

有限域上一类高次方程的解

钟可欣, 夏永波

(中南民族大学数学与统计学学院, 湖北 武汉 430074)

摘要: 设 m 是正整数, $\mathbb{F}_{2^{3m}}$ 是含有 2^{3m} 个元素的有限域. 本文研究了有限域 $\mathbb{F}_{2^{3m}}$ 上的如下方程

$$x^{2^{2m}} + ax^{2^m} + bx = 0,$$

其中 $a, b \in \mathbb{F}_{2^{3m}}^*$. 利用 Blüher 论文有关定理及线性化多项式、置换多项式的相关结论, 本文确定了方程解的个数, 并刻画了方程有相应解数时系数 a, b 所要满足的条件. 所得结果在序列的相关性研究、编码的构造研究及密码函数的差分性质研究中有潜在的应用.

关键词: 有限域; 线性化多项式; 置换多项式; 高次方程

MR(2010) 主题分类号: 11T06

中图分类号: O156.1

文献标识码: A

文章编号: 0255-7797(2026)03-0134-07

1 引言

有限域上高次方程的解在编码、序列和密码函数等多个方向的研究中发挥着重要的作用, 近年来得到了学者们的广泛关注和研究. 设 k 为奇素数, $n = 2k$, 文献 [1] 利用 Dickson 多项式发明了一种新方法, 结合 Niho 的相关定理, 分析了方程

$$F_y(x) = x^{2^{s-1}} + yx^s + \bar{y}x^{s-1} + 1 = 0$$

在有限域 \mathbb{F}_{2^n} 上的解, 研究了长度为 $2^n - 1$ 的二进制 m 序列之间的互相关函数 $C_d(\tau)$, 其中抽选指数 d 为 Niho 型. 针对一类特定的 d (即 $s = 3, d = 3 \cdot 2^k - 2$) 计算了函数 $f_d^*(y)$ 的六值互相关分布. 文献 [2] 对方程 $A_a(v) = a^2v^{2^l} + v^2 + av + 1 = 0$ 在有限域 \mathbb{F}_{2^k} 中解的分布以及方程 $L_a(z) = z^{2^{k+l}} + r^{2^l}a^{2^l}z^{2^{2l}} + raz = 0$ 在有限域 \mathbb{F}_{2^m} 中解的个数进行分析, 研究了长度为 $2^m - 1$ 的二进制 m 序列与长度为 $2^k - 1$ 的二进制 m 序列之间的互相关函数, 其中 $m = 2k, k, l$ 均为奇数, $\gcd(l, k) = 1, r$ 是 \mathbb{F}_{2^m} 中的非立方元, 且 $r^{2^k+1} = 1$. 证明了当 $d(2^l + 1) \equiv 2^l \pmod{2^k - 1}$ 时, 互相关函数为三值. 文献 [3] 通过对方程

$$\beta x^{2^{2k}} + \beta^{2^k} x + \gamma x^{2^k} = 0$$

以及方程

$$\beta r^{2^k+1} + \beta^{2^k} r^{2^k} + \gamma r + \beta^{2^{2k}} = 0$$

*收稿日期: 2025-10-21

接收日期: 2025-12-04

基金项目: 国家自然科学基金资助项目 (62171479); 中南民族大学中央高校基本科研业务费专项资金项目 (CZZ25008).

作者简介: 钟可欣 (2001-), 女, 湖北荆门, 研究生, 研究方向: 密码学. E-mail: zhongkexin819@163.com

通信作者: 夏永波 (1979-), 男, 湖北襄阳, 教授, 研究方向: 无线通讯中的序列设计、编码和密码学.

E-mail: xia@mail.scuec.edu.cn

解的情况进行分析, 提出了一个新的三重纠错码三元组, 并为已知的 Kasami 三元组提供了新的、更简洁的证明. 文献 [4] 分析了方程

$$ba^q x + a^{2^{2^i}} x^{2^i} + a^{2^i} x^{2^{2^i}} + bax^q + ca^{2^{2^i}q} x^{2^i q} + ca^{2^i q} x^{2^{2^i} q} = 0$$

和方程

$$x^{2^i+1} + cx^{2^i} + c^q x + 1 = 0,$$

对 Dillon 提出的差分一致性 ≤ 4 的六项式形式的二次函数的构造进行推广, 提出了更一般的二次多项式形式, 并提出了新的三项式 APN 函数族和六项式 APN 函数族. 文献 [5] 刻画了方程

$$P_a(x) = x^{2^i+1} + x + a = 0$$

在有限域 \mathbb{F}_{2^n} 上无解的充要条件, 其中 $a \in \mathbb{F}_{2^n}^*$, $n = 2k$, $\gcd(n, i) = 1$. 运用该结论构造了一类新的无限族 APN 函数, 证明了文献 [4] 提出的六项式 APN 函数族的存在性.

有限域上一般高次方程解的研究是困难的, 但学者们在此方向仍取得了重要成果. 文献 [6] 刻画出了奇特征有限域 \mathbb{F}_{p^n} 上变元 x, y, z 的方程

$$ax^2 + by^2 + cz^2 = 2dxyz + e \quad (abcd \neq 0)$$

和变元 x, y, z, t 的方程

$$ax^2 + by^2 + cz^2 + dt^2 = 2exyzt + 2f \quad (abcde \neq 0)$$

的解数公式. 在上文的基础上, Baoulina 对奇特征有限域 \mathbb{F}_{p^n} 上方程

$$a_1 x_1^2 + \cdots + a_r x_r^2 = 2bx_1 \cdots x_r \quad (1.1)$$

进行了分析. 令 $d = \gcd(r-2, \frac{p^n-1}{2})$. Baoulina 在文献 [7] 给出了方程 (1.1) 在 $d = 1$ 时和 $d = 2$ 时的解数公式. 在文献 [8] 中他又确定了方程 (1.1) 在正整数 l 满足 $2d \mid (p^l + 1)$ 时的解数公式, 还给出了 $d = 4$ 且 $p \not\equiv 7 \pmod{8}$ 时方程的解数公式. 在文献 [9] 中他又以高次对角方程 $a_1 x_1^{m_1} + \cdots + a_n x_n^{m_n} = 0$ 的解数和一些特征和为基础, 给出了 \mathbb{F}_q 上的方程

$$a_1 x_1^{m_1} + \cdots + a_n x_n^{m_n} = bx_1 \cdots x_n \quad (a_1 a_2 \cdots a_n b \neq 0)$$

在指数 m_1, m_2, \cdots, m_n 满足特定条件时的解数公式. Blüher 在文献 [10] 中系统地研究了有限域 \mathbb{F} 上形如 $f(x) = x^{q+1} + ax + b$ 的多项式, 完整刻画了其在 \mathbb{F} 中有理根个数的可能取值, 并给出每种情况的等价算数条件和计数公式, 其中 $ab \neq 0$, 有限域 \mathbb{F} 特征为 p , q 是 p 的方幂. 文献 [11] 通过巧妙分拆问题、深入利用 MCM 与 Dickson 多项式的性质, 并结合有限域中的显式求解技巧, 彻底解决了 $P_a(x) = x^{2^k+1} + x + a$ 在 $\gcd(n, k) = 1$ 条件下的求根问题. 该文献不仅给出了所有根的显式表达式, 还完成了零点个数的完整分类, 统一并推广了前人结果. 直到现在, 有限域上高次方程解的问题仍有很多学者进行研究并得到了很多优秀的结果, 如胡双年 [12], 王文松和孙琦 [13] 等学者也给出了有限域上一些高次方程在特定条件下的解数公式.

本文研究了有限域 $\mathbb{F}_{2^{3m}}$ 上的方程

$$x^{2^{2m}} + ax^{2^m} + bx = 0,$$

分析了方程的根的个数的可能取值, 并给出每种情况下系数 a, b 所要满足的条件, 其中 $a, b \in \mathbb{F}_{2^{3m}}^*$. 文章的结构如下: 第二节介绍本文所涉及的概念、符号及相关定理, 并证明后文所需要的引理. 第三节对方程进行分析, 证明方程的可能解数, 并给出每种情况下系数 a, b 的对应条件. 最后对文章进行总结.

2 基础知识

设 p 为素数, n 为正整数, \mathbb{F}_{p^n} 表示具有 p^n 个元素的有限域, 后文中也用符号 $GF(p^n)$ 表示具有 p^n 个元素的有限域. $\mathbb{F}_{p^n}^* = \mathbb{F}_{p^n} \setminus \{0\}$ 表示由有限域 \mathbb{F}_{p^n} 的非零元素构成的乘法群.

定义 2.1[14, Definition 2.22] 对 $\alpha \in F = \mathbb{F}_{p^n}$, $K = \mathbb{F}_p$, 定义 α 的迹 $Tr_{F/K}(\alpha)$ 为

$$Tr_{F/K}(\alpha) = \alpha + \alpha^p + \cdots + \alpha^{p^{n-1}}.$$

定义 2.2[14, Definition 2.27] 设 $\alpha \in F = \mathbb{F}_{p^n}$, $K = \mathbb{F}_p$. 定义 K 上 α 的范数 $N_{F/K}(\alpha)$ 为

$$N_{F/K}(\alpha) = \alpha \alpha^p \cdots \alpha^{p^{n-1}} = \alpha^{\frac{p^n-1}{p-1}}.$$

定理 2.1[10, Theorem 5.6, Table 2] 设 F 是特征为 p 的有限域, q 是 p 的幂方, $F \cap GF(q) = GF(Q)$. 令 N_i 为满足 $f_b(x) = x^{q+1} - bx + b$ 在 F 上有 i 个解的 b 的个数, 其中 $i \in \{0, 1, 2, Q+1\}$, $b \in F^*$. 定义 $m = [F : GF(Q)]$, 若 q 为偶数且 m 为奇数, 则

$$N_0 = \frac{Q^{m+1} + Q}{2(Q+1)}, N_1 = Q^{m-1} - 1, N_2 = \frac{(Q-2)(Q^m-1)}{2(Q-1)}, N_{Q+1} = \frac{Q^{m-1} - 1}{Q^2 - 1}.$$

且当 $f_b(x)$ 有 $Q+1$ 个解时, $f_b(x)$ 的根 x 均满足 $N_{F/GF(Q)}(x-1) = 1$.

引理 2.1 设 $F = \mathbb{F}_{2^{3m}}$, $q = 2^m$, $F \cap GF(q) = GF(Q) = GF(2^m)$. 令 $g_b(x) = x^{2^{2m+1}} + bx + b \in \mathbb{F}_{2^{3m}}[x]$, 其中 $b \in F^*$. 则 $g_b(x)$ 有 $2^m + 1$ 个解当且仅当 $b = 1$, 此时 $g_b(x)$ 的根均可开 $2^m - 1$ 次幂.

证 设 $a \in \mathbb{F}_{2^{3m}}^*$ 是方程 $x^{2^{2m}} + x^{2^m} + x = 0$ 的一个非零根, 则 a 满足

$$a^{2^{2m-1}} + a^{2^m-1} + 1 = a^{(2^m-1)(2^m+1)} + a^{2^m-1} + 1 = 0,$$

故该非零根 a 所对应的 a^{2^m-1} 满足方程 $y^{2^m+1} + y + 1 = 0$. 当方程 $x^{2^{2m}} + x^{2^m} + x = 0$ 有 $2^{2m} - 1$ 个不同的非零根时, 若非零 b, d 均满足方程 $x^{2^{2m}} + x^{2^m} + x = 0$ 且 $b^{2^m-1} = d^{2^m-1}$, 则 $(\frac{b}{d})^{2^m-1} = 1$, $b = k \cdot d$, $k \in \mathbb{F}_{2^m}^*$, 即满足 $x^{2^{2m}} + x^{2^m} + x = 0$ 的非零根 a , 每 $2^m - 1$ 个不同的非零 a , 对应同一个 a^{2^m-1} . 有 $2^{2m} - 1$ 个不同的非零根 a 满足 $x^{2^{2m}} + x^{2^m} + x = 0$, 所以有 $\frac{2^{2m}-1}{2^m-1} = 2^m + 1$ 个不同的 a^{2^m-1} 满足方程 $y^{2^m+1} + y + 1 = 0$. 因此, 方程 $y^{2^m+1} + y + 1 = 0$ 有 $2^m + 1$ 个不同根, 且每个根均可表示为 a^{2^m-1} 的形式, 即每个根均可开 $2^m - 1$ 次幂.

由定理 2.1, $q = 2^m$ 为偶数, $[F : GF(Q)] = [\mathbb{F}_{2^{3m}} : \mathbb{F}_{2^m}] = 3$ 为奇数, 当 $g_b(x)$ 有 $2^m + 1$ 个解时, 满足条件的 b 的个数 $N_{2^m+1} = \frac{(2^m)^{3-1}-1}{(2^m)^2-1} = 1$, 即仅有 1 个 $b \in F^*$ 使得

$g_b(x) = x^{2^m+1} + bx + b$ 有 $2^m + 1$ 个解. 又由上述证明知, 方程 $y^{2^m+1} + y + 1 = 0$ 有 $2^m + 1$ 个解. 故 $g_b(x)$ 有 $2^m + 1$ 个解当且仅当 $b = 1$, 此时 $g_b(x)$ 的根均可开 $2^m - 1$ 次幂.

定理 2.2[14, pp. 361] 设 \mathbb{F}_p 和 \mathbb{F}_{p^n} 是分别有 p 和 p^n 个元素的有限域. 令 $f(x) = a_0x + a_1x^p + \cdots + a_{n-1}x^{p^{n-1}}$ 是从 \mathbb{F}_{p^n} 到 \mathbb{F}_{p^n} 的一个线性化多项式. 定义

$$A(f) = \begin{bmatrix} a_0 & a_1 & \cdots & a_{n-1} \\ a_{n-1}^p & a_0^p & \cdots & a_{n-2}^p \\ \vdots & \vdots & \ddots & \vdots \\ a_1^{p^{n-1}} & a_2^{p^{n-1}} & \cdots & a_0^{p^{n-1}} \end{bmatrix}.$$

则 $f: \mathbb{F}_{p^n} \rightarrow \mathbb{F}_{p^n}$ 是一个置换多项式当且仅当 $\det A(f) \neq 0$.

3 主要结果及证明

基于上述预备知识, 本节将对方程 $x^{2^{2m}} + ax^{2^m} + bx = 0$ 在有限域 $\mathbb{F}_{2^{3m}}$ 上解的情况进行分析.

定理 3.1 设 m 为正整数, 令方程 $x^{2^{2m}} + ax^{2^m} + bx = 0$ 在有限域 $\mathbb{F}_{2^{3m}}$ 上解的个数为 $N(a, b)$, 则

$$N(a, b) = \begin{cases} 1, & \text{当 } a, b \text{ 满足 } N_{E/H}(a) + N_{E/H}(b) + \text{Tr}_{E/H}(ab^{2^{2m}}) + 1 \neq 0, \\ 2^{2m}, & \text{当 } a, b \text{ 满足 } N_{E/H}(a) = 1, b = a^{2^{2m}+1}, \\ 2^m, & \text{其它,} \end{cases}$$

其中 $a, b \in \mathbb{F}_{2^{3m}}^*$, $E = \mathbb{F}_{2^{3m}}$, $H = \mathbb{F}_{2^m}$.

证 $f(x) = x^{2^{2m}} + ax^{2^m} + bx$ 是有限域 $\mathbb{F}_{2^{3m}}$ 上的线性化多项式, 设方程 $x^{2^{2m}} + ax^{2^m} + bx = 0$ 解的个数 $N(a, b) = 2^i$, $0 \leq i \leq 2m$, i 为整数.

显然 $x = 0$ 是方程 $x^{2^{2m}} + ax^{2^m} + bx = 0$ 的解. 当 $x \neq 0$ 时, 原方程化为

$$x^{2^{2m}-1} + ax^{2^m-1} + b = 0. \quad (2.1)$$

此时方程 (2.1) 解的个数为 $2^i - 1$, $0 \leq i \leq 2m$, i 为整数.

令 $z = x^{2^m-1}$, 方程 (2.1) 转化为

$$z^{2^m+1} + az + b = 0. \quad (2.2)$$

由 $z = x^{2^m-1}$, 若方程 (2.2) 的解 z_0 可开 $2^m - 1$ 次方, 则 $x_0 = \sqrt[2^m]{z_0}$ 是方程 (2.1) 的解. 且由 $\gcd(2^m - 1, 2^{3m} - 1) = 2^m - 1$ 知, 一个 z_0 对应 $2^m - 1$ 个不同的 x_0 是方程 (2.1) 的解.

不妨设方程 (2.2) 有 k 个不同的解 z_0 可开 $2^m - 1$ 次方, 则方程 (2.1) 对应应有 $(2^m - 1)k$ 个不同的解 x_0 . 前面已知方程 (2.1) 解的个数为 $2^i - 1$, 则 $2^i - 1 = (2^m - 1)k$, 可知 i 必须满足 $2^m - 1 \mid 2^i - 1$. 又因为 $0 \leq i \leq 2m$, 且 i 为整数, 所以 i 的可能取值只有 $0, m, 2m$. 因此方程 $x^{2^{2m}} + ax^{2^m} + bx = 0$ 解的个数 $N(a, b) = 2^i$, $i \in \{0, m, 2m\}$.

下面证明方程 $x^{2^{2m}} + ax^{2^m} + bx = 0$ 分别有 2^{2m} 个, 1 个以及 2^m 个解时系数 a, b 满足的条件.

$N(a, b) = 2^{2m}$ 时, 方程 (2.1) 有 $2^{2m} - 1$ 个解. 由 z 与 x 的对应关系知, 此时方程 (2.2) 有 $\frac{2^{2m}-1}{2^m-1} = 2^m + 1$ 个不同的解 z . 令 $z = \frac{b}{a}y$, 方程 (2.2) 化为 $\frac{b^{2^m+1}}{a^{2^m+1}}y^{2^m+1} + by + b = 0$. 方程两边同乘 $\frac{a^{2^m+1}}{b^{2^m+1}}$ 得

$$y^{2^m+1} + \frac{a^{2^m+1}}{b^{2^m}}y + \frac{a^{2^m+1}}{b^{2^m}} = 0. \quad (2.3)$$

由 $z = \frac{b}{a}y$ 知, 方程 (2.3) 此时也有 $2^m + 1$ 个不同的解 y_0 . 由引理 2.1 知, 方程 (2.3) 有 $2^m + 1$ 个解当且仅当 $\frac{a^{2^m+1}}{b^{2^m}} = 1$, 则 $a^{2^m+1} = b^{2^m}$, 两边同时 2^{2m} 次幂得 $b^{2^{3m}} = a^{2^{3m+2^m}}$. 又因为 $a, b \in \mathbb{F}_{2^{3m}}^*$, 所以 $b = a^{2^{2m+1}}$. 由两次变量替换 $x^{2^m-1} = z = \frac{b}{a}y$ 知, 只有 $\frac{b}{a}y_0$ 可开 $2^m - 1$ 次幂时, 对应的 $x_0 = \sqrt[2^m]{\frac{b}{a}y_0}$ 为方程 (2.1) 的解. 由引理 2.1 知, 此时方程 (2.3) 的解 y_0 均可开 $2^m - 1$ 次幂, 因此 $\frac{b}{a}$ 也要满足可开 $2^m - 1$ 次幂, 即 $(\frac{b}{a})^{\frac{2^{3m}-1}{2^m-1}} = 1$. 将上面 $b = a^{2^{2m+1}}$ 代入得 $(a^{2^{2m}})^{\frac{2^{3m}-1}{2^m-1}} = (a^{\frac{2^{3m}-1}{2^m-1}})^{2^{2m}} = 1$, 两边同时 2^m 次幂得 $(a^{\frac{2^{3m}-1}{2^m-1}})^{2^{3m}} = a^{\frac{2^{3m}-1}{2^m-1}} = 1$, 此时 $\frac{b}{a}y_0$ 可开 $2^m - 1$ 次幂. 因此 a, b 满足 $a^{\frac{2^{3m}-1}{2^m-1}} = N_{E/H}(a) = 1$ 及 $b = a^{2^{2m+1}}$ 时, $N(a, b) = 2^{2m}$, 其中 $E = \mathbb{F}_{2^{3m}}, H = \mathbb{F}_{2^m}$.

$N(a, b) = 1$ 时, 方程 $x^{2^{2m}} + ax^{2^m} + bx = 0$ 仅有一个解 $x = 0$. 方程 $x^{2^{2m}} + ax^{2^m} + bx = 0$ 两边同时 2^m 次幂得 $x + a^{2^m}x^{2^{2m}} + b^{2^m}x^{2^m} = 0$, 对此式两边再同时 2^m 次幂得 $x^{2^m} + a^{2^{2m}}x + b^{2^{2m}}x^{2^{2m}} = 0$. 将三个方程联立后可表示为如下矩阵乘法形式:

$$\begin{pmatrix} 1 & a & b \\ a^{2^m} & b^{2^m} & 1 \\ b^{2^{2m}} & 1 & a^{2^{2m}} \end{pmatrix} \begin{pmatrix} x^{2^{2m}} \\ x^{2^m} \\ x \end{pmatrix} = 0.$$

令

$$A = \begin{pmatrix} 1 & a & b \\ a^{2^m} & b^{2^m} & 1 \\ b^{2^{2m}} & 1 & a^{2^{2m}} \end{pmatrix},$$

由定理 2.2 知, 方程仅有零解当且仅当 $\det(A) \neq 0$, 即 $\det(A) = (a^{2^{2m}}b^{2^m} + 1) + a(a^{2^m} \cdot a^{2^{2m}} + b^{2^{2m}}) + b(a^{2^m} + b^{2^m} \cdot b^{2^{2m}}) = 1 + ab^{2^{2m}} + a^{2^m}b + a^{2^{2m}}b^{2^m} + a^{2^{2m+2^m+1}} + b^{2^{2m+2^m+1}} \neq 0$. 由定义 2.1 及定义 2.2, $Tr_{E/H}(ab^{2^{2m}}) = ab^{2^{2m}} + (ab^{2^{2m}})^{2^m} + (ab^{2^{2m}})^{2^{2m}} = ab^{2^{2m}} + a^{2^m}b + a^{2^{2m}}b^{2^m}$, $N_{E/H}(a) = a^{\frac{(2^m)^3-1}{2^m-1}} = a^{2^{2m+2^m+1}}$, $N_{E/H}(b) = b^{2^{2m+2^m+1}}$, 所以 $\det(A) = Tr_{E/H}(ab^{2^{2m}}) + N_{E/H}(a) + N_{E/H}(b) + 1$, 其中 $E = \mathbb{F}_{2^{3m}}, H = \mathbb{F}_{2^m}$. 因此 a, b 满足 $Tr_{E/H}(ab^{2^{2m}}) + N_{E/H}(a) + N_{E/H}(b) + 1 \neq 0$ 时, $N(a, b) = 1$.

由于方程 $x^{2^{2m}} + ax^{2^m} + bx = 0$ 解的个数的可能取值只有 $2^{2m}, 1$ 及 2^m . 因此当 a, b 不满足 $N_{E/H}(a) = 1, b = a^{2^{2m+1}}$ 及 $Tr_{E/H}(ab^{2^{2m}}) + N_{E/H}(a) + N_{E/H}(b) + 1 \neq 0$ 时, $N(a, b) = 2^m$.

注: 当 a, b 满足 $N_{E/H}(a) = a^{\frac{2^{3m}-1}{2^m-1}} = 1, b = a^{2^{2m+1}}$ 时, $N_{E/H}(b) = N_{E/H}(a^{2^{2m+1}}) = (a^{2^{2m+1}})^{\frac{2^{3m}-1}{2^m-1}} = (a^{\frac{2^{3m}-1}{2^m-1}})^{2^{2m+1}} = 1^{\frac{2^{3m}-1}{2^m-1}} = 1$, $Tr_{E/H}(ab^{2^{2m}}) = Tr_{E/H}(a^{2^{4m+2^m+1}}) = Tr_{E/H}(a^{2^{2m+2^m+1}}) = Tr_{E/H}(a^{\frac{2^{3m}-1}{2^m-1}}) = Tr_{E/H}(1) = 1$, 则 $Tr_{E/H}(ab^{2^{2m}}) + N_{E/H}(a) + N_{E/H}(b) + 1 = 0$.

例 1: 令 $m = 1, z$ 为有限域 \mathbb{F}_{2^3} 的本原元. 取 $a = z^2, b = z^4$ 时, 通过 Magma 计算方程 $x^4 + z^2x^2 + z^4x = 0$ 在有限域 \mathbb{F}_{2^3} 上仅有 1 个解 $x = 0$. 此时 $Tr_{E/H}(ab^4) + N_{E/H}(a) + N_{E/H}(b) + 1 = 1$ 符合条件 $Tr_{E/H}(ab^{2^{2m}}) + N_{E/H}(a) + N_{E/H}(b) + 1 \neq 0$. 取 $a = 1, b = 1$

时, 通过 Magma 计算方程 $x^4 + x^2 + x = 0$ 在有限域 \mathbb{F}_{2^3} 上有 4 个解. 此时 $N_{E/H}(a) = N_{E/H}(1) = 1$, $a^{2^2+1} = 1 = b$ 符合条件 $N_{E/H}(a) = 1$, $b = a^{2^{2m}+1}$. 取 $a = z^2$, $b = z$ 时, 通过 Magma 计算方程 $x^4 + z^2x^2 + zx = 0$ 在有限域 \mathbb{F}_{2^3} 上有 2 个解. 此时 $N_{E/H}(a) = N_{E/H}(b) = \text{Tr}_{E/H}(ab^4) = 1$, $a^{2^2+1} = z^3 \neq b$, $\text{Tr}_{E/H}(ab^4) + N_{E/H}(a) + N_{E/H}(b) + 1 = 0$ 不满足 $b = a^{2^{2m}+1}$ 以及 $\text{Tr}_{E/H}(ab^{2^{2m}}) + N_{E/H}(a) + N_{E/H}(b) + 1 \neq 0$. 实验所得结果与论文结论一致.

例 2: 令 $m = 3$, z 为有限域 \mathbb{F}_{2^9} 的本原元. 取 $a = z^{31}$, $b = z^{32}$ 时, 通过 Magma 计算方程 $x^{64} + z^{31}x^8 + z^{32}x = 0$ 在有限域 \mathbb{F}_{2^9} 上仅有 1 个解 $x = 0$. 此时 $\text{Tr}_{E/H}(ab^4) + N_{E/H}(a) + N_{E/H}(b) + 1 = z^3$ 符合条件 $\text{Tr}_{E/H}(ab^{2^{2m}}) + N_{E/H}(a) + N_{E/H}(b) + 1 \neq 0$. 取 $a = z^{126}$, $b = z^{14}$ 时, 通过 Magma 计算方程 $x^{64} + z^{126}x^8 + z^{14}x = 0$ 在有限域 \mathbb{F}_{2^9} 上有 64 个解. 此时 $N_{E/H}(a) = 1$, $a^{2^6+1} = z^{14} = b$ 符合条件 $N_{E/H}(a) = 1$, $b = a^{2^{2m}+1}$. 取 $a = z^{64}$, $b = z^{12}$ 时, 通过 Magma 计算方程 $x^{64} + z^{64}x^8 + z^{12}x = 0$ 在有限域 \mathbb{F}_{2^9} 上有 8 个解. 此时 $N_{E/H}(a) = z$, $a^{2^6+1} = z^{72} \neq b$, $\text{Tr}_{E/H}(ab^4) + N_{E/H}(a) + N_{E/H}(b) + 1 = 0$ 不满足 $N_{E/H}(a) = 1$, $b = a^{2^{2m}+1}$ 以及 $\text{Tr}_{E/H}(ab^{2^{2m}}) + N_{E/H}(a) + N_{E/H}(b) + 1 \neq 0$. 实验所得结果与论文结论一致.

4 结论

本文分析了有限域上一类高次方程解的个数, 并刻画了方程有相应解数时系数 a, b 所要满足的条件. 本文利用变量代换对方程形式进行转化, 通过不同形式方程解的个数之间的关系确定原方程解的个数, 再通过 Bluhner 论文相关结论刻画了 a, b 需要满足的条件. 本文所得结论可推广到一般的奇特征有限域上, 证明过程类似因此未重复证明. 遗憾的是本文未能根据系数 a, b 对所要满足的条件求解出相应 a, b 对的个数, 后续我们也将继续深入研究, 旨在完整刻画出满足相应解数时对应 a, b 对的个数.

参 考 文 献

- [1] Dobbertin H, Felke P, Helleseht T, Rosendahl P. Niho type cross-correlation functions via Dickson polynomials and Kloosterman sums [J]. IEEE Trans. Inf. Theory, 2006, 52(2): 613–627.
- [2] Helleseht T, Kholosha A, Ness G J. Characterization of m-sequences of lengths 2^{2^k-1} and $2^k - 1$ with three-valued crosscorrelation [J]. IEEE Trans. Inf. Theory, 2007, 53(6): 2236–2245.
- [3] Bracken C, Helleseht T. Triple-error-correcting BCH-like codes [C]. Korea, Seoul: 2009 IEEE International Symposium on Information Theory, 2009.
- [4] Budaghyan L, Carlet C. Classes of quadratic APN trinomials and hexanomials and related structures [J]. IEEE Trans. Inf. Theory, 2008, 54(5): 2354–2357.
- [5] Bracken C, Tan C H, Tan Y. On a class of quadratic polynomials with no zeros and its application to APN functions [J]. Finite Fields and Their Applications, 2014, 25: 26–36.
- [6] Carlitz L. Certain special equations in a finite field [J]. Monatshefte für Mathematik, 1954, 58(1): 5–12.
- [7] Baoulina I. On the problem of explicit evaluation of the number of solutions of the equation $a_1x_1^2 + \dots + a_nx_n^2 = bx_1 \cdots x_n$ in a finite field [C]. In: S. D. Adhikari, S. A. Katre and B. Ramakrishnan (eds), Current Trends in Number Theory, Hindustan Book Agency, New Delhi, 2002, 27–37.

- [8] Baoulina I. Generalizations of the Markoff-Hurwitz equations over finite fields [J]. *Journal of Number Theory*, 2006, 118, 31–52.
- [9] Baoulina I. On the number of solutions of the equation $a_1x_1^{m_1} + \cdots + a_nx_n^{m_n} = bx_1 \cdots x_n$ in a finite field [J]. *Acta Applicandae Mathematicae*, 2005, 85(1): 35–39.
- [10] Blüher A W. On $x^{q+1} + ax + b$ [J]. *Finite Fields and Their Applications*, 2004, 10: 285–305.
- [11] Kwang H K, Sihem M. Solving $x^{2^k+1} + x + a = 0$ in \mathbb{F}_{2^n} with $\gcd(n, k) = 1$ [J]. *Finite Fields and Their Applications*, 2020, 63: 1–15.
- [12] Hu Shuangnian, Hong Shaofang, Zhao Wei. The number of rational points of a family of hypersurfaces over finite fields [J]. *Journal of Number Theory*, 2015, 156, 135–153.
- [13] Wang Wensong, Sun Qi. An explicit formula of solution of some special equations over a finite field (in Chinese) [J]. *Chinese Annals of Mathematics, Series A*, 2005, 26(3): 391–396.
- [14] Lidl R, Niederreiter H. Finite fields [M]. *Encyclopedia of Mathematics and Its Applications*, 20. Cambridge U.K: Cambridge University Press, 1997.
- [15] Helleseth T, Kholosha A. $x^{2^l+1} + x + a$ and related affine polynomials over $GF(2^k)$ [J]. *Cryptography and Communications*, 2010, 2(1): 85–109.
- [16] Helleseth T, Kholosha A. On the equation $x^{2^l+1} + x + a = 0$ over $GF(2^k)$ [J]. *Finite Fields and Their Applications*, 2008, 14: 159–176.
- [17] Lidl R. Introduction to finite fields and their applications [M]. Cambridge: Cambridge University Press, 1997.

SOLUTIONS FOR A HIGHER-DEGREE EQUATION OVER FINITE FIELDS

ZHONG Ke-xin, XIA Yong-bo

(College of Mathematics and Statistics, South-Central Minzu University, Wuhan 430074, China)

Abstract: Let m be a positive integer and $\mathbb{F}_{2^{3m}}$ the finite field with 2^{3m} elements. We investigate the following equation over the finite field $\mathbb{F}_{2^{3m}}$

$$x^{2^{2m}} + ax^{2^m} + bx = 0,$$

where $a, b \in \mathbb{F}_{2^{3m}}^*$. By applying relevant theorems from Blüher's work and properties of linearized polynomials and permutation polynomials, we determine the number of solutions to the above equation and characterize the conditions on a and b for each possible solution count. The result may have potential applications in the study of the correlation properties of certain sequences, code constructions, and differential properties of cryptographic functions.

Keywords: Finite field; linearized polynomial; permutation polynomial; equation of higher degree

2010 MR Subject Classification: 11T06.