_α *generated by* α *is given by the following table:*

	$p=2$	$p=3$	$p=5$	$p>6$
Complexity	$6n-21$	$6n-11$	$7n-15$	$7n-14$

We remark, as before, that the result for $q = 2$ is not new and appears in [2]. Our contribution in this case is to extend the known complexities to any characteristic.

Remark 3 *We have verified examples of each of the matrices given in the above sections using a Maple program.*

The lemmata in each section state that all of the subsets $S_{i,j}$ *defined in Lemma 2.3 are disjoint in the type* $(n,4)$*,* $(n,5)$ *and* $(n,6)$ *cases. However, a type* $(40,16)$ *(which is, unfortunately, too large to fit on the page) Gauss period over* $\mathbb{F}_7$ *contains* 3*s in multiple rows, indicating that the* $S_{i,j}$ *are not disjoint as n and t grow. This example shows that there is no hope of providing the multiplication table of Gauss periods of type* (n,t)*, for general t, using this analysis.*

It remains an open problem to find the multiplication tables of Gauss periods of type (n,t), for general t.

4 The trace of normal elements

In [3], the authors give the complexity of the basis generated by the trace of Type I and Type II optimal normal bases. In this section, we show that this sort of analysis holds for any normal basis. Then we give, as an example of this method, an analysis of the trace of a type $(n,3)$ Gauss period. As usual, for brevity we denote $\alpha_i = \alpha^{q^i}$ to be the ith conjugate of α over $\mathbb{F}_q$.

4.1 The trace of a general normal element

Theorem 4.1 *Let n,l,m be integers such that $n = lm$. Let $\mathbb{F}_q$ be the finite field with q elements, and let $\mathbb{F}_{q^n}$ be the extension of $\mathbb{F}_q$ of degree n. Let $\alpha \in \mathbb{F}_{q^n}$ be a normal element of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ with multiplication table T_α. Furthermore, let $\beta = Tr_{q^n/q^m}(\alpha) = \alpha + \alpha^{q^m} + \cdots + \alpha^{q^{(l-1)m}}$ be the trace of α over the subfield $\mathbb{F}_{q^m}$ of $\mathbb{F}_{q^n}$. Then, the jth row of the $m \times m$ multiplication table T_β is given by*

$$\beta\beta_j = \sum_{v=0}^{l-1} \sum_{s=0}^{r_{j+vm}-1} a_{s,j+vm}\beta_{\tau_{s,j+vm}},$$

where r_{j+vm} denotes the number of nonzero terms in row $j+vm$ of T_α, $a_{s,j+vm} \in \mathbb{F}_q^*$ and the $\tau_{s,j+vm}$ run over the indices $0,1,\ldots,m-1$.

PROOF. Let $\alpha \in \mathbb{F}_{q^n}$ be a normal element of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, and let $\beta = \mathrm{Tr}_{q^n/q^m}(\alpha) = \alpha + \alpha^{q^m} + \cdots + \alpha^{q^{(l-1)m}}$ be the trace of α over the subfield $\mathbb{F}_{q^m}$ of $\mathbb{F}_{q^n}$. It is easy to show that β is a normal element of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$.

Let T_α, T_β be the multiplication tables of α, β, respectively. Suppose row i of T_α has r_i nonzero values. Thus,

$$\alpha\alpha_i = \sum_{s=0}^{r_i-1} a_{s,i}\alpha_{\tau_{s,i}},$$

where $a_{s,i} \in \mathbb{F}_q^*, \tau_{s,i} \in \{0,1,\ldots,n-1\}$ and $\tau_{s,i} \neq \tau_{t,i}$ for $s \neq t$.

We compute the jth row of T_β as follows,

$$\begin{aligned}\beta\beta_j &= \left(\sum_{w=0}^{l-1} \alpha^{q^{mw}}\right)\left(\sum_{u=0}^{l-1} \alpha^{q^{mu+j}}\right) = \sum_w \sum_u \left(\alpha^{q^{mw}}\right)\left(\alpha^{q^{mu+j}}\right) \\ &= \sum_w \left(\alpha\alpha^{q^j}\right)^{q^{mw}} + \sum_w \left(\alpha\alpha^{q^{j+m}}\right)^{q^{mw}} + \cdots + \sum_w \left(\alpha\alpha^{q^{j+(l-1)m}}\right)^{q^{mw}}. \qquad (8)\end{aligned}$$

Explicit expressions for the jth row of T_β depend therefore on the number of nonzero elements in the rows of T_α defined by the mth coset of j modulo n. That is, on the number of nonzero entries in row $j, j+m, \ldots, j+(l-1)m$, where the values are taken modulo n.

As above, denote the number of nonzero entries in row i of T_α as r_i, then for any $v = 0,1,\ldots,l-1$ we find

$$\sum_w (\alpha\alpha_{j+vm})^{q^{mw}} = \sum_w \left(\sum_{s=0}^{r_{j+vm}-1} a_{s,j+vm}\alpha_{\tau_{s,j+vm}}\right)^{q^{mw}},$$

where $a_{s,j+vm} \in \mathbb{F}_q^*, \tau_{s,j+vm} \in \{0,1,\ldots,n-1\}$ and $\tau_{s,j+vm} \neq \tau_{t,j+vm}$ for $s \neq t$. Since $\beta = \sum_w \alpha^{q^{mw}}$ we find

$$\sum_w (\alpha\alpha_{j+vm})^{q^{mw}} = \sum_{s=0}^{r_{j+vm}-1} a_{s,j+vm}\beta_{\tau_{s,j+vm}}. \qquad (9)$$

Combining Equations (8) and (9) yields

$$\beta\beta_j = \sum_{v=0}^{l-1} \sum_{s=0}^{r_{j+vm}-1} a_{s,j+vm}\beta_{\tau_{s,j+vm}}.$$

Therefore, computing the complexity of the trace of a Gauss period requires knowledge of the number of nonzero elements in the rows of the multiplication table of the Gauss period. ■

In [3] the authors use the regular structure of the multiplication tables of optimal normal bases to give the complexity of the trace of these bases. In the following section we present the analysis of the trace of a Gauss period of type $(n,3)$ over any finite field $\mathbb{F}_q$. We notice that the analysis for Gauss periods of type (n,t), $t > 3$, will be similar with the changes arising some additional structure in the rows of the multiplication table.

4.2 The trace of a Gauss period of type $(n,3)$

Let α be a Gauss period of type $(n,3)$ which generates a normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Suppose $n = lm$ and let

$$\beta = \mathrm{Tr}_{q^n/q^m}(\alpha) = \sum_{i=0}^{l-1} \alpha^{q^{mi}}$$

be the trace of α with respect to the intermediate field $\mathbb{F}_{q^m}$. We apply the general trace construction of Section 4.1 to examine the complexity of the normal basis generated by β.

Remark 4 *In Section 3 we have seen that, in every characteristic, there are* 3 *distinct forms of the rows: the first row, the $n/2$ row and every other row. We check that there is no combination of $0 < j < m$, $j \neq m/2$ and $0 < v < l$ such that $j + vm \equiv 0 \pmod{n}$ or $j + vm \equiv n/2 \pmod{n}$. Indeed, if $j + vm = bn = blm$, for some l, then $j = m(bl - v)$ where $bl \geq l > 1$ and $v < l$. Thus, $j \geq m$, which contradicts the range of j. Also, we know n is even since $3n+1$ is an odd prime. Now, suppose $j + vm = n/2 = lm/2$. If m is odd then l is even, so $j = m(l/2 - v)$ where the right hand side is a nonzero multiple of m, contradicting the range of j. Similarly, if m is even then $j = m/2(l - 2v)$ and the right-hand side is a multiple of $m/2$ smaller than $2l$ but the left hand side is not, by the assumption on j.*

Thus, we can group the analysis into row 0*, row $m/2$ (if it exists) and combine all other rows.*

We present the complexity of the basis in each of the cases $q = 2$, q is a (non-trivial) power of two, q is a power of 3, and all other cases.

Theorem 4.2 *Let q be a power of a prime p, let $n = lm$ be integers and let α be a type $(n,3)$ Gauss period generating a normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Let $\beta = Tr_{q^n/q^m}(\alpha)$. Then, an upper bound for the complexity of the multiplication table of the basis generated by β is given by the following table. We observe that if m is odd, then the $m/2$ row does not exist and thus the value in the row "Total (m odd)" is given by the sum of the $j = 0$ row and $m - 1$ times the $j \neq 0$ row. If m is even, then the value in the row "Total (m even)" is given by the sum of the $j = 0$ row, the $j = m/2$ row and $m - 2$ times the $j \neq 0, m/2$ row.*

	$q = 2$		$q = 2^\tau, \tau > 1$	
	l even	*l odd*	*l even*	*l odd*
$j = 0$	1	1	$3l-3$	$3l-2$
$j = m/2$	$3l$	$m-2$	$3l$	$m-2$
$j \neq 0, m/2$	$3l$	$3l$	$3l$	$3l$
Total (m odd)	$3lm-3l+1$	$3lm-3l+1$	$3lm-3$	$3lm-2$
Total (m even)	$3lm-3l+1$	$(3l+1)m-6l-1$	$3lm-3$	$(3l+1)m-3l-4$

$q=3^\tau$		
	l even	*l odd*
$j=0$	$3l-2$	$3l-1$
$j=m/2$	$3l$	$3l-1$
$j\neq 0,m/2$	$3l$	$3l$
Total (m odd)	$3lm-2$	$3lm-1$
Total (m even)	$3lm-2$	$3lm-2$

	$q=p^\tau, p>3$			
	l even		*l odd*	
	$p\|l$	*other*	$p\|l$	*other*
$j=0$	$3l-2$	m	$3l-1$	$3l-1$
$j=m/2$	$3l$	$3l$	$3l-1$	m
$j\neq 0,m/2$	$3l$	$3l$	$3l$	$3l$
Total (m odd)	$3lm-2$	$(3l+1)m-3l$	$3lm-1$	$3lm-1$
Total (m even)	$3lm-2$	$(3l+1)m-3l$	$3lm-2$	$(3l+1)m-3l-1$

PROOF. We break the analysis into cases:

Case 1: $q=2$

Suppose $q=2$. Then, the multiplication table of a Gauss period of type $(n,3)$ is given by Theorem 3.4:

- the first row of the multiplication table has 1 nonzero entry in the second position,
- the $n/2$ row of the multiplication table contains $n-2$ nonzero entries,
- all other rows contain exactly 3 nonzero entries.

Let $\beta=\mathrm{Tr}_{2^n/2^m}(\alpha)$ and let T_β be the $m\times m$ multiplication table of β. Since $q=2$, we know that the first row of T_β has 1 nonzero entry as $\beta\beta=\beta^2=\beta_1$. Also, if m is odd, we can ignore row $m/2$ of T_β.

If m is even, then the $m/2$ row of T_β is given by

$$\beta\beta_{m/2}=\sum_{v=0}^{l-1}\sum_{s=0}^{r_{m/2+vm}-1}\beta_{\tau_s},$$

where we recall r_{j+vm} denotes the number of nonzero entries in row $j+vm$ of T_α and the τ_s run over the indices $0,1,\ldots,m-1$.

If l is even, then $m/2+vm\neq n/2$ for any v and $r_{m/2+vm}=3$ for all v. Thus,

$$\beta\beta_{m/2}=\sum_{v=0}^{l-1}\left(\beta_{\lambda_v}+\beta_{\mu_v}+\beta_{\eta_v}\right),$$

where λ_v,μ_v and η_v are indices in $0,1,\ldots,m-1$. Therefore, the $m/2$ row contributes at most $3l$ to the complexity.

If l is odd then, $m/2+m(l-1)/2=n/2$ and thus

$$\beta\beta_{m/2}=\sum_{v=0,v\neq(l-1)/2}^{l-1}\sum_{s=0}^{r_{m/2+vm}-1}\beta_{\tau_s}+\sum_{s=0}^{r_{n/2}-1}\beta_{\tau_s}.$$

We know $r_{n/2}=n-2$, and we write

$$\sum_{s=0}^{r_{n/2}-1}\beta_{\tau_s}=\sum_{s=0}^{n-1}\beta_s+\beta_{\lambda_{n/2}}+\beta_{\mu_{n/2}}=l\sum_{s=0}^{m-1}\beta_s+\beta_{\lambda_{n/2}}+\beta_{\mu_{n/2}},$$

where $\lambda_{n/2}, \mu_{n/2} \in \{0, 1, \ldots, m-1\}$. Thus,

$$\sum_{s=0}^{r_{n/2}-1} \beta_{\tau_s} = \sum_{s=0}^{m-3} \beta_{\tau_s},$$

where the τ_s run over the indices $0, 1, \ldots, m-1$. Therefore the $m/2$ row contributes at most $m-2$ to the complexity.

For $j \neq 0, m/2$, the derivation is identical to row $m/2$ when m and l are even, yielding a contribution to the complexity from these rows of at most $3l$.

Case 2: q is a power of 2

The difference when q is a (non-trivial) power of 2 comes in the analysis of the first row of the multiplication table. In particular, the form of the multiplication table remains the same, but for the derivation of the first row we have $\beta\beta = \beta^2 \neq \beta_1$. Since β^2 is now not a basis element, we need to determine β^2 as a combination of basis elements.

The first row of the multiplication table T_β is given by

$$\beta\beta = \sum_{v=0}^{l-1} \sum_{s=0}^{r_{vm}-1} \beta_{\tau_s}.$$

For $v = 0$ we have $r_0 = 1$. If l is odd, then there is no v such that $vm = n/2$ thus $r_{vm} = 3$ for all $0 < v < l$. Therefore,

$$\beta\beta = \beta_{\lambda_0} + \sum_{v=1}^{l-1} \left(\beta_{\lambda_v} + \beta_{\mu_v} + \beta_{\eta_v}\right),$$

and the contribution to the complexity from the first row is at most $3l-2$.

If l is even, then for $v = l/2$ we have $r_{vm} = r_{n/2} = n-2$. Thus, we write

$$\beta\beta = \beta_{\lambda_0} + \sum_{v=1, v\neq l/2}^{l-1} \left(\beta_{\lambda_v} + \beta_{\mu_v} + \beta_{\eta_v}\right) + \sum_{i=0}^{n-1} \beta_i + \beta_{\lambda_{n/2}} + \beta_{\mu_{n/2}}.$$

We write $\sum_{i=0}^{n-1} \beta_i = l \sum_{i=0}^{m-1} \beta_i = 0$ since l is even. Thus,

$$\beta\beta = \beta_{\lambda_0} + \sum_{v=1, v\neq l/2}^{l-1} \left(\beta_{\lambda_v} + \beta_{\mu_v} + \beta_{\eta_v}\right) + \beta_{\lambda_{n/2}} + \beta_{\mu_{n/2}},$$

and the contribution to the complexity from the first row is at most $1 + 3(l-2) + 2 = 3l - 3$.

Case 3: q is a power of 3

When q is a power of 3, the multiplication table of α, given by Theorem 3.3, has the following form:

- the first row has 2 nonzero terms, one equal to 1 and one equal to 2,
- the $n/2$ row has 2 nonzero terms, both of which are equal to 1,
- each other row has 3 nonzero terms, all of which are equal to 1.

The derivation to find the number of nonzero entries in each row differs from Case 1 and Case 2 only in the first row and in the $m/2$ row.

The first row of the multiplication table T_β is given by

$$\beta\beta = \sum_{v=0}^{l-1} \sum_{s=0}^{r_{vm}-1} \beta_{\tau_s}.$$

For $v = 0$ we have $r_0 = 2$. If l is odd, then there is no v such that $vm = n/2$ thus $r_{vm} = 3$ for all $0 < v < l$. Therefore,

$$\beta\beta = \beta_{\lambda_0} + 2\beta_{\mu_0} + \sum_{v=1}^{l-1} \left(\beta_{\lambda_v} + \beta_{\mu_v} + \beta_{\eta_v}\right),$$

and the contribution to the complexity from the first row is at most $3l - 1$.

If l is even, then for $v = l/2$ we have $r_{vm} = r_{n/2} = 2$. Thus, we write

$$\beta\beta = \beta_{\lambda_0} + 2\beta_{\mu_0} + \sum_{v=1, v\neq l/2}^{l-1} \left(\beta_{\lambda_v} + \beta_{\mu_v} + \beta_{\eta_v}\right) + \beta_{\lambda_{n/2}} + \beta_{\mu_{n/2}}.$$

Thus, the contribution to the complexity from the first row is $3l - 2$.

For the $m/2$ row, if l is even, then $m/2 + vm \neq n/2$ for any v and $r_{m/2+vm} = 3$ for all v. As before, the contribution to the complexity from the $m/2$ row in this case is at most $3l$. If l is odd, then $m/2 + m(l-1)/2 = n/2$, and thus

$$\beta\beta_{m/2} = \sum_{v=0, v\neq (l-1)/2}^{l-1} \left(\beta_{\lambda_v} + \beta_{\mu_v} + \beta_{\eta_v}\right) + \beta_{\lambda_{n/2}} + \beta_{\mu_{n/2}}.$$

Therefore, the contribution to the complexity from the $m/2$ row is at most $3l - 1$.

Case 4: $q = p^\tau, p > 3$

When q is a power of a prime $p > 3$, the multiplication table of α, given by Theorem 3.2, has the following form:

- the first row has 2 nonzero terms; one equal to 1 and one equal to 2,
- the $n/2$ row has n nonzero terms, exactly 2 of which are equal to -2 and the remainder equal to -3,
- each other row has 3 nonzero terms, all of which are equal to 1.

For the first row, we have $r_0 = 2$. If l is odd, then there is no v such that $vm = n/2$, and thus $r_{vm} = 3$ for all $0 < v < l$. The derivation for the first row in this case is identical to the Case 3, and the contribution to the complexity from the first row is at most $3l - 1$.

If l is even, then for $v = l/2$ we have $r_{vm} = r_{n/2} = n$. Thus, we write

$$\beta\beta = \beta_{\lambda_0} + 2\beta_{\mu_0} + \sum_{v=1, v\neq l/2}^{l-1} \left(\beta_{\lambda_v} + \beta_{\mu_v} + \beta_{\eta_v}\right) - 3\sum_{i=0}^{n-1} \beta_i + \beta_{\lambda_{n/2}} + \beta_{\mu_{n/2}}.$$

We write $\sum_{i=0}^{n-1} \beta_i = l \sum_{i=0}^{m-1} \beta_i$. We further split into the cases $l \equiv 0 \pmod{p}$ and all other cases. If $l \equiv 0 \pmod{p}$, then $-3\sum_{i=0}^{n-1} \beta_i = -3l\sum_{i=0}^{m-1} \beta_i = 0$ and thus the contribution to the complexity from the first row is at most $3l - 2$. For other values of $l \pmod{p}$, the contribution to the complexity from the first row contains more terms. In these cases, we give the trivial bound and the contribution to the complexity from the first row is at most m. We note, in other specific cases we can determine certain small cancelations in the rows of the multiplication tables. For example, if $l \equiv 1/3 \pmod{p}$, then $-3\sum_{i=0}^{n-1} \beta_i = -\sum_{i=0}^{m-1} \beta_i$ and thus the contribution in this case will cancel every term with a coefficient of 1 in the expression of this row. If $l \equiv 2/3 \pmod{p}$, there is one cancelation with one term from the $n/2$ row and the $2\beta_{\mu_0}$ term.

If m is odd, then there is no $m/2$ row of T_β. We consider the case where m is even. If l is even, then $m/2+vm \neq n/2$ for any v and $r_{m/2+vm} = 3$ for all v. Thus,

$$\beta\beta_{m/2} = \sum_{v=0}^{l-1} \left(\beta_{\lambda_v} + \beta_{\mu_v} + \beta_{\eta_v}\right),$$

where λ_v, μ_v and η_v are indices in $0, 1, \ldots, m-1$. Therefore, the $m/2$ row contributes at most $3l$ to the complexity.

If l is odd, then $m/2 + m(l-1)/2 = n/2$ and thus

$$\beta\beta_{m/2} = \sum_{v=0, v\neq(l-1)/2}^{l-1} \left(\beta_{\lambda_v} + \beta_{\mu_v} + \beta_{\eta_v}\right) + \sum_{s=0}^{r_{n/2}-1} a_{\tau_s}\beta_{\tau_s}.$$

We know $r_{n/2} = n$ and we write

$$\sum_{s=0}^{r_{n/2}-1} \beta_{\tau_s} = -3\sum_{s=0}^{n-1} \beta_s + \beta_{\lambda_{n/2}} + \beta_{\mu_{n/2}} = -3l\sum_{s=0}^{m-1} \beta_s + \beta_{\lambda_{n/2}} + \beta_{\mu_{n/2}}.$$

We further split into the cases $l \equiv 0 \pmod{p}$ and all other cases. If $l \equiv 0 \pmod{p}$, then $-3l\sum_{s=0}^{m-1}\beta_s = 0$ and the contribution from the $m/2$ row of the multiplication table is at most $3l-1$. Otherwise, we cannot claim any cancelations and so we upper bound the contribution from the $m/2$ row of the multiplication table by m. ∎

We remark that there is an implicit assumption in this paper about the range of l we consider. In particular, we assume that l is small enough such that the contribution to the complexity from each row does not exceed m. For example, in Section 4.2, Case 4 when l is odd, the first row contributes at most $3l-1$ to the complexity, so the implicit assumption is that l is at most $m/3$. Indeed, this assumption is not needed as Theorem 4.2 is valid (but trivial) for larger values of l.

4.3 Errata of [3]

We would like to take the opportunity to correct a couple of small typos and inconsistencies in our previous paper [3]. In particular, [3, Theorem 3] should indicate that the result, as all of the other results in that paper and in Section 4 of this paper, give upper bounds on the complexity of the normal basis obtained by traces. In the previous paper, in the statement of [3, Theorem 3] we say "...the complexity of the normal basis of $\mathbb{F}_{2^m}$ over $\mathbb{F}_2$ generated by β is $2km-2k+1$". This should read, "...the complexity of the normal basis of $\mathbb{F}_{2^m}$ over $\mathbb{F}_2$ generated by β is *at most* $2km-2k+1$." This change should also be reflected in [3, Corollary 2].

In addition, we notice in Section 4 that there is a difference in the derivation of the trace of Gauss periods when $q=2$ and when q is a (non-trivial) power of 2. In this case $\beta\beta = \beta^2$ is not a basis element and thus there is an addition contribution to the complexity from the first row. In [3] we indicate that we give the trace of Type I and Type II optimal normal bases for q even, but what we derive in [3] is the $q=2$ case.

Now, we would like to indicate an oversight in the derivation of the $m/2$ row of the multiplication table in [3, Theorem 1], which is again reflected in [3, Theorem 2]. In the equation below [3, Equation (5)], each term with a coefficient of -1 should read $-k$. Thus,

our bound of $m-k+1$ nonzero terms only applies when $k \equiv 1 \pmod{p}$. In the best case, when p divides k, the contribution from the $m/2$ line is at most $k-1$. In all other cases, we revise this bound on the contribution to the complexity from $m-k+1$ to m, which is the maximum allowable.

Below, find a table indicating the changes to the table found in the conclusions section of [3]. The notation for the table below is as in this paper: q is a power of a prime p and n, l, m are integers such that $n = lm$.

	Type I (q odd)	Type I ($q = 2$)
m even, l odd p divides l	$(l+1)m-l-1$	–
m even, l odd, $l \equiv 1 \pmod{p}$	$(l+2)m-3l+1$	$(l+1)m-3l+2$
m even, l odd, all other l	$(l+2)m-2l$	–

We regret any inconvenience that this discrepancy in the result has caused.

5 Concluding remarks

In this paper, we give the complexity of the multiplication tables of Gauss periods of type (n,t), $t = 3,4,5,6$. In addition, we give the format of the rows of the multiplication table of a Gauss period normal basis for $t = 3,4,5$. We also give a method of finding normal bases in subfields of a field containing a known normal basis, and apply this method to Gauss periods of type $(n,3)$. In principle, if the complexity of the normal basis in the original field is low and the size of the subfield is not too small compared to the original field (that is, if $n = lm$ and l is relatively large), then the complexity of the normal basis in the subfield should also be low.

We recall that Gauss periods of type (n,t) form self-dual normal bases if t is even, and the characteristic divides t. The dual basis of a type I optimal normal basis (Gauss periods of type $(n,1)$) appears in [21] and the dual basis of the trace of type I optimal normal bases can be found in [3]. We remark that the dual basis of the trace construction of Gauss periods of larger type presented in Section 4 could also be carried out in this paper in the same way as in [3,21].

We observe that it is possible in principle to extend this analysis to Gauss periods of small type. However, the number of pairs of elements given in Lemma 2.3 is $(t-1)(t-2)/2$ and so the number of pairs of elements to check is quadratic in t. In addition, the analysis of the cyclotomic numbers becomes more complicated as the degree of the t-th cyclotomic polynomial over $\mathbb{Q}$ grows. The problem of giving the multiplication tables (and therefore, the complexities) of Gauss periods of type (n,t), for general t, remains open.

References

1. O. Ahmadi, I. Shparlinski and J. F Voloch, On multiplicative order of Gauss periods, *International Journal of Number Theory*, to appear.
2. D. W. Ash, I. F. Blake and S. A. Vanstone, Low complexity normal bases, *Discrete Applied Mathematics*, **25** (1989), 191-210.
3. M. Christopoulou, T. Garefalakis, D. Panario, D. Thomson, The trace of an optimal normal element and low complexity normal bases, *Designs, Codes and Cryptography*, **49** (2008), 199-215.
4. R. Dahab, D. Hankerson, F. Hu, M. Long, J. López and A. Menezes, Software multiplication using Gaussian normal bases, *IEEE Transactions on Computers*, **55** (2006), 974-984.
5. S. Gao, J. von zur Gathen and D. Panario, Gauss periods: orders and cryptographical applications, *Mathematics of Computation*, **67** (1998), 343-352.
6. S. Gao, J. von zur Gathen, D. Panario and V. Shoup, Algorithms for exponentiation in finite fields, *Journal of Symbolic Computation*, **29** (2000), 879-889.

7. S. Gao and H. W. Lenstra, Optimal normal bases, *Designs, Codes and Cryptography*, **2** (1992), 315-323.
8. J. von zur Gathen and M. Nöcker, Fast arithmetic with general Gauss periods, *Theoretical Computer Science*, **315** (2004), 419-452.
9. J. von zur Gathen and F. Pappalardi, Density estimates related to Gauss periods, *Progress in Computer Science and Applied Logic*, **20** (2001), 33-41.
10. J. von zur Gathen and I. Shparlinski, Orders of Gauss periods in finite fields, *Applicable Algebra in Engineering, Communication and Computing*, **9** (1997), 15-24.
11. C. F. Gauss, *Disquisitiones Arithmeticae* English edition, Springer-Verlag, New York (1986).
12. M. A. Hasan, M. Z. Wang and V. K. Bhargava, A modified Massey-Omura parallel multiplier for a class of finite fields, *IEEE Transactions on Computers*, **42** (1993), 1278-1280.
13. D. Jungnickel, *Finite Fields: Structure and Arithmetic*, Wissenschaftsverlag (1993).
14. J. L. Massey and J. K. Omura, Computation method and apparatus for finite field arithmetic, *U.S Patent no.:4587627*, Issued: 6 May 1986.
15. 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.
16. 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.
17. A. Reyhani-Masoleh and M. A. Hasan, Efficient multiplication beyond optimal normal bases, *IEEE Transactions on Computers*, **52** (2003), 428-439.
18. A. Reyhani-Masoleh and M. A. Hasan, Low Complexity Word-Level Sequential Normal-Basis Multipliers, *IEEE Transactions on Computers*, **54** (2005), 98-110.
19. D. Silva and F. R. Kschischang, Fast encoding and decoding of Gabidulin codes, *Proceedings of the IEEE International Symposium of Information Theory*, Seoul, Korea (2009), 2858-2862.
20. B. Sunar and C. K. Koç, An efficient optimal normal basis type II multiplier, *IEEE Transactions on Computers*, **50** (2001), 83-87.
21. Z. Wan and K. Zhou, On the complexity of the dual basis of a type I optimal normal basis, *Finite Fields and Their Applications*, **13** (2007), 411417.
22. A. Wassermann, Konstruktion von Normalbasen, *Bayreuther Mathematische Scriften*, **31** (1990), 155-164.
23. B. Young and D. Panario, Low complexity normal bases in $\mathbb{F}_{2^n}$, *Finite Fields and their Applications*, **10** (2004), 53-64.