

有限域上一类非零迹多项式的计数公式

高伟, 黄华, 曹炜*

(宁波大学 理学院, 浙江 宁波 315211)

摘要: 设 $\mathbb{F}_q$ 为 q 元有限域. $\mathbb{F}_q$ 上 n 次多项式 $f(x)$ 的迹定义为 x^{n-1} 的系数. 本文利用 $\mathbb{F}_q$ 中多项式的普通分解与其线性 q -相伴式的符号分解之间的关系, 研究了 $\mathbb{F}_q$ 上非零迹多项式并得到了一类非零迹多项式的计数公式.

关键词: 有限域; 不可约多项式; 线性化多项式; 符号分解

中图分类号: O156.1

文献标志码: A

文章编号: 1001-5132 (2019) 02-0097-03

设 $\mathbb{F}_q$ 是含 q 个元素的有限域, 其中 $q = p^l$, p 为素数, l 是一个正整数. 用 $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$ 表示 $\mathbb{F}_q$ 中非零元素构成的乘法群, $\mathbb{F}_{q^m}$ 为 $\mathbb{F}_q$ 的 m 次扩张. 众所周知, 有限域上的多项式在密码、编码及组合设计等领域都具有重要应用, 人们对其周期、因式分解及特殊多项式的寻找与判定等问题进行了大量的研究^[1-7]. $\mathbb{F}_q$ 上 n 次多项式 $f(x)$ 的迹定义为 x^{n-1} 的系数. 设 $\gamma \in \mathbb{F}_q^*$, 用 $N_\gamma(n, q)$ 表示 $\mathbb{F}_q$ 上迹为 γ 的 n 次首一不可约多项式的个数. Ruskey 等^[8]通过广义的 Möbius 反演公式得到了 $N_\gamma(n, q)$ 的表达式, 即

$$N_\gamma(n, q) = \frac{1}{qn} \sum_{d|n, p \nmid d} \mu(d) q^{n/d}, \quad (1)$$

其中 $\mu(d)$ 是 Möbius 函数, 定义为 $\mu(d) = 1$ 若 d 无平方因子且有偶数个素因子, $\mu(d) = -1$ 若 d 无平方因子且有奇数个素因子, $\mu(d) = 0$ 若 d 有平方素因子. Carlitz^[9]和 Yucas^[10]分别用不同方法得到形式不同但本质上等价于(1)式的表达式. 我们发现, 有限域上线性化多项式的符号分解在研究非零迹多项式中发挥着独特的作用. 熟知, 由于多项式的系数与其根有着密切的关系, 因而线性化多项式的符号分解亦适用于研究对根有特殊限制的多项式. 我们^[11]利用这一方法对有限域上正规多项式(一类重要不可约多项式, 其根构成正规基)给出了新的刻画. 本文将利用线性化多项式的符号分解, 对 $\mathbb{F}_q$ 上限定其根所在子域且非零迹的多项式做进

一步的研究并得到相关的计数公式(见定理 1).

1 预备知识

首先简要介绍有关线性化多项式及其符号乘积的基本知识, 更多详情参见文献[1, 12-15].

定义 1 若 $L(x) = \sum_{i=0}^n a_i x^{q^i} \in \mathbb{F}_{q^m}[x]$, 则称之为 $\mathbb{F}_{q^m}$ 上的线性化多项式(或 q -多项式).

两个线性化多项式的普通乘积未必仍是线性化多项式. 设 $L_1(x), L_2(x) \in \mathbb{F}_{q^m}[x]$, 定义符号乘积 $L_1(x) \otimes L_2(x) = L_1(L_2(x))$. (2)

显见 $L_1(x) \otimes L_2(x)$ 是一个线性化多项式. $L(x)$ 的 m 次符号幂简记为 $L(x)^{\otimes m}$.

定义 2 设 $L_1(x)$ 和 $L_2(x)$ 是 $\mathbb{F}_q$ 上的 2 个 q -多项式, 如果对于 $\mathbb{F}_q$ 上某个 q -多项式 $L(x)$ 有 $L_2(x) = L_1(x) \otimes L(x)$, 则称 $L_1(x)$ 符号整除 $L_2(x)$ (或 $L_2(x)$ 被 $L_1(x)$ 符号整除).

类似地, 可以定义符号因子(或 q -因子), 符号互素(或 q -互素)与符号不可约多项式(或 q -不可约多项式)等概念. 称 $\mathbb{F}_{q^m}$ 上的多项式 $l(x) = \sum_{i=0}^n c_i x^{q^i}$ 与 $L(x) = \sum_{i=0}^n c_i x^{q^i}$ 互为 q -相伴; 特别地, 称 $L(x)$ 为 $l(x)$ 的线性 q -相伴式.

引理 1 设 $L_1(x)$ 与 $L_2(x)$ 分别是 $\mathbb{F}_q$ 上 $l_1(x)$ 和 $l_2(x)$ 的线性 q -相伴式. 则下列条件等价: (i) $L_1(x)$ 符号整除 $L_2(x)$; (ii) $l_1(x)$ 整除 $l_2(x)$.

更一般地, 假设 $l(x)$ 与 $L(x)$ 互为 q -相伴, 若

收稿日期: 2018-03-12.

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

基金项目: 国家自然科学基金(11871291); 宁波市自然科学基金(2017A610134).

第一作者: 高伟(1995-), 男, 安徽安庆人, 在读硕士研究生, 主要研究方向: 数论. E-mail: 912664929@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: 代数、数论. E-mail: caowei@nbu.edu.cn

$$L(x) = \bigotimes_{i=1}^m L_i(x)^{\otimes k_i}, \quad (3)$$

其中 $L_i(x) (i=1, \dots, m)$ 为 $\mathbb{F}_q$ 上两两符号互素的线性化多项式, 则有

$$l(x) = \prod_{i=1}^m l_i(x)^{k_i}, \quad (4)$$

其中 $L_i(x)$ 是 $l_i(x)$ 的线性 q -相伴式且 $l_i(x)$ 两两互素. 反之, 若已知形如(4)式的 $l(x)$ 的普通分解, 也能得到形如(3)式的 $L(x)$ 的符号分解.

为方便计, 以下总是假设 $n = mp^k$, 其中 $p \nmid m$. 令 $\mathfrak{A}(n) = \{p_1, \dots, p_r\}$ 为 n 的不同素因子的集合, $\phi(\cdot)$ 为欧拉函数. 对于正整数 d , 令 ζ_d 表示 d 次本原单位根, $\psi_d(x) = \prod_{1 \leq i \leq d, (i,d)=1} (x - \zeta_d^i)$ 表示次数为 $\phi(d)$ 的 d 次分圆多项式, $\Psi_d(x)$ 为 $\psi_d(x)$ 的线性 q -相伴式.

引理 2^[5]

$$x^n - 1 = (x^m - 1)^{p^k} = \left(\prod_{d|m} \psi_d(x) \right)^{p^k} = \prod_{d|m} (\psi_d(x))^{p^k}. \quad (5)$$

由引理 1 和引理 2 可得

$$\text{引理 3}^{[5]} \quad x^{q^n} - x = \bigotimes_{d|m} \Psi_d(x)^{\otimes p^k}.$$

定义集合 $A = \{\beta \in \mathbb{F}_{q^n} : \beta + \beta^q + \dots + \beta^{q^{n-1}} = 0\}$, 记 $A_i = A_{p_i}$. 对于每个 $p_i \in \mathfrak{A}(n)$, 则 $A_i = \{\beta \in \mathbb{F}_{q^n} : \beta^{q^{n/p_i}} - \beta = 0\}$.

引理 4

$$A = \{\beta \in \mathbb{F}_{q^n} : (\beta^q - \beta)^{\otimes p^{k-1}} \bigotimes_{1 < d|m} \Psi_d(\beta)^{\otimes p^k} = 0\}, \quad (6)$$

对于 $p_i \in \mathfrak{A}(n)$, 则有

$$A_i = \{\beta \in \mathbb{F}_{q^n} : \bigotimes_{d|m/p_i} \Psi_d(\beta)^{\otimes p^k} = 0\}. \quad (7)$$

特别地, 若 $p_i \neq p$, 则

$$A_i = \{\beta \in \mathbb{F}_{q^n} : \bigotimes_{d|m/p_i} \Psi_d(\beta)^{\otimes p^k} = 0\}, \quad (8)$$

$$A_p = \{\beta \in \mathbb{F}_{q^n} : \bigotimes_{d|m} \Psi_d(\beta)^{\otimes p^{k-1}} = 0\}. \quad (9)$$

证明 由(5)式易得 $x^n - 1 = (x^m - 1)^{p^k} = (x - 1)^{p^k} \cdot \prod_{1 < d|m} (\psi_d(x))^{p^k} = (x - 1)(x - 1)^{p^k - 1} \prod_{1 < d|m} (\psi_d(x))^{p^k}$, 从而

由引理 3 可得(6)式. 类似可以得到(7)~(9)式.

引理 5 假设集合 $J = \{p_{j_1}, \dots, p_{j_t}\}$ 为集合 $\mathfrak{A}(n)$ 的非空子集, 则

$$\left| \bigcap_{j \in J} A_j \right| = q^{n/(p_{j_1} \cdots p_{j_t})}, \quad (10)$$

$|A| = q^{n-1}$, 并且

$$\left| \bigcap_{j \in J} A_j \cap A \right| = \begin{cases} q^{n/(p_{j_1} \cdots p_{j_t})}, & p \in J, \\ q^{n/(p_{j_1} \cdots p_{j_t})-1}, & p \notin J. \end{cases} \quad (11)$$

证明 设 $H(x) = \bigotimes_{d|\frac{n}{p_{j_1} \cdots p_{j_t}}} \Psi_d(x)$, 由引理 4, 有

$\bigcap_{j \in J} A_j = \{\beta \in \mathbb{F}_{q^n} : H(\beta) = 0\}$, 又由欧拉函数的性质,

有 $\sum_{d|\frac{n}{p_{j_1} \cdots p_{j_t}}} \phi(d) = \frac{n}{p_{j_1} \cdots p_{j_t}}$, 因而 $H(x)$ 的次数为

$$q^{\sum_{d|\frac{n}{p_{j_1} \cdots p_{j_t}}} \phi(d)} = q^{\frac{n}{p_{j_1} \cdots p_{j_t}}}. \text{ 由此可知, } H(x) \text{ 有 } q^{\frac{n}{p_{j_1} \cdots p_{j_t}}}$$

个单根, 即(10)式得证. 注意到 $p^{k-1} < p^k - 1$, 对集合 $(\bigcap_{j \in J} A_j) \cap A$ 运用类似的方法可得到(11)式.

2 主要结论

定理 1 设 $n = mp^k$, 其中 $p \nmid m, m \neq 1$. 令 $\mathfrak{A}(n) = \{p_1, \dots, p_r \neq p\}$ 为 n 的不同素因子集合, 则 $\mathbb{F}_q$ 上非零迹且根不在除了 $\mathbb{F}_{q^{n/p_r}}$ 之外的 $\mathbb{F}_{q^n}$ 的任意真子域的 n 次首一多项式的个数为 $\frac{q-1}{qn} \sum_{d|\frac{m}{p_r}} \mu(d) q^{n/d}$.

证明 已知 $n = mp^k$, 其中 $p \nmid m$. 只考虑 $k \geq 1$ 的情形, 其他情形的证明与之类似. 记 $A_i = A_{p_i}$ ($i=1, \dots, r-1$). 令 $\beta \in \mathbb{F}_{q^n} \setminus (\bigcup_{i=1}^{r-1} A_i \cup A)$, 则 β 与其在 $\mathbb{F}_{q^n}$ 中的所有共轭元不在除了 $\mathbb{F}_{q^{n/p_r}}$ 之外的 $\mathbb{F}_{q^n}$ 的任意真子域且其迹非零. 由引理 5 和容斥原理有

$$\begin{aligned} |\mathbb{F}_{q^n} \setminus (\bigcup_{i=1}^{r-1} A_i \cup A)| &= q^n - |\bigcup_{i=1}^{r-1} A_i \cup A| = q^n - \\ & \left(\sum_{i=1}^{r-1} q^{\frac{n}{p_i}} + q^{n-1} - \sum_{1 \leq j_1 < j_2 \leq r-1} q^{\frac{n}{p_{j_1} p_{j_2}}} - \sum_{i=1}^{r-1} q^{\frac{n}{p_i}-1} + \right. \\ & \sum_{1 \leq j_1 < j_2 < j_3 \leq r-1} q^{\frac{n}{p_{j_1} p_{j_2} p_{j_3}}} + \sum_{1 \leq j_1 < j_2 \leq r-1} q^{\frac{n}{p_{j_1} p_{j_2}}-1} - \dots + \\ & \left. (-1)^{r-1} q^{\frac{n}{p_1 \cdots p_{r-1}}-1} \right) = q^n - \sum_{i=1}^{r-1} q^{\frac{n}{p_i}} - q^{n-1} + \\ & \sum_{1 \leq j_1 < j_2 \leq r-1} q^{\frac{n}{p_{j_1} p_{j_2}}} + \sum_{i=1}^{r-1} q^{\frac{n}{p_i}-1} - \\ & \sum_{1 \leq j_1 < j_2 < j_3 \leq r-1} q^{\frac{n}{p_{j_1} p_{j_2} p_{j_3}}} - \sum_{1 \leq j_1 < j_2 \leq r-1} q^{\frac{n}{p_{j_1} p_{j_2}}-1} + \dots - \end{aligned}$$

$$(-1)^{r-1} q^{\frac{n}{p_1 \cdots p_{r-1}} - 1} = \sum_{d \mid \frac{m}{p_r}} \mu(d) q^{n/d} - \sum_{d \mid \frac{m}{p_r}} \mu(d) q^{n/d-1} = \frac{q-1}{q} \sum_{d \mid \frac{m}{p_r}} \mu(d) q^{n/d}.$$

由上讨论可知, $\mathbb{F}_q$ 上非零迹且根不在除了 $\mathbb{F}_{q^{n/p_r}}$ 之外的 $\mathbb{F}_{q^n}$ 的任意真子域的 n 次首一多项式的个数为: $|\mathbb{F}_{q^n} \setminus \bigcup_{i=1}^{r-1} A_i \cup A|/n = \frac{q-1}{qn} \sum_{d \mid \frac{m}{p_r}} \mu(d) q^{n/d}$.

定理 1 得证.

推论 1 设 $\gamma \in \mathbb{F}_q^*$, $n = mp^k$, 其中 $p \nmid m$, $m \neq 1$. 令 $\mathfrak{A}(n) = \{p_1, \dots, p_r \neq p\}$ 为 n 的不同素因子的集合. 则下面的组合不等式成立:

$$\sum_{d \mid \frac{m}{p_r}} \mu(d) q^{n/d} \leq qn N_\gamma(n, q).$$

证明 由定理 1 知, $\frac{q-1}{qn} \sum_{d \mid \frac{m}{p_r}} \mu(d) q^{n/d} \leq \frac{q-1}{qn}$.

$\sum_{d \mid m} \mu(d) q^{n/d} = (q-1) N_\gamma(n, q)$. 结论立得.

参考文献:

- [1] Lidl R, Niederreiter H. Finite Fields[M]. Reading, MA: Addison-Wesley, 1983.
- [2] 韩山猛, 祝美玲, 曹炜. 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):92-101.
- [3] Cao W, Han S M, Wang R Y. Rational points on Fermat curves over finite fields[J/OL]. Journal of Algebra and Its Applications, 2017, 16:1750046 [2017-09-15]. <https://doi.org/10.1142/S0219498817500463>.
- [4] Wang R Y, Wen B B, Cao W. Degree matrices and enumeration of rational points of some hypersurfaces

- over finite fields[J]. Journal of Number Theory, 2017, 177:91-99.
- [5] Zan H X, Cao W. Powers of polynomials and bounds of value sets[J]. Journal of Number Theory, 2014, 143:286-292.
- [6] Zhu M L, Cao W. Invariant factors of degree matrices and L-functions of certain exponential sums[J]. Finite Fields and Their Applications, 2014, 28:188-198.
- [7] Pan X L, Zhao X R, Cao W. A problem of Carlitz and its generalizations[J]. Archiv der Mathematik (Basel), 2014, 102:337-343.
- [8] Ruskey L, Miers C R, Sawada J. The number of irreducible polynomials and Lyndon words with given trace[J]. SIAM Journal on Discrete Mathematics, 2001, 14:240-245.
- [9] Carlitz L. A theorem of Dickson on irreducible polynomial [J]. Proceedings of the American Mathematical Society, 1952, 3:693-700.
- [10] Yucas J L. Irreducible polynomials over finite fields with prescribed trace/prescribed constant term[J]. Finite Fields and Their Applications, 2006, 12:211-221.
- [11] Huang H, Han S M, Cao W. Normal bases and irreducible polynomials[J]. Finite Fields and Their Applications, 2018, 50:272-278.
- [12] Ore O. On a special class of polynomials[J]. Transactions of the American Mathematical Society, 1933, 35:559-584. Errata, ibid, 1934, 36:275.
- [13] Ore O. Theory of non-commutative polynomials[J]. Annals of Mathematics, 1933, 34:480-508.
- [14] Ore O. Contributions to the theory of finite fields[J]. Transactions of the American Mathematical Society, 1934, 36:243-274.
- [15] 陈引兰. 有限域上线性 q -相伴多项式及其应用[J]. 湖北师范学院学报, 2012, 32:1-3.

Counting formula for a class of polynomials with nonzero traces in finite fields

GAO Wei, HUANG Hua, CAO Wei*

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

Abstract: Let $\mathbb{F}_q$ be the finite fields of q elements, and the trace of a degree n polynomial $f(x)$ over $\mathbb{F}_q$ is defined to be the coefficient of x^{n-1} . Using the relationship between the ordinary factorization of a given polynomial and the symbolic factorization of its linearized q -associate, the polynomials with nonzero traces over $\mathbb{F}_q$ is investigated and the counting formula is thus obtained for a class of polynomials with nonzero traces over $\mathbb{F}_q$.

Key words: finite field; irreducible polynomial; linearized polynomial; symbolic factorization

(责任编辑 韩 超)