On the Complexity of the Dual Bases of the Gaussian Normal Bases

Alok Mishra  Rajendra Kumar Sharma  Wagish Shukla

Department of Mathematics, Indian Institute of Technology Delhi, New Delhi 110016, India
E-mail: alok.mishra.11@gmail.com  rksharma@maths.iitd.ac.in  wagishs@maths.iitd.ac.in

Received 21 September 2012
Revised 21 March 2013
Communicated by Zhongming Tang

Abstract. In this paper, we study the complexity of the dual bases of the Gaussian normal bases of type \((n, t)\), for all \(n\) and \(t = 3, 4, 5, 6\), of \(\mathbb{F}_{q^n}\) over \(\mathbb{F}_q\) and provide conditions under which the complexity of the Gaussian normal basis of type \((n, t)\) is equal to the complexity of the dual basis over any finite field.

2010 Mathematics Subject Classification: 11T99, 12E20, 12E30

Keywords: finite fields, trace map, complexity of a normal basis, Gaussian normal basis of type \((n, t)\), dual bases

1 Introduction

Let \(\mathbb{F}_q\) be a finite field, where \(q\) is a prime or a prime power. Consider an extension \(\mathbb{F}_{q^n}\) of \(\mathbb{F}_q\) and \(\alpha \in \mathbb{F}_{q^n}\). A normal basis of \(\mathbb{F}_{q^n}\) over \(\mathbb{F}_q\) is a basis of the form \(N = \{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}\), where we say that \(\alpha\) is a normal element of \(\mathbb{F}_{q^n}\), or that \(\alpha\) generates the normal basis \(N\). It is well-known that the normal bases exist in any finite extension of a finite field (see [5, Theorem 2.34]). Let \(N = \{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}\) be a normal basis of \(\mathbb{F}_{q^n}\) over \(\mathbb{F}_q\), where \(\alpha_i = \alpha^q^i\) for \(0 \leq i \leq n - 1\). Then for any \(0 \leq i, j \leq n - 1\), \(\alpha_i\alpha_j\) is a linear combination of \(\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\) with coefficients in \(\mathbb{F}_q\). In particular, \(\alpha_i\alpha_j = \sum_{j=0}^{n-1} t_{ij} \alpha_j\), \(0 \leq i \leq n - 1\) and \(t_{ij} \in \mathbb{F}_q\). For the normal basis \(N\) there is an associated matrix \(T_{\alpha} = (t_{ij})\) given by above relations. The number of nonzero entries in \(T_{\alpha}\) is called the complexity of the normal basis \(N\), denoted by \(c_N\). It is proved that \(c_N \geq 2n - 1\) for any normal basis \(N\) of \(\mathbb{F}_{q^n}\) over \(\mathbb{F}_q\) (see [1, Theorem 5.1]). Let \(M = \{\beta_0, \beta_1, \ldots, \beta_{n-1}\}\) be another basis of \(\mathbb{F}_{q^n}\) over \(\mathbb{F}_q\); \(M\) is said to be the dual basis of \(N\) if

\[\text{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha_i\beta_j) = \delta_{ij}, \quad 1 \leq i, j \leq n.\]

Here, \(\delta_{ij}\) denotes the Kronecker delta function, i.e., \(\delta_{ij} = 0\) if \(i \neq j\), and \(\delta_{ij} = 1\) if
The following are equivalent:

\[ \alpha \] generates a normal basis \( N \) of \( \mathbb{F}_{q^n} \) over \( \mathbb{F}_q \) and \( \beta \) generates the dual basis of \( N \), then \( \beta \) is a dual element of \( \alpha \). We know that the dual basis of a normal basis is also a normal basis (see [1, Corollary 1.4]). With the development of coding theory and appearance of several cryptosystems using finite fields, the implementation of finite field arithmetic, in either hardware or software, is required. Of course, the advantages of using a normal basis representation have been known from many years. The complexity of the hardware design of multiplication schemes due to Mullin, Onyszchuk and Vanstone [8] and Massey and Omura [6] by using normal bases to represent finite fields heavily depends on the choice of normal bases used.

Normal bases are widely used in applications of finite fields in many areas, such as coding theory, cryptography and signal processing. In particular, optimal normal bases are desirable, but not all finite fields have optimal normal bases. So, to work efficiently in other fields for practical applications, one needs to construct a normal basis of complexity as low as possible.

Christopoulos, Garefalakis, Panario, et al. [2] gave the complexity of the Gaussian normal basis of type \((n, t)\) for all \( n \) and \( t = 3, 4, 5 \) and 6 over any finite field. In this paper, we study the complexity of the dual basis of the Gaussian normal basis of type \((n, t)\) for all \( n \) and \( t = 3, 4, 5 \) and 6 over any finite field, and give conditions under which the complexity of the Gaussian normal basis of type \((n, t)\) is equal to the complexity of the dual basis over any finite field.

2 Preliminaries

In this section, we recall some notions and results on Gauss periods and Gaussian normal bases.

**Definition 2.1.** Let \( r = nt + 1 \) be a prime not dividing \( q \) and \( \kappa \) be the unique subgroup of order \( t \) in \( \mathbb{Z}_r^* \). Let \( \kappa_0, \ldots, \kappa_{n-1} \) be cosets of \( \kappa \) in \( \mathbb{Z}_r^* \) and \( \beta \) be a primitive \( r \)-th root of unity in \( \mathbb{F}_{q^r}^* \). The elements \( \alpha_i, i = 0, 1, \ldots, n - 1 \), are given by \( \alpha_i = \sum_{\kappa \in \kappa_i} \beta^\kappa \), 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 Gauss periods of type \((n, t)\) over \( \mathbb{F}_q \).

Note that Gauss periods are elements of \( \mathbb{F}_{q^r} \) and \( \text{Tr}_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\alpha) = -1 \). The following theorem gives conditions under which Gauss periods define normal elements.

**Theorem 2.2.** [2, 3] Let \( \alpha \in \mathbb{F}_{q^n} \) be a Gauss period of type \((n, t)\) as defined above. The following are equivalent:

\[ \begin{align*}
&\text{• The set } N = \{ \alpha, \alpha^2, \ldots, \alpha^{q^n-1} \} \text{ forms a normal basis of } \mathbb{F}_{q^n} \text{ over } \mathbb{F}_q. \\
&\text{• If } e \text{ is the order of } q \text{ modulo } r, \text{ then } \gcd(nt/e, n) = 1. \\
&\text{• The (disjoint) union of } \kappa_0, \kappa_1, \ldots, \kappa_{n-1} \text{ is } \mathbb{Z}_r^*. \text{ Equivalently, } \mathbb{Z}_r^* = \langle q, \kappa \rangle.
\end{align*} \]

Let \( \alpha_0, \alpha_1, \ldots, \alpha_{n-1} \) be the 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, Panario, Shoup, et al. [3]. First we define cyclotomic numbers \( t_{ij} = |(1 + \kappa_i) \cap \kappa_j| \). 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

\[ \mu_j = \begin{cases} 
0 & \text{if } j \neq j_0, \\
1 & \text{if } j = j_0.
\end{cases} \]
Then the form of the multiplication table $T_{\alpha}$ is $\alpha \alpha_i = \mu_i t + \sum_{j=0}^{n-1} t_{ij} \alpha_j$. An explicit determination of the multiplication table $T_{\alpha}$, therefore, depends on the cyclotomic numbers $t_{ij}$. In our results we use an equivalent form of the rows of the multiplication table. We have

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

where the last sum is $\mu_i t \cdot \text{Tr}_{\mathbb{Z}_q / \mathbb{Z}_q} (\alpha) = -\mu_i t$. Thus, $\alpha \alpha_i = \sum_{j=0}^{n-1} (t_{ij} - \mu_i t) \alpha_j$.

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

**Lemma 2.4.** [4] Suppose that $N$ is the Gaussian normal basis of type $(n, t)$ generated by $\alpha$ and $1 \leq t \leq n$. Then

$$\delta = \begin{cases} \frac{1}{tn+1}\alpha - \frac{t}{tn+1} & \text{if } t \equiv 0 \pmod{2}, \\ \frac{1}{tn+1}\alpha + \frac{t}{tn+1} & \text{otherwise} \end{cases}$$

generates the dual basis of $N$. Hence, $N$ is self-dual if and only if one of the following is true:

(i) $t \equiv 0 \pmod{2}$ and $p = 2$.

(ii) $p \equiv 1 \pmod{2}$ and $t \equiv 0 \pmod{2p}$.

(iii) $t \equiv 1 \pmod{2}$ and $n = p = 2$.

### 3 Main Results

In this paper, we give the complexities of the dual bases of the Gauss periods of type $(n, 3), (n, 4), (n, 5)$ and $(n, 6)$, and also conditions for which the complexity of the Gaussian normal basis of type $(n, t)$ and its dual basis are the same.

For finding the multiplication table of the Gauss periods of type $(n, 3)$, we have the following lemma.

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

**Theorem 3.2.** Let $\alpha$ be a Gauss period of type $(n, 3)$ and $N$ be the Gaussian normal basis of type $(n, 3)$ generated by $\alpha$. Further, let $\delta$ be a generator of the dual basis $M$ of $N$. Then

(i) The complexity of the dual basis $M$ is bounded by $5n - 3$ when $q$ is a power of some odd prime $p > 3$.

(ii) The complexity of the dual basis $M$ is $3n - 2$ when $q$ is a power of 3.
(iii) The complexity of the dual basis \( M \) is bounded by \( 3n - 1 \) when \( q \) is a power of 2.

Proof. (i) Let \( r = 3n + 1 \) be a prime and \( q \) be a power of some odd prime such that \( (3n + 1, q) = 1 \). Let \( \kappa = [1, \tau, \tau^2] \), where \( \tau \) is a primitive 3rd root of unity in \( \mathbb{Z}_p^* \) and \( \kappa_i = \{q^i : a : a \in \kappa\} \). Let \( \alpha \) be a Gauss period of type \((n, 3)\) over \( \mathbb{F}_q \) and \( N = \{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\} \), where \( \alpha_i = \alpha^i, \quad 0 \leq i \leq n - 1 \), is the Gaussian normal basis of type \((n, 3)\) generated by \( \alpha \). The multiplication table \( T_\alpha \) of \( N \) is given by

\[
\alpha \alpha_i = \sum_{j=0}^{n-1} (t_{ij} - \mu_i) \alpha_j, \quad 0 \leq i \leq n - 1.
\]

Let \( M = \{\delta_0, \delta_1, \ldots, \delta_{n-1}\} \), where \( \delta_i = \delta^q, \quad 0 \leq i \leq n - 1 \), be the dual basis of \( N \) of \( \mathbb{F}_q^* \) over \( \mathbb{F}_q \). In this case \( \delta = \frac{1}{3n+1} \alpha_{n/2} - \frac{1}{3n+1} \). To examine the multiplication table \( T_\delta \) of the dual basis \( M \) generated by \( \delta \), we require the expression of the products \( \delta \delta_i \) in terms of the basis elements \( \delta, \delta_1, \ldots, \delta_{n-1} \).

For \( i = 0, 1, \ldots, n - 1 \),

\[
\delta \delta_i = \left( \frac{1}{3n+1} \alpha_{n/2} - \frac{3}{3n+1} \right) \left( \frac{1}{3n+1} \alpha_{n/2+i} - \frac{3}{3n+1} \right) = \frac{1}{(3n+1)^2} \alpha_{n/2} \alpha_{n/2+i} - \frac{1}{3n+1} \alpha_{n/2} \delta_{n/2} - \frac{1}{3n+1} \delta_{n/2} \alpha_{n/2+i} + \frac{3^2}{(3n+1)^2}.
\]

Now we consider different cases for \( i \).

Case 1: \( i = 0 \).

The first row of the multiplication table \( T_\delta \) of the dual basis \( M \) is given by

\[
\delta \delta_0 = \frac{1}{3n+1} \left( \sum_{j=0}^{n-1} t_{0j} \delta_{j+n/2} \right) - \frac{3}{3n+1} \delta_{n/2} - \frac{3}{3n+1} \delta_{n/2} \delta_{n/2} + \frac{3}{(3n+1)^2} \left( \sum_{j=0}^{n-1} t_{0j} \right) - \frac{3^2}{(3n+1)^2}.
\]

As \( \mu_0 = 0 \). Since all \( \kappa_i \) for \( i = 0, 1, \ldots, n - 1 \) form a partition of \( \mathbb{Z}_p^* \) and \( \sum_{j=0}^{n-1} \mu_j = 3 \), it follows from Lemma 3.1 that \( t_{0j} = 2 \) for exactly one \( j \), where \( 0 \leq j \leq n - 1 \).

Thus from (2),

\[
\delta \delta_0 = \frac{1}{3n+1} (2 \delta_{j_1} + \delta_{j_2}) - \frac{6}{3n+1} \delta, \quad 0 \leq j_1, j_2 \leq n - 1.
\]

Hence, the first row of the multiplication table \( T_\delta \) of \( M \) contains at most three nonzero entries.
Case 2: \( i = n/2 \).

In this case \( \mu_{n/2} = 1 \), so from (1) we have

\[
\delta\delta_{n/2} = \frac{1}{3n+1} \left( \sum_{j=0}^{n-1} (t_{n/2,j} - 3)\delta_{j+n/2} \right) - \frac{3}{3n+1} \delta_{n/2} - \frac{3}{3n+1} \delta \\
+ \frac{3}{(3n+1)^2} \left( \sum_{j=0}^{n-1} (t_{ij} - 3) \right) - \frac{3^2}{(3n+1)^2}.
\]

(3)

Since \(-1 \in \kappa_0\) and \(\sum_{j=0}^{n-1} t_{n/2,j} = 2\), by Lemma 3.1 there exist \(j_1, j_2\) such that \(t_{n/2,j_1} = t_{n/2,j_2} = 1\). So from (3) we get

\[
\delta\delta_{n/2} = \frac{1}{3n+1} \left( -2\delta_{j_1} - 2\delta_{j_2} - 3\delta_{j_3} - \cdots - 3\delta_{j_n} \right) \\
- \frac{3}{3n+1} \delta_{n/2} + \frac{3}{3n+1} \sum_{j=0}^{n-1} \delta_j \\
= \frac{1}{3n+1} (\delta_{j_1} + \delta_{j_2}) - \frac{3}{3n+1} \delta_{n/2} - \frac{3}{3n+1} \delta.
\]

Thus, the \(n/2\)-th row of the multiplication table \(T_5\) of \(M\) contains at most four nonzero entries.

Case 3: \( i \neq 0, n/2 \).

As \( \mu = 0 \), from (1) we have

\[
\delta\delta_i = \frac{1}{3n+1} \left( \sum_{j=0}^{n-1} t_{ij}\delta_{j+n/2} \right) - \frac{3}{3n+1} \delta_{n/2} - \frac{3}{3n+1} \delta_{i+n/2} \\
+ \frac{3}{(3n+1)^2} \left( \sum_{j=0}^{n-1} t_{ij} \right) - \frac{3^2}{(3n+1)^2}.
\]

(4)

By Lemma 3.1 and the fact that \(\sum_{j=0}^{n-1} t_{mj} = 3\), it follows that each nonzero \(t_{ij} = 1\). So from (4),

\[
\delta\delta_i = \frac{1}{3n+1} (\delta_{h_1} + \delta_{h_2} + \delta_{h_3}) - \frac{3}{3n+1} \delta_{n/2} - \frac{3}{3n+1} \delta_{i+n/2},
\]

\(0 \leq h_1, h_2, h_3 \leq n - 1\). Thus for all \(i \neq 0, n/2\), the \(i\)-th row of the multiplication table \(T_5\) of \(M\) contains at most five nonzero entries.

Hence, the multiplication table \(T_5\) of \(M\) contains at most \(3+4+(n-2)\cdot5 = 5n-3\) nonzero entries. Consequently, the complexity of the dual basis \(M\) generated by \(\delta\) is bounded by \(5n - 3\).

(ii) The first row of the multiplication table \(T_5\) of the dual basis \(M\) is given by

\[
\delta\delta_0 = \frac{1}{3n+1} (2\delta_{j_1} + \delta_{j_2}) - \frac{6}{3n+1} \delta + \frac{3}{(3n+1)^2} \left( \sum_{j=0}^{n-1} t_{0j} \right) - \frac{3^2}{(3n+1)^2}
\]

\[
= \frac{1}{3n+1} (2\delta_{j_1} + \delta_{j_2}), \quad 0 \leq j_1, j_2 \leq n - 1,
\]

since the characteristic is 3. Thus, the first row of the multiplication table \(T_5\) of the dual basis \(M\) contains exactly two nonzero entries.
Since \(-1 \in \kappa_{n/2}\) and \(\sum_{j=0}^{n-1} t_{n/2,j} = 2\), it follows from Lemma 3.1 that \(t_{n/2,j} < 2\) for all \(j\). Thus from (1), the \(\frac{n}{2}\)-th row of the multiplication table \(T_δ\) of the dual basis \(M\) is given by

\[
\delta_{n/2} = \frac{1}{3n+1} \sum_{j=0}^{n-1} t_{n/2,j} \delta_{j+n/2} = \frac{1}{3n+1} (\delta_{j_1} + \delta_{j_2}), \quad 0 \leq j_1, j_2 \leq n-1.
\]

Therefore, the \(\frac{n}{2}\)-th row contains exactly two nonzero entries.

For \(i \neq 0, n/2\), the \(i\)-th row of the multiplication table \(T_δ\) of \(M\) is of the form

\[
\delta_i = \frac{1}{3n+1} (\delta_{h_1} + \delta_{h_2} + \delta_{h_3}),
\]

because by Lemma 3.1 and the fact \(\sum_{j=0}^{n-1} t_{ij} = 3\) we get that each nonzero \(t_{ij}\) is equal to 1. Thus, each of the remaining \(n - 2\) rows of \(T_δ\) of the dual basis \(M\) contains exactly three nonzero entries.

Consequently, the complexity of the dual basis \(M\) is exactly \(2 + 2 + (n - 2) \cdot 3 = 3n - 2\). In this case, the complexities of the Gaussian normal basis of type \((n, 3)\) and its dual basis are the same.

(iii) The proof is the same as above except for the first row and the \(\frac{n}{2}\)-th row.

When \(q\) is a power of 2, the expression for the first row of the multiplication table \(T_δ\) of the dual basis \(M\) is given by

\[
\delta_0 = \frac{1}{3n+1} (2\delta_{j_1} + \delta_{j_2}) = \frac{1}{3n+1} \delta_{j_2}, \quad 0 \leq j_2 \leq n-1.
\]

So the first row of the multiplication table \(T_δ\) of the dual basis \(M\) contains only one nonzero entry. The \(\frac{n}{2}\)-th row of \(T_δ\) of the dual basis \(M\) is of the form

\[
\begin{align*}
\delta_{n/2} &= \frac{1}{3n+1} (-\delta_{j_1} - \cdots - \delta_{j_{n-1}}) - \frac{1}{3n+1} \delta_{n/2} - \frac{1}{3n+1} \delta + \frac{1}{3n+1} \sum_{j=0}^{n-1} \delta_j \\
&= \frac{1}{3n+1} (\delta_{j_1} + \delta_{j_{n/2}}) - \frac{1}{3n+1} \delta_{n/2} - \frac{1}{3n+1} \delta,
\end{align*}
\]

where \(0 \leq j_{h_i} \leq n-1\). Thus, the \(\frac{n}{2}\)-th row of the multiplication table \(T_δ\) of the dual basis \(M\) contains at most four nonzero entries. Hence, the complexity of the dual basis \(M\) is at most \(1 + 4 + (n - 2) \cdot 3 = 3n - 1\).

For finding the multiplication table of the Gauss periods of type \((n, 4)\), we have the following lemma.

**Lemma 3.3.** [2, Lemma 3.5] Let \(n \in \mathbb{N}\) with \(n > 2\) and \(r = 4n + 1\) be an odd prime. Let \(\omega\) be a primitive 4th root of unity in \(\mathbb{F}_r\) and \(\kappa = \langle \omega \rangle\). There are three distinct subsets \(\{x, y\} \in \mathbb{F}_r \setminus \{0, -1\}\) such that \(x \neq y, \frac{x}{y} \in \kappa\) and \(\frac{-x}{4y} \in \kappa\). These sets are disjoint and exactly one is a subset of \(\kappa\).

**Theorem 3.4.** Let \(\alpha\) be a Gauss period of type \((n, 4)\) and \(N\) be the Gaussian normal basis of type \((n, 4)\) generated by \(\alpha\). Further, let \(\delta(\frac{1}{4n+1} \alpha - \frac{4}{4n+1})\) be a generator of the dual basis \(M\) of \(N\). Then

(i) The complexity of the dual basis \(M\) is bounded by \(6n - 5\) when \(q\) is a power of some odd prime \(p > 4\).
(ii) The complexity of the dual basis $M$ is $4n - 7$ when $q$ is a power of $2$.

(iii) The complexity of the dual basis $M$ is bounded by $6n - 5$ when $q$ is a power of $3$.

**Proof.** (i) The $i$-th row of the multiplication table $T_δ$ of the dual basis $M$ generated by $δ$ is given by

$$
δδ_{i} = \frac{1}{4n+1} \left( \sum_{j=0}^{n-1} (t_{ij} - μ_i 4) δ_j \right) - \frac{4}{4n+1} δ - \frac{4}{4n+1} δ_i + \frac{4}{(4n+1)^2} \left( \sum_{j=0}^{n-1} (t_{ij} - μ_i 4) \right) - \frac{4^2}{(4n+1)^2}.
$$

From Lemma 3.3, we observe that $t_{ij} < 3$ for all $0 \leq i, j \leq n - 1$ and the case where $t_{ij1} = t_{ij2} = 2$ is invalid. Now we give the number of nonzero entries in each row of the multiplication table $T_δ$.

The first row of the multiplication table $T_δ$ of the dual basis $M$ is given by

$$
δδ_0 = \frac{1}{4n+1} \left( \sum_{j=0}^{n-1} (t_{0j} - 4) δ_j \right) - \frac{8}{4n+1} δ + \frac{4}{(4n+1)^2} \left( \sum_{j=0}^{n-1} (t_{0j} - 4) \right) - \frac{16}{(4n+1)^2}.
$$

Since $-1 \in κ_0$ and $\sum_{j=0}^{n-1} t_{0j} = 3$, it follows from Lemma 3.3 that $t_{0j} = 2$ for some unique $j$, where $j \in \{0, 1, \ldots, n - 1\}$. Thus from (5), we have

$$
δδ_0 = \frac{1}{4n+1} \left( \sum_{j=0}^{n-1} (t_{0j} - 4) δ_j \right) - \frac{8}{4n+1} δ + \frac{4}{(4n+1)^2} \sum_{j=0}^{n-1} δ_j
$$

$$
= \frac{1}{4n+1} (2δ_{j1} + δ_{j2}) - \frac{8}{4n+1} δ, \quad 0 \leq j_1, j_2 \leq n - 1.
$$

Thus, the first row of the multiplication table $T_δ$ of the dual basis $M$ contains at most three nonzero entries.

The $i$-th ($i \neq 0$) row of the multiplication table $T_δ$ of the dual basis $M$ is given by

$$
δδ_i = \frac{1}{4n+1} \sum_{j=0}^{n-1} t_{ij} δ_j - \frac{4}{4n+1} δ - \frac{4}{4n+1} δ_i + \frac{4}{(4n+1)^2} \sum_{j=0}^{n-1} t_{ij} - \frac{16}{(4n+1)^2}.
$$

From $\sum_{j=0}^{n-1} t_{ij} = 4$ and Lemma 3.3, we have precisely two entries $t_{ij} = 2$ and $t_{i'j'} = 2$, where $i \neq i'$. Thus, there are exactly two rows of the form

$$
δδ_i = \frac{1}{4n+1} (2δ_{j1} + δ_{j2} + δ_{j3}) - \frac{4}{4n+1} δ - \frac{4}{4n+1} δ_i,
$$

having at most five nonzero entries, and $n - 3$ rows are of the form

$$
δδ_i = \frac{1}{4n+1} (δ_{j1} + δ_{j2} + δ_{j3} + δ_{j4}) - \frac{4}{4n+1} δ - \frac{4}{4n+1} δ_i,
$$

having at most six nonzero entries. Hence, the complexity of the dual basis generated by $δ$ is at most $3 + 2 \cdot 5 + (n - 3) \cdot 6 = 6n - 5$. 

Let \( \delta \) be the Gaussian normal basis of type \((n, 5)\). There are six distinct subsets \( \{x, y\} \in \mathbb{F}_r \setminus \{0, -1\} \) such that \( x \neq y, \frac{2}{x} \in \kappa \) and \( \frac{1+x+y}{r+x+y} \in \kappa \), and these sets are disjoint. Furthermore, exactly two of these subsets are subsets of \( \kappa \).

**Lemma 3.5.** [2, Lemma 3.9] Let \( n \in \mathbb{N} \) with \( n > 2 \) and \( r = 5n+1 \) be an odd prime. Let \( \omega \) be a primitive 5th root of unity in \( \mathbb{F}_r \) and \( \kappa = \langle \omega \rangle \). There are six distinct subsets \( \{x, y\} \in \mathbb{F}_r \setminus \{0, -1\} \) such that \( x \neq y, \frac{2}{x} \in \kappa \) and \( \frac{1+x+y}{r+x+y} \in \kappa \), and these sets are disjoint. Furthermore, exactly two of these subsets are subsets of \( \kappa \).

**Theorem 3.6.** Let \( \alpha \) be a Gauss period of type \((n, 5)\) and \( N \) be the Gaussian
normal basis of type \((n,4)\) generated by \(\alpha\). Furthermore, let \(\delta\) be a generator of the dual basis \(M\) of \(N\). Then

(i) The complexity of the dual basis \(M\) is bounded by \(7n - 8\) when \(q\) is a power of some odd prime \(p \neq 5\).

(ii) The complexity of the dual basis \(M\) is bounded by \(7n - 15\) when \(q\) is a power of 2.

(iii) The complexity of the dual basis \(M\) is \(5n - 7\) when \(q\) is a power of 5.

Proof. (i) The \(i\)-th row of the multiplication table \(T_\delta\) of the dual basis \(M\) generated by \(\delta\) is of the form

\[
\delta_\delta_i = \frac{1}{5n+1} \left( \sum_{j=0}^{n-1} (t_{ij} - \mu_i) \delta_{j+n/2} \right) - \frac{5}{5n+1} \delta_{n/2} - \frac{5}{5n+1} \delta_{i+n/2}
\]

(6)

where \(\mu_i = 1\) if \(i = n/2\) and \(\mu_i = 0\) if \(i \neq n/2\). By Lemma 3.5, we have \(t_{ij} < 3\) for \(0 \leq i, j \leq n - 1, i \neq n/2\). Next, we observe that the case \(t_{j_1} = t_{j_2} = 2\) is invalid for a fixed \(i\). Finally, we analyze the multiplication table \(T_\delta\) for different rows.

Case 1: \(i = 0\).

The first row of the multiplication table \(T_\delta\) of the dual basis \(M\) generated by \(\delta\) is given by

\[
\delta_\delta_0 = \frac{1}{5n+1} \left( \sum_{j=0}^{n-1} t_{0j} \delta_{j+n/2} \right) - \frac{10}{5n+1} \delta_{n/2} + \frac{5}{(5n+1)^2} \left( \sum_{j=0}^{n-1} t_{0j} \right) - \frac{5^2}{(5n+1)^2}.
\]

By Lemma 3.5 and \(\sum_{j=0}^{n-1} t_{0j} = 5\), it follows that \(t_{0j_1} = t_{0j_2} = 2\) for \(j_1 \neq j_2\). Thus,

\[
\delta_\delta_0 = \frac{1}{5n+1} \left( 2\delta_{j_1+n/2} + 2\delta_{j_2+n/2} + \delta_{j_3+n/2} \right) - \frac{10}{5n+1} \delta_{n/2}.
\]

Hence, there are at most four nonzero entries in the first row of the multiplication table \(T_\delta\) of the dual basis \(M\).

Case 2: \(i = n/2\).

Since \(-1 \in \kappa_{n/2}\), \(\sum_{j=0}^{n-1} t_{n/2,j} = 4\) and \(\mu_{n/2} = 1\), from (6) the \(\frac{n}{2}\)-th row of the multiplication table \(T_\delta\) of the dual basis \(M\) is given by

\[
\delta_\delta_{n/2} = \frac{1}{5n+1} \left( \sum_{j=0}^{n-1} (t_{n/2,j} - 5) \delta_{j+n/2} \right) - \frac{5}{5n+1} \delta_{n/2} - \frac{5}{5n+1} \delta
\]

(6)

\[
+ \frac{5}{(5n+1)^2} \left( \sum_{j=0}^{n-1} (t_{ij} - 5) \right) - \frac{5^2}{(5n+1)^2}
\]

\[
= \frac{1}{5n+1} \left( \delta_{j_1} + \delta_{j_2} + \delta_{j_3} + \delta_{j_4} \right) - \frac{5}{5n+1} \delta_{n/2} - \frac{5}{5n+1} \delta,
\]

where \(j_h \in \{0, 1, \ldots, n-1\}\). Consequently, the \(\frac{n}{2}\)-th row of the multiplication table \(T_\delta\) contains at most six nonzero entries.

Case 3: \(i \neq 0, n/2\).
The $i$-th row of the multiplication table $T_\delta$ of the dual basis $M$ is given by

$$
\delta\delta_i = \frac{1}{5n+1} \left( \sum_{j=0}^{n-1} t_{ij} \delta_j \right) + \frac{5}{5n+1} \delta_{i+n/2} - \frac{5}{5n+1} \delta_{i+2n/2} - \frac{5}{5n+1} \delta_{i+3n/2} - \frac{5}{5n+1} \delta_{i+4n/2} - \frac{5}{5n+1} \delta_{i+5n/2} - \frac{5}{5n+1} \delta_{i+6n/2}.
$$

By Lemma 3.5 and $\sum_{j=0}^{n-1} t_{ij} = 5$, we get $t_{ij} = 2$ for four different $i$. Thus, we observe that there are exactly four rows of the form

$$\delta\delta_m = \frac{1}{5n+1} \left( 2\delta_j + \delta_2 + \delta_3 + \delta_4 \right) - \frac{5}{5n+1} \delta_{i+n/2} - \frac{5}{5n+1} \delta_{i+2n/2},$$

having at most six nonzero entries, and $n-6$ rows of the form

$$\delta\delta_m = \frac{1}{5n+1} \left( \delta_j + \delta_2 + \delta_3 + \delta_4 + \delta_5 \right) - \frac{5}{5n+1} \delta_{i+n/2} - \frac{5}{5n+1} \delta_{i+2n/2},$$

having at most seven nonzero entries. Hence, the complexity of the dual basis $M$ generated by $\delta$ is at most $4 + 6 + (n - 6) \cdot 7 + 4 \cdot 6 = 7n - 8$.

(ii) The $i$-th row of the multiplication table $T_\delta$ of the dual basis $M$ generated by $\delta$ is given by

$$\delta\delta_i = \frac{1}{5n+1} \left( \sum_{j=0}^{n-1} (t_{ij} - \mu) \delta_j \right) - \frac{1}{5n+1} \delta_{i+n/2} - \frac{1}{5n+1} \delta_{i+2n/2} - \frac{1}{5n+1} \delta_{i+3n/2} - \frac{1}{5n+1} \delta_{i+4n/2} - \frac{1}{5n+1} \delta_{i+5n/2} - \frac{1}{5n+1} \delta_{i+6n/2}.$$

The first row of the multiplication table $T_\delta$ of the dual basis $M$ is given by

$$\delta\delta_0 = \frac{1}{5n+1} \delta_{n/2+1}.$$

Thus, the first row of the multiplication table $T_\delta$ contains only one nonzero entry.

The $\frac{n}{2}$-th row of the multiplication table $T_\delta$ of the dual basis $M$ is given by

$$\delta\delta_{n/2} = \frac{1}{5n+1} \left( \delta_j + \delta_{j+2} + \delta_{j+4} + \delta_{j+6} \right) + \frac{1}{5n+1} \delta_{n/2} + \frac{1}{5n+1} \delta + \frac{1}{5n+1} \sum_{j=0}^{n-1} \delta_j$$

$$= \frac{1}{5n+1} \left( \delta_j + \delta_{j+2} + \delta_{j+4} + \delta_{j+6} \right) + \frac{1}{5n+1} \delta_{n/2} + \frac{1}{5n+1} \delta.$$

Thus, the $\frac{n}{2}$-th row of the multiplication table $T_\delta$ contains at most six nonzero entries.

For $i \neq 0, n/2$, there are exactly four rows of the form

$$\delta\delta_i = \frac{1}{5n+1} \left( \delta_j + \delta_{j+2} + \delta_{j+4} + \delta_{j+6} \right) + \frac{1}{5n+1} \delta_{n/2} + \frac{1}{5n+1} \delta_{m+n/2},$$

having at most five nonzero entries, and $n-6$ rows of the form

$$\delta\delta_i = \frac{1}{5n+1} \left( \delta_j + \delta_{j+2} + \delta_{j+4} + \delta_{j+6} \right) - \frac{1}{5n+1} \delta_{n/2} - \frac{1}{5n+1} \delta_{m+n/2},$$

having at most seven nonzero entries.
Hence, the complexity of the dual basis $M$ is at most $1 + 6 + (n - 6) \cdot 7 + 4 \cdot 5 = 7n - 15$.

(iii) The $i$-th row of the multiplication table $T_δ$ of the dual basis $M$ generated by $δ$ is given by

$$δδ_i = \frac{1}{5n+1} \left( \sum_{j=0}^{n-1} t_{ij} δ_{j+n/2} \right).$$

Then the first row of the multiplication table $T_δ$ of the dual basis $M$ is given by

$$δδ_0 = \frac{1}{5n+1} (2δ_{j_1+n/2} + 2δ_{j_2+n/2} + δ_{j_3+n/2}).$$

Thus, the first row of the multiplication table $T_δ$ contains exactly three nonzero entries.

The $\frac{n}{2}$-th row of the multiplication table $T_δ$ of the dual basis $M$ is given by

$$δδ_{n/2} = \frac{1}{5n+1} (δ_{j_1} + δ_{j_2} + δ_{j_3} + δ_{j_4}).$$

So the $\frac{n}{2}$-th row of the multiplication table $T_δ$ contains four nonzero entries.

We observe that there are exactly four rows of the form

$$δδ_m = \frac{1}{5n+1} (2δ_{j_1} + δ_{j_2} + δ_{j_3} + δ_{j_4}),$$

having four nonzero entries, and $n - 6$ rows of the form

$$δδ_m = \frac{1}{5n+1} (δ_{j_1} + δ_{j_2} + δ_{j_3} + δ_{j_4} + δ_{j_5}),$$

having five nonzero entries. Hence, the complexity of the dual basis $M$ is

$$3 + 4 + (n - 6) \cdot 5 + 4 \cdot 4 = 5n - 7.$$ 

Thus when the characteristic is $5$, the complexity of Gaussian normal basis of type $(n, 5)$ is the same as the complexity of the dual basis, i.e, $5n - 7$. □

For finding the multiplication table of the Gauss periods of type $(n, 6)$, we have the following lemma.

**Lemma 3.7.** [2, Lemma 3.13] Let $n \in \mathbb{N}$ with $n > 2$ and $r = 6n + 1$ be an odd prime. Let $ω$ be a primitive $6$th root of unity in $\mathbb{F}_r$ and $κ = \langle ω \rangle$. There are ten distinct subsets $\{x, y\} \in \mathbb{F}_r \setminus \{0, -1\}$ such that $x \neq y$, $\frac{x}{y} \in κ$ and $\frac{x+y}{1+y} \in κ$. These sets are disjoint and exactly two of them are subsets of $κ$.

**Theorem 3.8.** Let $α$ be a Gauss period of type $(n, 6)$ and $N$ be the Gaussian normal basis of type $(n, 6)$ generated by $α$. Further, let $δ$ be a generator of the dual basis $M$ of $N$. Then

(i) The complexity of the dual basis $M$ is bounded by $8n - 12$ when $q$ is a power of some odd prime $p > 3$.

(ii) The complexity of the dual basis $M$ is $6n - 21$ when $q$ is a power of $2$.

(iii) The complexity of the dual basis $M$ is bounded by $6n - 11$ when $q$ is a power of $3$. 


Proof. (i) The first row of the multiplication table $T_3$ of the dual basis $M$ is given by
\[
\delta \delta_0 = \frac{1}{6n+1} \left( \sum_{j=0}^{n-1} (t_{0j} - 6) \delta_j \right) - \frac{12}{6n+1} \delta + \frac{6}{(6n+1)^2} \left( \sum_{j=0}^{n-1} (t_{0j} - 6) \right) - \frac{36}{(6n+1)^2} \delta.
\]
Since $-1 \in \kappa_0$ and $\sum_{j=0}^{n-1} t_{0j} = 5$, it follows from Lemma 3.7 that there exist exactly two $j$ for which $t_{0j} = 2, 0 \leq j \leq n - 1$. Therefore,
\[
\delta \delta_0 = \frac{1}{6n+1} \left( \sum_{j=0}^{n-1} (t_{0j} - 6) \delta_j \right) - \frac{12}{6n+1} \delta + \frac{6}{(6n+1)^2} \sum_{j=0}^{n-1} \delta_j
\]
for some $0 \leq j_1, j_2, j_3 \leq n - 1$. Thus, the first row of the multiplication table $T_3$ contains at most four nonzero entries.

The $i$-th $(i \neq 0)$ row of the multiplication table $T_3$ of the dual basis $M$ is given by
\[
\delta \delta_i = \frac{1}{6n+1} \sum_{j=0}^{n-1} t_{ij} \delta_j - \frac{6}{6n+1} \delta \delta_i + \frac{6}{(6n+1)^2} \sum_{j=0}^{n-1} t_{ij} - \frac{36}{(6n+1)^2} \delta,
\]
by $\sum_{j=0}^{n-1} t_{ij} = 6$ and Lemma 3.7, we have precisely eight entries having $t_{ij} = 2$ for distinct $i$. Thus, there are exactly eight rows of the form
\[
\delta \delta_i = \frac{1}{6n+1} \left( 2\delta_{j_1} + \delta_{j_2} + \delta_{j_3} + \delta_{j_4} + \delta_{j_5} \right) - \frac{6}{6n+1} \delta - \frac{6}{6n+1} \delta_i,
\]
having at most seven nonzero entries, and $n - 9$ rows of the form
\[
\delta \delta_i = \frac{1}{6n+1} \left( \delta_{j_1} + \delta_{j_2} + \delta_{j_3} + \delta_{j_4} + \delta_{j_5} + \delta_{j_6} \right) - \frac{6}{6n+1} \delta - \frac{6}{6n+1} \delta_i,
\]
having at most eight nonzero entries. Consequently, the complexity of the dual basis $M$ generated by $\delta$ is at most $4 + 8 \cdot 7 + (n - 9) \cdot 8 = 8n - 12$.

(ii) The first row of the multiplication table $T_3$ of the dual basis $M$ is given by $\delta \delta_0 = \frac{1}{6n+1} \delta_j$. Thus, the first row of the multiplication table $T_3$ contains only one nonzero entry. If the characteristic is 2, then in the multiplication table $T_3$ there are exactly eight rows of the form
\[
\delta \delta_i = \frac{1}{6n+1} \left( \delta_{j_1} + \delta_{j_2} + \delta_{j_3} + \delta_{j_4} \right),
\]
having four nonzero entries, and $n - 9$ rows of the form
\[
\delta \delta_i = \frac{1}{6n+1} \left( \delta_{j_1} + \delta_{j_2} + \delta_{j_3} + \delta_{j_4} + \delta_{j_5} + \delta_{j_6} \right),
\]
having six nonzero entries. Consequently, the complexity of the dual basis $M$ is $1 + 8 \cdot 4 + (n - 9) \cdot 6 = 6n - 21$, which is the same as that of the Gaussian normal basis of type $(n, 6)$.

(iii) The first row of the multiplication table $T_3$ of the dual basis $M$ is given by $\delta \delta_0 = \frac{1}{6n+1} \left( 2\delta_{j_1} + \delta_{j_2} + \delta_{j_3} \right)$. Thus, the first row of the multiplication table $T_3$ contains three nonzero entries. If the characteristic is 3, then in the multiplication
table $T_3$ there are exactly eight rows of the form
\[
\delta \delta_i = \frac{1}{6n+1} (2\delta_{i_1} + \delta_{i_2} + \delta_{i_3} + \delta_{i_4} + \delta_{i_5}),
\]
having exactly five nonzero entries, and $n - 9$ rows of the form
\[
\delta \delta_i = \frac{1}{6n+1} (\delta_{i_1} + \delta_{i_2} + \delta_{i_3} + \delta_{i_4} + \delta_{i_5}),
\]
having exactly six nonzero entries. Therefore, the complexity of the dual basis $M$ is
\[
3 + 8 \cdot 5 + (n - 9) \cdot 6 = 6n - 11,
\]
which is the same as that of the Gaussian normal basis of type $(n, 6)$.

From the previous discussion, we observe that in some cases the complexity of the dual basis is the same as that of the corresponding Gaussian normal basis. So now we give conditions for which the complexity of the Gaussian normal basis of type $(n, t)$ is the same as that of its dual basis.

**Theorem 3.9.** Let $\alpha$ be a Gauss period of type $(n, t)$ and $N$ be the Gaussian normal basis of type $(n, t)$ generated by $\alpha$. Further, let $\delta$ generate the dual basis $M$ of $N$. If the Gaussian normal basis is a self-dual basis or $t$ is odd and $t \equiv 0 \pmod{p}$, then the complexities of the Gaussian normal basis $N$ and its dual basis $M$ are the same.

**Proof.** Let $\alpha$ generate the Gaussian normal basis of type $(n, t)$. Furthermore, let $\delta$ be the dual element of $\alpha$ and generate the dual normal basis $M$. The multiplication table $T_\alpha$ of $N$ is given by the expression
\[
\alpha \alpha_i = \mu_i t + \sum_{j=0}^{n-1} t_{ij} \alpha_j, \quad 0 \leq i \leq n - 1,
\]
which is equivalent to
\[
\alpha \alpha_i = \sum_{j=0}^{n-1} (t_{ij} - \mu_i t) \alpha_j
\]
(7)
since $\text{Tr}_{\mathbb{F}_q^n/\mathbb{F}_q}(\alpha) = -1$. Let the complexity of the Gaussian normal basis $N$ be $C_N$. Now we consider two cases.

**Case 1:** $t$ is odd. The multiplication table $T_\delta$ of the dual basis $M$ generated by $\delta$ is given by the following expression
\[
\delta \delta_i = \frac{1}{tn+1} \left( \sum_{j=0}^{n-1} (t_{ij} - \mu_i t) \delta_{j+n/2} \right) - \frac{t}{tn+1} \delta_{n/2} - \frac{t}{tn+1} \delta_{i+n/2}
\]
\[
+ \frac{t}{(tn+1)^2} \left( \sum_{j=0}^{n-1} (t_{ij} - \mu_i t) \right) - \frac{t^2}{(tn+1)^2}, \quad 0 \leq i \leq n - 1.
\]
If $t \equiv 0 \pmod{p}$, where $p$ is the characteristic of the field $\mathbb{F}_q$, then it follows that
\[
\delta \delta_i = \frac{1}{tn+1} \left( \sum_{j=0}^{n-1} (t_{ij} - \mu_i t) \delta_{j+n/2} \right).
\]
(8)
Since the complexities of the Gaussian normal basis of type $(n, t)$ and its dual basis $M$ depend on cyclotomic numbers $t_{ij}$, from (7) and (8) the complexity of the dual basis $M$ is the same as that of the Gaussian normal basis $N$. 

□
Case 2: t is even. The multiplication table $T_δ$ of the dual basis $M$ is given by the following expression

$$\delta δ_i = \frac{1}{tn+1} \left( \sum_{j=0}^{n-1} (t_{ij} - \mu_i t) \delta_j \right) - \frac{t}{tn+1} \delta - \frac{t}{tn+1} \delta_i$$

$$+ \frac{t}{(tn+1)^2} \left( \sum_{j=0}^{n-1} (t_{ij} - \mu_i t) \right) - \frac{t^2}{(tn+1)^2} \delta, \quad 0 \leq i \leq n-1.$$  (9)

If the characteristic is 2 or $t \equiv 0 \pmod{p}$, where $p > 3$ is the characteristic of the field $F_q$, then from (9) we have

$$\delta δ_i = \frac{1}{tn+1} \left( \sum_{j=0}^{n-1} (t_{ij} - \mu_i t) \delta_j^{n/2} \right).$$  (10)

From (7) and (10), it is easy to see that the complexity of the Gaussian normal basis $N$ is the same as that of its dual basis $M$. As we know that the Gaussian normal basis of type $(n, t)$ is a self-dual normal basis if and only if $t$ is even and $t \equiv 0 \pmod{p}$, where $p$ is the characteristic (see [7]), so in this case the Gaussian normal basis is a self-dual basis. □

Acknowledgements. The authors gratefully acknowledge the valuable comments and suggestions from the anonymous referees.

References


