doi:10. 11920/xnmdzk. 2019. 04. 013

有限域子集上的 Hermite 判别法及推广

郭 异,张起帆
(四川大学数学学院,四川 成都 610064)

摘 要:利用有限生成代数的语言重述关于置换多项式的经典的 Hermite 判别法,并将其推广到有限域的子集上,另外也推广了其他一些关于有限域上置换多项式的结果,并给出了一定条件下相关函数的值集大小估计. 最后,给出主要结果在有限域上 n 阶单位根群中的应用实例,并得到了一些有趣的结果.

关键词:有限域;子集;双射;置换多项式;Hermite 判别法;有限生成代数
中图分类号:O242 **文献标志码**:A **文章编号**:2095-4271(2019)04-0415-07

Hermite Criterion on subsets of finite fields and its generalization

GUO Yi, ZHANG Qi - fan
(School of Mathematics, Sichuan University, Chengdu 610064, P. R. C.)

Abstract: The classical Hermite Criterion for permutation polynomials is rewritten via finite generated algebra, and generalization of the criterion for subsets of finite fields is given. Moreover, generalizations of some other results about permutation polynomials over finite fields are also given, and cardinality of value sets of the related function under specific conditions is estimated. Finally, for a given finite field, some interesting results are obtained for the group of n - th roots of unity by the use of our main theorem.

Key words: finite field; subset; bijection; permutation polynomial; Hermite Criterion; finite generated algebra

在数论研究中,关于有限域的研究占据了相当重要的地位. 有限域在现代数学及计算机科学的多个领域都有着重要的应用. 令 F_q 为 q 元有限域,其中 $q = p^r$,我们自然对 F_q 上的函数及其性质感兴趣. 特别地,对 F_q 上的双射函数,自 19 世纪以来,已有学者进行了大量研究,重要的成果包括 Hermite[1],Dickson[2],Cohen[3],Wan[4],Turnwald[5] 及 Zieve[6-7].

尽管关于有限域 F_q 上的双射已有不少重要成果,关于有限域 F_q 上子集的函数却缺少相关研究. 本文研究重点将集中于有限域 F_q 上子集,通过引入有限生成代数的观点,说明对于有限域 F_q 上子集也有类似有限域上 Hermite 判别法的结论成立,且可将一些基于有限域 F_q 上 Hermite 判别法的研究成果平行地推广到子集上.

1 相关背景回顾

本节主要回顾本文将会用到的已有研究成果与结论. 由于任意一个 F_q 到 F_q 上的函数,都可唯一表示为 F_q 上次数小于 q 的多项式 g,对于有限域上的双射函数自然转化为对置换多项式的研究. 置换多项式的研究已有

收稿日期:2019-04-23
作者简介:郭异(1994-),男,汉族,四川成都人,硕士研究生,研究方向:有限域. E - mail:1814273167@ qq. com
通信作者:张起帆(1966-),男,汉族,重庆涪陵人,教授,硕士生导师,研究方向:有限域. E - mail:zhangqifan@ scu. edu. cn
基金项目:国防应用项目(0020105501055)

相当长的历史. 这一方面的早期结果,参见 Lidl and Niederreiter[8].

称 F_q 上多项式 f 满足第 k 个 Hermite 条件,若成立等式 $\sum_{x\in F_q} f^k(x) = \sum_{x\in F_q} x^k$. 关于置换多项式,有下面的重要结果:

定理 1.1 (Hermite 判别法)

$f(X)$ 是置换多项式 $\Leftrightarrow f$ 满足前 $q-1$ 个 Hermite 条件

由于对有限域 F_q,有正交性:

$$\sum_{x\in F_q} x^k = \begin{cases} 0, & 0 \le k \le q-2 \\ -1, & k = q-1 \end{cases}$$

因此,对 F_q 上多项式 $g(X)$, $\sum_{x\in F_q} g(x)$ 由 $g \bmod X^q - X$ 的 $q-1$ 次项决定. 进而,对 $k \le q-2$, f 满足前 k 个 Hermite 条件等价于 $f^k \bmod X^q - X$ 的次数小于 $q-1$,即有常见版本的 Hermite 判别法:

定理 1.2 (Hermite 判别法,经典形式)

$f(X)$ 是置换多项式 $\Leftrightarrow$ 下列两个条件成立:

1) $f(X)$ 在 F_q 中恰有一个零点.

2) $f^k \bmod X^q - X$ 的次数小于 $q-1$,其中 $1 \le k \le q-2$.

置换多项式,虽然定义简单,但却难于研究. 为此,人们引入了例外多项式的概念来帮助研究置换多项式. 例外多项式(最早由 Davenport and Lewis[9] 提出),基于几何性质定义,更易通过较为深刻的几何工具来帮助研究;基于 Lang - Weil 估计[10] 可知,次数远小于 q 的置换多项式均为例外多项式. 另一方面,由 Davenport and Lewis[9] 猜测,并由 S. D. Cohen[3] 证明了下列重要定理:

定理 1.3 (Cohen, 1970) F_q 上例外多项式都是置换多项式.

进一步的,M. Zieve 等人[6-7] 于 2010 年几乎完全刻画了有限域上例外多项式,取得了对有限域上置换多项式的结构刻画的重大进展.

S. D. Cohen[3] 给出的证明大量利用了群论工具,这使得证明稍显复杂. 其后多人改进/拓展了这个证明,下面列举一些有代表性的相关成果:

K. S. Williams[11-12] 利用 Newton 公式,对大特征情形给出了一个非常简洁的证明. 他得到:

定理 1.4 (Williams,1968). 有限域 F_q 上多项式 $f(X)$ 是置换多项式,当且仅当存在正整数 $m < p$,使得

1) f 满足前 m 个 *Hermite* 条件.

2) $|f(F_q)| \ge q - m$.

推论 1.5 有限域 F_q 上多项式 $f(X)$ 是置换多项式,如果存在正整数 $m < p$,使得

1) $\deg(f) < \dfrac{q-1}{m}$.

2) $|f(F_q)| \ge q - m$.

等价地,有

等价描述 若有限域 F_q 上次数为 d 的多项式 $f(x)$ 不是置换多项式,那么对任意满足 $m < \min\{p, \dfrac{q-1}{d}\}$ 的正整数 m, f 的值集大小 $|f(F_q)| \le q - 1 - m$. 特别地, f 有值集大小上界

$$|f(F_q)| \le q - 1 - [\frac{q-2}{d}].$$

这个上界对于 $q = p$ 的情况相当好,但对于一般情形,Newton 公式可能失效,因而不适用于小特征情形. 1991 年,万大庆[4] 注意到推论 1.5 中条件(1)包含了比定理 1.4 中更多的信息. 充分利用这个条件,万大庆成功将 Williams 的证明提升到了 Newton 公式适用的 p -adic 数域上,从而克服了小特征障碍,给出了 Cohen 定理的

一个新的完整证明. 事实上,他得到了以下结论:

定理 1.6 (Wan)　有限域 F_q 上多项式 $f(X)$ 是置换多项式,如果存在正整数 m ,使得

1) $\deg(f) < \frac{q-1}{m}$.

2) $|f(F_q)| \geq q - m$.

等价地,我们有

等价描述　若有限域 F_q 上次数为 d 的多项式 $f(X)$ 不是置换多项式,那么对任意满足 $m < \frac{q-1}{d}$ 的正整数 m , f 的值集大小 $|f(F_q)| \leq q - 1 - m$. 特别地, f 有值集大小上界

$$|f(F_q)| \leq q - 1 - [\frac{q-2}{d}].$$

最近,张起帆利用线性代数理论推广了 Hermite 判别法. 张起帆注意到,在有限域上 Hermite 判别法恰好可以看作 Newton 公式的补充. 在 Williams 的证明中使用 Hermite 判别法取代 Newton 公式,就可以规避小特征障碍,从而改进了 Williams[12] 的结果,并得到了一个完全线性代数化的初等证明. 事实上,他得到了

定理 1.7 (Zhang)　有限域 F_q 上多项式 $f(X)$ 是置换多项式,当且仅当存在正整数 m ,使得

1) f 满足前 $2m-1$ 个 Hermite 条件.

2) $|f(F_q)| \geq q - m$.

定理 1.8　有限域 F_q 上多项式 $f(X)$ 是置换多项式,当且仅当存在正整数 m ,使得

1) f 满足前 $m-1$ 个 Hermite 条件.

2) f 在 F_q 中有 $(q-m)$ 个单簇点.

其中,称 $a \in F_q$ 为 f 的一个单簇点,若 $f(X) = a$ 在 F_q 中有唯一解.

推论 1.9　有限域 F_q 上多项式 $f(X)$ 是置换多项式,如果存在正整数 m ,使得

1) $\deg f < \frac{q-1}{2m-1}$.

2) $|f(F_q)| \geq q - m$.

等价地,我们有

等价描述　设有限域 F_q 上次数为 d 的多项式 $f(X)$ 不是置换多项式,若存在正整数 m ,使得 f 满足前 $2m-1$ 个 Hermite 条件,那么 f 的值集大小 $|f(F_q)| \leq q - 1 - m$. 特别地,

$$|f(F_q)| \leq q - 1 - [\frac{u_q(f)+1}{2}].$$

其中 $u_q(f)$ 为 f 满足前 k 个 Hermite 条件的最大的 $k \leq q-2$,而且万大庆与张起帆的结果均可导出 Cohen 定理 1.3.

2　一些预备工作

首先介绍一下所要用到的有限生成代数相关知识(详细参见文献[13-14]). 令 K 为一个域,称 A 为域 K 上(有限生成) n 维代数,若 A 既是域 K 上 n 维向量空间,本身又是环,且满足

$$a(\xi\eta) = (a\xi)\eta = \xi(a\eta), \forall \xi, \eta \in K, a \in A.$$

对 $\forall \xi \in A$,存在自然的线性变换 T_ξ :

$$T_\xi : a \to \xi a, \forall a \in K.$$

自然对线性变换 T_ξ ,可以定义(线性代数的)迹 $Tr(T_\xi)$,从而也可以定义 A 中元素 ξ 对于 A/K 的迹为 $Tr(T_\xi)$;进一步地,设线性变换 T_ξ 在取定的某组基 $(\xi_1, \cdots, \xi_n)$ 下有变换矩阵 $M(\xi)$,对应特征值为 $\lambda_1, \cdots, \lambda_n$,

则 ξ 对于 A/K 的迹还可写作:

$$Tr_{A/K}(\xi) = Tr(T_\xi) = Tr(A(\xi)) = \sum_{i=1}^{n} \lambda_i .$$

特别地,令 $K = F_q$,设 $F_q[x]$ 为 F_q 上全体函数的集合,则易验证知 $F_q[x]$ 构成域 F_q 上的 q 维代数,且有同构成立:

$$F_q[x] \cong F_q[X]/(X^q - X).$$

对于 $F_q[x]$ 中函数 $f: x \mapsto f(x)$,直接记为 $f(x)$ 或 f;特别地,F_q 上恒等函数 Id_{F_q} 记作 x.

由上述知,对 $\forall f \in F_q[x]$,可以定义 f 对于 $F_q[x]/F_q$ 的迹;进一步地,对 $F_q[x]$,有一组自然的基 $\delta_i, i = 1, \cdots, q$,此处 $\delta_i(x)$ 为 F_q 中元素 a_i 的特征函数,而在这组基下,f 对应特征值恰为 $f(a_i)$,从而有:

$$Tr_{F_q[x]/F_q}(f) = \sum_{c \in F_q} f(c), \text{特别地 } Tr_{F_q[x]/F_q}(x) = \sum_{c \in F_q} c .$$

利用上述的结果,我们也可重述 Hermite 判别法为:

定理 2.1 (Hermite 判别法,迹形式)

$f(X)$ 是置换多项式 $\Leftrightarrow Tr_{F_q[x]/F_q}(f^k) = Tr_{F_q[x]/F_q}(x^k), k = 1, 2, \cdots, q-1$.

同理,令 S 为有限域 F_q 上一个给定的 n 元子集. 设 A_S 为 S 到 F_q 上的所有函数全体构成的集合,则 A_S 也构成 F_q 上(有限生成)的 n 维代数,且有自然的同构:

$$A_S \cong F_q[X]/(m(X)) .$$

此处 $m(X) = \prod_{s \in S}(x - s)$ 为集合 S 的极小多项式,即零化 S 的次数最小的多项式;进一步地,对 A_S,依然有一组自然的基 $\delta_i, i = 1, \cdots, n$,此处 $\delta_i(x)$ 仍为 S 中元素 s_i 的特征函数,而 f 的对应特征值恰为 $f(s_i)$,从而有:

$$Tr_{A_S/F_q}(f) = \sum_{s \in S} f(s), \text{特别地 } Tr_{A_S/F_q}(x) = \sum_{s \in S} s .$$

之后讨论中,若无特别注明,均将 A_S 中函数 f 对于 A_S/F_q 的迹略写为 $Tr(f)$.

3 主要定理与推论

定理 3.1 对 S 到 F_q 上函数 $f(x)$,有

$f(x)$ 为 S 到 S 上的双射 $\Leftrightarrow Tr(f^k) = Tr(x^k), k = 0, 1, \cdots, 2n-1$.

这里右侧等式中 x 指 S 上的恒等函数

证明 必要性显然,只需证明充分性. 事实上,令 $g \in F_q[X]$ 为满足下列条件的多项式函数:

$$g(x) = \begin{cases} f(x), & x \in S \\ Id_{F_q \backslash S}, & x \in F_q \backslash S \end{cases} \tag{1}$$

那么在此定义下,$g(x)$ 至少有 $(q-n) - n = q - 2n$ 个不动点,且有

$$\begin{aligned} Tr_{F_q[x]/F_q}(g^k) &= Tr_{A_S/F_q}(f^k) + Tr_{A_{F_q \backslash S}/F_q}(Id_{F_q \backslash S}^k) = Tr_{A_S/F_q}(Id_S^k) + Tr_{A_{F_q \backslash S}/F_q}(Id_{F_q \backslash S}^k) = \\ & Tr_{F_q/F_q}(Id_{F_q}^k) = 0, k = 0, 1, \cdots, 2n-1. \end{aligned} \tag{2}$$

由定理 1.8,g 必然是 F_q 上的置换多项式,从而 f 必然是 S 到 S 上的双射.

如果 $S = F_q$,那么定理 3.1 自然导出 F_q 上经典形式的 Hermite 判别法,因而定理 3.1 确为 Hermite 判别法在子集上的推广.

进一步地,利用类似方法,有

定理 3.2 对 S 到 F_q 上函数 $f(x)$,$f(x)$ 是 S 上双射当且仅当存在正整数 m,使得

1) $Tr(f^k) = Tr(x^k), k = 0, 1, \cdots, 2m-1$.

2) $|f(S) \cap S| \geq n - m$.

特别地,限制 f 为 S 到 S 上函数,则 $f(x)$ 是 S 上双射当且仅当存在正整数 m ,使得

1) $Tr(f^k) = Tr(x^k), k = 0,1,\cdots,2m-1.$

2) $|f(S)| \geq n - m.$

证明　同定理 3.1 一样构造多项式函数 $g(x)$,迹等式条件自然成立;只需再注意到

$$|g(F_q)| = |f(S) \cap S| + |F_q \backslash S| \geq n - m + q - n = q - m \tag{3}$$

由定理 1.7 即知 g 必然是 F_q 上的置换多项式,从而 f 必然是 S 到 S 上的双射.

现在考虑次数推论的推广;考虑 f 的 Lagrange 插值多项式 $f_0(X)$,我们有

推论 3.3　对 S 到 F_q 上函数 $f(x)$, $f(x)$ 是 S 上双射,如果存在正整数 $m \leq [\frac{U_f + 1}{2}]$ 满足

1) $\deg f_0 < \frac{U_f}{2m-1}.$

2) $|f(S) \cap S| \geq n - m.$

其中 U_f 是使得 $Tr(x^k) = 0, 1 \leq i \leq k$ 成立的最大的 $k \leq n-2$.

特别地,限制 f 为 S 到 S 上函数,则 $f(x)$ 是 S 上双射,如果存在正整数 m ,使得

1) $\deg f_0 < \frac{U_f}{2m-1}$.

2) $|f(S)| \geq n - m$.

其中 U_f 是使得 $Tr(x^k) = 0, 1 \leq i \leq k$ 成立的最大的 $k \leq n-2$.

证明　注意到 f_0^k 有自然的多项式表示,从而 $Tr(f_0^k)$ 可由 x 的不超过 $k\deg f_0$ 次幂的迹线性表出,而所给条件表明对 $0 \leq k \leq 2m-1$,这些迹均为 0,从而 $Tr(f^k)$ 和 $Tr(x^k)$ 均为 0,满足迹等式条件,从而由定理 3.2 得证.

最后,同置换多项式的情况类似,如果 S 到 F_q 上函数 f 在 S 上不满,且 f 满足前一些迹等式条件,那么 $f(S)$ 不能包含太多 S 中的元素(否则依前述, f 为双射,矛盾). 由此,我们可以将 F_q 中多项式上界估计推广到子集上. 事实上,我们有

推论 3.4　假设函数 $f: S \to F_q$, $f(S) \neq S$. 如果存在正整数 m 使得 $Tr(f^k - x^k) = 0, k = 0,1,\cdots,2m-1$,那么 $f(S)$ 不能包含多于 $n-1-m$ 个 S 中的元素. 特别地,

$$|f(S) \cap S| \leq n - 1 - [\frac{u(f) + 1}{2}].$$

若限制 f 为 S 到 S 上函数,则函数 f 值集大小有上界估计

$$|f(S)| \leq n - 1 - [\frac{u(f) + 1}{2}].$$

其中 $u(f)$ 是使得 $Tr(f^k - x^k) = 0, 1 \leq i \leq k$ 成立的最大的 $k \leq n-2$.

4. 特殊子集上的讨论

作为应用实例,考虑 F_q^* 中 n 阶子群,即 n 次单位根群 $\mu_n < F_q^*$,其中 $n \mid q-1$.(关于 n 次单位根群 μ_n 的其他性质,详情参见文献[15])

μ_n 上所有函数的集合 A_{μ_n} 显然构成 F_q 上有限生成 n 维代数,进一步有自然的同构:

$$A_{\mu_n} \cong F[X]/(X^n - 1) .$$

对子集 μ_n ,有

定理 4.1

$$f(x) \text{ 是 } n \text{ 次单位根群} \mu_n \text{ 上的双射}$$
$$\Leftrightarrow Tr(f^k) = 0, k = 1,2,\cdots,n-1$$
$$\Leftrightarrow f_0^k(X) \bmod X^n - 1 \text{ 无常数项, 其中 } k = 1,\cdots,n-1$$

证明 对 $S = \mu_n$,应用定理3.1,有

$$f(x) \text{ 为} \mu_n \text{ 到} \mu_n \text{ 上的双射} \Leftrightarrow Tr(f^k) = Tr(x^k), k = 0,1,\cdots,2n-1$$

注意到 n 次单位根群 μ_n 是循环群,即 $\mu_n = (\xi_0)$,其中 ξ_0 为 n 次本原单位根,从而只需验证前 n 个迹等式条件成立. $k \neq 0$ 时, $\xi_0^k \neq 1$,从而

$$Tr(x^k) = \sum_{i=0}^{n-1} (\xi_0^k)^i = \frac{(\xi_0^k)^n - 1}{\xi_0^k - 1} = 0. \tag{4}$$

而 $k = 0$ 时 $Tr(x^k) = Tr(f^k) = Tr(1) = n$ 自然成立,从而第一个等价条件成立. 又对插值多项式 $f_0(X) = \sum_{i=0}^{n-1} b_i X^i$,有

$$Tr(f_0) = \sum_{i=0}^{n-1} b_i Tr(x^i) = b_0 Tr(1) = n\, b_0. \tag{5}$$

即知第二个等价条件成立.

特别地,当 $n = q - 1$ 时, $\mu_n = F_q^*$,补充定义 $f(0) = 0$,则上述定理自然导出 Hermite 判别法(定理1.2)

进一步地,我们有推论

推论 4.2 对 μ_n 到 μ_n 上函数 $f(x)$, $f(x)$ 是 μ_n 上双射当且仅当存在正整数 m,使得

1) $Tr(f^k) = 0, k = 1,\cdots,2m-1$.

2) $|f(\mu_n)| \geq n - m$.

等价地,我们有

等价描述 假设函数 $f:\mu_n \to \mu_n$ 不是双射,如果存在正整数 m 使得 $Tr(f^k) = 0, k = 1,\cdots,2m-1$,那么 $f(\mu_n)$ 取值个数不能多于 $n - 1 - m$. 特别地,函数 f 值集大小有上界估计

$$|f(\mu_n)| \leq n - 1 - [\frac{u(f) + 1}{2}].$$

其中 $u(f)$ 是使得 $Tr(f^k) = 0, 1 \leq i \leq k$ 成立的最大的 $k \leq n - 2$.

最后,若插值多项式 f_0 无常数项且次数足够小,那么可以导出与万大庆类似的结果:

推论 4.3 对 μ_n 到 μ_n 上函数 $f(x)$, $f(x)$ 是 μ_n 上双射,如果存在正整数 m,使得

1) $f_0(0) = 0, \deg f_0 < \frac{n-1}{m}$.

2) $|f(\mu_n)| \geq n - m$.

其中 $f_0(X)$ 是 f 在 $\mu_n[x]$ 上的 Lagrange 插值多项式.

等价地,我们有

等价描述 假设函数 $f:\mu_n \to \mu_n$ 不是双射, $d = \deg(f_0)$ 为 Lagrange 插值多项式 $f_0(X)$ 的次数,若 $f_0(0) = 0$,那么对任意满足 $m < \frac{n-1}{d}$ 的正整数 m, $f(\mu_n)$ 取值个数不能多于 $n - 1 - m$. 特别地,函数 f 值集大小有上界估计

$$|f(\mu_n)| \leq n - 1 - [\frac{n-2}{d}].$$

5　结论

通过导入有限生成代数观点,将有限域上 Hermite 判别法成功推广到了其子集上,并在子集上推广了有限域上的函数相关的多个重要结果,并给出了计算实例;为有限域相关的理论在一般子集上的推广提供了一个新思路,主要结果对于有限域上特定子集的函数及自同态相关研究也有一定意义.

参考文献

[1] HERMITE C. Sur les fonctions de sept lettres[J]. Comptes rendus de l'Académie des Sciences,1863,51:750 – 757

[2] DICKSON L E. The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group[J]. Annals of Mathematics, 1897, 11:161 – 183.

[3] COHN S D. The distribution of polynomials over finite fields[J]. Acta Arithmetica, 1970, 17:255 – 271.

[4] WAN D. A p – adic lifting lemma and its applications to permutation polynomials[C]//Proceedings of the International Conference on Finite Fields, Coding Theory and Advances in Communications and Computing, Lecture Notes in Pure and Appl Math, 1992:209 – 216

[5] TURNWALD G. A New Criterion for Permutation Polynomials[J]. Finite Fields and Their Applications, 1995, 1:64 – 82.

[6] GURALNICK R M, ZIEVE M E. Polynomials with PSL(2) monodromy[J]. Annals of Mathematics, 2010, 172 (2):1315 – 1359.

[7] GURALNICK R M, ZIEVE M E. A new family of exceptional polynomials in characteristic two[J]. Annals of Mathematics, 2010, 172 (2): 1361 – 1390.

[8] LIDL R, NIEDERREITER H. Finite Fields[M]. Reading MA: Addison – Wesley, 1983: 347 – 393

[9] DAVENPORT H, LEWIS D J. Notes on congruences(II)[J]. The Quarterly Journal of Mathematics, 1963, 14(2): 51 – 60.

[10] LANG S, WEIL A. Number of Points of Varieties in Finite Fields [J]. American Journal of Mathematics, 1954, 74(4):819 – 827.

[11] WILLIAMS K S. On extremal polynomials[J]. Canadian Mathematical Bulletin, 1967, 10:585 – 594.

[12] WILLIAMS K S. On exceptional polynomials[J]. Canadian Mathematical Bulletin, 1968, 11:279 – 282.

[13] ATIYAH M F, MACDONALD I G. Introduction to commutative algebra[M]. Reading MA: Addison – Wesley Publishing Co – London – Don Mills, Ont, 1969:29 – 30.

[14] 冯克勤. 代数数论[M]. 北京: 科学出版社,2000: 57.

[15] LANG S. Algebra[M]. New York: Springer – Verlag, 2002: 276 – 277.

(责任编辑:付强,张阳,李建忠,罗敏;英文编辑:周序林)