

有限域上线性化多项式与正规基

徐碧云¹, 肖义丽¹, 曹 炜^{2*}

(1. 宁波大学 数学与统计学院, 浙江 宁波 315211; 2. 闽南师范大学 数学与统计学院, 福建 漳州 363000)

摘要: 设 $\mathbb{F}_q$ 为 q 阶有限域, $\mathbb{F}_{q^n}$ 为 $\mathbb{F}_q$ 的 n 次扩域. $\mathbb{F}_{q^n}$ 上形如 $\{\alpha, \alpha^q, \dots, \alpha^{q^{n-1}}\}$ 的一组基称为 $\mathbb{F}_{q^n}/\mathbb{F}_q$ 的正规基, 此时 α 称为 $\mathbb{F}_{q^n}/\mathbb{F}_q$ 上的正规元. 设 k 为 n 的一个正因子, 用 $\mathcal{N}_k$ 表示 $\mathbb{F}_{q^n}/\mathbb{F}_q$ 的正规元集合, 用 $G_{n,k}$ 表示 $\mathbb{F}_{q^n}$ 中满足 $\mathbb{F}_{q^k}(\alpha) = \mathbb{F}_{q^n}$ 且 $\sum_{j=0}^{n/k-1} \alpha^{q^{kj}} \in \mathcal{N}_k$ 的元素 α 的集合. 本文利用有限域上线性化多项式的性质, 给出了 $\mathcal{N}_n$ 与 $G_{n,k}$ 的计数公式.

关键词: 有限域; 正规基; 线性化多项式

中图分类号: O156

文献标志码: A

文章编号: 1001-5132 (2022) 02-0022-05

设 p 为素数, $n \in \mathbb{Z}^+$ 且 $n \geq 2$, $\mathbb{F}_q$ 表示特征为 p 的 q 阶有限域, $\mathbb{F}_{q^n}$ 为 $\mathbb{F}_q$ 的 n 次扩域. $\mathbb{F}_{q^n}$ 上形如 $\{\alpha, \alpha^q, \dots, \alpha^{q^{n-1}}\}$ 的一组基称为 $\mathbb{F}_{q^n}/\mathbb{F}_q$ 的正规基, 此时 α 称为 $\mathbb{F}_{q^n}/\mathbb{F}_q$ 上的正规元. 设 $f(x)$ 是 $\mathbb{F}_q[x]$ 中的 n 次不可约多项式, 如果它的所有根 $\alpha, \alpha^q, \dots, \alpha^{q^{n-1}}$ 在 $\mathbb{F}_q$ 上是线性无关的, 称 $f(x)$ 是正规多项式^[1]. 对任意 $\alpha \in \mathbb{F}_{q^n}$, 定义 α 的迹 $Tr(\alpha) = \alpha + \alpha^q + \dots + \alpha^{q^{n-1}}$. 更多有限域上正规基的相关知识可参考文献[1-2].

设 $\mathcal{N}_n$ 为 $\mathbb{F}_{q^n}/\mathbb{F}_q$ 的正规元集合, G_n 表示 $\mathbb{F}_{q^n}$ 中满足 $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^n}$ 且 $Tr(\alpha) \neq 0$ 的元素 α 的集合. 显然 $\mathcal{N}_n \subseteq G_n$.

1942 年, Perlis^[3] 利用多项式环 $\mathbb{F}_q[x]$ 中的欧拉函数以及 $x^n - 1$ 在 $\mathbb{F}_q[x]$ 中的分解, 证明了定理 1.

定理 1^[3] 设 $n = p^e, e \geq 1$, 则 $\mathcal{N}_n = G_n$.

1986 年, Pei 等^[4] 证明了定理 2.

定理 2^[4] 设 n 是一个与 p 互异的素数, 且 q 是模 n 的一个原根, 则 $\mathcal{N}_n = G_n$.

2001 年, Chang 等^[5] 进一步证明了定理 1 和定理 2 的充分条件也是必要的, 从而得到了定理 3.

定理 3^[5] 若 $\mathcal{N}_n = G_n$, 则 n 是 p 的方幂, 或 n 是一个与 p 互异的素数, 且 q 是模 n 的一个原根.

2018 年, Huang 等^[6] 通过比较 $\mathcal{N}_n$ 和 G_n 的个数, 利用线性化多项式给出了定理 1、定理 2 和定理 3 的一个统一且更为简洁的证明方法.

Hachenberger^[7] 推广了上述定理. 熟知 $\mathbb{F}_{q^n}/\mathbb{F}_q$ 为 n 次循环伽罗瓦扩张, 设 σ 为 $\mathbb{F}_{q^n}/\mathbb{F}_q$ 的循环伽罗瓦群的生成元, 对于 n 的每个正因子 k , 用 $\mathbb{F}_{q^k}$ 表示 $\mathbb{F}_q$ 上 $\mathbb{F}_{q^n}/\mathbb{F}_q$ 的唯一 k 次中间域. 定义迹映射 $Tr_k^n(\alpha) = \sum_{j=0}^{n/k-1} \sigma^{kj}(\alpha)$, 其中 $\alpha \in \mathbb{F}_{q^n}$; 显然, 当 $k=1$ 时, Tr_k^n 即为前面定义的 Tr . 设 $\mathcal{N}_k$ 为 $\mathbb{F}_{q^n}/\mathbb{F}_q$ 的正规元集合, 用 $G_{n,k}$ 表示 $\mathbb{F}_{q^n}$ 中满足 $\mathbb{F}_{q^k}(\alpha) = \mathbb{F}_{q^n}$ 且 $Tr_k^n(\alpha) \in \mathcal{N}_k$ 的元素 α 的集合. Hachenberger^[7] 利用广义迹映射性质证明了定理 4.

定理 4^[7] $\mathcal{N}_n = G_{n,k}$ 当且仅当 n/k 是 p 的幂, 或 $n = r^l, k = r^{l-1}$, 其中 r 是不同于 $\mathbb{F}_q$ 的特征的素数, 且 r^l 阶分圆多项式在 $\mathbb{F}_q[x]$ 上不可约.

本文利用线性化多项式研究有限域上的正规基, 主要是利用 $x^n - 1$ 的普通分解与对应的 $x^{q^n} - x$ 的符号分解来计算集合 $\mathcal{N}_n$ 和 $G_{n,k}$ 中的元素个数.

1 线性化多项式

线性化多项式的许多相关性质与结论可参考文献[1,8-11].

定义 1^[1] 设 $\mathbb{F}_{q^n}$ 为 $\mathbb{F}_q$ 的一个扩域. 形如 $L(x) = \sum_{i=0}^m \alpha_i x^{q^i}$ 的多项式称作 $\mathbb{F}_{q^n}$ 上的线性化多项式(也称 q -多项式), 其中 $\alpha_i \in \mathbb{F}_{q^n}$.

设 F 是 $\mathbb{F}_{q^n}$ 的一个扩域, $L(x)$ 是 $\mathbb{F}_{q^n}$ 上的 q -多项式, 则任给 $\alpha, \beta \in F, c \in \mathbb{F}_q$, 有:

$$L(\alpha + \beta) = L(\alpha) + L(\beta), L(c\alpha) = cL(\alpha).$$

定义 2^[1] $\mathbb{F}_{q^n}$ 上的多项式 $l(x) = \sum_{i=0}^m \alpha_i x^i$ 和 $L(x) = \sum_{i=0}^m \alpha_i x^{q^i}$ 称互为 q -相伴. 特别地, $l(x)$ 是 $L(x)$ 传统 q -相伴式, $L(x)$ 是 $l(x)$ 的线性 q -相伴式.

定义 3^[1] 设 $L_1(x)$ 和 $L_2(x)$ 是 $\mathbb{F}_{q^n}$ 上的两个 q -多项式, 定义符号乘积为:

$$L_1(x) \otimes L_2(x) = L_1(L_2(x)).$$

显然, $\mathbb{F}_{q^n}$ 上的两个 q -多项式的普通乘积不一定是 q -多项式. 但 $\mathbb{F}_{q^n}$ 上的两个 q -多项式 $L_1(x)$ 和 $L_2(x)$ 的复合 $L_1(L_2(x))$ 仍是一个 q -多项式.

引理 1^[1] 设 $L_1(x)$ 和 $L_2(x)$ 分别是 $\mathbb{F}_q$ 上 $l_1(x)$ 和 $l_2(x)$ 的线性 q -相伴式, 则 $l(x) = l_1(x)l_2(x)$ 和 $L(x) = L_1(x) \otimes L_2(x)$ 互为 q -相伴.

推论 1^[1] 设 $L_1(x)$ 和 $L(x)$ 分别是 $\mathbb{F}_q$ 上 $l_1(x)$ 和 $l(x)$ 的线性 q -相伴式, 则 $L_1(x)$ 符号整除 $L(x)$ 当且仅当 $l_1(x)$ 整除 $l(x)$. 特别地, $L(x)$ 在 $\mathbb{F}_q$ 上符号不可约当且仅当 $l(x)$ 在 $\mathbb{F}_q$ 上不可约.

设 $L(x)$ 是 $\mathbb{F}_q$ 上的 q -多项式, 则 $L(x)$ 的 e 次符号幂记作 $L(x)^{\otimes e}$. 设 $L(x)$ 和 $l(x)$ 互为 q -相伴, 若

$$L(x) = \bigotimes_{i=1}^r L_i(x)^{\otimes e_i}$$

为 $L(x)$ 的符号分解, 其中 $L_i(x) (i=1, \dots, r)$ 为 $\mathbb{F}_q$ 上两两符号互素的 q -多项式, 则

$$l(x) = \prod_{i=1}^r l_i(x)^{e_i}$$

为 $l(x)$ 的标准普通分解, 其中 $l_i(x)$ 为 $L_i(x)$ 的传统 q -相伴式且 $l_i(x)$ 两两互素.

2 $\mathcal{N}_n$ 的计数公式

设 $n = mp^e, p \nmid m, k = m_1 p^{e_1}, m_1 \mid m, e \geq e_1 \geq 0$, 则 $n/k = (m/m_1)p^{e-e_1} \triangleq m_2 p^{e_2}$.

引理 2^[1]

$$x^n - 1 = \prod_{d \mid m} \varphi_d(x)^{p^e} = \prod_{d \mid m} \prod_{j=1}^{\phi(d)/\tau(d)} h_{d_j}(x)^{p^e}, \quad (1)$$

其中: $\varphi_d(x)$ 表示 d 阶分圆多项式, 其次数为 $\phi(d)$, 且有 $\phi(d)/\tau(d)$ 个不同的首一不可约因子 $h_{d_j}(x)$, 每个次数均为 $\tau(d)$, 这里 $\phi(d)$ 表示 d 的欧拉函数, $\tau(d)$ 表示 q 模 d 的次数.

设 $\Psi_d(x)$ 和 $H_{d_j}(x)$ 分别为 $\varphi_d(x)$ 和 $h_{d_j}(x)$ 的线性 q -相伴式.

推论 2

$$x^{q^n} - x = \bigotimes_{d \mid m} \Psi_d(x)^{\otimes p^e} = \bigotimes_{d \mid m} \bigotimes_{j=1}^{\phi(d)/\tau(d)} H_{d_j}(x)^{\otimes p^e}. \quad (2)$$

设 $\mathcal{J}(x^{q^n} - x)$ 表示 $x^n - 1$ 中所有不可约因子的集合, 即式(1)中 $h_{d_j}(x)$ 的集合. 对式(2)中任一符号不可约因子 $H_{d_j}(x)$, 存在唯一的 $x^{q^n} - x$ 的符号极大因子 $K_{d_j}(x)$, 使得 $x^{q^n} - x = K_{d_j}(x) \otimes H_{d_j}(x)$. 设 $\mathcal{M}(x^{q^n} - x)$ 表示 $x^{q^n} - x$ 中所有符号极大因子的集合. 显然

$$|\mathcal{J}(x^{q^n} - x)| = |\mathcal{M}(x^{q^n} - x)| = \sum_{d \mid m} \phi(d) / \tau(d).$$

引理 3^[1]

$$\mathcal{N}_n = \left\{ \alpha \in \mathbb{F}_{q^n} : K(\alpha) \neq 0, \forall K(x) \in \mathcal{M}(x^{q^n} - x) \right\}.$$

定理 5^[12]

$$|\mathcal{N}_n| = q^{n-m} \prod_{d \mid m} (q^{\tau(d)} - 1)^{\phi(d)/\tau(d)}.$$

证明

$$\text{令 } \mathcal{B}(m) = \{d_j : 1 \leq d \mid m, j=1, \dots, \phi(d)/\tau(d)\}.$$

对 $\forall d_j \in \mathcal{B}(m)$, 考虑集合 $A_{d_j} = \{\alpha \in \mathbb{F}_{q^n} : K_{d_j}(\alpha) = 0\}$. 由引理 3 可知, α 为 $\mathbb{F}_{q^n} / \mathbb{F}_q$ 上的正规元当且仅当 $\alpha \in \mathbb{F}_{q^n} \setminus (\bigcup_{d_j \in \mathcal{B}(m)} A_{d_j})$. 故有:

$$|\mathcal{N}_n| = \left| \mathbb{F}_{q^n} \setminus \left(\bigcup_{d_j \in \mathcal{B}(m)} A_{d_j} \right) \right|,$$

假设 $\emptyset \neq M \subseteq \mathcal{B}(m)$, 显然

$$\left| \bigcap_{d_j \in M} A_{d_j} \right| = q^{n - \sum_{d_j \in M} \tau(d)}.$$

由容斥原理得:

$$\begin{aligned} \left| \mathbb{F}_{q^n} \setminus \left(\bigcup_{d_j \in \mathcal{B}(m)} A_{d_j} \right) \right| &= q^n - \sum_{M \subseteq \mathcal{B}(m)} (-1)^{|M|} \cdot \\ &= \left| \bigcap_{d_j \in M} A_{d_j} \right| = q^n - \sum_{M \subseteq \mathcal{B}(m)} (-1)^{|M|} q^{n - \sum_{d_j \in M} \tau(d)} = \\ &= q^n \prod_{d \mid m} (1 - q^{-\tau(d)})^{\phi(d)/\tau(d)} = \\ &= q^n \prod_{d \mid m} q^{-\phi(d)} (q^{\tau(d)} - 1)^{\phi(d)/\tau(d)} = \\ &= q^{n-m} \prod_{d \mid m} (q^{\tau(d)} - 1)^{\phi(d)/\tau(d)}. \end{aligned}$$

3 $G_{n,k}$ 的计数公式

定义 4 设 $\mathcal{L}(n/k) = \{p_1, p_2, \dots, p_u\}$ 为 n/k 的不同素因子, 设

$$\mathcal{B}(m_1) = \{l_1, \dots, d_1, d_2, \dots, d_{\phi(d)/\tau(d)}, \dots, m_1, \dots, m_{1_{\phi(m_1)/\tau(m_1)}}\} = \{y_1, \dots, y_{l_1}\},$$

其中: $d \mid m_1, l_1 = \sum_{d \mid m_1} (\phi(d)/\tau(d))$. 定义集合

$$S = \{\alpha \in \mathbb{F}_{q^n} : \alpha + \alpha^{q^k} + \alpha^{q^{2k}} + \dots + \alpha^{q^{n-k}} = 0\}.$$

对任意 $p_i \in \mathcal{L}(n/k)$, 定义:

$$S_{p_i} = \left\{ \alpha \in \mathbb{F}_{q^n} : \alpha^{q^{n/p_i}} - \alpha = 0 \right\}.$$

对任意 $y_j \in \mathcal{B}(m_1)$, 定义:

$$A_{y_j} = \left\{ \alpha \in \mathbb{F}_{q^n} : K_{y_j}(\alpha) \otimes (\alpha + \alpha^{q^k} + \cdots + \alpha^{q^{n-k}}) = 0 \right\},$$

这里 $K_{y_j}(x)$ 为 $x^{q^k} - x$ 的符号极大因子.

注 1 (i) 从 S_{p_i} 的定义可以看出, 设

$$\alpha \in \mathbb{F}_{q^n} \setminus \left(\bigcup_{p_i \in \mathcal{L}(n/k)} S_{p_i} \right),$$

$\mathbb{F}_{q^k}$ 上 α 的极小多项式的次数是 n/k .

(ii) 由于 $x^{q^k} - x$ 的每个符号真因子至少符号整除这些 $K_{y_j}(x)$ 中的一个, 则由 A_{y_j} 的定义可知, 设

$$\alpha \in \mathbb{F}_{q^n} \setminus \left(\bigcup_{y_j \in \mathcal{B}(m_1)} A_{y_j} \right),$$

α 满足 $Tr_k^n(\alpha) \in \mathcal{N}_k$.

引理 4 由定义 4, 得到如下集合:

$$S = \left\{ \alpha \in \mathbb{F}_{q^n} : (\alpha^{q^k} - \alpha)^{\otimes p^{e_2}-1} \otimes \bigotimes_{1 < c | m_2} \Psi_c(\alpha)^{\otimes p^{e_2}} = 0 \right\}, \quad (3)$$

对任意 $p_i \in \mathcal{L}(n/k)$,

$$S_{p_i} = \left\{ \alpha \in \mathbb{F}_{q^n} : \bigotimes_{c | \frac{n}{kp_i}} \Psi_c(\alpha) = 0 \right\}, \quad (4)$$

特别地, 若 $p_i \neq p$, 则

$$S_{p_i} = \left\{ \alpha \in \mathbb{F}_{q^n} : \bigotimes_{c | \frac{n}{kp_i}} \Psi_c(\alpha)^{\otimes p^{e_2}} = 0 \right\}, \quad (5)$$

$$S_p = \left\{ \alpha \in \mathbb{F}_{q^n} : \bigotimes_{c | m_2} \Psi_c(\alpha)^{\otimes p^{e_2}-1} = 0 \right\}, \quad (6)$$

其中: $\Psi_c(x)$ 表示 c 阶分圆多项式 $\varphi_c(x)$ 的线性 q^k -相伴式.

证明 由于

$$\begin{aligned} x^{n/k} - 1 &= (x^{m_2} - 1)^{p^{e_2}} = \prod_{c | m_2} \varphi_c(x)^{p^{e_2}} = \\ &= (x-1)(x-1)^{p^{e_2}-1} \prod_{1 < c | m_2} \varphi_c(x)^{p^{e_2}}, \end{aligned}$$

又因为

$$x^{n/k} - 1 = (x-1)(1+x+x^2+\cdots+x^{n/k-1}),$$

所以

$$1+x+x^2+\cdots+x^{n/k-1} = (x-1)^{p^{e_2}-1} \prod_{1 < c | m_2} \varphi_c(x)^{p^{e_2}},$$

可得:

$$\begin{aligned} x + x^{q^k} + x^{q^{2k}} + \cdots + x^{q^{n-k}} &= x + x^{q^k} + x^{q^{2k}} + \cdots + \\ x^{q^{k(n/k-1)}} &= (x^{q^k} - x)^{\otimes p^{e_2}-1} \otimes \bigotimes_{1 < c | m_2} \Psi_c(x)^{\otimes p^{e_2}}, \end{aligned}$$

由定义 4 可得式(3), 同理可得式(4)~(6).

引理 5 假设

$\emptyset \neq J = \{p_{j_1}, p_{j_2}, \cdots, p_{j_r}\} \subseteq \mathcal{L}(n/k)$, 有:

$$\left| \bigcap_{j \in J} S_j \right| = q^{\frac{n}{p_{j_1} \cdots p_{j_r}}}, \quad (7)$$

假设 $\emptyset \neq M = \{y_{i_1}, \cdots, y_{i_l}\} \subseteq \mathcal{B}(m_1)$, 有:

$$\left| \bigcap_{y \in M} A_y \right| = q^{n-\tau(y_{i_1})-\tau(y_{i_2})-\cdots-\tau(y_{i_l})}, \quad (8)$$

以及 $|S| = q^{n-k}$, 且

$$\left| \left(\bigcap_{j \in J} S_j \right) \cap \left(\bigcap_{y \in M} A_y \right) \right| = \begin{cases} q^{\frac{n}{p_{j_1} \cdots p_{j_r}} - \tau(y_{i_1}) - \tau(y_{i_2}) - \cdots - \tau(y_{i_l})}, & \text{若 } p \notin J, \\ q^{\frac{n}{p_{j_1} \cdots p_{j_r}}}, & \text{若 } p \in J. \end{cases} \quad (9)$$

证明 由定义 4, $|S| = q^{n-k}$ 易证. 设

$$R(x) = \bigotimes_{c | \frac{n}{kp_{j_1} \cdots p_{j_r}}} \Psi_c(x),$$

由引理 4 可以得到:

$$\bigcap_{j \in J} S_j = \{ \alpha \in \mathbb{F}_{q^n} : R(\alpha) = 0 \}.$$

由欧拉函数性质得:

$$\sum_{c | \frac{n}{kp_{j_1} \cdots p_{j_r}}} \phi(c) = n / (kp_{j_1} \cdots p_{j_r}),$$

从而 $R(x)$ 的次数为:

$$q^{\sum_{c | \frac{n}{kp_{j_1} \cdots p_{j_r}}} \phi(c)} = q^{\frac{kn}{kp_{j_1} \cdots p_{j_r}}} = q^{\frac{n}{p_{j_1} \cdots p_{j_r}}},$$

由上可知, $R(x)$ 有 $q^{n/(p_{j_1} \cdots p_{j_r})}$ 个单根, 式(7)得证. 设

$$G(x) = K(x) \otimes (x^{q^k} - x)^{\otimes p^{e_2}-1} \otimes \bigotimes_{1 < c | m_2} \Psi_c(x)^{\otimes p^{e_2}},$$

其中 $K(x)$ 为 $K_y(x)$, $y \in M$ 的符号最大公因子.

由定义 4 得:

$$\bigcap_{y \in M} A_y = \{ \alpha \in \mathbb{F}_{q^n} : G(\alpha) = 0 \}.$$

由于 $K_y(x)$, $y \in M$ 为 $x^{q^k} - x$ 的符号极大因子, 故 $K(x)$ 的次数为 $q^{k-\tau(y_{i_1})-\tau(y_{i_2})-\cdots-\tau(y_{i_l})}$, 从而 $G(x)$ 的次数为:

$$q^{k-\tau(y_{i_1})-\tau(y_{i_2})-\cdots-\tau(y_{i_l})+n-k} = q^{n-\tau(y_{i_1})-\tau(y_{i_2})-\cdots-\tau(y_{i_l})},$$

即式(8)得证.

令 $T = \left(\bigcap_{j \in J} S_j \right) \cap \left(\bigcap_{y \in M} A_y \right)$, 集合 T 运用类似的方法即可得式(9).

当 $p \notin J$ 时,

$$R(x) = (x^{q^k} - x)^{\otimes p^{e_2}} \otimes \bigotimes_{1 < c | \frac{m_2}{p_{j_1} \cdots p_{j_r}}} \Psi_c(x)^{\otimes p^{e_2}},$$

由于 $p^{e_2} - 1 < p^{e_2}$, 所以

$$T = \left\{ \alpha \in \mathbb{F}_{q^n} : K(\alpha) \otimes (\alpha^{q^k} - \alpha)^{\otimes p^{e_2}-1} \otimes \bigotimes_{1 < c | \frac{m_2}{p_{j_1} \cdots p_{j_r}}} \Psi_c(\alpha)^{\otimes p^{e_2}} = 0 \right\},$$

则 T 中元素个数为:

$$q^{k-\tau(y_{j_1})-\tau(y_{j_2})-\cdots-\tau(y_{j_l})+k \left[p^{e_2}-1+(\frac{m_2}{p_{j_1} \cdots p_{j_r}}-1)p^{e_2} \right]} = q^{\frac{n}{p_{j_1} \cdots p_{j_r}}-\tau(y_{j_1})-\tau(y_{j_2})-\cdots-\tau(y_{j_l})}.$$

当 $p \in J$ 时, 不妨令 $p = p_{j_r}$, 则有:

$$p^{e_2-1} < p^{e_2} - 1, \\ R(x) = (x^{q^k} - x)^{\otimes p^{e_2-1}} \otimes \bigotimes_{1 < c | \frac{m_2}{p_{j_1} \cdots p_{j_{r-1}}}} \Psi_c(x)^{\otimes p^{e_2-1}},$$

所以

$$T = \left\{ \alpha \in \mathbb{F}_{q^n} : (\alpha^{q^k} - \alpha)^{\otimes p^{e_2-1}} \otimes \bigotimes_{1 < c | \frac{m_2}{p_{j_1} \cdots p_{j_{r-1}}}} \Psi_c(\alpha)^{\otimes p^{e_2-1}} = 0 \right\},$$

则 T 中元素个数为:

$$q^{k \left[p^{e_2-1} + (\frac{m_2}{p_{j_1} \cdots p_{j_{r-1}}} - 1)p^{e_2-1} \right]} = q^{n/(p_{j_1} \cdots p_{j_r})}.$$

引理 6 $G_{n,k} = \{ \alpha \in \mathbb{F}_{q^n} : L(\alpha) \neq 0, \forall L(x) \in H \},$

其中:

$$H = \bigcup_{G(x)} \left\{ G(x) \otimes (x + x^{q^k} + \cdots + x^{q^{n-k}}) \right\}. \\ \bigcup_r \{ x^{q^{n/r}} - x \},$$

这里 $G(x)$ 遍历 $x^{q^k} - x$ 的所有符号真因子, r 遍历 n/k 的所有素因子.

定理 6

$$|G_{n,k}| = q^{-m_1} \sum_{c | \frac{m}{m_1}} \mu(c) q^{n/c} \prod_{d | m_1} (q^{\tau(d)} - 1)^{\phi(d)/\tau(d)}.$$

证明 已设 $n = mp^e$, 其中 $p \nmid m$. 设 $k = m_1 p^{e_1}$,

其中 $m_1 | m, e \geq e_1 \geq 0$.

$$\mathcal{L}(n/k) = \{ p_1 \neq p, \cdots, p_{u-1} \neq p, p_u = p \}$$

为 n/k 不同素因子的集合. 记 $S_i = S_{p_i} (i = 1, \cdots, u)$.

$$\mathfrak{B}(m_1) = \{ 1, \cdots, d_1, d_2, \cdots, d_{\phi(d)/\tau(d)}, \cdots, \\ m_1, \cdots, m_{\phi(m_1)/\tau(m_1)} \} = \{ y_1, \cdots, y_{l_1} \},$$

其中: $d | m_1, l_1 = \sum \frac{\phi(d)}{\tau(d)}$, 记

$$A_j = A_{y_j} (j = 1, \cdots, l_1), \text{ 令}$$

$$\alpha \in \mathbb{F}_{q^n} \setminus \left(\left(\bigcup_{i=1}^u S_i \right) \bigcup \left(\bigcup_{j=1}^{l_1} A_j \right) \right).$$

由注 1 可知, $\mathbb{F}_{q^k}$ 上 α 的极小多项式的次数是

n/k , 即 $\mathbb{F}_{q^k}(\alpha) = \mathbb{F}_{q^n}$, 且有 $Tr_k^n(\alpha) \in \mathfrak{N}_k$, 所以有:

$$|G_{n,k}| = \left| \mathbb{F}_{q^n} \setminus \left(\left(\bigcup_{i=1}^u S_i \right) \bigcup \left(\bigcup_{j=1}^{l_1} A_j \right) \right) \right|. \quad (10)$$

由容斥原理和引理 5 可得:

$$\begin{aligned} & \left| \mathbb{F}_{q^n} \setminus \left(\left(\bigcup_{i=1}^u S_i \right) \bigcup \left(\bigcup_{j=1}^{l_1} A_j \right) \right) \right| = q^n - \sum_{i=1}^{u-1} q^{\frac{n}{p_i}} - q^{\frac{n}{p}} - \\ & \sum_{j=1}^{l_1} q^{n-\tau(y_j)} + \sum_{1 \leq j_1 < j_2 \leq u-1} q^{\frac{n}{p_{j_1} p_{j_2}}} + \sum_{i=1}^{u-1} q^{\frac{n}{p_i p}} + \\ & \sum_{j=1}^{l_1} \sum_{i=1}^{u-1} q^{\frac{n}{p_i} - \tau(y_j)} + q^{\frac{n}{p}} + \sum_{1 \leq j_1 < j_2 \leq l_1} q^{n-\tau(y_{j_1})-\tau(y_{j_2})} - \\ & \sum_{1 \leq j_1 < j_2 < j_3 \leq u-1} q^{\frac{n}{p_{j_1} p_{j_2} p_{j_3}}} - \sum_{1 \leq j_1 < j_2 \leq u-1} q^{\frac{n}{p_{j_1} p_{j_2} p}} - \\ & \sum_{j=1}^{l_1} \sum_{1 \leq j_1 < j_2 \leq u-1} q^{\frac{n}{p_{j_1} p_{j_2}} - \tau(y_j)} - \sum_{i=1}^{u-1} \sum_{1 \leq j_1 < j_2 \leq l_1} q^{\frac{n}{p_i} - \tau(y_{j_1}) - \tau(y_{j_2})} - \\ & \sum_{i=1}^{u-1} q^{\frac{n}{p_i p} - \tau(y_j)} - \sum_{1 \leq j_1 < j_2 < j_3 \leq l_1} q^{n-\tau(y_{j_1})-\tau(y_{j_2})-\tau(y_{j_3})} + \cdots + \\ & (-1)^{u+l_1-1} \left(\sum_{1 \leq j_1 < \cdots < j_{u-2} \leq u-1} q^{\frac{n}{p_{j_1} \cdots p_{j_{u-2} p}}} + \right. \\ & \left. q^{\frac{n}{p_{j_1} \cdots p_{j_{u-1}} - \tau(y_1) - \tau(y_2) - \cdots - \tau(y_{l_1})}} + l_1 q^{\frac{n}{p_{j_1} \cdots p_{j_u}}} \right) + \\ & (-1)^{u+l_1} q^{\frac{n}{p_{j_1} \cdots p_{j_u}}} = q^n - \sum_{i=1}^{u-1} q^{\frac{n}{p_i}} - \sum_{j=1}^{l_1} q^{n-\tau(y_j)} + \\ & \sum_{1 \leq j_1 < j_2 \leq u-1} q^{\frac{n}{p_{j_1} p_{j_2}}} + \sum_{j=1}^{l_1} \sum_{i=1}^{u-1} q^{\frac{n}{p_i} - \tau(y_j)} + \\ & \sum_{1 \leq j_1 < j_2 \leq l_1} q^{n-\tau(y_{j_1})-\tau(y_{j_2})} - \sum_{1 \leq j_1 < j_2 < j_3 \leq u-1} q^{\frac{n}{p_{j_1} p_{j_2} p_{j_3}}} - \\ & \sum_{j=1}^{l_1} \sum_{1 \leq j_1 < j_2 \leq u-1} q^{\frac{n}{p_{j_1} p_{j_2}} - \tau(y_j)} - \\ & \sum_{i=1}^{u-1} \sum_{1 \leq j_1 < j_2 \leq l_1} q^{\frac{n}{p_i} - \tau(y_{j_1}) - \tau(y_{j_2})} - \\ & \sum_{1 \leq j_1 < j_2 < j_3 \leq l_1} q^{n-\tau(y_{j_1})-\tau(y_{j_2})-\tau(y_{j_3})} + \cdots + \end{aligned}$$

$$\begin{aligned}
& (-1)^{u+l_1-1} q^{\frac{n}{p_1 \cdots p_{u-1}} - \tau(y_1) - \tau(y_2) - \cdots - \tau(y_{l_1})} = \\
& \sum_{c|\frac{n}{m_1}} \mu(c) q^{n/c} + q^{n-m_1} \prod_{d|m_1} (q^{\tau(d)} - 1)^{\phi(d)/\tau(d)} - \\
& q^n + \left(q^n - \sum_{c|\frac{n}{m_1}} \mu(c) q^{n/c} \right) \cdot \\
& \left(1 - q^{-m_1} \prod_{d|m_1} (q^{\tau(d)} - 1)^{\phi(d)/\tau(d)} \right) = \\
& q^{-m_1} \sum_{c|\frac{n}{m_1}} \mu(c) q^{n/c} \prod_{d|m_1} (q^{\tau(d)} - 1)^{\phi(d)/\tau(d)},
\end{aligned}$$

则由式(10), 得到:

$$|G_{n,k}| = q^{-m_1} \sum_{c|\frac{n}{m_1}} \mu(c) q^{n/c} \prod_{d|m_1} (q^{\tau(d)} - 1)^{\phi(d)/\tau(d)}.$$

参考文献:

- [1] Lidl R, Niederreiter H. Finite Fields[M]. Cambridge: Cambridge University Press, 1997.
- [2] Mullen G L, Panario D. Handbook of Finite Fields[M]. London: Chapman and Hall, 2013.
- [3] Perlis S. Normal bases of cyclic fields of prime-power degree[J]. Duke Mathematical Journal, 1942, 9(3):507-517.
- [4] Pei D, Wang C, Omura J. Normal basis of finite field $GF(2^m)$ [J]. IEEE Transactions on Information Theory, 1986, 32(2):285-287.
- [5] Chang Y, Truong T K, Reed I S. Normal bases over $GF(q)$ [J]. Journal of Algebra, 2001, 241(1):89-101.
- [6] Huang H, Han S M, Cao W. Normal bases and irreducible polynomials[J]. Finite Fields and Their Applications, 2018, 50:272-278.
- [7] Hachenberger D. Characterizing normal bases via the trace map[J]. Communications in Algebra, 2004, 32(1):269-277.
- [8] Zan H X, Cao W. Powers of polynomials and bounds of value sets[J]. Journal of Number Theory, 2014, 143:286-292.
- [9] Polverino O, Zullo F. On the number of roots of some linearized polynomials[J]. Linear Algebra and Its Applications, 2020, 601:189-218.
- [10] Polverino O, Zini G, Zullo F. On certain linearized polynomials with high degree and kernel of small dimension[J]. Journal of Pure and Applied Algebra, 2021, 225(2):106491.
- [11] Hu W Y, Zhang Z C, Tu Z H, et al. Efficient computation of the nearest polynomial by linearized alternating direction method[J]. Applied Mathematics and Computation, 2021, 395:125860.
- [12] von zur Gathen J, Giesbrecht M. Constructing normal bases in finite fields[J]. Journal of Symbolic Computation, 1990, 10(6):547-570.

Linearized polynomials and normal bases in finite fields

XU Biyun¹, XIAO Yili¹, CAO Wei^{2*}

(1.School of Mathematics and Statistics, Ningbo University, Ningbo 315211, China;

2.School of Mathematics and Statistics, Minnan Normal University, Zhangzhou 363000, China)

Abstract: Let $\mathbb{F}_q$ be the finite field of q elements, and $\mathbb{F}_{q^n}$ be its extension of degree n . A normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ is a basis of the form $\{\alpha, \alpha^q, \dots, \alpha^{q^{n-1}}\}$ and α is called a normal element of $\mathbb{F}_{q^n}/\mathbb{F}_q$. For a positive divisor k of n , let $\mathcal{N}_k$ denote the set of all the normal elements of $\mathbb{F}_{q^k}/\mathbb{F}_q$, $G_{n,k}$ denote the set of $\alpha \in \mathbb{F}_{q^n}$ satisfying $\mathbb{F}_{q^k}(\alpha) = \mathbb{F}_{q^n}$ and $\sum_{j=0}^{n/k-1} \alpha^{q^{kj}} \in \mathcal{N}_k$. In this paper, we provide the counting formulae for $\mathcal{N}_n$ and $G_{n,k}$ using properties of linearized polynomials in finite fields.

Key words: finite field; normal basis; linearized polynomial

(责任编辑 史小丽)