doi: 103969/j. issn. 0490-6756. 2016. 01. 002

有限域上的(4,7)型高斯正规基及其对偶基和迹基

魏　杰，李雪连，廖群英
(四川师范大学数学与软件科学学院，成都 610066)

摘　要：设 q 为素数 p 的 n 次方幂，n 为正整数. 最近廖和胡通过刻画有限域上分圆数的性质给出了有限域上一类高斯正规基复杂度的准确计算公式，并证明了有限域 F_{q^n} 在 F_q 上的 7-型高斯正规基满足所给条件当且仅当 $n \neq 4$. 本文完善了上述结果，确定了 F_{q^4} 在 F_q 上的 7-型高斯正规基及其对偶基和迹基的准确复杂度.

关键词：有限域；高斯正规基；对偶基；迹正规基度
中图分类号：O156.2　　**文献标识码**：A　　**文章编号**：0490-6756(2016)01-0007-06

Dual and trace bases of the type (4,7) Gauss period normal basis over finite fields

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

Abstract: Let q be a power of the prime p and F_q be the finite field with q elements. Recently, by characterizing some properties of cyclotomic numbers, Liao and Li obtained the explicit formula for the complexity of a class of Gauss period normal bases over finite fields. Furthermore, they showed that the type 7 -Gauss period normal basis of F_{q^n} over F_q is just the desired basis except for $n = 4$, her n is an integer. In this paper, we complete the above results and obtain the explicit formula for the complexity of type 7 -Gauss period basis of F_{q^4} over F_q.

Key words: Finite field; Gauss period normal basis; Dual basis; Trace normal basis
(2010 MSC 12E10, 12E30, 11T99)

1　引　言

设 q 为素数 p 的 n 次方幂，n 是正整数，F_{q^n} 是有限域 F_q 的 n 次扩张 ($n \geqslant 2$)，因而也是 F_q 上的 n 维向量空间，从而可知 F_{q^n} 在 F_q 上有许多基. 在众多基中，特别重要的是两类基：一类形如 $\{1,\beta,\cdots,\beta^{n-1}\}$ 的基；叫做多项式基. 一类形如 $\{\alpha,\alpha^q,\cdots,\alpha^{q^{n-1}}\}$ 的基叫做正规基，其中 $\alpha,\beta \in F_{q^n}$. 由于正规基形式特殊性，其应用也最为广泛. 正规基的优越性质被应用于硬件和软件中，从而快速实现大规模的有限域运算. 若

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

为 F_{q^n} 在 F_q 上的一组正规基，则称 α 为 F_{q^n} 在 F_q 上的一个正规元. 进而令

$$\alpha \cdot \alpha^{q^i} = \sum_{j=0}^{n-1} t_{i,j}\alpha^{q^j}, 0 \leqslant i \leqslant n-1,$$

则 $T = (t_{i,j})_{n\times n}$ 为 N 的乘法表，T 中非零元素的个数称为 N 的复杂度，记为 C_N. 由于 $T = (t_{i,j})_{n\times n}$ 中的非零元越少，F_{q^n} 中乘法计算的计算量也就越小，所以寻找低复杂度的正规基是一个重要课题.

收稿日期：2015-4-22
基金项目：国家自然科学基金(11401408)；四川省教育厅重点项目(14ZA0034)；四川师范学院科研重点培育项目(13ZDL06)
作者简介：魏杰(1991－)，硕士生，主要研究方向为编码和密码学理论.
通信作者：廖群英. E-mail: qunyingliao@sicnu.edu.cn

Mullin [1] 等人证明了 $C_N \geqslant 2n-1$，且当 $C_N = 2n-1$ 时，称 N 为最优正规基，进而给出了两类最优正规基的构造定理，分别为Ⅰ型最优正规基和Ⅱ型最优正规基，并猜想最优正规基只有这两类. 随后，Gao 和 Lenstra[2] 证明了这个猜想. 从而寻找次优的正规基也成了很重要的课题. 1990 年，Wassermann[3] 把最优正规基推广到了高斯正规基，而这正是一类低复杂度的正规基.

由 k- 型高斯正规基的构造定理[3]，设 q 为素数 p 的方幂，k 和 n 是正整数，满足 $kn+1$ 为素数且 $(kn+1,p)=1$. 假定 $\delta \in F_{q^n}$ 是 $kn+1$ 次本原单位根，s 是 q 模 $kn+1$ 的次数. 若 $(\frac{kn}{s},n)=1$，l 是 Z_{kn+1} 中的 k 次本原单位根，则

$$\alpha = \sum_{j=0}^{k-1} \delta^{l^j}$$

生成 F_{q^n} 在 F_q 上的正规基 N，且其复杂度满足

$$C_N \leqslant \begin{cases} (k+1)n-k, & (p,k)=1, \\ kn-1, & \text{其他.} \end{cases}$$

称 N 为 F_{q^n} 在 F_q 上的 k- 型高斯正规基.

注 1 当 $k=1$ 时，1- 型高斯正规基即是Ⅰ型最优正规基，当 $q=k=2$ 时，2- 型高斯正规基即是Ⅱ型最优正规基.

另一方面，在有限域的众多基中，对偶基也是一个很重要的概念. 对于 F_{q^n} 在 F_q 上的任意两组基：$N=\{\alpha,\alpha^q,\cdots,\alpha^{q^{n-1}}\}$ 和 $B=\{\beta,\beta^q,\cdots,\beta^{q^{n-1}}\}$，称 B 为 N 的对偶基当且仅当对任意的 $i,j=0,1,\cdots,n-1$，都有

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

其中 $Tr(\gamma)=\sum_{i=0}^{n-1}\gamma^{q^i}$ 是 $\gamma\in F_{q^n}$ 在 F_q 上的迹映射. 文献[4]证明了有限域上正规基的存在性，对偶基的存在唯一性以及正规基的对偶基仍为正规基等. 2012 年，廖[5] 给出了高斯正规基的对偶基，即证明了如下的结果：

引理 1.1[5] 设 q 为素数 p 的方幂，$N=\{\alpha,\alpha^q,\cdots,\alpha^{q^{n-1}}\}$ 为 F_{q^n} 在 F_q 上的 k 型高斯正规基 $(1\leqslant k\leqslant n)$，则 N 的对偶基生成元为

$$\beta = \begin{cases} \dfrac{\alpha}{kn+1} - \dfrac{k}{kn+1}, & 2\mid k, \\ \dfrac{\alpha^{\frac{n}{2}}}{kn+1} - \dfrac{k}{kn+1}, & \text{其他.} \end{cases}$$

设 q 为素数 p 的方幂，n 是正整数，F_{q^n} 是有限域 F_q 的 n 次扩张 $(n\geqslant 2)$. 若正整数 m 为 n 的因数，且 $N=\{\alpha,\alpha^q,\cdots,\alpha^{q^{n-1}}\}$ 为 F_{q^n} 在 F_q 上正规基，则 $\gamma=Tr_{q^n/q^m}(\alpha)$ 生成 F_{q^m} 在 F_q 上的正规基 $M=\{\gamma,\gamma^q,\cdots,\gamma^{q^{m-1}}\}$，称为 N 的迹正规基.

2005 年，廖和孙[6] 给出了有限域上Ⅰ型最优正规基和Ⅱ型最优正规基的乘法表. 2012 年，Christopoulou 等[7] 给出了 $k=3,4,5,6$ 时有限域 F_{q^n} 在 F_q 上的 k- 型高斯正规基的乘法表和复杂度的准确公式. 最近廖和胡[8] 把文献[7]的结果推广到了一般情形，给出了有限域 F_{q^n} 在 F_q 上一类高斯正规基的乘法表和复杂度的具体计算公式，并且证明了有限域 F_{q^n} 在 F_q 上的 7- 型高斯正规基满足所给条件当且仅当 $n\neq 4$. 本文进一步该问题的研究，完善了文献[8]的结果，给出了 $n=4$ 时，F_{q^n} 在 F_q 上的 7- 型高斯正规基及其对偶基和迹基的准确复杂度，即证明了如下主要结果：

定理 1.2 设 q 为素数 p 的方幂，n 是正整数，若 N 为 F_{q^4} 在 F_q 上的 7- 型高斯正规基，B 为 N 的对偶基，M 为 N 的迹正规基，C_N, C_B, C_M 分别为 N, B, M 的复杂度，则

$$C_N = \begin{cases} 9, & P=2, \\ 10, & P=3, \\ 15, & \text{其他;} \end{cases} \quad C_B = \begin{cases} 7, & P=2, \\ 7, & P=3, \\ 15, & \text{其他;} \end{cases}$$

$$C_M = \begin{cases} 3, & P=2, \\ 4, & P=3, \\ 4, & \text{其他,} \end{cases}$$

即 $p=2,3$ 时，B 为 F_{q^4} 在 F_q 上的最优正规基；$p=2$ 时，M 为 F_{q^2} 在 F_q 上的最优正规基.

2 主要结果的证明

为了证明定理 1.2，我们需要如下几个引理和命题.

引理 2.1[9] 设 q 为素数 p 的方幂，$N=\{\alpha,\alpha^q,\cdots,\alpha^{q^{n-1}}\}$ 为 F_{q^n} 在 F_q 上的 k 型高斯正规基. $Tr(\alpha)=\sum_{i=0}^{n-1}\alpha^{q^i}$ 是 $\alpha\in F_{q^n}$ 在 F_q 上的迹映射，则 $Tr(\alpha)=-1$.

引理 2.2[10] 设 q 为素数 p 的方幂，F_{q^n} 是 F_q 的 n 次扩张，F_{q^n} 在 F_q 上的一组正规基 $N=\{\alpha,\alpha^q,\cdots,\alpha^{q^{n-1}}\}$ 的对偶基为 $B=\{\beta,\beta^q,\cdots,\beta^{q^{n-1}}\}$，$T=(t_{i,j})$ 和 $H=(h_{i,j})$ 分别为 N,B 的乘法表. 则存在 $a,b\in F_q$ 以及 $r\in\{0,1,\cdots,n-1\}$，使得 $\beta=a+b\alpha_r$ 的充分必要条件是以下两式同时成立：

$$\sum_{j=0}^{n-1} h_{i,j} = \begin{cases} a+bTr(\alpha), & i=r, \\ a, & \text{其他,} \end{cases}$$

$$h_{i,j}=\begin{cases}2a+bt_{0,0}, & i=j=0,\\ bt_{0,j}, & i=0,j=1,\cdots.n-1,\\ bt_{r,j}, & i=r,j=0,r,\\ -a+bt_{r,j}, & i=r,j\neq 0,r,\\ a+bt_{t,j}, & i\neq 0,r,j=0,i,\\ bt_{i,j}, & i\neq 0,r,j\neq 0,i.\end{cases}$$

命题 2.3[11]　设 k 为奇数，n 为偶数，$\alpha=\sum_{j=0}^{k-1}\gamma^{l^j}$ 生成 F_{q^n} 在 F_q 上的 k －型高斯正规基 $N=\{\alpha,\alpha^q,\cdots,\alpha^{q^{n-1}}\}$，则 $\alpha_{\frac{n}{2}}=\sum_{j=0}^{k-1}\gamma^{-1^j}$.

定理 1.2 的证明　易知 $Z_{29}^*=A_1\cup A_2\cup A_3\cup A_4\cup A_5\cup A_6$，其中

$A_1=\{\alpha\in\mathbf{Z}_{29}^*\mid ord\alpha=28\}$,

$A_2=\{\alpha\in\mathbf{Z}_{29}^*\mid ord\alpha=14\}$,

$A_3=\{\alpha\in\mathbf{Z}_{29}^*\mid ord\alpha=7\}$,

$A_4=\{\alpha\in\mathbf{Z}_{29}^*\mid ord\alpha=4\}$,

$A_5=\{\alpha\in\mathbf{Z}_{29}^*\mid ord\alpha=2\}$,

$A_6=\{\alpha\in\mathbf{Z}_{29}^*\mid ord\alpha=1\}$.

进而若取模 29 的一个原根 $g=2$，则可将上述集合改写成 2 的方幂形式：

$A_1=\{2^1,2^5,2^3,2^{23},2^{25},2^{13},2^{27},2^{11},2^9,2^{17},2^{19},2^{15}\}$,

$A_2=\{2^2,2^{22},2^6,2^{10},2^{18},2^{26}\}$,

$A_3=\{2^4,2^8,2^{12},2^{16},2^{20},2^{24}\}$,

$A_4=\{2^7,2^{21}\}$ $A_5=\{2^{14}\}$, $A_6=\{2^0\}$.

由 k- 型高斯正规基的构造定理可知：当 $n=4,k=7$ 时，$4\cdot 7+1=29$ 是素数，此时取 $\gamma\in F_{q^{28}}$ 是 29 次本原单位根，s 是 q 模 29 的次数，且 $(\frac{28}{s},4)=1$. 又 $l=16$ 是 Z_{29} 中的 7 次本原单位根，则 $\alpha=\sum_{j=0}^{k-1}\gamma^{16^j}=\gamma+\gamma^{16}+\gamma^{24}+\gamma^7+\gamma^{25}+\gamma^{23}+\gamma^{20}$ 生成 F_{q^4} 在 F_q 上的 7 -型高斯正规基. 由 $(\frac{28}{s},4)=1$ 可知 s 有两种取法：$s_1=28,s_2=4$. 因此若存在 F_{q^4} 在 F_q 上的 7 -型高斯正规基，则 $q\equiv 12,17,k(\mathrm{mod}29)$，其中 $k\in A_1$.

由于取定原根 $g=2$ 后，将满足构造定理的 q 改写成 2 的方幂后指数只有 $4k+1$ 和 $4k+3$ 两种情况，这里的 $k\in\mathbf{N}^+$ 从而 F_{q^4} 在 F_q 上的 7 -型高斯正规基也只有两种情况. 为此令

$A=\{17,2,3,19,14,21,11\}=\{2^{21},2^1,2^5,2^9,2^{13},2^{17},2^{25}\}$,

$B=\{12,8,18,26,27,10,15\}=\{2^7,2^3,2^{11},2^{15},2^{19},2^{23},2^{27}\}$.

显然 $A\cup B$ 包含了模 29 单位群的所有 4 阶和 28 阶元素.

情形一. 若存在 $a\in A$，使 $q\equiv a(\mathrm{mod}29)$时，

$$\alpha=\gamma+\gamma^{16}+\gamma^{24}+\gamma^7+\gamma^{25}+\gamma^{23}+\gamma^{20},$$

因此

$$\alpha_1=\alpha^q=\gamma^q+\gamma^{16q}+\gamma^{24q}+\gamma^{7q}+\gamma^{25q}+\gamma^{23q}+\gamma^{20q}.$$

注意到 α 的指数集合为

$$\{2^0,2^4,2^8,2^{12},2^{16},2^{20},2^{24}\}=\{2^\delta\mid\delta\equiv 0(\mathrm{mod}4),0\leqslant\delta\leqslant 28\},$$

$\gamma^{29}=1$ 以及集合 A 中元素的指数均模 4 余 1，所以此时 α_1 的指数集合为

$$\{2^1,2^5,2^9,2^{13},2^{17},2^{21},2^{25}\}=\{2^\delta\mid\delta\equiv 1(\mathrm{mod}4),0\leqslant\delta\leqslant 28\}.$$

从而

$$\alpha_1=\gamma^{17}+\gamma^{11}+\gamma^2+\gamma^3+\gamma^{19}+\gamma^{14}+\gamma^{21}.$$

类似地

$$\alpha_2=\gamma^{28}+\gamma^{13}+\gamma^5+\gamma^{22}+\gamma^4+\gamma^6+\gamma^9,$$

$$\alpha_3=\gamma^8+\gamma^{10}+\gamma^{12}+\gamma^{15}+\gamma^{18}+\gamma^{26}+\gamma^{27}.$$

事实上，也可以用命题 2.3 直接验证 $\alpha_2=\gamma^{28}+\gamma^{13}+\gamma^5+\gamma^{22}+\gamma^4+\gamma^6+\gamma^9$. 为简便，设 $\alpha_i=\alpha^{q^i}(0\leqslant i\leqslant 3)$，其中 $\alpha_0=\alpha$. 因此

$$\alpha\alpha=2\alpha+3\alpha_1+2\alpha_3 \tag{1}$$

$$\alpha\alpha_1=\alpha+\alpha_1+2\alpha_2+3\alpha_3 \tag{2}$$

$$\alpha\alpha_2=7+2\alpha+\alpha_1+2\alpha_2+\alpha_3 \tag{3}$$

$$\alpha\alpha_3=\alpha+2\alpha_1+3\alpha_2+\alpha_3 \tag{4}$$

(i) 当 $p=2$ 时，(1)～(4)式等价于

$\alpha\alpha=\alpha_1$, $\alpha\alpha_1=\alpha+\alpha_1+\alpha_3$,

$\alpha\alpha_2=1+\alpha_1+\alpha_3=\alpha+\alpha_2$,

$\alpha\alpha_3=\alpha+\alpha_2+\alpha_3$,

此时 N 的乘法表

$$T_N=\begin{pmatrix}0&1&0&0\\1&1&0&1\\1&0&1&0\\1&0&1&1\end{pmatrix} \tag{5}$$

从而 $C_N=9$.

下面计算 N 的对偶基 B 的复杂度. 由引理 1.1 可知 B 的生成元为

$$\beta=\frac{\alpha_{\frac{n}{2}}}{kn+1}-\frac{k}{kn+1}=\frac{\alpha_2}{29}-\frac{7}{29}=1+\alpha_2,$$

从而

$\beta_1 = \beta^q = 1+\alpha_2^q = 1+\alpha_3$,

$\beta_2 = \beta_1^q = 1+\alpha_3^q = 1+\alpha$,

$\beta_3 = \beta_2^q = 1+\alpha^q = 1+\alpha_1$.

进而

$\beta\beta = 1+\alpha_2\alpha_2 = 1+\alpha_3 = \beta_1$,

$\beta\beta_1 = 1+\alpha_2+\alpha_3+\alpha_2\alpha_3 = \beta_3$,

$\beta\beta_2 = 1+\alpha_2+\alpha+\alpha_2\alpha = \beta+\beta_1+\beta_2+\beta_3$,

$\beta\beta_3 = 1+\alpha_2+\alpha_1+\alpha_1\alpha_2 = \beta_2$.

此时 B 的乘法表

$$T_B = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \tag{6}$$

则 $C_B = 2\cdot 4-1 = 7$,即 B 为 F_{q^4} 在 F_q 上的最优正规基. 又由迹正规基的定义可知:N 的迹正规基 $M = \{\delta_0, \delta_1\}$,其中

$\delta_0 = \mathrm{Tr}_{q^4/q^2}(\alpha) = \alpha+\alpha^{q^2} = \alpha+\alpha_2$,

$\delta_1 = \delta^q = \alpha_1+\alpha_3$,

且 M 为 F_{q^2} 在 F_q 上的正规基. 从而

$\delta_0\delta_0 = (\alpha+\alpha_2)^2 = \alpha\alpha+\alpha_2\alpha_2 =$

$\alpha\alpha+(\alpha\alpha)^{q^2} = \alpha_1+\alpha_3 = \delta_1$,

$\delta_0\delta_1 = (\alpha+\alpha_2)(\alpha_1+\alpha_3) =$

$\alpha+\alpha_1+\alpha_2+\alpha_3 = \delta_0+\delta_1$.

因此 M 的乘法表

$$T_M = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \tag{7}$$

故 $C_M = 2\cdot 2-1 = 3$,即 M 为 F_{q^2} 在 F_q 上的最优正规基.

(ii) 当 $p = 3$ 时,式(1)~(4)等价于

$\alpha\alpha = 2\alpha+2\alpha_3$,

$\alpha\alpha_1 = \alpha+\alpha_1+2\alpha_2$,

$\alpha\alpha_2 = 1+2\alpha+\alpha_1+2\alpha_2 = \alpha+\alpha_2$,

$\alpha\alpha_3 = \alpha+2\alpha_1+\alpha_3$.

此时 N 的乘法表

$$T_N = \begin{pmatrix} 2 & 0 & 0 & 2 \\ 1 & 1 & 2 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 2 & 0 & 1 \end{pmatrix} \tag{8}$$

则 $C_N = 10$.

下面计算 N 的对偶基 B 的复杂度. 由引理 1.1 可知 B 的生成元为

$$\beta = \frac{\alpha^{\frac{n}{2}}}{kn+1} - \frac{k}{kn+1} = \frac{\alpha_2}{29} - \frac{7}{29} = 1+2\alpha_2,$$

从而

$\beta_1 = \beta^q = 1+2\alpha_2^q = 1+2\alpha_3$,

$\beta_2 = \beta_1^q = 1+2\alpha_3^q = 1+2\alpha$,

$\beta_3 = \beta_2^q = 1+2\alpha^q = 1+2\alpha_1$.

类似有

$\beta\beta = \beta_3$, $\beta\beta_1 = \beta_2$,

$\beta\beta_2 = 2\beta+2\beta_1+2\beta_2+2\beta_3$, $\beta\beta_3 = \beta_1$.

此时 B 的乘法表

$$T_B = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 2 & 2 & 2 & 2 \\ 0 & 1 & 0 & 0 \end{pmatrix} \tag{9}$$

则 $C_B = 2\cdot 4-1 = 7$,即 B 为 F_{q^4} 在 F_q 上的最优正规基.

又由迹正规基的定义可知:N 的迹正规基 $M = \{\delta_0, \delta_1\}$,其中

$\delta_0 = \mathrm{Tr}_{q^4/q^2}(\alpha) = \alpha+\alpha^{q^2} = \alpha+\alpha_2$,

$\delta_1 = \delta^q = \alpha_1+\alpha_3$,

且 M 为 F_{q^2} 在 F_q 上的正规基,从而

$\delta_0\delta_0 = (\alpha+\alpha_2)^2 = \delta_0+2\delta_1$,

$\delta_0\delta_1 = (\alpha+\alpha_2)(\alpha_1+\alpha_3) = \delta_0+\delta_1$,

因此 M 的乘法表

$$T_M = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix} \tag{10}$$

故 $C_M = 4$.

注 2 由 k- 型高斯正规基的构造定理可以得到 q 模 29 的阶只能是 4 或 28,显然有 $p \neq 5,7,13,23,\cdots$,以下的 $p \neq 2,3$ 均指排除了不满足构造定理的 q.

(iii) 当 $p \neq 2,3$ 时,式(1)~(4)等价于

$\alpha\alpha = 2\alpha+3\alpha_1+2\alpha_3$, $\alpha\alpha_1 = \alpha+\alpha_1+2\alpha_2+3\alpha_3$,

$\alpha\alpha_2 = 7+2\alpha+\alpha_1+2\alpha_2+\alpha_3 =$

$-5\alpha-6\alpha_1-5\alpha_2-6\alpha_3$,

$\alpha\alpha_3 = \alpha+2\alpha_1+3\alpha_2+\alpha_3$.

此时 N 的乘法表

$$T_N = (t_{i,j})_{4\times 4} = \begin{pmatrix} 2 & 3 & 0 & 2 \\ 1 & 1 & 2 & 3 \\ -5 & -6 & -5 & -6 \\ 1 & 2 & 3 & 1 \end{pmatrix} \tag{11}$$

则 $C_N = 15$.

下面计算 N 的对偶基 B 的复杂度. 由引理 1.1 可知 B 的生成元为

$$\beta = \frac{\alpha^{\frac{n}{2}}}{kn+1} - \frac{k}{kn+1} = \frac{\alpha_2}{29} - \frac{7}{29} = \frac{\alpha_2-7}{29}.$$

现令 $\beta = a + b\alpha_2$，其中 $a = -\frac{7}{29}, b = \frac{1}{29}$. 则由引理 2.2 及式(11)可知 B 的乘法表第一行元素分布为：

$$\begin{cases} h_{0,0} = 2a + bt_{0,0} = -\frac{12}{29}, \\ h_{0,1} = bt_{0,1} = \frac{3}{29}, \\ h_{0,2} = bt_{0,2} = 0, \\ h_{0,3} = bt_{0,3} = \frac{2}{29} \end{cases} \tag{12}$$

第二行元素分布为：

$$\begin{cases} h_{1,0} = a + bt_{1,0} = -\frac{6}{29}, \\ h_{1,1} = a + bt_{1,1} = -\frac{6}{29}, \\ h_{1,2} = bt_{1,2} = \frac{2}{29}, \\ h_{1,3} = bt_{1,3} = \frac{3}{29} \end{cases} \tag{13}$$

第三行元素分布为：

$$\begin{cases} h_{2,0} = bt_{2,0} = -\frac{5}{29}, \\ h_{2,1} = -a + bt_{2,1} = \frac{1}{29}, \\ h_{2,2} = bt_{2,2} = -\frac{5}{29}, \\ h_{2,3} = -a + bt_{2,3} = \frac{1}{29} \end{cases} \tag{14}$$

第四行元素分布为：

$$\begin{cases} h_{3,0} = a + bt_{3,0} = -\frac{6}{29}, \\ h_{3,1} = bt_{3,1} = \frac{2}{29}, \\ h_{3,2} = bt_{3,2} = \frac{3}{29}, \\ h_{3,3} = a + bt_{3,3} = -\frac{6}{29} \end{cases} \tag{15}$$

由式(12)～(15)可知 B 的乘法表

$$T_B = \frac{1}{29}\begin{pmatrix} -12 & 3 & 0 & 2 \\ -6 & -6 & 2 & 3 \\ -5 & 1 & -5 & 1 \\ -6 & 2 & 3 & -6 \end{pmatrix} \tag{16}$$

则 $C_B = 15$. 又由迹正规基的定义可知：N 的迹正规基 $M = \{\delta_0, \delta_1\}$，其中

$$\delta_0 = Tr_{q^4/q^2}(\alpha) = \alpha + \alpha^{q^2} = \alpha + \alpha_2,$$

$$\delta_1 = \delta^q = \alpha_1 + \alpha_3,$$

且 M 为 F_{q^2} 在 F_q 上的正规基. 从而

$$\delta_0\delta_0 = (\alpha + \alpha_2)^2 = -8\delta_0 - 7\delta_1,$$

$$\delta_0\delta_1 = (\alpha + \alpha_2)(\alpha_1 + \alpha_3) = 7\delta_0 + 7\delta_1.$$

因此 M 的乘法表

$$T_M = \begin{pmatrix} -8 & -7 \\ 7 & 7 \end{pmatrix} \tag{17}$$

故 $C_M = 4$.

情形二. 若存在 $b \in B$，使 $q \equiv b(\mathrm{mod}29)$ 时，

$$\alpha = \gamma + \gamma^{16} + \gamma^{24} + \gamma^7 + \gamma^{25} + \gamma^{23} + \gamma^{20}.$$

因此

$$\alpha_1 = \alpha^q = \gamma^q + \gamma^{16q} + \gamma^{24q} + \gamma^{7q} + \gamma^{25q} + \gamma^{23q} + \gamma^{20q}.$$

注意到此时集合 B 中元素的指数均模 4 余 3，所以此时 α_1 的指数集合为

$$\{2^7, 2^{11}, 2^{15}, 2^{19}, 2^{23}, 2^{27}, 2^3\} = \{2^\delta \mid \delta \equiv 3(\mathrm{mod}4), 0 \leqslant \delta \leqslant 28\}.$$

从而

$$\alpha_1 = \gamma^8 + \gamma^{10} + \gamma^{12} + \gamma^{15} + \gamma^{18} + \gamma^{26} + \gamma^{27}.$$

类似地

$$\alpha_2 = \gamma^{28} + \gamma^{13} + \gamma^5 + \gamma^{22} + \gamma^4 + \gamma^6 + \gamma^9,$$

$$\alpha_3 = \gamma^{17} + \gamma^{11} + \gamma^2 + \gamma^3 + \gamma^{19} + \gamma^{14} + \gamma^{21}.$$

所以情形一和情形二的正规基、只是 α_1 和 α_3 交换了顺序，复杂度必然相同，从而定理得证.

下面给出这种情形的正规基、对偶基和迹基的乘法表.

$$\alpha\alpha = 2\alpha + 3\alpha_1 + 2\alpha_3,$$

$$\alpha\alpha_1 = \alpha + \alpha_1 + 3\alpha_2 + 2\alpha_3,$$

$$\alpha\alpha_2 = 7 + 2\alpha + \alpha_1 + 2\alpha_2 + \alpha_3,$$

$$\alpha\alpha_3 = \alpha + 3\alpha_1 + 2\alpha_2 + \alpha_3.$$

类似于情形一的证明，可知有以下三种情形：

(i) 当 $p = 2$ 时，

$$T_N = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{pmatrix},$$

$$T_B = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix},$$

$$T_M = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}.$$

(ii) 当 $p = 3$ 时，

$$T_N = \begin{pmatrix} 2 & 2 & 0 & 0 \\ 1 & 1 & 0 & 2 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 2 & 1 \end{pmatrix},$$

$$T_B = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 2 & 2 & 2 & 2 \\ 0 & 0 & 1 & 0 \end{pmatrix},$$

$$T_M = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}.$$

(iii) 当 $p \neq 2,3$ 时,

$$T_N = \begin{pmatrix} 2 & 2 & 0 & 3 \\ 1 & 1 & 3 & 2 \\ -5 & -6 & -5 & -6 \\ 1 & 3 & 2 & 1 \end{pmatrix},$$

$$T_B = \frac{1}{29}\begin{pmatrix} -12 & 2 & 0 & 3 \\ -6 & -6 & 3 & 2 \\ -5 & 1 & -5 & 1 \\ -6 & 3 & 2 & -6 \end{pmatrix},$$

$$T_M = \begin{pmatrix} -8 & -7 \\ 7 & 7 \end{pmatrix}.$$

参考文献:

[1] Mullin R, Onyszchuk I, Vanstone S, *et al*. Optimal bases in $GF(p^m)$ [J]. Discrete Applied Math, 1988/1989, 22(2): 149.

[2] Gao S H. Nomal bases over finite fields[D]. Ontario: Waterloo, 1993.

[3] Wassermann A. Konstruktion von normal bases[J]. Bayreuther Mathematische Schriften, 1990, 31: 155.

[4] Menezes A J, Blake I F, Gao X H, etal. Applictions of Finite Fields[M]. New York: Kluwer Academic Publishers, 1993.

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

[6] 廖群英, 孙琦. 有限域上最优正规基的乘法表[J]. 数学学报, 2005, 48(5): 947.

[7] Christopoulou M, Garefalakis T, Panario D, *et al*. Gauss periods as constructions of low complexity normal bases[J]. Designs, Codes and Cryptography, 2012, 62(1): 43.

[8] 廖群英, 胡晓兰. 有限域上一类高斯正规基的复杂度的准确计算公式[J]. 数学学报, 2014, 57(5): 863.

[9] 廖群英, 苏丹丹, 付萍. 有限域上 2- 型高斯正规基及其对偶基[J]. 四川大学学报: 自然科学版, 2010, 47(6): 1221.

[10] 苏丹丹, 廖群英. 有限域上一类特殊对偶基的推广[J]. 四川大学学报: 自然科学版, 2011, 48(1): 27.

[11] 李俊, 黄琴, 李波, 廖群英. 有限域上的 k- 型高斯正规基及其对偶基[J]. 四川师范大学学报, 2011, 34(3): 289.