

有限域上 n 元 n 次方程只有零解的充要条件

陈 玺¹, 屈龙江¹, 李 超^{1,2}

(1. 国防科技大学理学院数学与系统科学系, 湖南 长沙 410073)

(2. 信息保障科学与技术实验室, 北京 100072)

摘要: 本文研究了有限域上只有零解的 n 元 n 次方程的结构问题. 利用对有限域上不可约多元多项式在其扩域中的分解特征的刻画, 结合 Chevalley 定理, 得到了有限域上 n 元 n 次方程只有零解的一个充要条件, 并给出这类方程的一些新的具体构造.

关键词: 有限域; 方程只有零解; 多元多项式分解; 不可约多项式

MR(2010) 主题分类号: 12E12; 12E20

中图分类号: O153.4

文献标识码: A

文章编号: 0255-7797(2017)01-0138-07

1 引言

有限域上的多项式理论在编码密码、有限几何、组合设计等领域均有非常重要的应用, 近年来得到了许多学者的关注和研究, 详见文 [1, 2] 及其中的参考文献. 多元多项式方程解数的计算和估计是有限域上多项式理论的重要内容, 在工程实际中应用广泛, 如应用多项式理论构造密码系统、纠错码或者组合设计对象时, 构造对象的参数计算问题往往可以转化为有限域上多项式方程解数的计算问题. 然而, 有限域上多元多项式方程的解的问题一直是困难的数学问题. Chevalley 定理是该方面的一个重要结果: 设 $f \in F_q[x_1, \dots, x_n]$ 且满足 $f(0, \dots, 0) = 0$, $\deg(f(x_1, \dots, x_n)) < n$, 则方程 $f(x_1, \dots, x_n) = 0$ 在 F_q 上有非平凡解, 即存在

$$(c_1, \dots, c_n) \neq (0, \dots, 0), c_k \in F_q, k = 1, \dots, n,$$

使得 $f(c_1, \dots, c_n) = 0$. 但是当 $n = \deg(f(x_1, \dots, x_n))$ 时, 上述结论并不成立. Dickson^[3,4] 给出了如下反例: 设 $n \in \mathbb{Z}^+$, $\{\alpha_1, \dots, \alpha_n\}$ 为 F_{q^n} 在 F_q 上的一组基. 令

$$f(x_1, \dots, x_n) = \prod_{j=0}^{n-1} (\alpha_1^{q^j} x_1 + \dots + \alpha_n^{q^j} x_n),$$

则 $f(x_1, \dots, x_n)$ 为系数在 F_q 上的多项式, 且方程 $f(x_1, \dots, x_n) = 0$ 在 F_q 上只有零解 $(0, \dots, 0)$. 该反例中的函数通常被称为具有范形式, 一个自然的问题是: 有限域上只有零解的 n 元 n 次方程应该具有什么样的特征呢? 能否构造出更多这样的例子呢? Carlitz^[5] 证明了若 $q \geq 13$, $f \in F_q[x_1, x_2, x_3]$ 为一个齐三次多项式, 且满足 f 在 F_q 上仅在 $(0, 0, 0)$ 处为零, 则 f 必然具有范形式. Terjanian^[6] 证明了若 n 次多项式 $f \in F_q[x_1, \dots, x_n]$ 且在 F_q 上仅有

*收稿日期: 2014-03-25

接收日期: 2014-09-09

基金项目: 国家自然科学基金资助 (61272484); 信息保障科学技术实验室开放基金资助 (KJ-12-02).

作者简介: 陈玺 (1990-), 男, 辽宁大连, 硕士, 主要研究方向: 编码密码理论及其应用.

零解, 则对任意次数小于 n 的多项式 $g \in F_q[x_1, \dots, x_n]$, 方程 $f(x_1, \dots, x_n) = g(x_1, \dots, x_n)$ 在 F_q 上至少有一解. Carlitz [7], Felszeghy [8], Francis [9] 等人先后给出了一些有限域上特殊的多元多项式方程的解的个数及解法. 本文是对该问题的一个一般回答. 首先给出了有限域上不可约多元多项式在其扩域中分解特性. 在此基础上, 结合 Chevalley 定理, 得到了有限域上 n 元 n 次多项式方程 $f = 0$ 在 F_q 上只有零解的一个充要条件. 该条件在 f 不是完全不可约的情形下, 更为具体的描述了 f 必须具有范形式.

全文结构如下: 第 2 节刻画了有限域上不可约多元多项式在其扩域中分解特征; 第 3 节给出了有限域上 n 元 n 次多项式方程 $f = 0$ 在 F_q 上只有零解的充要条件, 并给出了一些具体的构造实例; 第 4 节总结并提出有待进一步研究的问题.

2 不可约多元多项式在其扩域中分解特征

为刻画有限域上不可约多元多项式在其扩域中分解特点, 首先引进一些基本概念和相关性质.

定义 1 设 $f(x_1, \dots, x_n) = \sum_{i_1, \dots, i_n} c_{i_1, \dots, i_n} x_1^{i_1} \cdots x_n^{i_n}$ 为有限域 F_{q^N} 上的 n 元多项式. 令

$$f^{(q^j)}(x_1, \dots, x_n) = \sum_{i_1, \dots, i_n} c_{i_1, \dots, i_n}^{q^j} x_1^{i_1} \cdots x_n^{i_n},$$

其中 $j \geq 0$, 即将多项式的每个系数都做 q^j 次提升, 称 $f^{(q^j)}(x_1, \dots, x_n)$ 为 $f(x_1, \dots, x_n)$ 的 q^j 次提升.

由定义直接可得如下结论.

引理 1 $(f_1(x_1, \dots, x_n)f_2(x_1, \dots, x_n))^{(q)} = f_1^{(q)}(x_1, \dots, x_n)f_2^{(q)}(x_1, \dots, x_n)$.

引理 2 $f(x_1, \dots, x_n)$ 不可约当且仅当 $f^{(q)}(x_1, \dots, x_n)$ 不可约.

引理 3 设 $f(x_1, \dots, x_n) \in F_q[x_1, \dots, x_n]$, $f_1(x_1, \dots, x_n) \in F_{q^N}[x_1, \dots, x_n]$ 且满足

$$f_1(x_1, \dots, x_n) \mid f(x_1, \dots, x_n).$$

则 $f_1^{(q)}(x_1, \dots, x_n) \mid f(x_1, \dots, x_n)$. 进一步, $f_1^{(q^j)}(x_1, \dots, x_n) \mid f(x_1, \dots, x_n)$, $0 \leq j \leq N-1$.

证 设 $f(x_1, \dots, x_n) = f_1(x_1, \dots, x_n)H(x_1, \dots, x_n)$, $H(x_1, \dots, x_n) \in F_{q^N}[x_1, \dots, x_n]$. 于是, 由引理 1 有

$$f^{(q)}(x_1, \dots, x_n) = (f_1(x_1, \dots, x_n)H(x_1, \dots, x_n))^{(q)} = f_1^{(q)}(x_1, \dots, x_n)H^{(q)}(x_1, \dots, x_n).$$

另一方面, 由 $f(x_1, \dots, x_n) \in F_q[x_1, \dots, x_n]$ 知 $f(x_1, \dots, x_n) = f^{(q)}(x_1, \dots, x_n)$. 结合两式, 得 $f_1^{(q)}(x_1, \dots, x_n) \mid f(x_1, \dots, x_n)$. 进而对任意非负整数 j ($0 \leq j \leq N-1$), 均有

$$f_1^{(q^j)}(x_1, \dots, x_n) \mid f(x_1, \dots, x_n).$$

定理 1 设 $f(x_1, \dots, x_n)$ 为 F_q 上 n 元 M 次不可约多项式, $f_1(x_1, \dots, x_n)$ 为 F_{q^N} 上 n 元 l 次首一不可约多项式, 且满足 $f_1(x_1, \dots, x_n) \mid f(x_1, \dots, x_n)$. 则有 $l \mid M$, $F_{q^{M/l}}$ 为包含 $f_1(x_1, \dots, x_n)$ 系数的最小域, 且

$$f(x_1, \dots, x_n) = c \prod_{j=0}^{M/l-1} (f_1^{(q^j)}(x_1, \dots, x_n))$$

对某个 $c \in F_q$ 成立.

证 设 t 为使得 $f_1^{(q^t)}(x_1, \dots, x_n) = bf_1(x_1, \dots, x_n)$ 对某个 $b \in F_{q^N}$ 成立的最小正整数. 由 $f_1(x_1, \dots, x_n) = f_1^{(q^N)}(x_1, \dots, x_n)$ 知这样的 t 一定存在. 又因为 $f_1(x_1, \dots, x_n)$ 是首一的, 故 $b = 1$, 即 $f_1^{(q^t)}(x_1, \dots, x_n) = f_1(x_1, \dots, x_n)$. 进一步, F_{q^t} 为包含 $f_1(x_1, \dots, x_n)$ 所有系数的最小域.

由引理 2 和 $f_1(x_1, \dots, x_n)$ 为 $F_{q^N}[x_1, \dots, x_n]$ 中首一不可约多项式知, $f_1^{(q^t)}(x_1, \dots, x_n)$, $j = 0, \dots, t-1$ 均为 $F_{q^N}[x_1, \dots, x_n]$ 中的首一不可约多项式, 因此多项式

$$f_1^{(q^0)}(x_1, \dots, x_n), \dots, f_1^{(q^{t-1})}(x_1, \dots, x_n)$$

两两互素. 由引理 3, 对任意非负整数 j , 有 $f_1^{(q^j)}(x_1, \dots, x_n) \mid f(x_1, \dots, x_n)$, 故

$$\prod_{j=0}^{t-1} f_1^{(q^j)}(x_1, \dots, x_n) \mid f(x_1, \dots, x_n).$$

记 $\tilde{f}(x_1, \dots, x_n) := \prod_{j=0}^{t-1} f_1^{(q^j)}(x_1, \dots, x_n)$, 则 $\tilde{f}(x_1, \dots, x_n) \mid f(x_1, \dots, x_n)$. 于是

$$\begin{aligned} \tilde{f}^{(q)}(x_1, \dots, x_n) &= \prod_{j=0}^{t-1} f_1^{(q^{j+1})}(x_1, \dots, x_n) = f_1^{(q^t)}(x_1, \dots, x_n) \prod_{j=1}^{t-1} f_1^{(q^j)}(x_1, \dots, x_n) \\ &= \tilde{f}(x_1, \dots, x_n). \end{aligned}$$

这表明 $\tilde{f}(x_1, \dots, x_n) \in F_q[x_1, \dots, x_n]$. 再由 $f(x_1, \dots, x_n)$ 在 F_q 上不可约知, 存在 $c \in F_q$, 使得

$$f(x_1, \dots, x_n) = c\tilde{f}(x_1, \dots, x_n) = c \prod_{j=0}^{t-1} (f_1^{(q^j)}(x_1, \dots, x_n)).$$

因此

$$M = \deg(f(x_1, \dots, x_n)) = \deg(\tilde{f}(x_1, \dots, x_n)) = tl.$$

于是 $l \mid M$, 且 $t = M/l$. 由 t 的定义知, 显然 $F_{q^{M/l}}$ 为包含 $f_1(x_1, \dots, x_n)$ 系数的最小域.

3 主要结果

3.1 n 元 n 次方程只有零解时的充要条件

引理 4 (见文 [1, 推论 6.9]) 设 $f_1(x_1, \dots, x_n), \dots, f_m(x_1, \dots, x_n) \in F_q[x_1, \dots, x_n]$, 对 $i = 1, \dots, m$, 满足 $f_i(0, \dots, 0) = 0$, 且

$$\deg(f_1(x_1, \dots, x_n)) + \dots + \deg(f_m(x_1, \dots, x_n)) < n.$$

则存在 $(c_1, \dots, c_n) \neq (0, \dots, 0)$, $c_k \in F_q$, $k = 1, \dots, n$ 使得 $f_i(c_1, \dots, c_n) = 0$ 对 $i = 1, \dots, m$ 成立.

定理 2 设 $f(x_1, \dots, x_n)$ 为 F_q 上 n 元 n 次多项式, 则 $f(x_1, \dots, x_n) = 0$ 在 F_q 上只有零解当且仅当对 n 的某个正因子 l , f 可以表示为如下形式

$$f(x_1, \dots, x_n) = c \prod_{j=0}^{n/l-1} \left(\sum_{i=1}^{n/l} r_i^{q^j} g_i(x_1, \dots, x_n) \right), \quad (3.1)$$

其中 $c \in F_q^*$, $r_1, \dots, r_{n/l}$ 为 $F_{q^{n/l}}$ 在 F_q 上的一组基, 对任意 $1 \leq i \leq n/l$, $g_i(x_1, \dots, x_n)$ 均为 F_q 上 l 次多项式, 而且方程组 $g_i(x_1, \dots, x_n) = 0$, $1 \leq i \leq n/l$, 在 F_q 上只有零解.

证 (充分性) 设 f 如 (3.1) 式表示. 容易验证 $f(x_1, \dots, x_n)$ 确为 F_q 上 n 元 n 次多项式. 下面只需证 $f(x_1, \dots, x_n) = 0$ 在 F_q 上只有零解. 设存在 $(c_1, \dots, c_n)$, 其中 $c_k \in F_q$, $k = 1 \cdots n$, 使得 $f(c_1, \dots, c_n) = 0$. 则由 (3.1) 式知, 存在 $0 \leq r \leq n/l - 1$, 使得

$$\sum_{i=1}^{n/l} r_i^{q^r} g_i(c_1, \dots, c_n) = \left(\sum_{i=1}^{n/l} r_i g_i(c_1, \dots, c_n) \right)^{q^r} = 0.$$

于是 $\sum_{i=1}^{n/l} r_i g_i(c_1, \dots, c_n) = 0$. 由于 $r_1, \dots, r_{n/l}$ 为 $F_{q^{n/l}}$ 在 F_q 上的一组基, 这意味着 $g_i(c_1, \dots, c_n) = 0$, $1 \leq i \leq n/l$. 而由条件知该方程组在 F_q 上只有零解, 于是 $(c_1, \dots, c_n) = (0, \dots, 0)$, 即证明了 $f(x_1, \dots, x_n) = 0$ 在 F_q 上只有零解.

(必要性) 设 $f(x_1, \dots, x_n) = 0$ 在 F_q 上只有零解, 则由 Chevalley 定理知 $f(x_1, \dots, x_n)$ 必在 F_q 上不可约. 假若不然, 设

$$f(x_1, \dots, x_n) = f_1(x_1, \dots, x_n) f_2(x_1, \dots, x_n)$$

为 $f(x_1, \dots, x_n)$ 在 F_q 上的一个非平凡分解, 则有 $f_1(0, \dots, 0) = 0$ 或者 $f_2(0, \dots, 0) = 0$. 不妨设 $f_1(0, \dots, 0) = 0$. 但由 $1 \leq \deg f_1(x_1, \dots, x_n) \leq n - 1$ 和 Chevalley 定理知 $f_1(x_1, \dots, x_n) = 0$ 在 F_q 上必有非零解, 从而 $f(x_1, \dots, x_n) = 0$ 在 F_q 上也有非零解, 矛盾! 从而 $f(x_1, \dots, x_n)$ 必在 F_q 上不可约.

若 $f(x_1, \dots, x_n)$ 完全不可约, 即其在 F_q 的任何扩域上均不可约, 则有 $l = n$, 令 $c = r_1 = 1, g_1 = f$. 于是结论成立.

若 $f(x_1, \dots, x_n)$ 不是完全不可约的, 则存在 F_q 的某个扩域 F_{q^N} 上的 l ($1 \leq l < n$) 次不可约多项式 $f_1(x_1, \dots, x_n)$ 满足 $f_1(x_1, \dots, x_n) \mid f(x_1, \dots, x_n)$. 由定理 1 得 $l \mid n$, $F_{q^{n/l}}$ 为包含 $f_1(x_1, \dots, x_n)$ 系数的最小域, 且

$$f(x_1, \dots, x_n) = c \prod_{j=0}^{n/l-1} (f_1^{(q^j)}(x_1, \dots, x_n)).$$

因为 $f_1(x_1, \dots, x_n)$ 是 F_{q^N} 上的 l 次多项式, 所以存在 $r_1, \dots, r_m$ 为 $F_{q^{n/l}}$ 中一组在 F_q 上线性无关的元素, $g_1(x_1, \dots, x_n), \dots, g_m(x_1, \dots, x_n)$ 为 F_q 上一组次数均不超过 l 的多项式, 使

$$f_1(x_1, \dots, x_n) = \sum_{i=1}^m r_i g_i(x_1, \dots, x_n).$$

于是

$$f(x_1, \dots, x_n) = c \prod_{j=0}^{n/l-1} \left(\sum_{i=1}^m r_i^{q^j} g_i(x_1, \dots, x_n) \right).$$

由 $f(x_1, \dots, x_n) = 0$ 在 F_q 上只有零解知 $f_1(x_1, \dots, x_n) = 0$ 在 F_q 上只有零解, 又因为 $r_1, \dots, r_m \in F_{q^N}$ 在 F_q 上线性无关, 所以方程组 $g_i(x_1, \dots, x_n) = 0, i = 1, \dots, m$ 在 F_q 上只有零解.

因为 $\deg(g_i(x_1, \dots, x_n)) \leq l$, 所以

$$d = \deg(g_1(x_1, \dots, x_n)) + \dots + \deg(g_m(x_1, \dots, x_n)) \leq ml.$$

若 $d < n$, 由引理 4, 方程组 $g_i(x_1, \dots, x_n) = 0, i = 1, \dots, m$ 在 F_q 上有非零解, 矛盾! 所以 $n \geq d \geq ml$.

另一方面, 由 $r_1, \dots, r_m \in F_{q^{n/l}}$ 在 F_q 上线性无关知 $n/l \geq m$. 于是 $m = n/l$, 且等号当且仅当 $\deg(g_1(x_1, \dots, x_n)) = \dots = \deg(g_m(x_1, \dots, x_n)) = l$ 时成立.

综上所述, 此时

$$f(x_1, \dots, x_n) = c \prod_{j=0}^{n/l-1} \left(\sum_{i=1}^{n/l} r_i^{q^j} g_i(x_1, \dots, x_n) \right),$$

其中 $c \in F_q^*$, $g_i(x_1, \dots, x_n) \in F_q[x_1, \dots, x_n]$, $1 \leq i \leq n/l$ 均为 l 次多项式, $r_1, \dots, r_{n/l}$ 为 $F_{q^{n/l}}$ 在 F_q 上的一组基, 而且方程组 $g_i(x_1, \dots, x_n) = 0, 1 \leq i \leq n/l$ 在 F_q 上只有零解.

3.2 应用及举例

例 1 F_3 上的 4 元 4 次多项式

$$\begin{aligned} f(x_1, x_2, x_3, x_4) &= [(x_1 + x_2)^2 + (x_3 + x_4)^2 + \alpha(x_1x_2 + x_3x_4)] \\ &\quad [(x_1 + x_2)^2 + (x_3 + x_4)^2 + \alpha^3(x_1x_2 + x_3x_4)] = 0, \end{aligned}$$

在 F_3 上只有零解, 其中 $\alpha \in F_{3^2} \setminus F_3$.

证 显然 $f(x_1, x_2, x_3, x_4)$ 是 F_3 上的 4 元 4 次多项式. 由于 F_{3^2} 是 F_3 的二次扩张, $\alpha \in F_{3^2} \setminus F_3$, 故 $1, \alpha$ 为 F_{3^2} 在 F_3 上的一组基. 由定理 2 可得, $f(x_1, x_2, x_3, x_4) = 0$ 在 F_3 上只有零解当且仅当方程组

$$\begin{cases} g_1(x_1, x_2, x_3, x_4) = (x_1 + x_2)^2 + (x_3 + x_4)^2 = 0, \\ g_2(x_1, x_2, x_3, x_4) = x_1x_2 + x_3x_4 = 0. \end{cases} \quad (3.2)$$

在 F_3 上只有零解. 注意到 1 是 F_3 上的非平方元, $g_1 = 0$ 当且仅当 $x_1 = -x_2$ 且 $x_3 = -x_4$, 代入 $g_2 = 0$ 得 $-(x_1^2 + x_3^2) = 0$, 从而 $x_1 = x_3 = 0$. 进一步, $x_2 = x_4 = 0$, 即 $f(x_1, x_2, x_3, x_4) = 0$ 在 F_3 上只有零解.

推论 1 设 n 为正整数, l 为 n 的某个正因子, $x_1, \dots, x_n$ 为 n 个不同的变元, $x_{i1}, \dots, x_{il}$, $0 \leq i \leq n/l - 1$ 为变元 $x_1, \dots, x_n$ 的一个分划. 设

$$f(x_1, \dots, x_n) = c \prod_{j=0}^{n/l-1} \left(\sum_{i=1}^{n/l} r_i^{q^j} g_i(x_{i1}, \dots, x_{il}) \right),$$

其中 $c \in F_q^*$, $r_1, \dots, r_{n/l}$ 为 $F_{q^{n/l}}$ 在 F_q 上的一组基, 对任意的 $i = 1 \cdots n/l$, $g_i(x_{i1}, \dots, x_{il}) \in F_q[x_1, \dots, x_n]$ 是 l 次多项式, 且方程组 $g_i(x_{i1}, \dots, x_{il}) = 0$ 限制在自身 l 个变元时在 F_q 上只有零解. 则 n 元 n 次多项式 $f(x_1, \dots, x_n) = 0$ 在 F_q 上只有零解.

证 因为每个方程 $g_i(x_{i1}, \dots, x_{il}) = 0$, $i = 1 \cdots n/l$ 限制在自身 l 个变元上时, 在 F_q 上只有零解, 所以方程组 $g_i(x_1, \dots, x_n) = 0$, $i = 1 \cdots n/l$ 在 F_q 上只有零解. 由定理 2, 命题成立.

在上述推论中, 令 $l = 1$; 对 $i = 1, \dots, n/l = n$ 令 $g_i(x_i) = x_i$, 则得到前文 Dickson 的实例.

在推论 1 中, 每个方程 $g_i(x_{i1}, \dots, x_{il}) = 0$, $i = 1 \cdots n/l$ 限制在自身 l 个变元上时, 可以看做 l 元 l 次多项式

$$g_i(x_{i1}, \dots, x_{il}) \in F_q[x_{i1}, \dots, x_{il}], \quad g_i(x_{i1}, \dots, x_{il}) = 0$$

在 F_q 上只有零解. 这表明可以用任意 m 个在 F_q 上只有零解的 l 元 l 次多项式, 构造出在 F_q 上只有零解的 ml 元 ml 次多项式. 下面是一个具体的例子.

例 2 设 q 为奇数, $n \geq 4$ 为一偶数, 令 $l = 2$, $c \in F_q^*$, $r_1, \dots, r_{n/2}$ 为 $F_{q^{n/2}}$ 在 F_q 上的一组基, 对任意 $i = 1, \dots, n/2$, 令 $g_i(x_{i1}, x_{i2}) = a_i x_{i1}^2 + b_i x_{i2}^2$, 其中 $a_i, b_i \in F_q^*$, a_i/b_i 是 F_q 上的非平方元. 设

$$f(x_1, \dots, x_n) = \prod_{j=0}^{n/2-1} \left(\sum_{i=1}^{n/2} r_i^{q^j} (a_i x_{i1}^2 + b_i x_{i2}^2) \right).$$

则 n 元 n 次方程 $f = 0$ 在 F_q 上只有零解.

注意到例 2 中的 f 没有交叉项, 利用反证法容易证明 f 不含一次因式, 因此是与 Dickson 实例不同构的只有零解的 n 元 n 次方程. 例 2 利用 $n/2$ 个限制在自身两个变元上在 F_q 上只有零解的 2 次方程, 构造出了高次的只有零解的方程.

从定理 2 的证明可以看出, 若 $f(x_1, \dots, x_n)$ 完全不可约, 则得到对应定理 2 的 $l = n$ 的平凡情形. 但对于给定的有限域 F_q 和正整数 n , 这种平凡情形可能发生, 也可能不能发生. 如文 [5] 中表明对于给定有限域 F_q , $q \geq 13$ 和正整数 $n = 3$, $l = 3$ 时, 定理 2 中的平凡情形是不存在的.

例 3 设 F_3 上的 4 元 4 次多项式

$$f(x_1, x_2, x_3, x_4) = x_1^4 + x_2^4 + x_3^4 + x_4^4 + 2x_1^2 x_3^2 + 2x_1^2 x_4^2 + 2x_2^2 x_4^2.$$

容易验证 $f(x_1, x_2, x_3, x_4)$ 在 F_3 上只有零解, 且其在 F_3 的任何扩域上均不可约. 此时对应定理 2 中 $l = n$ 的平凡情形.

4 总结与展望

本文首先刻画了有限域上不可约多元多项式在其扩域中分解特征, 然后结合 Chevalley 定理, 得到了有限域上 n 元 n 次多项式方程 $f = 0$ 在 F_q 上只有零解的充要条件, 并进一步构造了一些具体实例. 该条件在 f 不是完全不可约的情形下, 更为具体的描述了 f 必须具有范形式. 进一步也可以考虑给出更多具体的例子. 例 3 表明了当 f 完全不可约时, 定理 2 是平凡的, 因此如何刻画有限域上完全不可约的 n 元 n 次方程只有零解的条件依旧是一个值得研究的方向.

参 考 文 献

- [1] Lidl R, Niederreiter H. Finite fields[M]. Cambridge: Cambridge University Press, 1997.
- [2] Gary L Mullen, Daniel Panario. Handbook of finite fields[M]. Boca Raton: CRC Press, 2013.
- [3] Dickson L E. On triple algebras and ternary cubic forms[J]. Bulletin of the American Math. Soc., 1908, 14(4): 160–169.
- [4] Dickson L E. On the representation of numbers by modular forms[J]. Bulletin of the American Math. Soc., 1909, 15(7): 338–347.
- [5] Carlitz L. A theorem of Dickson on nonvanishing cubic forms in a finite field[J]. Proc. American Math. Soc., 1957, 8(5): 975–977.
- [6] Terjanian, Guy. Sur les corps finis [J]. C. R. Acad. Sci. Paris Sér., 1966, 262: A167–A169.
- [7] Carlitz L. Solvability of certain equations in a finite field[J]. Acta Arith., 1961, 7: 389–397.
- [8] Felszeghy, Bálint. On the solvability of some special equations over finite fields[J]. Publ. Math. Debrecen, 2006, 68(1-2): 15–23.
- [9] Francis N Castro. On systems of linear and diagonal equation of degree $pi + 1$ over finite fields of characteristic p [J]. Finite Fields Appl., 2008, 14(3): 648–657.

THE STRUCTURE OF THE EQUATION OVER FINITE FIELDS WITH n UNKNOWN AND WITH DEGREE n WHICH VANISH ONLY AT ZERO

CHEN Xi ¹, QU Long-jiang ¹, LI Chao ^{1,2}

(1. *Departement of Mathematics and System Science, National University of Defense Technology,
Changsha 410073, China*)

(2. *Information Assurance Science and Technology Laboratory, Beijing 100072, China*)

Abstract: In this paper, we investigate the structure of the equation over finite fields with n unknowns and with degree n which vanish only at zero. By using the factorization of the irreducible multivariable polynomial in some extension field and with the Chevalley Theorem, a sufficient and necessary condition of the equation with n unknowns and with degree n which vanish only at zero is obtained. Furthermore, we construct some explicit equations of this class.

Keywords: finite field; equation which vanish only at zero; multivariate polynomial factorization; irreducible polynomial

2010 MR Subject Classification: 12E12; 12E20