

广义对角多项式的指数和

韩山猛, 曹 炜*

(宁波大学 理学院, 浙江 宁波 315211)

摘要: 指数和是数论中的重要研究对象. 本文研究了有限域上的广义对角多项式的两类指数和, 通过次数矩阵的 Smith 标准形, 得到了它们在特殊情形下的具体表达式.

关键词: 有限域; 多项式; 指数和; L-函数

中图分类号: O156.1

文献标志码: A

文章编号: 1001-5132 (2018) 05-0073-04

设 $\mathbb{F}_q$ 是含有 q 个元素的有限域, 其中 $q = p^h$, $h \geq 1$, p 是一个素数, $\mathbb{F}_q^*$ 为其乘法群. 对给定的正整数 r , 用 $\mathbb{F}_{q^r}$ 表示 $\mathbb{F}_q$ 的 r 次扩域. 设 $f(x_1, \dots, x_n) \in \mathbb{F}_q[x_1, \dots, x_n]$, 定义两类指数和如下:

$$S_r^*(f) = \sum_{x_1, \dots, x_n \in \mathbb{F}_{q^r}^*} \xi_p^{\text{Tr}_r(f(x_1, \dots, x_n))},$$

$$S_r(f) = \sum_{x_1, \dots, x_n \in \mathbb{F}_{q^r}} \xi_p^{\text{Tr}_r(f(x_1, \dots, x_n))},$$
(1)

它们对应的 L-函数分别为:

$$L^*(f, s) = \exp\left(\sum_{r=1}^{\infty} (S_r^*(f) \frac{s^r}{r})\right),$$

$$L(f, s) = \exp\left(\sum_{r=1}^{\infty} (S_r(f) \frac{s^r}{r})\right),$$
(2)

其中, ξ_p 为一个复本原单位根, Tr_r 表示从 $\mathbb{F}_{q^r}$ 到 $\mathbb{F}_p$ 的绝对迹映射. L-函数蕴藏着深刻的算术信息, 是现代数论研究中的热点之一^[1-2]. 由 Dwork-Bombieri-Grothendieck 定理可知, $L^*(f, s)$ 是有理函数, 即

$$L^*(f, s) = \prod_{i=1}^{d_1} (1 - \alpha_i s) / \prod_{j=1}^{d_2} (1 - \beta_j s), \quad (3)$$

其中, 有限多个零点 $\alpha_i (1 \leq i \leq d_1)$ 和极点 $\beta_j (1 \leq j \leq d_2)$ 是非零的代数整数; 等价地, 对于每个正整数 r , 均有以下公式成立:

$$S_r^*(f) = \sum_{j=1}^{d_2} \beta_j^r - \sum_{i=1}^{d_1} \alpha_i^r. \quad (4)$$

$L(f, s)$ 和 $S_r(f)$ 也有类似的结论. 用 $N_q^*(f)$ 和

$N_q(f)$ 分别表示方程 $f = 0$ 在 $\mathbb{F}_q^*$ 和 $\mathbb{F}_q$ 中解的个数, 它们与上面定义发指数和及其 L-函数联系密切. 由于在一般情形下很难给出 $N_q(f)$ 和 $N_q^*(f)$, 因而人们寻找其在特定情形下的表达式, 或某种形式的估计. 著名 Chevalley-Waring 定理给出 P-adic 估计: 若 $n > d$, 则 $p \nmid N_q(f)$. Ax^[3]改进 Chevalley-Waring 定理, 他证明了 $\text{ord}_q N_q(f) \geq \lceil (n-d)/d \rceil$, 其中 $\lceil x \rceil$ 为不小于 x 的最小整数, ord_q 是 q 进制加法赋值, 满足 $\text{ord}_q q = 1$. 1997 年, 孙琦^[4]给出了下列形式的方程:

$$a_1 x_1^{d_{11}} \cdots x_n^{d_{n1}} + \cdots + a_n x_1^{d_{1n}} \cdots x_n^{d_{nn}} = c,$$

在满足 $\gcd(\det(D_f), q-1) = 1$ 下的解数公式, 其中 $D_f = (d_{ij})_{1 \leq i, j \leq n}$, $a_i \in \mathbb{F}_q^*$, $c \in \mathbb{F}_q$, $d_{ij} \in \mathbb{Z}_{\geq 0}$. 2007 年, 曹炜和孙琦^[5]推广了上述结论, 给出方程:

$$a_1 x_1^{d_{11}} \cdots x_n^{d_{n1}} + \cdots + a_m x_1^{d_{1m}} \cdots x_n^{d_{nm}} = c,$$

在其次数矩阵满足特定奇异条件下的解数公式, 其中, $a_i \in \mathbb{F}_q^*$, $c \in \mathbb{F}_q$, $d_{ij} \in \mathbb{Z}_{\geq 0}$, $m \leq n$. 2009 年, Cao^[6]发现增广次数矩阵的 Smith 标准形可以用来计算有限域上超曲面上有理点的个数, 并且给出了当其最大不变因子与 $q-1$ 互素时有理点的个数公式. 2013 年, Chen 等^[7]利用 Smith 标准形给出了 $N_q^*(f)$ 的一个估计.

2017 年, 韩山猛等^[8]研究了有限域上一类多项式的指数和 $S_r^*(f)$ 与 $S_r(f)$ 及其相应的 L-函数 $L^*(f, s)$ 与 $L(f, s)$, 并给出了它们的具体表达式.

收稿日期: 2017-08-09.

宁波大学学报(理工版)网址: <http://journalg.nbu.edu.cn/>

基金项目: 国家自然科学基金(11371208); 浙江省自然科学基金(LY17A010008); 宁波市自然科学基金(2017A610134).

第一作者: 韩山猛(1991-), 男, 河南信阳人, 在读硕士研究生, 主要研究方向: 数论. E-mail: 3095325129@qq.com

*通信作者: 曹炜(1974-), 男, 湖北潜江人, 博士/教授, 主要研究方向: 数论与密码学. E-mail: caowei@nbu.edu.cn

本文将考虑如下形状的广义对角多项式:

$$\sum_{i=1}^t \sum_{j_i=m_{i-1}+1}^{m_i} a_{j_i} x_{n_{i-1}+1}^{d_{n_{i-1}+1,j_i}} \cdots x_{n_i}^{d_{n_i,j_i}} = c, \quad (5)$$

其中, $t > 0, 0 = n_0 < n_1 < \cdots < n_t, 0 = m_0 < m_1 < \cdots < m_t$, $a_{j_i} \in \mathbb{F}_{q^r}^*, c \in \mathbb{F}_{q^r}$. 显然, 当 $n_i = m_i = 1 (1 \leq i \leq t)$ 时, 式(5)就是一般的简单对角多项式. 因此, 我们将研究形如式(5)的广义对角多项式的指数和, 并通过次数矩阵的 Smith 标准形, 得到它们在特殊情形下的具体表达式.

1 预备知识

首先给出有关广义对角多项式的次数矩阵、分块矩阵及 Smith 标准形的定义及引理, 它们是本文研究指数和的重要工具.

定义 1 设广义对角多项式 $f(x_1, \cdots, x_{n_t}) \in \mathbb{F}_q[x_1, \cdots, x_{n_t}]$ 有如下稀疏表达式:

$$f(x_1, \cdots, x_{n_t}) = \sum_{i=1}^t f_i(x_{n_{i-1}+1}, \cdots, x_{n_i}) = \sum_{i=1}^t \sum_{j_i=m_{i-1}+1}^{m_i} a_{j_i} x_{n_{i-1}+1}^{d_{n_{i-1}+1,j_i}} \cdots x_{n_i}^{d_{n_i,j_i}} = \sum_{i=1}^t \sum_{j_i=m_{i-1}+1}^{m_i} a_{j_i} X^{V_{j_i}},$$

其中,

$$f_i(x_{n_{i-1}+1}, \cdots, x_{n_i}) \in \mathbb{F}_q[x_{n_{i-1}+1}, \cdots, x_{n_i}],$$

$$V_{j_i} = (d_{n_{i-1}+1,j_i}, \cdots, d_{n_i,j_i})^T \in \mathbb{Z}_{\geq 0}^{n_i - n_{i-1}},$$

$$X^{V_{j_i}} = x_{n_{i-1}+1}^{d_{n_{i-1}+1,j_i}} \cdots x_{n_i}^{d_{n_i,j_i}},$$

$$0 = m_0 < m_1 < \cdots < m_t, a_{j_i} \in \mathbb{F}_{q^r}^*,$$

$$0 = n_0 < n_1 < \cdots < n_t, t > 0, c \in \mathbb{F}_q, i = 1, \cdots, t.$$

定义 f_i 的次数矩阵为:

$$D_i = (V_{m_{i-1}+1}, \cdots, V_{m_i}) = (d_{s_i, k_i})_{n_{i-1}+1 \leq s_i \leq n_i, m_{i-1}+1 \leq k_i \leq m_i},$$

则 f 的次数矩阵为 $D_f = \text{diag}(D_1, \cdots, D_t)$, 即除对角线上的块矩阵 D_i 外, 其余元素均为零.

对于任意环 R , 用 $\text{GL}_n(R)$ 表示 R 上阶为 n 的一般线性群, 即 R 上所有 $n \times n$ 阶可逆方阵关于矩阵乘法构成的群. 特别地, 当 $R = \mathbb{Z}$ 时, $\text{GL}_n(\mathbb{Z})$ 里的元素称为幺模矩阵. 设 $f \in \mathbb{F}_q[x_1, \cdots, x_{n_t}]$, 考虑其次数矩阵 D , 由于对任意的 $a \in \mathbb{F}_q$, 有 $a^q = a$, 因此不妨将 D 看成是剩余类环 $\mathbb{Z}_{q-1}$ 上的一个矩阵. 若 D 在 $\mathbb{Z}_{q-1}$ 上可逆, 则记为 $D \in \text{GL}_{n_t}(\mathbb{Z}_{q-1})$.

引理 1^[8] 设 $A \in \mathbb{Z}^{n \times m}$ 的秩为 k , 则存在 2 个

幺模矩阵 $H \in \text{GL}_n(\mathbb{Z})$ 和 $K \in \text{GL}_m(\mathbb{Z})$ 使得 $HAK = (\lambda_{ij})$, 其中, $\lambda_{ij} = 0$ 若 $i \neq j$, 对角元 $\lambda_i := \lambda_{ii}$ 满足 $\lambda_i | \lambda_{i+1}, \lambda_i > 0$, 这里, $1 \leq i \leq k-1$, 且 $\lambda_k > 0$.

上面引理 1 中的 $\lambda_i (1 \leq i \leq k)$ 由 A 唯一确定, 称为 A 第 i 个不变因子, HAK 称为 A 的 Smith 标准形, 记为 $\text{SNF}(A)$.

引理 2^[8] 设 A 为整数矩阵. 则方程组 $AX = 0$ 和 $\text{SNF}(A)Y = 0$ 的整数解之间存在一一对应关系. 特别地, $AX = 0$ 只有零解当且仅当 $\text{SNF}(A)Y = 0$ 只有零解.

引理 3^[8] $D_i X_i \equiv 0 \pmod{q^r - 1}$ 只有零解当且仅当 $\text{SNF}(D_i)Y_i \equiv 0 \pmod{q^r - 1}$ 只有零解.

关于两类高斯和的定义和性质简单介绍如下. 设 ω 是乘法群 $\mathbb{F}_{q^r}^*$ 上的 Teichmüller 特征, 对于任意的 $a \in \mathbb{F}_{q^r}^*$, $\omega(a)$ 是 $q^r - 1$ 次复单位根. Tr_r 为从 $\mathbb{F}_{q^r}$ 到素域 $\mathbb{F}_p$ 上的迹映射. 特征 ω 具有如下的正交性质:

$$\sum_{a \in \mathbb{F}_{q^r}^*} \omega(a)^l = \begin{cases} 0, & \text{若 } (q^r - 1) \nmid l, \\ q^r - 1, & \text{若 } (q^r - 1) | l. \end{cases} \quad (6)$$

为将 Teichmüller 特征 ω 推广到 $\mathbb{F}_{q^r}$ 上, 定义 $\omega^0(0) = 1, \omega^l(0) = 0$, 若 $l > 0$, 则由(6)式可得:

$$\sum_{a \in \mathbb{F}_{q^r}^*} \omega(a)^l = \begin{cases} 0, & \text{若 } (q^r - 1) \nmid l, \\ q^r - 1, & \text{若 } (q^r - 1) | l, l \neq 0, \\ q^r, & \text{若 } l = 0. \end{cases} \quad (7)$$

定义高斯和 $G_r(l) = -\sum_{a \in \mathbb{F}_{q^r}^*} \omega(a)^{-l} \zeta_p^{\text{Tr}_r(a)}, 0 \leq l \leq q^r - 2$. 易知 $G_r(0) = 1$. 可以验证, 对所有的 $a \in \mathbb{F}_{q^r}^*$, 有

$$\zeta_p^{\text{Tr}_r(a)} = \sum_{l=0}^{q^r-2} \frac{G_r(l)}{1 - q^r} \omega(a)^l. \quad (8)$$

类似地, 定义高斯和为:

$$g_r(l) = \sum_{a \in \mathbb{F}_{q^r}^*} \omega(a)^{-l} \zeta_p^{\text{Tr}_r(a)}, \quad 1 \leq l \leq q^r - 2.$$

令 $g_r(0) = q^r - 1, g_r(q^r - 1) = -q^r$, 则对所有的 $\alpha \in \mathbb{F}_{q^r}^*$, 有

$$\zeta_p^{\text{Tr}_r(a)} = \sum_{l=0}^{q^r-1} \frac{g_r(l)}{q^r - 1} \omega(a)^l. \quad (9)$$

2 主要结论

2.1 第一类指数和 $S_r^*(f)$

首先我们研究广义对角多项式的第一类指数

和 $S_r^*(f)$.

定理 1 设 f 为形如式(5)的广义对角多项式. 则

$$S_r^*(f) = (-1)^{m_t} (q^r - 1)^{n_t - m_t} \cdot$$

$$\prod_{i=1}^t \sum \left(\prod_{j_i=m_{i-1}+1}^{m_i} \omega(\alpha_{j_i})^{l_{j_i}} G_r(l_{j_i}) \right),$$

其中, 和号遍历所有的向量 $\mathbf{I}_i = (l_{m_{i-1}+1}, \dots, l_{m_i}), 0 \leq l_{j_i} \leq q^r - 2 (j_i = m_{i-1} + 1, \dots, m_i)$, 且满足

$$\sum_{j_i=m_{i-1}+1}^{m_i} l_{j_i} V_{j_i} \equiv 0 \pmod{q^r - 1}.$$

证明 利用式(6)和式(8), 有

$$\begin{aligned} S_r^*(f) &= \sum_{x_1, \dots, x_{n_t} \in \mathbb{F}_{q^r}^*} \xi_p^{\text{Tr}_r(f(x_1, \dots, x_{n_t}))} = \\ &= \sum_{x_1, \dots, x_{n_t} \in \mathbb{F}_{q^r}^*} \prod_{i=1}^t \prod_{j_i=m_{i-1}+1}^{m_i} \xi_p^{\text{Tr}_r(a_{j_i} X^{V_{j_i}})} = \\ &= \prod_{i=1}^t \left(\sum_{x_{n_{i-1}+1}, \dots, x_{n_i} \in \mathbb{F}_{q^r}^*} \prod_{j_i=m_{i-1}+1}^{m_i} \sum_{l_{j_i}=0}^{q^r-2} \frac{G_r(l_{j_i})}{1-q^r} \right. \\ &\quad \left. \omega(a_{j_i})^{l_{j_i}} \omega(X^{V_{j_i}})^{l_{j_i}} \right) = \\ &= \prod_{i=1}^t \left(\sum_{j_i=m_{i-1}+1}^{m_i} \sum_{l_{j_i}=0}^{q^r-2} \left(\prod_{j_i=m_{i-1}+1}^{m_i} \frac{G_r(l_{j_i})}{1-q^r} \omega(\alpha_{j_i})^{l_{j_i}} \right) \right. \\ &\quad \left. \sum_{x_{n_{i-1}+1}, \dots, x_{n_i} \in \mathbb{F}_{q^r}^*} \omega(X^{l_{m_{i-1}+1} V_{m_{i-1}+1} + \dots + l_{m_i} V_{m_i}}) \right) = \\ &= \prod_{i=1}^t (-1)^{m_i - m_{i-1}} (q^r - 1)^{n_i - m_i - (n_{i-1} - m_{i-1})} \cdot \\ &\quad \sum \left(\prod_{j_i=m_{i-1}+1}^{m_i} \omega(\alpha_{j_i})^{l_{j_i}} G_r(l_{j_i}) \right). \end{aligned} \quad (10)$$

定理 1 得证.

由指数和的定义式(1)及定理 1 证明中的式(10)可得推论 1.

推论 1 设 f 为形如式(5)的广义对角多项式. 则有

$$S_r^*(f) = \prod_{i=1}^t (S_r^*(f_i)).$$

注 推论 1 亦可由指数和 $S_r^*(f)$ 的定义式(1)直接推得, 但定理 1 显然给出了比式(1)更明确的表达式(虽然从形式上看更为复杂). 事实上, 当某些 f_i 的次数矩阵满足一定条件时, 可以进一步化简定理 1 中的公式, 也可由引理 3 及定理 1 可得下面

推论 2.

推论 2 设 f 为形如式(5)的广义对角多项式, 次数矩阵为 $\mathbf{D}_f = \text{diag}(\mathbf{D}_1, \dots, \mathbf{D}_t)$. 不失一般情形, 设 $\mathbf{D}_f$ 的前 $r (1 \leq r \leq t)$ 个块矩阵 $\mathbf{D}_i$ 的最大不变因子均与 $q^r - 1$ 互素, 则有

$$S_r^*(f) = (-1)^{m_t} (q^r - 1)^{n_t - m_t} \cdot$$

$$\prod_{i=r+1}^t \sum \left(\prod_{j_i=m_{i-1}+1}^{m_i} \omega(\alpha_{j_i})^{l_{j_i}} G_r(l_{j_i}) \right),$$

其中, 和号遍历所有的向量 $\mathbf{I}_i = (l_{m_{i-1}+1}, \dots, l_{m_i}), 0 \leq l_{j_i} \leq q^r - 2 (j_i = m_{i-1} + 1, \dots, m_i)$, 且满足

$$\sum_{j_i=m_{i-1}+1}^{m_i} l_{j_i} V_{j_i} \equiv 0 \pmod{q^r - 1}.$$

特别地, 若 $r = t$, 即 $\mathbf{D}_f$ 的所有块矩阵 $\mathbf{D}_i$ 的最大不变因子均与 $q^r - 1$ 互素, 则有

$$S_r^*(f) = (-1)^{m_t} (q^r - 1)^{n_t - m_t}.$$

2.2 第二类指数和 $S_r(f)$

下面我们研究广义对角多项式的第二类指数和 $S_r(f)$.

由于这类指数和的变量可取零值, 因而情况比较复杂. 为便于讨论, 我们需要引进更多符号.

令 $\Omega \subseteq \{0, 1, \dots, q^r - 1\}$ 及 $\Omega^{m_t} = \prod_{i=1}^{m_t} \Omega$.

对于给定的一个向量 $\mathbf{I} = (I_1, I_2, \dots, I_t) \in \Omega^{m_t}$, 其中 $\mathbf{I}_i = (l_{m_{i-1}+1}, \dots, l_{m_i}) \in \Omega^{m_i - m_{i-1}}$. 令

$$(v_{n_{i-1}+1}, \dots, v_{n_i})^T := l_{m_{i-1}+1} V_{m_{i-1}+1} + \dots + l_{m_i} V_{m_i},$$

并用 $\sigma(\mathbf{I}_i)$ 和 $s(\mathbf{I}_i)$ 分别表示 $\mathbf{I}_i = (l_{m_{i-1}+1}, \dots, l_{m_i})$ 和 $(v_{n_{i-1}+1}, \dots, v_{n_i})$ 中的非零元的个数.

定理 2 设 f 为形如式(5)的广义对角多项式. 则有

$$S_r(f) = \prod_{i=1}^t \left(\sum (q^r - 1)^{s(\mathbf{I}_i) - (m_i - m_{i-1})} q^{r(n_i - n_{i-1} - s(\mathbf{I}_i))} \cdot \prod_{j_i=m_{i-1}+1}^{m_i} \omega(\alpha_{j_i})^{l_{j_i}} g_r(l_{j_i}) \right),$$

其中, 和号遍历所有的向量

$$\mathbf{I}_i = (l_{m_{i-1}+1}, \dots, l_{m_i}) \in \Omega^{m_i - m_{i-1}},$$

这里, $0 \leq l_{j_i} \leq q^r - 1 (j_i = m_{i-1} + 1, \dots, m_i)$, 且满足

$$\sum_{j_i=m_{i-1}+1}^{m_i} l_{j_i} V_{j_i} \equiv 0 \pmod{q^r - 1}.$$

证明 利用式(7)和式(9), 有

$$S_r(f) = \sum_{x_1, \dots, x_{n_t} \in \mathbb{F}_{q^r}} \xi_p^{\text{Tr}_r(f(x_1, \dots, x_{n_t}))} =$$

$$\sum_{x_1, \dots, x_{n_i} \in \mathbb{F}_{q^r}} \prod_{i=1}^t \prod_{j_i=m_{i-1}+1}^{m_i} \xi_p^{\text{Tr}_r(\sum_{l=1}^t a_{j_i} X^{V_{j_i}})} =$$

$$\prod_{i=1}^t \left(\sum_{x_{n_{i-1}+1}, \dots, x_{n_i} \in \mathbb{F}_{q^r}} \prod_{j_i=m_{i-1}+1}^{m_i} \sum_{l_{j_i}=0}^{q^r-1} \frac{g_r(l_{j_i})}{q^r-1} \cdot \right.$$

$$\omega(a_{j_i})^{l_{j_i}} \omega(X^{V_{j_i}})^{l_{j_i}} =$$

$$\prod_{i=1}^t \left(\sum_{j_i=m_{i-1}+1}^{m_i} \sum_{l_{j_i}=0}^{q^r-1} \left(\prod_{j_i=m_{i-1}+1}^{m_i} \frac{g_r(l_{j_i})}{q^r-1} \omega(\alpha_{j_i})^{l_{j_i}} \right) \right)$$

$$\sum_{x_{n_{i-1}+1}, \dots, x_{n_i} \in \mathbb{F}_{q^r}} \omega(X^{l_{m_{i-1}+1} V_{m_{i-1}+1} + \dots + l_{m_i} V_{m_i}}) =$$

$$\prod_{i=1}^t \left(\sum (q^r-1)^{s(I_i)-(m_i-m_{i-1})} q^{r(n_i-n_{i-1}-s(I_i))} \cdot \right.$$

$$\left. \prod_{j_i=m_{i-1}+1}^{m_i} \omega(\alpha_{j_i})^{l_{j_i}} g_r(l_{j_i}) \right).$$

定理 2 得证.

我们亦可得到类似推论 1 与推论 2 的结论, 在此省略.

参考文献:

- [1] 冯克勤, 廖群英. 有限域及其应用[M]. 大连: 大连理工大学出版社, 2011:57-59.
- [2] Lidl R, Niederreiter H. Finite Fields[M]. UK, Cambridge: Cambridge University Press, 1997:121-136.
- [3] Ax J. Zeros of polynomials over finite fields[J]. American Journal of Mathematics, 1964(2):255-261.
- [4] 孙琦. 有限域上一类方程的解数公式[J]. 数学年刊(A辑), 1997, 18(4):403-408.
- [5] Cao W, Sun Q. On a class of equations with special degrees over finite fields[J]. Acta Arithmetica, 2007, 130(2):195-202.
- [6] Cao W. Smith normal form of augmented degree matrix and its applications[J]. Linear Algebra & its Applications, 2009, 431(10):1778-1784.
- [7] Chen J M, Cao W. Smith normal form of augmented degree matrix and rational points on toric hypersurface[J]. Algebra Colloquium, 2013, 20(2):327-332.
- [8] 韩山猛, 祝美玲, 曹伟. 有限域上多项式的指数和及其 L-函数[J]. 纯粹数学与应用数学, 2017, 33(1):92-110.

Exponential sums of generalized diagonal polynomials

HAN Shan-meng, CAO Wei*

(Faculty of Science, Ningbo University, Ningbo 315211, China)

Abstract: Exponential sums are an important research objective in number theory. In this paper the authors investigate two types of exponential sums of generalized diagonal polynomials over finite fields and obtain their explicit formulas under certain cases using the Smith normal form of degree matrices.

Key words: finite field; polynomial; exponential sum; L-function

(责任编辑 章践立)