doi: 103969/j. issn. 0490-6756. 2016. 03. 001

有限域上 $(n,k)(k \geqslant 3)$ 型高斯正规基的对偶基的复杂度

廖群英，李雪连
(四川师范大学数学与软件科学学院，成都，610066)

摘　要：确定有限域上的正规基，特别是高斯正规基的复杂度是一个有趣的问题. 本文利用有限域的性质给出了有限域上一类 $(n,k)(k \geqslant 3)$ 型高斯正规基的对偶基的复杂度的上下界，由此确定了有限域上 $(n,k)(k=1,2)$ 型高斯正规基的对偶基的准确复杂度，从而简化了万哲先等人在 2007 年给出的证明.

关键词：有限域；分圆数；正规基；对偶基；迹映射；复杂度；乘法表
中图分类号：O157.4　　**文献标识码**：A　　**文章编号**：0490-6756(2016)02-0235-12

Complexity of the dual bases for Gauss normal bases of type $(n,k)(k \geqslant 3)$ over finite fields

LIAO Qun-Ying, *LI Xue-Lian*
(Sichuan Normal University, College of Mathematics and Software Science, Chengdu 610066, China)

Abstract: It is well known that 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. Therefore to determine the complexity for normal bases, especially Gauss normal bases over finite fields, is interesting. By properties for finite fields and elementary techniques, we obtain the upper and lower bounds of the complexity for the dual basis of a class of the type $(n,k)(k \geqslant 3)$ Gauss normal bases, and determine the explicit complexity of the dual basis for the type $(n,k)(k=1,2)$ Gauss normal bases over finite fields, which is an elementary proof for the main results given by Wan and Zhou in 2007.

Key words: Finite field; Cyclotomic number; Normal basis; Dual basis; Trace mapping; Complexity; Multiplication table
(2010 MSC 12E20, 11T71)

1　Introduction

Let q be a power of the prime p and let F_q be the finite field with q elements. For any element $\alpha \in F_{q^n}$, the conjugates of α are given by α^{q^i}, $i=0,\ldots,n-1$. If $N=\{\alpha_i=\alpha^{q^i} \mid i=0,\ldots,n-1\}$ forms a basis for F_{q^n} over F_q, then we call N a normal basis and α the normal basis generator. For the normal basis N there is an associated matrix $T_\alpha=(t_{i,j})$ given by the relations

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

收稿日期：2014-08-08
基金资助：国家自然科学基金项目(11401408)；四川省教育厅重点项目(14ZA0034)
通信作者：廖群英(1974－)，教授，主要从事编码和密码学理论研究. E-mail: qunyingliao@sicnu.edu.cn

The number of nonzero entries in T_α is called the complexity (also sometimes called the density) of the basis$N$ [1]. Mullin et al.[1] prove that the complexity of any normal basis of F_{q^n} over F_q is at least $2n-1$. Normal bases which achieve this lower bound are called optimal normal bases. Mullin et al. also 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 [2] later prove this claim.

It is well known that normal bases over finite fields have been implemented efficiently in software, see, for example, Refs. [3~15]. 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. Therefore optimal normal bases are the most desirable since they have the lowest complexity. While 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. In 1989, Ash, Blake and Vanstone[6] introduce the Gauss period, and then by using Gauss period they generalize optimal normal bases to be Gauss normal bases, which are just with lower complexity[4,7]. Recent years, Christopolou et al.[8], Liao and Hu[13] obtain the explicit computing formula for the complexity of a class of Gauss normal bases over finite fields.

In the present paper, we obtain the upper and lower bounds for the complexities of Gauss normal bases over finite fields, and determine the explicit complexity of the dual basis for the type $(n,k)(k=1,2)$ Gauss normal bases, which is an elementary proof for Theorem 2.2 given by Wan and Zhou[15].

2 Preliminary and main results

Definition 2.1[4,6,7] Let $r=kn+1$ be a prime not dividing q. Furthermore, let Abe the unique subgroup of order k in $\mathbf{Z}_r^*$ and $A_i=\{q^i\cdot x \mid x\in A\}\subseteq \mathbf{Z}_r^*$. Also let β be a primitive r-th root of unity in $F_{q^{kn}}$. The elements $\alpha_i=\sum_{a\in A_i}\beta^a, 0\leqslant i\leqslant n-1$, are called to be the type (n,k) Gauss period of F_{q^n} over F_q. Furthermore, if the order e of q modulo r satisfies $\gcd(nk/e,n)=1$, then the set

$$N=\{\alpha_0,\cdots,\alpha_{n-1}\}=\{\alpha,\alpha^q,\cdots,\alpha^{q^{n-1}}\}$$

forms a normal basis of F_{q^n} over F_q, called the type (n,k) Gauss normal basis of F_{q^n} over F_q. It is well known that 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. [1] For general cases, the multiplication table of the Gauss normal basis over finite fields is closely related to the cyclotomic numbers.

Proposition 2.2[4,7] Let $N=\{\alpha_i \mid 0\leqslant i\leqslant n-1\}$ be the type (n,k) Gauss normal basis of F_{q^n} over F_q. Suppose that $j_0<n$ is the unique index such that $-1\in A_{j_0}$. Then

$$j_0=\begin{cases}0, 2\mid k,\\ n/2, \text{otherwise},\end{cases}$$

and the form of the multiplication table T_α of N is

$$\alpha\alpha_i=\delta_i t+\sum_{j=0}^{n-1}m_{i,j}\alpha_j=\sum_{j=0}^{n-1}(m_{i,j}-\delta_i t)\alpha_j \tag{1}$$

where $m_{i,j}=\mid (1+A_i)\cap A_j\mid$ is the cyclotomic numbers, and

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

Therefore the explicit determination of the multiplication table T_α depends on studying the cyclotomic numbers $m_{i,j}$.

***Remark* 1** Note that $m_{j,h}>1$ is the same as $\mid (1+A_j)\cap A_h\mid>1$. In this case, it is enough to show that if $x,y\in A_j$then $1+x,1+y\in A_h$. In other words, we require $x\neq y$ such that $x/y\in A$ and $(1+x)/(1+y)\in A$.

Proposition 2.3[8] Let $n>2$ be a positive integer, and let $r=kn+1$ be an odd prime. Let ω be a primitive k-th root of unity in $\mathbf{Z}_r^*$ and $A=[\omega]$.

(1) $m_{j,j+h}=m_{n-j,h}$ for all $0<j<n/2$;

(2) If k is even, then $m_{j,h}=m_{h,j}$ for all $0\leqslant j,h\leqslant n-1$;

(3) There are $(k-1)(k-2)/2$ distinct subsets $\{x,y\}\subseteq \mathbf{Z}_r\backslash\{0,-1\}$ such that $x\neq y, x/y\in A$ and $(1+x)/(1+y)\in A$, given by $S_{i,j}=\{x_{i,j},$

$y_{i,j}\}$, where

$$x_{i,j}=\frac{\omega^j-1}{1-\omega^{i+j}}, y_{i,j}=\omega^i x_{i,j}, 1\leqslant i,j\leqslant k-1,$$
$$i+j<k.$$

Furthermore, $S_{k-2j,j}\subseteq A, 1\leqslant j\leqslant\frac{k-1}{2}$.

Till now, we can only determine some special cycloyomic numbers. In 2012, by computing the cyclotomic numbers $m_{i,j}$ one by one, Christopolou, et al.[8] present the multiplication tables and the complexities of the type (n,k) Gauss normal bases for $k=3,4,5$ and give a slightly weaker result for the type $(n,6)$ Gauss normal bases. Recently, we[13] generalize their main results to the general case, and obtain the explicit computing formula for the complexity of the type (n,k) Gauss normal bases over finite fields when the sets $S_{i,j}$ are disjoint to each others. As examples, we[13] show that the type (n,k) with $k<6$ Gauss normal basis satisfies the condition, and the type $(n,7)$ Gauss normal basis satisfies the condition if and only if $n\neq 4$.

On the other hand, dual bases are very important in finite fields and their applications. For two bases $N=\{\alpha_i \mid i=0,\cdots,n-1\}$ and $B=\{\beta_i \mid i=0,\cdots,n-1\}$ of F_{q^n} over F_q. B is the dual basis of N if for any $i,j=0,\cdots,n-1$,

$$Tr(\alpha_i\beta_j)=\begin{cases}1, i=j,\\ 0, \text{otherwise},\end{cases}$$

where $Tr(\alpha)$ is the trace map of $\alpha\in F_{q^n}$ over F_q. N is a self-dual basis when $B=N$. In particular, if N is a normal basis, then B is the dual basis of N if and only if for any $i=0,\cdots,n-1$,

$$Tr(\alpha\beta_i)=\begin{cases}1, i=0,\\ 0, \text{otherwise}.\end{cases}$$

It is well-known that for a basis N of F_{q^n} over F_q, the dual basis B is unique and also a normal basis when$N$ is a normal basis. It is well-known that for a fixed normal basis N, it is not easy to determine the unique dual basis of N. In 2000, Gao et al.[4] obtain the dual basis of the type (n,k) Gauss normal basis over finite fields. In 2012, Liao[12] obtains the dual basis and its trace basis of a Gauss normal basis for arbitrary medium subfields F_{q^m} over F_q with $m\mid n$ and $1\leqslant m\leqslant n$.

Proposition 2.4[4]　Suppose that $1\leqslant k\leqslant n$ and $N=\{\alpha=\alpha_0,\cdots,\alpha_{n-1}\}$ is the type (n,k) Gauss normal basis ofF_{q^n} over F_q. Then the dual basis of N is generated by

$$\beta=\begin{cases}\frac{1}{kn+1}\alpha-\frac{k}{kn+1}, & if \quad k\equiv 0(\mathrm{mod}2),\\ \frac{1}{kn+1}\alpha^{\frac{n}{2}}-\frac{k}{kn+1}, & \text{otherwise}.\end{cases}\qquad(2)$$

In particular, from Proposition 2.4, when $q=k=2$ we can get $\beta=\frac{1}{2n+1}\alpha$, which means that the type II optimal normal basis is self-dual. When $k=1$, i.e., for the type I optimal normal basis N of F_{q^n} over F_q, through determining the multiplication table of the dual basis of N, Wan and Zhou[15] prove that the complexity of the dual basis B is $3n-3$ or $3n-2$ depending on q is even or odd, respectively. While in general cases, even if the multiplication table or the complexity of a normal basis over finite fields is given, to determine the complexity of the dual basis is not easy. In recent years, for the case the normal basis and its dual have linear generators, the relationship between their multiplication tables is given.

Proposition 2.5[10]　Let q be a power of the prime p and let $N=\{\alpha_i=\alpha^{q^i} \mid i=0,1,\cdots,n-1\}$ be a normal basis of F_{q^n} over F_q. Suppose that the dual basis B of N is generated by $\beta=a+b\alpha$ for some $a\in F_q$ and $b\in F_q^*$. Denote $T_\alpha=(t_{i,j})$ and $H_\beta=(h_{i,j})$ to be the multiplication tables of N and B, respectively. Then for any $i,j=0,\cdots,n-1$,

$$h_{i,j}=\begin{cases}a+bt_{i,0}, j=0,\\ -a+bt_{0,j}, i=0, j=1,\cdots,n-1,\\ a+bt_{i,i}, i=j=1,\cdots,n-1,\\ bt_{i,j}, i=1,\cdots,n-1, j\neq 0,i\end{cases}\qquad(3)$$

In 2011, Su and Liao[14] generalize the above result to the case $\beta=a+b\alpha_r$, where $a\in F_q$, $b\in F_q^*$ and $r\in\{1,\cdots,n-1\}$.

Proposition 2.6　[14] Let q be a power of the prime and let $N=\{\alpha_i=\alpha^{q^i} \mid i=0,1,\cdots,n-1\}$ be a normal basis of F_{q^n} over F_q. Suppose that the dual basis B of N is generated by $\beta=a+b\alpha_r$ for

some $a \in F_q$, $b \in F_q^*$. and $r \in \{1,\cdots,n-1\}$. Denote $T_\alpha = (t_{i,j})$ and $H_\beta = (h_{i,j})$ to be the multiplication tables of N and B, respectively. Then for any $i,j = 0,\cdots,n-1$,

$$h_{i,j} = \begin{cases} 2a + bt_{0,0}, i = j = 0, \\ bt_{0,j}, i = 0, j = 1,\cdots,n-1, \\ bt_{r,j}, i = r, j = 0, r, \\ -a + bt_{r,j}, i = r, j \neq 0, r, \\ a + bt_{i,j}, i \neq r, 0, j = 0, i, \\ bt_{i,j}, i \neq r, 0, j \neq 0, i \end{cases} \quad (4)$$

In the present paper, by Propositions 2.4~2.6, we obtain the upper and lower bounds for the complexities of class of the type $(n,k)(k \geqslant 3)$ Gauss normal bases, and determine the explicit complexity of the dual basis for the type $(n,k)(k = 1,2)$ Gauss normal bases over finite fields, which is an elementary proof for Theorem 2.2 given by Wan and Zhou[15]. In fact we prove the following main results.

Theorem 2.7 Let q be a power of the prime p, $3 \leqslant k \leqslant n$ and B be the dual basis of the type (n,k) Gauss normal basis $N = \{\alpha = \alpha_0,\cdots,\alpha_{n-1}\}$ of F_{q^n} over F_q. Suppose that the set $S_{i,j}(1 \leqslant i,j \leqslant k-1, i+j \leqslant k-1)$ defined in Proposition 2.4 are disjoint to each others. Then the complexity C_B for the dual basis$B$ of N is given as follows.

(1) For the case $k \equiv 0(\mathrm{mod}2)$,

$$C_B = c_0 + \frac{(k-2)^2}{2}c_m + (n-1-\frac{(k-2)^2}{2})c,$$

where

$$c_0 \in \{\frac{k}{2}, \frac{k}{2} \pm 1\}, c_m \in \{k-3,k-2,k-1,k\},$$

$$c \in \{k-2,k,k+1,k+2\}.$$

Hence

$$n(k-2) - \frac{k^2-3k+1}{2} \leqslant C_B \leqslant n(k+2) - 5 + \frac{7}{2}k - k^2.$$

(2) For the case $k \equiv 1(\mathrm{mod}2)$,

$$C_B = c_0 + c_{\frac{n}{2}} + \frac{(k-1)(k-3)}{2}c_m + (n-2-\frac{(k-1)(k-3)}{2})c,$$

where

$$c_0 \in \{1, \frac{k \pm 1}{2}, \frac{k+3}{2}\}, c_{\frac{n}{2}} \in \{k-3, k \pm 1, k\},$$

and

$$c_m \in \{k-4,k-3,k-2,k \pm 1,k\},$$

$$c \in \{k \pm 2,k,k+1\}.$$

Hence

$$n(k-2) - k^2 + 3k - 1 \leqslant C_B \leqslant n(k+2) - 5 - \frac{k(k-3)}{2}.$$

Corollary 2.8[15] Let B be the dual basis of the type $(n,1)$ Gauss normal basis $N = \{\alpha = \alpha_0, \cdots, \alpha_{n-1}\}$ of F_{q^n} over F_q. Then the complexity for the dual basis B of N

$$C_B = \begin{cases} 3n-3, 2 \mid q, \\ 3n-2, \text{otherwise}. \end{cases}$$

Corollary 2.9 Let B be the dual basis of the type $(n,2)$ Gauss normal basis $N = \{\alpha = \alpha_0,\cdots, \alpha_{n-1}\}$ of F_{q^n} over F_q. Then the complexity for the dual basis B of N is equal

$$C_B = \begin{cases} 2n-1, 2 \mid q, \\ 3n-2, \text{otherwise}. \end{cases}$$

3 The proofs of main results

To prove our main results, the following lemmas are very important.

Lemma 3.1[13] Let q be a power of the prime p, and let $T = (t_{i,j})$ be the multiplication table of the type $(n,k)(k \geqslant 3)$ Gauss normal basis $N = \{\alpha = \alpha_0,\cdots,\alpha_{n-1}\}$ of F_{q^n} over F_q. Suppose that $S_{i,j}(1 \leqslant i,j \leqslant k-1, i+j \leqslant k-1)$ defined in Proposition 2.3 are disjoint to each others.

(1) For the case $k \equiv 0(\mathrm{mod}2)$.

(i) The first row of the multiplication table T_α has exactly $\frac{k}{2} - 1$ entries equal to $2-k$, only one another entry equal to $1-k$, and the other $n - \frac{k}{2}$ entries equal to $-k$.

(ii) There are exactly $l = \frac{(k-2)^2}{2}$ subsets $S_{i_m,j_m} \subseteq \mathbf{Z}_r^* \setminus A_0 (1 \leqslant m \leqslant l)$, which means that for the i_m-th row, there are just $k-2$ nonzero entries equal to 1, only another nonzero entry equal to 2, and the remain $n-1-l$ entries are zero.

(iii) For the i-th row with $i \neq 0, i_1, \cdots, i_l (l = \frac{(k-2)^2}{2})$, there are exactly k nonzero terms

which equals to 1.

(2) For the case $k\equiv 1(\mathrm{mod}2)$,

(i) There are exactly $\frac{k-1}{2}$ entries $t_{0,j}=2$ and only one another nonzero entry, equal to 1.

(ii) For the $\frac{n}{2}$ -th row of T_α, there are exactly $k-1$ terms equal to $1-k$, and the other $n-k+1$ terms, each of them equal to $-k$.

(iii) For the i -th row with $i=1,\cdots,n-1$ and $i\neq\frac{n}{2}$, there are exactly $l=\frac{(k-1)(k-3)}{2}$ subsets $S_{i_m,j_m}\subseteq \mathbf{Z}_r^*\backslash A_0(1\leqslant m\leqslant l)$, which means that for the i_m -th row, there are just only one entry equal to 2 another $k-2$ nonzero entries equal to 1, and the remains $n-1-k$ entries equal 0.

(iv) For the i -th row with $i\neq 0,\frac{n}{2},i_l,\cdots,i_l(l=\frac{(k-1)(k-3)}{2})$, each of these rows has exactly k nonzero entries, equal to 1.

Lemma 3.2[11,12] (1) Suppose that N is the type $(n,1)$ Gauss normal basis and $T=(t_{i,j})$ is the multiplication table of N. Then

$$t_{\frac{n}{2},j}=-1,j=0,\cdots,n-1$$

and for any $i=0,\cdots,n-1$ and $i\neq\frac{n}{2}$,

$$t_{i,j}=\begin{cases}1, & q^j\equiv q^i+1(\mathrm{mod}\ n+1),\\ 0, & \text{otherwise.}\end{cases}$$

(2) Suppose that N is the type $(n,2)$ Gauss normal basis and $T=(t_{i,j})$ is the multiplication table of N.

(I) If $q\equiv\pm 2(\mathrm{mod}\ 2n+1)$, then

$$t_{0,j}=\begin{cases}-1, & j=1,\\ -2, & \text{otherwise.}\end{cases}$$

$$t_{n-1,j}=\begin{cases}1, & j=n-1 \text{ or } q^j\equiv\pm(n-1)(\mathrm{mod}2n+1),\\ 0, & \text{otherwise.}\end{cases}$$

and for any $i=1,\cdots,n-2$,

$$t_{i,j}=\begin{cases}1, & j=i \text{ or } q^j\equiv\pm(q^i-2)(\mathrm{mod}2n+1),\\ 0, & \text{otherwise.}\end{cases}$$

(II) If $q\neq\pm 2(\mathrm{mod}2n+1)$. Set $q^r\equiv\pm n(\mathrm{mod}2n+1)$ then $r\neq 0,n-1$,

$$t_{0,j}=\begin{cases}-1, & q^j\equiv\pm 2(\mathrm{mod}2n+1),\\ -2, & \text{otherwise.}\end{cases}$$

$$t_{r,j}=\begin{cases}1, & j=i \text{ or } q^j\equiv\pm(n-1)(\mathrm{mod}2n+1),\\ 0, & \text{otherwise,}\end{cases}$$

and for any $i=1,\cdots,n-1,i\neq r$,

$$t_{i,j}=\begin{cases}1, & j=i \text{ or } q^j\equiv\pm(q^i-2)(\mathrm{mod}2n+1),\\ 0, & \text{otherwise.}\end{cases}$$

(III) The complexity of N

$$C_N=\begin{cases}2n-1, & q\equiv 0(\mathrm{mod}2),\\ 3n-2, & \text{otherwise.}\end{cases}$$

Proof for Theorem 2.7 Suppose that $T_\alpha=(t_{i,j})$ and $H_\beta=(h_{i,j})$ are the multiplication tables of N and its dual basis B, respectively. If $p\mid k$, by Proposition 2.4 we have $B=\frac{1}{kn+1}N$ and so $C_B=C_N$. Without loose of the generality, we can assume that $\gcd(p,k)=1$.

(1) For the case $k\equiv 0(\mathrm{mod}2)$. Then p is an odd prime and so $\gcd(p,2k)=1$. By the formulas (2),(3) we have

$$\begin{aligned}h_{0,0}&=\frac{-k}{kn+1}+\frac{1}{kn+1}t_{0,0},\\ h_{0,j}&=\frac{k}{kn+1}+\frac{1}{kn+1}t_{0,j}(j=1,\cdots,n-1)\end{aligned}\tag{5}$$

and for any $i=1,\cdots,n-1$,

$$\begin{aligned}h_{i,0}&=\frac{-k}{kn+1}+\frac{1}{kn+1}t_{i,0},\\ h_{i,i}&=\frac{-k}{kn+1}+\frac{1}{kn+1}t_{i,i},\\ h_{i,j}&=\frac{1}{kn+1}t_{i,j}(j\neq 0,i)\end{aligned}\tag{6}$$

A. We first consider the number c_0 of nonzero elements in the first row of H_β. From (1) of Lemma 3.1, there has exactly $\frac{k}{2}-1$ entries $t_{0,j}=2-k$, only one another $t_{0,j}=1-k$, and the others $n-\frac{k}{2}$ entries $t_{0,j}=-k$. Therefore from (5), there are three cases as follows.

Case 1. If $t_{0,0}=2-k$. Then $h_{0,0}=\frac{2-2k}{kn+1}$, and for any $j=1,\cdots,n-1$, there are exactly $\frac{k}{2}-2$ entries $h_{0,j}=\frac{k}{kn+1}+\frac{2-k}{kn+1}=\frac{2}{kn+1}\neq 0$ for

$\gcd(p,2k)=1$, only one another $h_{0,j}=\frac{k}{kn+1}+\frac{1-k}{kn+1}=\frac{1}{kn+1}(\neq 0)$, and the remains $n-\frac{k}{2}$ elements $h_{0,j}=\frac{k}{kn+1}+\frac{-k}{kn+1}=0$. Hence the number of nonzero elements in the first row of the matrix H_β

$$c_0=\begin{cases}\frac{k}{2}-1, & p\mid k-1,\\ \frac{k}{2}, & \text{otherwise}\end{cases} \tag{7}$$

Case 2. If $t_{0,0}=1-k$. Then $h_{0,0}=\frac{1-2k}{kn+1}$, and for any $j=1,\cdots,n-1$, there are exactly $\frac{k}{2}-1$ entries $h_{0,j}=\frac{2}{kn+1}\neq 0$ for $\gcd(p,2k)=1$, and the remains $n-\frac{k}{2}$ elements $h_{0,j}=0$. Hence the number of nonzero elements in the first row of the matrix H_β

$$c_0=\begin{cases}\frac{k}{2}-1, & p\mid 2k-1,\\ \frac{k}{2}, & \text{otherwise}\end{cases} \tag{8}$$

Case 3. If $t_{0,0}=-k$. Then $h_{0,0}=\frac{-2k}{kn+1}\neq 0$ since $\gcd(p,2k)=1$. And for any $j=1,\cdots,n-1$, there are exactly $\frac{k}{2}-1$ entries $h_{0,j}=\frac{2}{kn+1}\neq 0$, and only one another $h_{0,j}=\frac{1}{kn+1}(\neq 0)$, the remains $n-\frac{k}{2}-1$ entries $h_{0,j}=0$. Hence the number of nonzero elements in the first row of the matrix H_β

$$c_0=\frac{k}{2}+1 \tag{9}$$

From Lemma 3.1 and (5),(6), in the same way we can get the nonzero elements in the $i(i\neq 0)$-th rows of H. The details is left to the appendix.

Thus we complete the proof of (2).

Proof for Corollary 2.8.

(1) For the type $(n,1)$ Gauss normal basis N of F_{q^n} over F_q. Note that for any $i=0,\cdots,n-1$, $q^i\neq q^i+1(\mathrm{mod}\,n+1)$ and $q^0\neq q^0+1(\mathrm{mod}\,n+1)$. Hence by (1) of Lemma 3.2 we have $t_{i,i}=t_{i,0}=0$. Thus from (11), we can get $h_{0,0}=\frac{-2}{n+1}$ and for any $j=1,\cdots,n-1$,

$$h_{0,j}=\begin{cases}\frac{1}{n+1}(\neq 0), & q^j\equiv q^0+1=2(\mathrm{mod}\,n+1),\\ 0, & \text{otherwise.}\end{cases}$$

Therefore the number of nonzero elements in the first row of H_β is 1 or 2 depending on p is even or odd, respectively. Now from (1) of Lemma 3.2 and (12), we have

$$h_{\frac{n}{2},0}=h_{\frac{n}{2},\frac{n}{2}}=\frac{-1}{n+1}\neq 0, h_{\frac{n}{2},j}=0(j\neq 0,\frac{n}{2})$$

which means that the number of nonzero elements in the $\frac{n}{2}$-th row of H_β is equal 2. Finally, from $t_{i,i}=t_{i,0}=0(0\leqslant i\leqslant n-1)$, (1) of Lemma 3.2 and (13), we have

$$h_{i,0}=h_{i,i}=\frac{-1}{n+1}\neq 0,$$

and for any $j=0,\cdots,n-1, j\neq 0,i$,

$$h_{i,j}=\begin{cases}1, & q^j\equiv q^i+1=2(\mathrm{mod}\,n+1),\\ 0, & \text{otherwise.}\end{cases}$$

This means that the number of nonzero elements in the $i(\neq 0,\frac{n}{2})$-th row of H_β is equal 3.

From the above, the complexity of the dual basis of the type $(n,1)$ is equal to

$$C_B=3(n-2)+2+\begin{cases}1, & p=2,\\ 2, & \text{otherwise.}\end{cases}=\begin{cases}3n-3, & p=2,\\ 3n-2, & \text{otherwise.}\end{cases}$$

Thus we complete the proof of Corollary 2.8.

Proof for Corollary 2.9. By (2) of Lemma 3.2 and (1)-(2), in the same proof for Corollary 2.9, the result is immediate.

4 Conclusions and remarks

It is well known that normal bases, especially optimal normal bases, are widely used in applications of finite fields in areas such as coding theory, cryptography, signal processing, and so on (see [9] for instance). However, for many finite fields, there exist no optimal normal bases. For these finite fields, it is desirable to have normal

bases of low complexity. The well-known Gauss normal basis is just with lower complexity. Therefore to determine the multiplication table and complexity for Gauss normal bases and their dual bases is interesting in recent years.

Based on the closed relationship between the cyclotomic numbers and Gauss normal bases over finite fields, to determine the complexity of Gauss normal bases, it is sufficient to compute the corresponding cyclotomic numbers. With regret, untill now people can only determine some special cycloyomic numbers. Therefore to determine the explicit complexity for Gauss normal bases and their dual bases remains open.

In [13] and the present paper, when the sets $S_{i,j}$ defined in Proposition 2.4 are disjoint each others, we give the explicit formula for the complexity of Gauss normal bases and their dual bases over finite fields. Thus we solve the open problem partially. Although we cannot find some sufficient conditions for that our disjointness requirement is satisfied even if n is a prime, we show that Guass normal bases satisfying the requirement exists. For example, for the type $(n,k)(1\leqslant k\leqslant 6)$ Gauss normal bases and for $n\neq 4$ the type $(n,7)$ Gauss normal basis, the sets $S_{i,j}$ are disjoint to each others [13].

Appendix Now we consider the nonzero elements in the $i_1,\cdots,i_l(l=\frac{(k-2)^2}{2})$-th rows of H_β. From (1) of Lemma 3.1, for each $m=1,\cdots,l$, there are exactly $k-2$ nonzero entries $t_{i_m,j}=1$ only another nonzero $t_{i_m,j}=2$, and the remain $n-k+1$ entries $t_{i_m,j}=0$. Hence by (4) there are 8 cases as follows.

Case 1. If $t_{0,0}=t_{i_m,i_m}=1$. Then $h_{i_m,0}=h_{i_m,i_m}=\frac{-k+1}{kn+1}$ and there are exactly $k-4$ entries $h_{i_m,j}=\frac{1}{kn+1}(\neq 0)$, only one another $h_{i_m,j}=\frac{2}{kn+1}(\neq 0)$ for $\gcd(p,2k)=1$, the remains $n-k+1$ entries $h_{i_m,j}=0$. Hence the number of nonzero elements in the i_m-th row of H_β

$$c_{i_m}=\begin{cases}k-3, & p\mid k-1,\\ k-1, & \text{otherwise}\end{cases}\tag{10}$$

Case 2. If $t_{0,0}=1$ and $t_{i_m,i_m}=2$. Then $h_{i_m,o}=\frac{-k+1}{kn+1}$, $h_{i_m,i_m}=\frac{-k+2}{kn+1}$, and there are exactly $k-3$ entries $h_{i_m,j}=\frac{1}{kn+1}(\neq 0)$, the remains $n-k+1$ entries $h_{i_m,j}=0$. Hence the number of nonzero elements in the i_m-th row of H_β

$$c_{i_m}=\begin{cases}k-2, & p\mid (k-1)(k-2),\\ k-1, & \text{otherwise}\end{cases}\tag{11}$$

Case 3. If $t_{0,0}=1$ and $t_{i_m,i_m}=0$. Then $h_{i_m,0}=\frac{-k+1}{kn+1}$, $h_{i_m,i_m}=\frac{-k}{kn+1}\neq 0$ for $\gcd(p,2k)=1$, and there are exactly $k-3$ entries $h_{i_m,j}=\frac{1}{kn+1}(\neq 0)$, only one another $h_{i_m,j}=\frac{2}{kn+1}\neq 0$ for $\gcd(p,2k)=1$, and the remains $n-k$ entries $h_{i_m,j}=0$. Hence the number of nonzero elements in the i_m-th row of H_β

$$c_{i_m}=\begin{cases}k-1, & p\mid k-1,\\ k, & \text{otherwise}\end{cases}\tag{12}$$

Case 4. If $t_{0,0}=2$ and $t_{i_m,i_m}=1$. Then $h_{i_m,0}=\frac{-k+2}{kn+1}$, $h_{i_m,i_m}=\frac{-k+1}{kn+1}$ and there are exactly $k-3$ entries $h_{i_m,j}=\frac{1}{kn+1}(\neq 0)$, and the remains $n-k+1$ entries $h_{i_m,j}=0$. Hence the number of nonzero elements in the i_m-th row of H_β

$$c_{i_m}=\begin{cases}k-2, & p\mid (k-1)(k-2),\\ k-1, & \text{otherwise}\end{cases}\tag{13}$$

Case 5. If $t_{0,0}=2$ and $t_{i_m,i_m}=0$. Then $h_{i_m,0}=\frac{-k+2}{kn+1}$, $h_{i_m,i_m}=\frac{-k}{kn+1}\neq 0$ for $\gcd(p,2k)=1$, and there are exactly $k-2$ entries $h_{i_m,j}=\frac{1}{kn+1}(\neq 0)$, and the remains $n-k$ entries $h_{i_m,j}=0$. Note that $\gcd(p,2k)=1$, hence the number of nonzero elements in the i_m-th row of H_β

$$c_{i_m}=\begin{cases}k-1, & p\mid k-2,\\ k, & \text{otherwise}\end{cases}\tag{14}$$

Case 6. If $t_{0,0}=0$ and $t_{i_m,i_m}=1$. Then $h_{i_m,0}=\frac{-k}{kn+1}\neq 0$ for $\gcd(p,2k)=1$, $h_{i_m,i_m}=\frac{-k+1}{kn+1}$, and there are exactly $k-3$ entries $h_{i_m,j}=$

$\frac{1}{kn+1}(\neq 0)$, only one another $h_{i_m,j}=\frac{2}{kn+1}\neq 0$ for $\gcd(p,2k)=1$, and the remains $n-k$ entries $h_{i_m,j}=0$. Hence the number of nonzero elements in the i_m-th row of H_β

$$c_{i_m}=\begin{cases}k-1, & p\mid k-1,\\ k, & \text{otherwise}\end{cases} \tag{15}$$

Case 7. If $t_{0,0}=0$ and $t_{i_m,i_m}=2$. Then $h_{i_m,0}=\frac{-k}{kn+1}\neq 0$ for $\gcd(p,2k)=1$, $h_{i_m,i_m}=\frac{-k+2}{kn+1}$, and there are exactly $k-2$ entries $h_{i_m,j}=\frac{1}{kn+1}(\neq 0)$, and the remains $n-k$ entries $h_{i_m,j}=0$. Note that $\gcd(p,2k)=1$, hence the number of nonzero elements in the i_m-th row of H_β

$$c_{i_m}=\begin{cases}k-1, & p\mid k-2,\\ k, & \text{otherwise}\end{cases} \tag{16}$$

Case 8. If $t_{0,0}=t_{i_m,i_m}=0$. Then $h_{i_m,0}=h_{i_m,i_m}=\frac{-k}{kn+1}$, and there are exactly $k-2$ entries $h_{i_m,j}=\frac{1}{kn+1}(\neq 0)$, only one another $h_{i_m,j}=\frac{2}{kn+1}\neq 0$ for $\gcd(p,2k)=1$, and the remains $n-k-1$ entries $h_{i_m,j}=0$. Hence the number of nonzero elements in the i_m-th row of H_β

$$c_{i_m}=k+1 \tag{17}$$

C. Now we consider the nonzero elements in the $i(\neq 0,i_1,\cdots,i_l,l=\frac{(k-2)^2}{2})$-th rows of H_β. From (1) of Lemma 3.1, there are exactly k nonzero $t_{i,j}=1$, and the remain $n-k$ entries $t_{i,j}=0$. Hence by (2.2) there are 4 cases as follows.

Case 1. If $t_{i,0}=t_{i,i}=1$. Then $h_{i,0}=h_{i,i}=\frac{-k+1}{kn+1}$, and there are exactly $k-2$ entries $h_{i,j}=\frac{1}{kn+1}(\neq 0)$, and the remains $n-k$ entries $h_{i,j}=0$. Hence the number of nonzero elements in the i-th row of H_β

$$c_i=\begin{cases}k-2, & p\mid k-1,\\ k, & \text{otherwise}\end{cases} \tag{18}$$

Case 2. If $t_{i,0}=1$ and $t_{i,i}=0$ Then $h_{i,0}=\frac{-k+1}{kn+1}$, $h_{i,i}=\frac{-k}{kn+1}\neq 0$ for $\gcd(p,2k)=1$, and there are exactly $k-1$ entries $h_{i,j}=\frac{1}{kn+1}(\neq 0)$, and the remains $n-k-1$ entries $h_{i,j}=0$. Hence the number of nonzero elements in the i-th row of H_β

$$c_i=\begin{cases}k, & p\mid k-1,\\ k+1, & \text{otherwise}\end{cases} \tag{19}$$

Case 3. If $t_{i,0}=0$ and $t_{i,i}=1$ Then $h_{i,0}=\frac{-k}{kn+1}\neq 0$ for $\gcd(p,2k)=1$, $h_{i,i}=\frac{-k+1}{kn+1}$, and there are exactly $k-1$ entries $h_{i,j}=\frac{1}{kn+1}(\neq 0)$, and the remains $n-k-1$ entries $h_{i,j}=0$. Hence the number of nonzero elements in the i-th row of H_β

$$c_i=\begin{cases}k, & p\mid k-1,\\ k+1, & \text{otherwise}\end{cases} \tag{20}$$

Case 4. If $t_{i,0}=t_{i,i}=0$. Then $h_{i,0}=h_{i,i}=\frac{-k}{kn+1}\neq 0$ since $\gcd(p,k)=1$, and there are exactly k entries $h_{i,j}=\frac{1}{kn+1}(\neq 0)$, and the remains $n-k-2$ entries $h_{i,j}=0$. Hence the number of nonzero elements in the i-th row of H_β

$$c_i=k+2 \tag{21}$$

Now from the definition of the complexity, (7)~(9) and (10)~(21), we have

$$C_B=c_0+\frac{(k-2)^2}{2}c_{i_m}+(n-1-\frac{(k-2)^2}{2})c_i,$$

and so

$$n(k-2)-\frac{k^2-3k+1}{2}\leqslant C_B\leqslant n(k+2)-5+\frac{7}{2}k-k^2 \tag{22}$$

Thus we complete the proof of (1).

(2) For the case $k\equiv 1(\mathrm{mod}2)$. From (2) and (4) we have

$$\begin{cases}h_{0,0}=\frac{-2k}{kn+1}+\frac{1}{kn+1}t_{0,0},\\ h_{0,j}=\frac{1}{kn+1}t_{0,j}(j=1,\cdots,n-1),\end{cases} \tag{23}$$

$$\begin{cases}h_{\frac{n}{2},j}=\frac{1}{kn+1}t_{\frac{n}{2},j}(j=0,\frac{n}{2}),\\ h_{\frac{n}{2},j}=\frac{k}{kn+1}+\frac{1}{kn+1}t_{\frac{n}{2},j}(j\neq 0,\frac{n}{2})\end{cases} \tag{24}$$

and for any $i=1,\cdots,n-1,i\neq\frac{n}{2}$,

$$\begin{cases} h_{i,0} = \dfrac{-k}{kn+1} + \dfrac{1}{kn+1}t_{i,0}, \\ h_{i,i} = \dfrac{-k}{kn+1} + \dfrac{1}{kn+1}t_{i,i}, \\ h_{i,j} = \dfrac{1}{kn+1}t_{i,j}(j \neq 0,i) \end{cases} \tag{25}$$

A. We first consider the number c_0 of nonzero elements in the first row of H_β.

From (2) of Lemma 3.1, there are exactly $\dfrac{k-1}{2}$ entries $t_{0,j}=2$, only one another $t_{0,j}=1$, and the others $n-1-\dfrac{k-1}{2}$ entries $t_{0,j}=0$. Therefore from (23), there are three cases as follows.

Case 1. If $t_{0,0}=2$, then $h_{0,0}=\dfrac{-2k+2}{kn+1}$. And for any $j=1,\cdots,n-1$, there are exactly $\dfrac{k-3}{2}$ entries $h_{0,j}=\dfrac{2}{kn+1}$, only one another $h_{0,j}=\dfrac{1}{kn+1}(\neq 0)$, and the remain $n-1-\dfrac{k-1}{2}$ entries $h_{0,j}=0$. Therefore the number of nonzero elements in the first row of H_β

$$c_0 = \begin{cases} 1, & p=2, \\ \dfrac{k-1}{2}, & p\neq 2, p \mid k-1, \\ \dfrac{k+1}{2}, & \text{otherwise} \end{cases} \tag{26}$$

Case 2. If $t_{0,0}=1$, then $h_{0,0}=\dfrac{-2k+1}{kn+1}$. Hence there are exactly $\dfrac{k-1}{2}$ entries $h_{0,j}=\dfrac{2}{kn+1}$, and the remain $n-1-\dfrac{k-1}{2}$ entries $h_{0,j}=0$. Therefore the number of nonzero elements in the first row of H_β

$$c_0 = \begin{cases} 1, & p=2, \\ \dfrac{k-1}{2}, & p\neq 2, p \mid 2k-1, \\ \dfrac{k+1}{2}, & \text{otherwise} \end{cases} \tag{27}$$

Case 3. If $t_{0,0}=0$, then $h_{0,0}=\dfrac{-2k}{kn+1}$. Hence for any $j=1,\cdots,n-1$, there are exactly $\dfrac{k-1}{2}$ entries $h_{0,j}=\dfrac{2}{kn+1}$, only one another $h_{0,j}=\dfrac{1}{kn+1}(\neq 0)$, and the remain $n-2-\dfrac{k-1}{2}$ entries $h_{0,j}=0$. Note that $\gcd(p,k)=1$, therefore the number of nonzero elements in the first row of H_β

$$c_0 = \begin{cases} 1, & p=2, \\ \dfrac{k+3}{2}, & \text{otherwise} \end{cases} \tag{28}$$

B. Now we consider the nonzero elements in the $\dfrac{n}{2}$-th rows of H_β. From (2) of Lemma 3.1, there are exactly just $k-1$ nonzero $t_{\frac{n}{2},j}=1-k$, and the remain $n-k+1$ entries $t_{\frac{n}{2},j}=-k$. Hence by (A.15) there are 4 cases as follows.

Case 1. If $t_{\frac{n}{2},0}=t_{\frac{n}{2},\frac{n}{2}}=1-k$, then $h_{\frac{n}{2},0}=h_{\frac{n}{2},\frac{n}{2}}=\dfrac{1-k}{kn+1}$. Hence for any $j\neq 1,\dfrac{n}{2}$, there are exactly $k-3$ entries $h_{\frac{n}{2},j}=\dfrac{1}{kn+1}(\neq 0)$, and the remains $n-k+1$ entries $h_{\frac{n}{2},j}=0$. Therefore the number of nonzero elements in the $\dfrac{n}{2}$-th row of H_β

$$c_{\frac{n}{2}} = \begin{cases} k-3, & p \mid k-1, \\ k-1, & \text{otherwise} \end{cases} \tag{29}$$

Case 2. If $t_{\frac{n}{2},0}=1-k$ and $t_{\frac{n}{2},\frac{n}{2}}=-k$, then $h_{\frac{n}{2},0}=\dfrac{1-k}{kn+1}$ and $h_{\frac{n}{2},\frac{n}{2}}=\dfrac{-k}{kn+1}(\neq 0)$ since $\gcd(p,k)=1$. Hence for any $j\neq 1,\dfrac{n}{2}$, there are exactly $k-2$ entries $h_{\frac{n}{2},j}=\dfrac{1}{kn+1}(\neq 0)$, and the remains $n-k$ entries $h_{\frac{n}{2},j}=0$. Therefore the number of nonzero elements in the $\dfrac{n}{2}$-th row of H_β

$$c_{\frac{n}{2}} = \begin{cases} k-1, & p \mid k-1, \\ k, & \text{otherwise} \end{cases} \tag{30}$$

Case 3. If $t_{\frac{n}{2},0}=-k$ and $t_{\frac{n}{2},\frac{n}{2}}=1-k$, then $h_{\frac{n}{2},0}=\dfrac{-k}{kn+1}\neq 0$ for $\gcd(p,k)=1$, $h_{\frac{n}{2},\frac{n}{2}}=\dfrac{1-k}{kn+1}$. Hence for any $j\neq 1,\dfrac{n}{2}$, there are exactly $k-2$ entries $h_{\frac{n}{2},j}=\dfrac{1}{kn+1}(\neq 0)$, and the remains $n-k$ entries $h_{\frac{n}{2},j}=0$. Therefore the number of nonzero elements in the $\dfrac{n}{2}$-th row of H_β

$$c_{\frac{n}{2}} = \begin{cases} k-1, & p \mid k-1, \\ k, & \text{otherwise} \end{cases} \tag{31}$$

Case 4. If $t_{\frac{n}{2},0}=t_{\frac{n}{2},\frac{n}{2}}=-k$, then $h_{\frac{n}{2},0}=h_{\frac{n}{2},\frac{n}{2}}=\dfrac{-k}{kn+1}\neq 0$ since $\gcd(p,k)=1$. Hence

for any $j \neq 1, \frac{n}{2}$, there are exactly $k-1$ entries $h_{\frac{n}{2},j} = \frac{1}{kn+1}(\neq 0)$, and the remains $n-k-1$ entries $h_{\frac{n}{2},j} = 0$. Therefore the number of nonzero elements in the $\frac{n}{2}$-th row of H_β

$$c_{\frac{n}{2}} = k+1 \tag{32}$$

C. Now we consider the nonzero elements in the $i(i \neq 0, \frac{n}{2}, i = i_1, \cdots, i_1, l = \frac{(k-1)(k-3)}{2})$-th rows of H_β.

From (2) of Lemma 3.1, for any $m = 1, \cdots, l$, in the i_m-th row there are exactly $k-2$ nonzero $t_{i_m,j} = 1$, only one another entries $t_{i_m,j} = 2$, and the remain $n-k+1$ entries $t_{i_m,j} = 0$. Hence by (A.16) there are 8 cases as follows.

Case 1. If $t_{i_m,0} = 2$ and $t_{i_m,i_m} = 1$, then $h_{i_m,0} = \frac{-k+2}{kn+1}$ and $h_{i_m,i_m} = \frac{-k+1}{kn+1}$. Hence for any $j \neq 0, i_m$, there are exactly $k-3$ entries $h_{i_m,j} = \frac{1}{kn+1}(\neq 0)$, and the remains $n-k+1$ entries $h_{i_m,j} = 0$. Therefore the number of nonzero elements in the i_m-th row of H_β

$$c_{i_m} = \begin{cases} k-2, & p \mid (k-1)(k-2), \\ k-1, & \text{otherwise} \end{cases} \tag{33}$$

Case 2. If $t_{i_m,0} = 2$ and $t_{i_m,i_m} = 0$, then $h_{i_m,0} = \frac{-k+2}{kn+1}$ and $h_{i_m,i_m} = \frac{-k}{kn+1} \neq 0$ for $\gcd(p,k) = 1$. Hence for any $j \neq 0, i_m$, there are exactly $k-2$ entries $h_{i_m,j} = \frac{1}{kn+1}(\neq 0)$, and the remains $n-k$ entries $h_{i_m,j} = 0$. Therefore the number of nonzero elements in the i_m-th row of H_β

$$c_{i_m} = \begin{cases} k-1, & p \mid k-2, \\ k, & \text{otherwise} \end{cases} \tag{34}$$

Case 3. If $t_{i_m,0} = 1$ and $t_{i_m,i_m} = 2$, then $h_{i_m,0} = \frac{-k+1}{kn+1}$ and $h_{i_m,i_m} = \frac{-k+2}{kn+1}$, Hence for any $j \neq 0, i_m$, there are exactly $k-3$ entries $h_{i_m,j} = \frac{1}{kn+1}(\neq 0)$, and the remains $n-k+1$ entries $h_{i_m,j} = 0$. Therefore the number of nonzero elements in the i_m-th row of H_β

$$c_{i_m} = \begin{cases} k-2, & p \mid (k-2)(k-1), \\ k-1, & \text{otherwise} \end{cases} \tag{35}$$

Case 4. If $t_{i_m,0} = t_{i_m,i_m} = 1$, then $h_{i_m,0} = h_{i_m,i_m} = \frac{-k+1}{kn+1}$. Hence for any $j \neq 0, i_m$, there are exactly $k-4$ entries $h_{i_m,j} = \frac{1}{kn+1}(\neq 0)$, only one another $h_{i_m,j} = \frac{2}{kn+1}$, and the remains $n-k+1$ entries $h_{i_m,j} = 0$. Therefore the number of nonzero elements in the i_m-th row of H_β

$$c_{i_m} = \begin{cases} k-4, & p = 2, \\ k-3, & \\ k-1, & \\ \text{otherwise} \end{cases} \tag{36}$$

Case 5. If $t_{i_m,0} = 1$, $t_{i_m,i_m} = 0$, then $h_{i_m,0} = \frac{-k+1}{kn+1}$, $h_{i_m,i_m} = \frac{-k}{kn+1} \neq 0$ since $\gcd(p,k) = 1$. Hence for any $j \neq 0, i_m$, there are exactly $k-3$ entries $h_{i_m,j} = \frac{1}{kn+1}(\neq 0)$, only one another $h_{i_m,j} = \frac{2}{kn+1}$, and the remains $n-k$ entries $h_{\frac{n}{2},j} = 0$. Therefore the number of nonzero elements in the i_m-th row of H_β

$$c_{i_m} = \begin{cases} k-2, & p = 2, \\ k-1, & \\ k, & \\ \text{otherwise} \end{cases} \tag{37}$$

Case 6. If $t_{i_m,0} = 0$ and $t_{i_m,i_m} = 2$, then $h_{i_m,0} = \frac{-k}{kn+1} \neq 0$ since $\gcd(p,k) = 1$, and $h_{i_m,i_m} = \frac{-k+2}{kn+1}$. Hence for any $j \neq 0, i_m$, there are exactly $k-2$ entries $h_{i_m,j} = \frac{1}{kn+1}(\neq 0)$, and the remains $n-k$ entries $h_{i_m,j} = 0$. Therefore the number of nonzero elements in the i_m-th row of H_β

$$c_{i_m} = \begin{cases} k-1, & p \mid k-2, \\ k, & \text{otherwise} \end{cases} \tag{38}$$

Case 7. If $t_{i_m,0} = 0$ and $t_{i_m,i_m} = 1$, then $h_{i_m,0} = \frac{-k}{kn+1} \neq 0$ since $\gcd(p,k) = 1$, and $h_{i_m,i_m} = \frac{-k+1}{kn+1}$. Hence for any $j \neq 0, i_m$, there are exactly $k-3$ entries $h_{i_m,j} = \frac{1}{kn+1}(\neq 0)$, only one another $h_{i_m,j} = \frac{2}{kn+1}$, and the remains $n-k$ entries

$h_{i_m,j}=0$. Therefore the number of nonzero elements in the i_m-th row of H_β

$$c_{i_m}=\begin{cases}k-2, & p=2,\\ k-1, & \\ k, & \\ \text{otherwise}\end{cases} \tag{39}$$

Case 8. If $t_{i_m,0}=t_{i_m,i_m}=0$, then $h_{i_m,0}=h_{i_m,0}=\frac{-k}{kn+1}(\neq 0)$ since $\gcd(p,k)=1$. Hence for any $j\neq 0,i_m$, there are exactly $k-2$ entries $h_{i_m,j}=\frac{1}{kn+1}(\neq 0)$, only one another $h_{i_m,j}=\frac{2}{kn+1}$, and the remains $n-k-1$ entries $h_{i_m,j}=0$. Therefore the number of nonzero elements in the i_m-th row of H_β

$$c_{i_m}=\begin{cases}k, & p=2,\\ k+1, & \text{otherwise}\end{cases} \tag{40}$$

D. Now we consider the nonzero elements in the $i(i\neq 0,\frac{n}{2},i=i_1,\cdots,i_l,l=\frac{(k-1)(k-3)}{2})$-th rows of H_β. From (2) of Lemma 3.1, there are exactly k nonzero $t_{i,j}=1$, and the remain $n-k$ entries $t_{i,j}=0$. Hence by (A.16) there are 4 cases as follows.

Case 1. If $t_{i,0}=t_{i,i}=1$, then $h_{i,0}=h_{i,i}=\frac{-k+1}{kn+1}$. Hence for any $j\neq 0,i$, there are exactly $k-2$ entries $h_{i,j}=\frac{1}{kn+1}(\neq 0)$, and the remain $n-k$ entries $h_{i,j}=0$. Therefore the number of nonzero elements in the i-th row of H_β

$$c_i=\begin{cases}k-2, & p\mid k-1,\\ k, & \text{otherwise}\end{cases} \tag{41}$$

Case 2. If $t_{i,0}=1$ and $t_{i,i}=0$, then $h_{i,0}=\frac{-k+1}{kn+1}$ and $h_{i,i}=\frac{-k}{kn+1}\neq 0$ since $\gcd(p,k)=1$. Hence for any $j\neq 0,i$, there are exactly $k-1$ entries $h_{i,j}=\frac{1}{kn+1}(\neq 0)$, and the remain $n-k-1$ entries $h_{i,j}=0$. Therefore the number of nonzero elements in the i-th row of H_β

$$c_i=\begin{cases}k, & p\mid k-1,\\ k+1, & \text{otherwise}\end{cases} \tag{42}$$

Case 3. If $t_{i,0}=0$ and $t_{i,i}=1$, then $h_{i,0}=\frac{-k}{kn+1}\neq 0$ since $\gcd(p,k)=1$, and $h_{i,i}=\frac{-k+1}{kn+1}$. Hence for any $j\neq 0,i$, there are exactly $k-1$ entries $h_{i,j}=\frac{1}{kn+1}(\neq 0)$, and the remain $n-k-1$ entries $h_{i,j}=0$. Therefore the number of nonzero elements in the i-th row of H_β

$$c_i=\begin{cases}k, & p\mid k-1,\\ k+1, & \text{otherwise}\end{cases} \tag{43}$$

Case 4. If $t_{i,0}=t_{i,i}=0$, then $h_{i,0}=h_{i,i}=\frac{-k}{kn+1}\neq 0$ since $\gcd(p,k)=1$. Hence for any $j\neq 0,i$, there are exactly k entries $h_{i,j}=\frac{1}{kn+1}(\neq 0)$, and the remain $n-k-2$ entries $h_{i,j}=0$. Therefore the number of nonzero elements in the i-th row of H_β

$$c_i=k+2 \tag{44}$$

Now by (26～44) and

$$C_B=c_0+c_{\frac{n}{2}}+\frac{(k-1)(k-3)}{2}c_{i_m}+(n-2-\frac{(k-1)(k-3)}{2})c_i$$

we can get

$$n(k-2)-k^2+3k-1\leqslant C_B\leqslant n(k+2)-5-\frac{k(k-3)}{2}$$

Thus we complete the proof for Theorem 2.7.

References:

[1] Mullin R C, Onyszchuk I M, Vanstone S A, Wilson R M. Optimal normal bases in GF_{q^n} [J]. Discrete Appl Math, 1989, 22: 149.

[2] Gao S H, Lenstra H W. Optimal normal bases[J]. Des Codes Cryptogr, 1992, 2: 315.

[3] Dahab R, *et al*. Software multiplication using Gaussian normal bases [J]. IEEE Trans Comput, 2006, 55: 974.

[4] Gao S H, Gathen J von zur, Panario D, *et al*. Algorithms for exponentiation in finite fields [J]. J Symbol Comput, 2000, 29: 879.

[5] Gathen J von zur, M. Nocker. Fast arithmetic with general Gauss periods [J]. Theor Comput Sci, 2004, 315: 419.

[6] Ash D W, Blake I F, S. A. Vanstone. Low complexity normal bases [J]. Discrete Appl Math, 1989, 25: 191.

[7] Wassermann A, Konstruktion von Normalbasen[J].

Bayreuther Mathematische Scriften. 1990, 31: 155.

[8] Christopolou M, Garefalakis T, Panario D, *et al*. Gauss periods as constructions of low complexity normal bases [J]. Des Codes Cryptogr, 2012, 62: 43.

[9] Cohen H, Frey G. Handbook of elliptic and hyperelliptic curve cryptography [J]. Discrete Math Appl, 2005, 458: 280.

[10] Liao Q Y. On some special normal bases over finite fields[J]. J Sichuan Univ: Nat Sci Ed(四川大学学报: 自然科学版), 2005, 42(1): 41.

[11] Liao Q Y, Sun Q. On multiplication tables of optimal normal bases over finite fields[J]. Acta Math Sinica: Chin Ser, 2005, 48(5): 947.

[12] Liao Q Y. The Gaussian normal basis and its trace basis over finite fields[J]. J Number Theory, 2012, 132(7): 1507.

[13] Liao Q Y, Hu X L. The explicit formula for the complexity of a class of Gauss period normal bases over finite fields[J]. Acta Mathe maticasinica Sinica: Chin Ser, 2014, 57(5): 863.

[14] Su D D, Liao Q Y. On extensions for a special dual normal bases over finite fields[J]. J Sichuan Univ: Nat Sci Ed(四川大学学报: 自然科学版) 2011, 48(1): 27.

[15] Wan Z X, Zhou K. On the complexity of the dual bases of a type I optimal normal bases[J]. Finite Fields and Their Applications, 2007, 13(4): 411.