

基于置换多项式簇的五类置换码构造及其参数分析

叶娜, 夏永波

(中南民族大学数学与统计学学院, 湖北 武汉 430074)

摘要: 本文研究了基于有限域上的置换多项式构造置换码的问题. 利用有限域上形如 $f(x) = \alpha x^m + \beta x$ (其中 m 为正整数) 的置换多项式簇, 构造了五类置换码, 并借助求解有限域上代数方程的一些方法, 确定了这五类置换码的参数, 包括码长、码字数量和极小汉明距离, 所得结果丰富了置换码的构造理论.

关键词: 置换多项式; 置换码; 极小汉明距离; 码字数量; 有限域

MR(2010) 主题分类号: 11T06; 94B60; 94A24

中图分类号: O157.4; O153.4

文献标识码: A

文章编号: 0255-7797(2026)01-020-11

1 引言

置换码凭借其独特性质及在各类通信系统中的潜在应用价值, 已成为编码理论领域的重要研究方向^[1]. 它们在多个领域都有实际应用, 尤其在通信系统中^[2], 可有效对抗噪声与干扰. 例如在电力线通信中^[3,4], 置换码被用于保障信息的可靠传输, 同时维持稳定的功率输出. 随着现代通信技术的飞速发展, 置换码凭借其独特的符号置换特性和抗干扰能力, 在闪存存储^[5](解决存储单元耐久性问题) 等场景中进一步展现出不可替代的优势.

自 Slepian 在 1965 年奠定置换码理论框架^[6]以来, 学界对置换码的研究不断深入, 其中构造方法优化^[7]、参数上下界分析^[8]及参数优化^[9]始终是研究热点. 要增强码的纠错能力, 需使其极小汉明距离尽可能大; 要传输更多信息, 则需在给定码长和极小汉明距离的情况下, 使码中包含的码字数量尽可能多^[1]. 记 $M(n, d)$ 为一个长为 n 且极小汉明距离为 d 的置换码的码字数量, 构造一个 $M(n, d)$ 的值以及 d 的值尽可能大的置换码是编码理论的中心问题^[10].

由于有限域上的置换多项式具有双射特性, 故可用于生成置换码码字. Chu 等人^[11]利用有限域上的低次置换多项式(次数小于等于 5), 构造了置换码并给出置换码的码容量下界. 然而其框架的核心在于按次数分类枚举低次置换多项式(次数小于等于 5), 并基于此集合构建置换码以获取码容量下界, 未能针对某一类特定形式(如某种参数化的多项式簇)的多项式深入研究置换码的参数. 基于此, 本文结合文献^[12]给出的五类置换多项式簇, 构造了五类置换码, 严格计算其码长、码字数量和极小汉明距离, 并对其参数展开分析.

*收稿日期: 2025-08-24

接收日期: 2025-09-23

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: 叶娜(2001-), 女, 湖北咸宁, 研究生, 研究方向: 编码理论. E-mail: yena2025@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

文章的结构如下: 第一部分介绍基础知识(定义、符号及核心引理), 其中引理 2-4 介绍了五类置换多项式簇, 是本文构造置换码的理论基石. 第二部分计算出五类置换码的码长、码字数量 $M(n, d)$ 和极小汉明距离 d . 第三部分分析了所构造置换码的参数. 最后对文章进行总结.

2 基础知识

设 p 为奇素数, n 为正整数, $q = p^n$, \mathbb{F}_q 表示具有 q 个元素的有限域, $\mathbb{F}_{q^*} = \mathbb{F}_q \setminus \{0\}$ 表示有限域 \mathbb{F}_q 去掉零元素后得到的乘法群.

定义 2.1^[13] 设集合 $N_n = 1, 2, \dots, n!$, 一个置换就是一个从 N_n 到 N_n 的双射 $\sigma_i, i = 1, 2, \dots, n!$. 置换可较直观地表达为

$$\sigma_i = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma_i(1) & \sigma_i(2) & \cdots & \sigma_i(n) \end{pmatrix},$$

用 S_n 来表示 N_n 上的所有置换组成的集合. 一个长为 n 的置换码就是 S_n 的一个子集, 置换码可以表示为 $\mathcal{C} = \{\sigma | \sigma \in S_n\}$, 置换码中的置换称为置换码的码字.

定义 2.2^[13] 对于 S_n 中的任意两个置换 $\sigma_1, \sigma_2 \in S_n$, 设 $\sigma_1 = (\sigma_1(1), \sigma_1(2), \dots, \sigma_1(n)), \sigma_2 = (\sigma_2(1), \sigma_2(2), \dots, \sigma_2(n))$, 则函数 $\delta(\sigma_1, \sigma_2) = |x \in N_n | \sigma_1(x) \neq \sigma_2(x)|, (\sigma_1, \sigma_2 \in S_n)$ 定义为置换 σ_1 和 σ_2 之间的汉明距离. 一个置换码中任意两个置换的汉明距离的最小值定义为这个置换码的极小汉明距离, 记为 d . 将码长为 n , 码字数量为 $M(n, d)$, 极小汉明距离为 d 的置换码记为 (n, M, d) - 置换码.

定义 2.3^[14] 若多项式 $f \in \mathbb{F}_q[x]$ 诱导的映射 $x \mapsto f(x)$ 是 \mathbb{F}_q 上的一个置换, 则称多项式 f 为 \mathbb{F}_q 上的一个置换多项式. 置换多项式 f 是一个从有限域 \mathbb{F}_q 到它自身的双射. 另一方面, 有限域 \mathbb{F}_q 上的每一个置换都可以表示成有限域 \mathbb{F}_q 上的一个置换多项式^[15]. 而置换多项式簇则是满足一定条件的置换多项式的集合.

定义 2.4^[16] 若元素 $\omega \in \mathbb{F}_q^*$, 则 ω 为 m 次本原单位根当且仅当 $\omega^k \neq 1, 1 \leq k < m$ 且 $\omega^m = 1$. 即 m 是满足 $\omega^k = 1$ 的最小正整数.

引理 2.1^[17] 对于任意整除 $q-1$ 的正整数 m , 有限域 \mathbb{F}_q 中存在 $\phi(m)$ 个 m 次本原单位根.

为了构造置换码, 关键步骤是找到置换多项式簇. 接下来三个引理介绍了五类置换多项式簇, 这将是后续构造置换码的理论基础.

引理 2.2^[12, Corollary 5.11] 若 $\alpha \in \mathbb{F}_{q^2}^*, \beta \in \mathbb{F}_q$, 则多项式 $P(x) = \alpha x^{q+2} + \beta x$ 是一个在有限域 \mathbb{F}_{q^2} 上的置换多项式当且仅当下列任一条件满足:

- (1) $q \equiv 5 \pmod{6}$ 且 α^{q-1} 的阶为 6;
- (2) $q \equiv 2 \pmod{6}$ 且 α^{q-1} 的阶为 3;
- (3) $q \equiv 0 \pmod{3}$ 且 $\alpha^{q-1} = -1$.

引理 2.3^[12, Corollary 5.12] 若 $\alpha \in \mathbb{F}_{q^3}^*, \beta \in \mathbb{F}_q$, 则多项式 $P(x) = \alpha x^{q^2+q+2} + \beta x$ 是在有限域 \mathbb{F}_{q^3} 上的一个置换多项式当且仅当 $q \equiv 0 \pmod{2}$ 且 $\alpha^{q^2} + \alpha^{q^2-q+1} + \alpha = 0$.

引理 2.4^[12, Theorem 3.5] 若 $\alpha \in \mathbb{F}_{q^2}^*, \beta \in \mathbb{F}_q$, 则多项式 $P(x) = \alpha x^{2q+3} + \beta x$ 是一个在有限域 \mathbb{F}_{q^3} 上的置换多项式当且仅当 $q = 5^n$ 且 $\alpha^{q-1} = -1$.

3 主要结果及证明

下来我们将利用引理 2.2、引理 2.3 和引理 2.4 中给出的置换多项式簇来构造置换码, 并确定所构造置换码的码长、码字数量和极小汉明距离. 对于置换码的极小汉明距离的求解问题, 我们首先给出如下的统一分析方法.

设 θ 是有限域 \mathbb{F}_q^* 上的一个本原元, 则有限域 $\mathbb{F}_q^* = \{\theta^0, \theta^1, \dots, \theta^{q-2}\} = \{x_1, x_2, \dots, x_{q-1}\}$. 设 $A \subseteq \mathbb{F}_q \times \mathbb{F}_q$, $|A| = l$, 当 $(\alpha, \beta) \in A$ 时, $f_{\alpha, \beta}(x) = \alpha x^m + \beta x$ 为有限域 \mathbb{F}_q 上的置换多项式. 由于 $f(0) = 0$, 则我们可以将 $f_{\alpha, \beta}(x) = \alpha x^m + \beta x$ 视为作用在有限域 \mathbb{F}_q^* 上的置换.

记码字 $c_{\alpha, \beta}$ 为置换多项式 $f_{\alpha, \beta}(x) = \alpha x^m + \beta x$ 诱导出的置换, 它可以写作

$$c_{\alpha, \beta} = \begin{pmatrix} x_1 & x_2 & \cdots & x_{q-1} \\ f_{\alpha, \beta}(x_1) & f_{\alpha, \beta}(x_2) & \cdots & f_{\alpha, \beta}(x_{q-1}) \end{pmatrix}.$$

记 $\mathcal{C} = \{c_{\alpha, \beta} \mid (\alpha, \beta) \in A\}$, 则 \mathcal{C} 是一个码长为 $q-1$, 码字数量为 l 的置换码. 对于任意两个多项式 $f_{\alpha_i, \beta_i}(x) = \alpha_i x^m + \beta_i x$, $f_{\alpha_j, \beta_j}(x) = \alpha_j x^m + \beta_j x$ ($i \neq j$, $i, j \in [1, 2, \dots, l]$), 将它们分别作用在集合 $\{x_1, x_2, \dots, x_{q-1}\}$ 上, 可以得到两个码字:

$$c_{\alpha_i, \beta_i} = \begin{pmatrix} x_1 & x_2 & \cdots & x_{q-1} \\ f_{\alpha_i, \beta_i}(x_1) & f_{\alpha_i, \beta_i}(x_2) & \cdots & f_{\alpha_i, \beta_i}(x_{q-1}) \end{pmatrix}$$

和

$$c_{\alpha_j, \beta_j} = \begin{pmatrix} x_1 & x_2 & \cdots & x_{q-1} \\ f_{\alpha_j, \beta_j}(x_1) & f_{\alpha_j, \beta_j}(x_2) & \cdots & f_{\alpha_j, \beta_j}(x_{q-1}) \end{pmatrix}.$$

现分别比较这两个码字的 $q-1$ 个分量是否相等, 即计算对任意给定的 x_t ($t \in [1, 2, \dots, q-1]$), $f_{\alpha_i, \beta_i}(x_t)$ 是否等于 $f_{\alpha_j, \beta_j}(x_t)$. 这两个码字之间的汉明距离等于使得 $f_{\alpha_i, \beta_i}(x_t) \neq f_{\alpha_j, \beta_j}(x_t)$ 的 x_t ($t \in [1, 2, \dots, q-1]$) 的个数. 若 $f_{\alpha_i, \beta_i}(x_t) = f_{\alpha_j, \beta_j}(x_t)$, 则 $\alpha_i x^m + \beta_i x = \alpha_j x^m + \beta_j x$. 提出 x 得

$$(\alpha_i x^{m-1} + \beta_i)x = (\alpha_j x^{m-1} + \beta_j)x.$$

当 $x \neq 0$ 时, 有

$$\alpha_i x^{m-1} + \beta_i = \alpha_j x^{m-1} + \beta_j. \quad (2.1)$$

记方程 (2.1) 的解数为 $\chi_{(i, j)}$. 因为置换码的极小汉明距离就等于所有不同的两个码字之间的汉明距离的最小值, 所以置换码的极小汉明距离

$$d = q - 1 - \max_{i \neq j, i, j \in [1, 2, \dots, l]} \chi_{(i, j)}.$$

基于上述框架, 本节将依次计算五类置换码的码长、码字数量和极小汉明距离.

定理 3.1 设 $q \equiv 0 \pmod{2}$, $\alpha \in \mathbb{F}_{q^3}^*$, 且 α 满足 $\alpha^{q^2} + \alpha^{q^2-q+1} + \alpha = 0$, $\beta \in \mathbb{F}_q$. 记基于有限域 $\mathbb{F}_{q^3}^*$ 上的置换多项式簇 $P(x) = \alpha x^{q^2+q+2} + \beta x$ 构造的置换码为 \mathcal{C}_1 , 则 \mathcal{C}_1 是一个 $(q^3 - 1, q^3 - q, q^3 - 1)$ - 置换码.

证 该置换码的码长为 $q^2 - 1$. 要求解置换码 \mathcal{C}_1 的码字数量, 则需求出对应有有限域上的置换多项式簇的个数. 我们首先求出满足条件 $\alpha^{q^2} + \alpha^{q^2-q+1} + \alpha = 0$ 的 α 的个数. 因为

$\alpha^{q^2} + \alpha^{q^2-q+1} + \alpha = 0$, 则有 $\alpha^{q+1}(\alpha^{q^2-1} + \alpha^{q^2-q} + 1) = 0$, 从而 $\alpha^{q^2+q} + \alpha^{q^2+1} + \alpha^{q+1} = 0$. 由迹函数的定义知, 这等价于 $\text{Tr}_{\mathbb{F}_{q^3}/\mathbb{F}_q}(\alpha^{q+1}) = 0$. 注意到 $\text{Tr}_{\mathbb{F}_{q^3}/\mathbb{F}_q}(x) = 0$ 的非零解有 $\frac{q^3}{q} - 1 = q^2 - 1$ 个. 又因为当 $q \equiv 0 \pmod{2}$ 时, 有 $(q+1, q^3-1) = 1$, 所以满足 $\text{Tr}_{\mathbb{F}_{q^3}/\mathbb{F}_q}(\alpha^{q+1}) = 0$ 的 α 也有 $q^2 - 1$ 个. 故满足条件 $\alpha^{q^2} + \alpha^{q^2-q+1} + \alpha = 0$ 的 α 的个数为 $q^2 - 1$. 由于 β 遍历 \mathbb{F}_q , 故 β 有 q 种取法. 综上可得置换码 \mathcal{C}_1 的码字数量为 $q^3 - q$.

接下来计算该置换码的极小汉明距离, 置换码的极小汉明距离就等于所有不同的两个码字之间的汉明距离的最小值. 任取置换码 \mathcal{C}_1 中的两个码字 c_{α_1, β_1} 和 c_{α_2, β_2} , 由本节起始给出的统一分析方法知, c_{α_1, β_1} 和 c_{α_2, β_2} 这两个码字间的汉明距离可以转化为确定如下方程解的个数

$$\alpha_1 x^{q^2+q+2} + \beta_1 x = \alpha_2 x^{q^2+q+2} + \beta_2 x. \quad (2.2)$$

下面分三种情况讨论该方程解的个数:

情形 1: 当 $\alpha_1 = \alpha_2, \beta_1 \neq \beta_2$ 时, 方程 (2.2) 可化简为 $\beta_1 x = \beta_2 x$, 显然这个方程无解. 故此时置换码中任意两个码字之间的汉明距离为 $q^3 - 1 - 0 = q^3 - 1$.

情形 2: 当 $\alpha_1 \neq \alpha_2, \beta_1 = \beta_2$ 时, 方程 (2.2) 可化简为 $\alpha_1 x^{q^2+q+2} = \alpha_2 x^{q^2+q+2}$, 显然这个方程无解. 故此时置换码中任意两个码字之间的汉明距离为 $q^3 - 1 - 0 = q^3 - 1$.

情形 3: 当 $\alpha_1 \neq \alpha_2, \beta_1 \neq \beta_2$ 时, 方程 (2.2) 可化简为 $x^{q^2+q+1} = \frac{\beta_2 - \beta_1}{\alpha_1 - \alpha_2}$, 等式两边同时 $q-1$ 次方可得 $x^{q^3-1} = \frac{(\beta_2 - \beta_1)^{q-1}}{(\alpha_1 - \alpha_2)^{q-1}}$. 注意到 $\beta_1, \beta_2 \in \mathbb{F}_q^*, x \in \mathbb{F}_{q^3}^*$, 则有 $(\beta_2 - \beta_1)^{q-1} = 1, x^{q^3-1} = 1$, 故上式可化简为 $(\alpha_1 - \alpha_2)^{q-1} = 1$. 这说明方程 (2.2) 有非零解的必要条件是 $\alpha_1 - \alpha_2 \in \mathbb{F}_q^*$, 不妨假设 $\alpha_1 - \alpha_2 \in \mathbb{F}_q^*$, 即 $(\alpha_1 - \alpha_2)^{q-1} = 1$, 等式两边同时乘以 $\alpha_1 - \alpha_2$ 可得 $(\alpha_1 - \alpha_2)^q = \alpha_1^q - \alpha_2^q = \alpha_1 - \alpha_2$. 因为 α_1 和 α_2 满足条件

$$\alpha_1^{q^2} + \alpha_1^{q^2-q+1} + \alpha_1 = 0, \quad (2.3)$$

$$\alpha_2^{q^2} + \alpha_2^{q^2-q+1} + \alpha_2 = 0, \quad (2.4)$$

(2.3) 式减去 (2.4) 式可得

$$\alpha_1^{q^2} - \alpha_2^{q^2} + \alpha_1^{q^2-q+1} - \alpha_2^{q^2-q+1} + \alpha_1 - \alpha_2 = 0.$$

又由于 α_1 和 α_2 满足等式 $(\alpha_1 - \alpha_2)^{q-1} = 1$, 则上式可化为 $\alpha_1^{q^2-q+1} - \alpha_2^{q^2-q+1} = 0$, 即 $\alpha_1^{q^2-q+1} = \alpha_2^{q^2-q+1}$, 在等式两边同时取 $q-1$ 次方可得 $\alpha_1^{q^3+1} = \alpha_2^{q^3+1}$. 注意到 $\alpha_1 \in \mathbb{F}_{q^3}, \alpha_2 \in \mathbb{F}_{q^3}$, 则有 $\alpha_1^2 = \alpha_2^2$, 故 $\alpha_1 = \alpha_2$, 矛盾. 所以假设不成立, 方程 (2.2) 无解, 故此时置换码中任意两个码字之间的汉明距离为 $q^3 - 1 - 0 = q^3 - 1$.

由以上三种情况可知, 置换码 \mathcal{C}_1 的极小汉明距离为 $q^3 - 1$. 故 \mathcal{C}_1 是一个 $(q^3 - 1, q^3 - q, q^3 - 1)$ -置换码. 证毕.

定理 3.2 设 $q \equiv 0 \pmod{3}$, $\alpha \in \mathbb{F}_{q^2}^*$, 且 α 满足 $\alpha^{q-1} = -1, \beta \in \mathbb{F}_q$. 记基于有限域 \mathbb{F}_{q^2} 上的置换多项式簇 $P(x) = \alpha x^{q+2} + \beta x$ 构造的置换码为 \mathcal{C}_2 , 则 \mathcal{C}_2 是一个 $(q^2 - 1, q^2 - q, q^2 - 1)$ -置换码.

证 该置换码的码长为 $q^2 - 1$. 要求解置换码 \mathcal{C}_2 的码字数量, 首先需求出满足条件的

$$\alpha^{q-1} = -1 \quad (2.5)$$

的个数. 设 g 是有限域 $\mathbb{F}_{q^2}^*$ 中的一个本原元, 则存在正整数 m , 使得 $\alpha = g^m$. 由于在有限域 \mathbb{F}_{q^2} 中, -1 可以用本原元表示为 $-1 = g^{\frac{q^2-1}{2}}$. 则条件 (2.5) 可以转化为 $(g^m)^{q-1} = g^{\frac{q^2-1}{2}}$, 这等价于求解关于 m 的同余方程

$$m(q-1) \equiv \frac{q^2-1}{2} \pmod{q^2-1}. \quad (2.6)$$

由于 $\gcd(q-1, q^2-1) = q-1$, 且 $q-1 \mid \frac{q^2-1}{2}$, 故方程 (2.6) 有 $q-1$ 个解. 又因为 β 遍历 \mathbb{F}_q , 故 β 有 q 种取法. 综上可得置换码 \mathcal{C}_2 的码字数量为 $q^2 - q$.

在确定了置换码 \mathcal{C}_2 的码字数量后, 我们现在来计算其极小汉明距离. 任取置换码 \mathcal{C}_2 中的两个码字 c_{α_1, β_1} 和 c_{α_2, β_2} , 由本节起始给出的分析方法可知, 这两个码字间的汉明距离可以转化为讨论方程解的个数. 由定理 3.1 的证明过程可类似得到, 当 $\alpha_1 = \alpha_2, \beta_1 \neq \beta_2$ 或 $\alpha_1 \neq \alpha_2, \beta_1 = \beta_2$ 时, 方程

$$\alpha_1 x^{q+2} + \beta_1 x = \alpha_2 x^{q+2} + \beta_2 x \quad (2.7)$$

不存在解, 故此时该置换码的任意两个码字之间的汉明距离为 $q^2 - 1 - 0 = q^2 - 1$. 当 $\alpha_1 \neq \alpha_2, \beta_1 \neq \beta_2$ 时, 方程 (2.7) 可化简为 $x^{q+1} = \frac{\beta_2 - \beta_1}{\alpha_1 - \alpha_2}$, 等式两边同时 $q-1$ 次方可得 $x^{q^2-1} = \frac{(\beta_2 - \beta_1)^{q-1}}{(\alpha_1 - \alpha_2)^{q-1}}$. 注意到 $\beta_1 - \beta_2 \in \mathbb{F}_q^*, x \in \mathbb{F}_{q^2}^*$, 则有 $(\beta_1 - \beta_2)^{q-1} = 1, x^{q^2-1} = 1$, 故上式可化简为 $(\alpha_1 - \alpha_2)^{q-1} = 1$. 这说明方程 (2.7) 有非零解的必要条件是 $\alpha_1 - \alpha_2 \in \mathbb{F}_q^*$. 现假设 $\alpha_1 - \alpha_2 \in \mathbb{F}_q^*$, 即 $(\alpha_1 - \alpha_2)^{q-1} = 1$, 等式两边同时乘以 $\alpha_1 - \alpha_2$ 可得

$$\alpha_1^q - \alpha_2^q = \alpha_1 - \alpha_2. \quad (2.8)$$

又因为 α_1 和 α_2 满足条件 $\alpha_1^{q-1} = -1, \alpha_2^{q-1} = -1$, 故有

$$\alpha_1^q = -\alpha_1, \quad \alpha_2^q = -\alpha_2. \quad (2.9)$$

将 (2.9) 式代入 (2.8) 式可得 $-\alpha_1 - (-\alpha_2) = \alpha_1 - \alpha_2$, 即 $2\alpha_1 = 2\alpha_2$, 从而得到 $\alpha_1 = \alpha_2$. 这与假设矛盾, 即 $\alpha_1 - \alpha_2 \notin \mathbb{F}_q^*$, 所以方程 (2.7) 无解, 故此时该置换码的任意两个码字之间的汉明距离为 $q^2 - 1 - 0 = q^2 - 1$.

综上所述可得, 置换码 \mathcal{C}_2 的极小汉明距离为 $q^2 - 1$. 故 \mathcal{C}_2 是一个 $(q^2 - 1, q^2 - q, q^2 - 1)$ -置换码. 证毕.

定理 3.3 设 $q \equiv 5 \pmod{6}$, $\alpha \in \mathbb{F}_{q^2}^*$, 且 α^{q-1} 的阶为 6, $\beta \in \mathbb{F}_q$, 记基于有限域 \mathbb{F}_{q^2} 上的置换多项式簇 $P(x) = \alpha x^{q+2} + \beta x$ 构造的置换码为 \mathcal{C}_3 , 则 \mathcal{C}_3 是一个 $(q^2 - 1, 2(q^2 - q), q^2 - q - 2)$ -置换码.

证 该置换码的码长为 $q^2 - 1$. 要求该置换码的码字数量, 则需求出对应有限域上的置换多项式簇的个数. 我们首先求出所有满足 $\alpha^{6(q-1)} = 1$ 的 α 的个数. 定义集合:

$$\begin{aligned} A &= \{\alpha \in \mathbb{F}_{q^2}^* \mid \alpha^q = \alpha\}, & B &= \{\alpha \in \mathbb{F}_{q^2}^* \mid \alpha^{2q} = \alpha^2\}, \\ C &= \{\alpha \in \mathbb{F}_{q^2}^* \mid \alpha^{3q} = \alpha^3\}, & D &= \{\alpha \in \mathbb{F}_{q^2}^* \mid \alpha^{6q} = \alpha^6\}. \end{aligned}$$

设 g 是有限域 $\mathbb{F}_{q^2}^*$ 中的一个本原元, 则存在正整数 m , 使得 $\alpha = g^m$. 从而 $\alpha^{6(q-1)} = 1$ 可以转化为 $(g^m)^{6(q-1)} = g^0$, 这等价于求解关于 m 的同余方程

$$6m(q-1) \equiv 0 \pmod{q^2-1}. \quad (2.10)$$

由于 $q \equiv 5 \pmod{6}$, $\gcd(6(q-1), q^2-1) = 6(q-1)$, 且 $6(q-1)$ 整除 0, 故同余方程 (2.10) 有解, 且解的个数为 $6(q-1)$. 故集合 D 中包含 $6(q-1)$ 个元素, 同理可以求得集合 C , 集合 B 和集合 A 中包含的元素个数分别为 $3(q-1)$, $2(q-1)$ 和 $q-1$. 又由于集合 $A, B, C \subseteq D$, 则可以求得满足条件 $\alpha^{6(q-1)} = 1$ 的 α 的个数等于

$$\begin{aligned} |D - (A \cup B \cup C)| &= |D| - |A \cup B \cup C| = |D| - |B \cup C| = |D| - |B| - |C| + |B \cap C| \\ &= 6(q-1) - 3(q-1) - 2(q-1) + (q-1) = 2(q-1). \end{aligned}$$

所以在有限域 \mathbb{F}_{q^2} 中, 存在 $2(q-1)$ 个 α 满足 $\text{ord}(\alpha) = 6$. 又因为 β 遍历 \mathbb{F}_q , 故 β 有 q 种不同的取法. 综上所述, 置换码 C_3 的码字数量为 $2(q^2 - q)$.

接下来计算该置换码的极小汉明距离. 任取置换码 C_3 中的两个码字 c_{α_1, β_1} 和 c_{α_2, β_2} , 它们的汉明距离可以转化为讨论方程解的个数. 当 $\alpha_1 = \alpha_2$, $\beta_1 \neq \beta_2$ 或 $\alpha_1 \neq \alpha_2$, $\beta_1 = \beta_2$ 时, 方程

$$\alpha_1 x^{q+2} + \beta_1 x = \alpha_2 x^{q+2} + \beta_2 x \quad (2.11)$$

不存在解, 故此时该置换码的任意两个码字之间的汉明距离为 $q^2 - 1 - 0 = q^2 - 1$. 当 $\alpha_1 \neq \alpha_2$, $\beta_1 \neq \beta_2$ 时, 方程 (2.11) 可化简为 $x^{q+1} = \frac{\beta_2 - \beta_1}{\alpha_1 - \alpha_2}$, 等式两边同时 $q-1$ 次方可得 $x^{q^2-1} = \frac{(\beta_2 - \beta_1)^{q-1}}{(\alpha_1 - \alpha_2)^{q-1}}$. 注意到 $\beta_1 - \beta_2 \in \mathbb{F}_q^*$, $x \in \mathbb{F}_{q^2}^*$, 则有 $(\beta_1 - \beta_2)^{q-1} = 1$, $x^{q^2-1} = 1$, 故上式可化简为 $(\alpha_1 - \alpha_2)^{q-1} = 1$. 这说明方程 (2.11) 有非零解的必要条件是 $\alpha_1 - \alpha_2 \in \mathbb{F}_q^*$. 接下来我们证明若 $\alpha_1 - \alpha_2 \in \mathbb{F}_q^*$, 则方程 (2.11) 有 $q+1$ 个解, 从而这两个码字之间的汉明距离为 $(q^2 - 1) - q - 1 = q^2 - q - 2$.

当 $\alpha_1 - \alpha_2 \in \mathbb{F}_q^*$ 时, 有 $\frac{\beta_2 - \beta_1}{\alpha_1 - \alpha_2} \in \mathbb{F}_q^*$. 由于 $x \in \mathbb{F}_{q^2}^*$, 则存在正整数 i, i_0 使得 $x = g^i$, $\frac{\beta_2 - \beta_1}{\alpha_1 - \alpha_2} = (g^{q-1})^{i_0}$, 则方程 $x^{q+1} = \frac{\beta_2 - \beta_1}{\alpha_1 - \alpha_2}$ 可以转化为关于 i 的同余方程

$$i(q+1) \equiv i_0(q-1) \pmod{q^2-1}.$$

由于 $(q+1, q^2-1) = q+1$, 则该同余方程有解, 且解数为 $q+1$. 故若存在 $\alpha_1, \alpha_2 \in \mathbb{F}_{q^2}^*$ 满足定理所述的条件且使得 $\alpha_1 - \alpha_2 \in \mathbb{F}_q^*$, 则方程 (2.11) 有 $q+1$ 个解.

接下来我们证明存在 $\alpha_1, \alpha_2 \in \mathbb{F}_{q^2}^*$, 其中 $\text{ord}(\alpha_1^{q-1}) = \text{ord}(\alpha_2^{q-1}) = 6$, 使得 $\alpha_1 - \alpha_2 \in \mathbb{F}_q^*$ 成立. 即证明存在 $\alpha_1, \alpha_2 \in D$, $\alpha_1, \alpha_2 \notin A \cup B \cup C$, 使得 $\alpha_1 - \alpha_2 \in \mathbb{F}_q^*$, 其中集合 A, B, C, D 定义同前.

将 \mathbb{F}_{q^2} 看作 \mathbb{F}_q 上的二维向量空间, 记它的一组基为 $\{1, a\}$, 其中 $a \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$, 并设 $b = a^q$. 由于 $q \equiv 5 \pmod{6}$, 则 $6 \mid q^2 - 1$. 由引理 2.1 可知, $\mathbb{F}_{q^2}^*$ 中存在两个六次本原单位根, 不妨设它们分别为 c 和 c^5 . 对 $\mathbb{F}_{q^2}^*$ 中的任意元素 z , 存在 $x, y \in \mathbb{F}_q$, 使得 $z = x + ay$, 则 $z^q = (x + ay)^q = x + by$, 故 $z^{q-1} = \frac{z^q}{z} = \frac{x+by}{x+ay}$. 记 $r = z^{q-1}$, 则

$$z \in A \Leftrightarrow r = 1, z \in B \Leftrightarrow r^2 = 1, z \in C \Leftrightarrow r^3 = 1, z \in D \Leftrightarrow r^6 = 1.$$

若 z 满足 $z \in D$, $z \notin A \cup B \cup C$, 则有 $r^6 = 1$, 且 $r \neq 1$, $r^2 \neq 1$, $r^3 \neq 1$. 这说明 r 是 $\mathbb{F}_{q^2}^*$ 中的六次本原单位根, 即 $r = c$ 或 $r = c^5$. 由于 $r = z^{q-1} = \frac{x+by}{x+ay}$, 下面固定 $y \in \mathbb{F}_q^*$, 我们利用 c 给出 z 的表示. 若 $r = c$, 即 $\frac{x+by}{x+ay} = c$, 则有 $x + by = c(x + ay)$, 从而 $x(1-c) = y(ac - b)$, 故 $\frac{x}{y} = \frac{ac-b}{1-c}$. 将 $\frac{x}{y} = \frac{ac-b}{1-c}$ 记作 u , 则 $x = yu$, 于是可以解得

$z_c = x + ay = y\left(\frac{x}{y} + a\right) = y(u + a) = y\left(\frac{ac-b}{1-c} + a\right)$. 若 $r = c^5$, 类似上述步骤可以解出 $z_{c^5} = y\left(\frac{ac^5-b}{1-c^5} + a\right)$. 此时令 $\alpha_1 = z_c, \alpha_2 = z_{c^5}$, 下面验证 α_1, α_2 满足下列条件:

1. $\alpha_1, \alpha_2 \in D, \alpha_1, \alpha_2 \notin A \cup B \cup C$;
2. $\alpha_1 - \alpha_2 \in \mathbb{F}_q^*$.

由于 $c \in \mathbb{F}_{q^2}^*, q \equiv 5 \pmod{6}$ 且 $c^6 = 1$, 则 $c^q = c^{5+6k} = c^5 \cdot c^{6k} = c^5$. 从而

$$\begin{aligned}\alpha_1^q &= \left[y \left(\frac{ac-b}{1-c} + a \right) \right]^q = y^q \cdot \left(\frac{ac-b}{1-c} + a \right)^q \\ &= y \cdot \left(\frac{a^q c^q - b^q}{1-c^q} + a^q \right) = y \cdot \left(\frac{bc^5 - a}{1-c^5} + b \right) = \frac{y(b-a)}{1-c^5},\end{aligned}$$

进一步可得

$$\alpha_1^{q-1} = \frac{\alpha_1^q}{\alpha_1} = \frac{\frac{y(b-a)}{1-c^5}}{\frac{y(a-b)}{1-c}} = \frac{y(b-a)}{1-c^5} \cdot \frac{1-c}{y(a-b)} = \frac{c-1}{1-c^5} = \frac{c-1}{1-c^4} = c.$$

故 $\alpha_1^{6(q-1)} = (\alpha_1^{q-1})^6 = c^6 = 1$, 这说明 $\alpha_1 \in D$. 因为 c 是 $\mathbb{F}_{q^2}^*$ 中的一个六次本原单位根, 所以 $c \neq 1, c^2 \neq 1, c^3 \neq 1$, 故 $\alpha_1 \notin A \cup B \cup C$. 同理可证, $\alpha_2 \in D$ 且 $\alpha_2 \notin A \cup B \cup C$. 故条件 1 满足. 由于

$$\alpha_1 - \alpha_2 = y \left(\frac{ac-b}{1-c} - \frac{ac^5-b}{1-c^5} \right) = \frac{y(a-b)(c-c^5)}{2-c-c^5},$$

可知 $\alpha_1 \neq \alpha_2$. 下面证明 $\alpha_1 - \alpha_2 \in \mathbb{F}_q^*$. 因为

$$(\alpha_1 - \alpha_2)^q = \frac{y^q(a-b)^q(c-c^5)^q}{(2-c-c^5)^q} = \frac{y(b-a)(c^q-c^{5q})}{2-c^q-c^{5q}},$$

$c^q = c^5, c^{5q} = (c^5)^5 = c$, 故

$$(\alpha_1 - \alpha_2)^q = \frac{y(b-a)(c^5-c)}{2-c^5-c} = \alpha_1 - \alpha_2,$$

即 $\alpha_1 - \alpha_2 \in \mathbb{F}_q^*$, 所以条件 2 也满足.

综上, 我们证明了存在 $\alpha_1, \alpha_2 \in \mathbb{F}_{q^2}^*$ 使得 $\text{ord}(\alpha_1^{q-1}) = \text{ord}(\alpha_2^{q-1}) = 6$ 且 $\alpha_1 - \alpha_2 \in \mathbb{F}_q^*$ 成立. 所以, 置换码 \mathcal{C}_3 的极小汉明距离为 $q^2 - q - 2$, 故 \mathcal{C}_3 是一个 $(q^2 - 1, 2(q^2 - q), q^2 - q - 2)$ -置换码. 证毕.

定理 3.4 设 $q \equiv 2 \pmod{6}$, $\alpha \in \mathbb{F}_{q^2}^*$, 且 α^{q-1} 的阶为 3, $\beta \in \mathbb{F}_q$, 记基于有限域 $\mathbb{F}_{q^2}^*$ 上的置换多项式簇 $P(x) = \alpha x^{q+2} + \beta x$ 构造的置换码为 \mathcal{C}_4 , 则 \mathcal{C}_4 是一个 $(q^2 - 1, 2(q^2 - q), q^2 - q - 2)$ -置换码.

证 该置换码的码长为 $q^2 - 1$. 要求该置换码的码字数, 则需求出对应有限域上的置换多项式簇的个数. 我们首先求出所有满足 $\alpha^{3(q-1)} = 1$ 的 α 的个数. 定义集合:

$$E = \{ \alpha \in \mathbb{F}_{q^2}^* \mid \alpha^q = \alpha \}, \quad F = \{ \alpha \in \mathbb{F}_{q^2}^* \mid \alpha^{3q} = \alpha^3 \}.$$

设 g 是有限域 $\mathbb{F}_{q^2}^*$ 中的一个本原元, 则存在正整数 m , 使得 $\alpha = g^m$. 从而 $\alpha^{3(q-1)} = 1$ 可以转化为 $(g^m)^{3(q-1)} = g^0$, 这等价于求解关于 m 的同余方程

$$3m(q-1) \equiv 0 \pmod{q^2-1}. \quad (2.12)$$

由于 $q \equiv 2 \pmod{6}$, $\gcd(3(q-1), q^2-1) = 3(q-1)$, 故同余方程 (2.12) 有解, 且解的个数为 $3(q-1)$. 故集合 F 中包含 $3(q-1)$ 个元素, 同理可以求得集合 E 中包含的元素个数为 $q-1$. 又由于集合 $E \subseteq F$, 则可以求得满足条件 $\alpha^{3(q-1)} = 1$ 的 α 的个数等于

$$|F - E| = 3(q-1) - (q-1) = 2(q-1).$$

所以在有限域 \mathbb{F}_{q^2} 中, 存在 $2(q-1)$ 个 α 满足 $\text{ord}(\alpha^{q-1}) = 3$. 又因为 β 遍历 \mathbb{F}_q , 故 β 有 q 种不同的取法. 综上所述, 置换码 \mathcal{C}_4 的码字数量为 $2(q^2 - q)$.

接下来计算该置换码的极小汉明距离, 任取置换码 \mathcal{C}_4 中的两个码字 c_{α_1, β_1} 和 c_{α_2, β_2} , 它们之间的汉明距离可以转化为确定如下方程解的个数

$$\alpha_1 x^{q+2} + \beta_1 x = \alpha_2 x^{q+2} + \beta_2 x, \quad (2.13)$$

其中 $x \in \mathbb{F}_q^*$. 当 $\alpha_1 = \alpha_2, \beta_1 \neq \beta_2$ 或 $\alpha_1 \neq \alpha_2, \beta_1 = \beta_2$ 时, 方程 (2.13) 无解. 当 $\alpha_1 \neq \alpha_2$ 且 $\beta_1 \neq \beta_2$, 类似定理 3.3 的证明过程可证得: 方程 (2.13) 有非零解 (此时有 $(q+1)$ 个非零解) 的充要条件是 $\alpha_1 - \alpha_2 \in \mathbb{F}_q^*$.

接下来我们证明存在 $\alpha_1, \alpha_2 \in \mathbb{F}_{q^2}^*$ 满足 $\text{ord}(\alpha_1^{q-1}) = \text{ord}(\alpha_2^{q-1}) = 3$, 且使得 $\alpha_1 - \alpha_2 \in \mathbb{F}_q^*$ 成立. 设 $\{1, a\}$ 为 \mathbb{F}_{q^2} 在 \mathbb{F}_q 上的一组基, 其中 $a \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$, 并设 $b = a^q$. 由于 $q \equiv 2 \pmod{6}$, 则 $3 \mid q^2 - 1$. 由引理 2.1 可知, $\mathbb{F}_{q^2}^*$ 中存在两个三次本原单位根, 不妨设它们分别为 c 与 c^2 . 对 \mathbb{F}_{q^2} 中的任意元素 z , 存在 $x, y \in \mathbb{F}_q$, 使得 $z = x + ay$, 且有 $z^{q-1} = \frac{z^q}{z} = \frac{x+by}{x+ay}$. 记 $r = z^{q-1}$. 若 $r \in F \setminus E$, 则 r 是 $\mathbb{F}_{q^2}^*$ 中的三次本原单位根, 即 $r = c$ 或 $r = c^2$. 现固定 $y \in \mathbb{F}_q^*$, 利用 $r = z^{q-1} = \frac{x+by}{x+ay} = c$ (或 c^2) 解出 z . 若 $\frac{x+by}{x+ay} = c$, 则有 $x + by = c(x + ay)$, 从而 $x(1-c) = y(ac-b)$, 故 $\frac{x}{y} = \frac{ac-b}{1-c}$. 将 $\frac{x}{y} = \frac{ac-b}{1-c}$ 记作 u , 有 $x = yu$, 于是可以解得

$$z_c = x + ay = y \left(\frac{x}{y} + a \right) = y(u + a) = y \left(\frac{ac-b}{1-c} + a \right).$$

对于 $\frac{x+by}{x+ay} = c^2$, 类似上述步骤可以解出 $z_{c^2} = y \left(\frac{ac^2-b}{1-c^2} + a \right)$. 令 $\alpha_1 = z_c, \alpha_2 = z_{c^2}$. 类似定理 3.3 的证明, 我们可以验证 α_1, α_2 满足下列条件:

1. $\alpha_1, \alpha_2 \in E \setminus F$;
2. $\alpha_1 - \alpha_2 \in \mathbb{F}_q^*$.

因此我们证明了存在 $\alpha_1, \alpha_2 \in \mathbb{F}_{q^2}^*$ 满足 $\text{ord}(\alpha_1^{q-1}) = \text{ord}(\alpha_2^{q-1}) = 3$ 且使得 $\alpha_1 - \alpha_2 \in \mathbb{F}_q^*$ 成立. 故当 $\alpha_1 \neq \alpha_2$ 且 $\beta_1 \neq \beta_2$ 时方程 (13) 有 $q+1$ 个解, 此时这两个码字之间的汉明距离为 $q^2 - 1 - q - 1 = q^2 - q - 2$. 故置换码 \mathcal{C}_4 的极小汉明距离为 $q^2 - q - 2$, \mathcal{C}_4 是一个 $(q^2 - 1, 2(q^2 - q), q^2 - q - 2)$ -置换码. 该定理得证.

定理 3.5 设 $q = 5^n$, $\alpha \in \mathbb{F}_{q^2}^*$, 且 α 满足 $\alpha^{q-1} = -1$, $\beta \in \mathbb{F}_q$, 记基于有限域 $\mathbb{F}_{q^2}^*$ 上的置换多项式簇 $P(x) = \alpha x^{2q+3} + \beta x$ 构造的置换码为 C_5 , 则 C_5 是一个 $(q^2 - 1, q^2 - q, q^2 - 1)$ - 置换码.

证 该置换码的码长为 $q^2 - 1$, 置换码 C_5 中码字数量即为满足条件 $\alpha^{q-1} = -1$ 的 α 的个数. 设 g 是有限域 $\mathbb{F}_{q^2}^*$ 中的一个本原元, 则存在正整数 m , 使得 $\alpha = g^m$. 由于在有限域 \mathbb{F}_{q^2} 中, -1 可以用本原元表示为 $-1 = g^{\frac{q^2-1}{2}}$. 则条件 $\alpha^{q-1} = -1$ 可以转化为 $(g^m)^{q-1} = g^{\frac{q^2-1}{2}}$, 这等价于求解关于 m 的同余方程

$$m(q-1) \equiv \frac{q^2-1}{2} \pmod{q^2-1}. \quad (2.14)$$

由于 $\gcd(q-1, q^2-1) = q-1$, 且 $q-1 \mid \frac{q^2-1}{2}$, 故同余方程 (2.14) 有 $q-1$ 个解. 又因为 β 遍历 \mathbb{F}_q , 共有 q 种不同的取法. 从而置换码 C_5 的码字数量为 $(q-1) \times q = q^2 - q$.

下面我们现在来确定 C_5 的极小汉明距离. 任取置换码 C_5 中的两个码字 c_{α_1, β_1} 和 c_{α_2, β_2} , 当 $\alpha_1 = \alpha_2, \beta_1 \neq \beta_2$ 或 $\alpha_1 \neq \alpha_2, \beta_1 = \beta_2$ 时, 方程

$$\alpha_1 x^{2q+3} + \beta_1 x = \alpha_2 x^{2q+3} + \beta_2 x \quad (2.15)$$

不存在解, 故此时该置换码中任意两个码字之间的汉明距离为 $q^2 - 1 - 0 = q^2 - 1$. 当 $\alpha_1 \neq \alpha_2, \beta_1 \neq \beta_2$ 时, 方程 (2.15) 可化简为 $x^{2(q+1)} = \frac{\beta_2 - \beta_1}{\alpha_1 - \alpha_2}$, 等式两边同时 $q-1$ 次方可得

$$x^{2(q^2-1)} = \frac{(\beta_2 - \beta_1)^{q-1}}{(\alpha_1 - \alpha_2)^{q-1}}.$$

注意到 $\beta_1 - \beta_2 \in \mathbb{F}_q^*$, $x \in \mathbb{F}_{q^2}^*$, 则有 $(\beta_1 - \beta_2)^{q-1} = 1$, $x^{2(q^2-1)} = 1$, 故上式可化简为 $(\alpha_1 - \alpha_2)^{q-1} = 1$. 这说明方程 (2.15) 有解的必要条件是 $\alpha_1 - \alpha_2 \in \mathbb{F}_q^*$. 下面说明在题设条件下, $\alpha_1 - \alpha_2 \notin \mathbb{F}_q^*$. 假设 $\alpha_1 - \alpha_2 \in \mathbb{F}_q^*$, 可得 $\alpha_1^q - \alpha_2^q = \alpha_1 - \alpha_2$. 又因为 α_1 和 α_2 满足条件 $\alpha_1^{q-1} = -1, \alpha_2^{q-1} = -1$, 代回上式可得 $\alpha_2 - \alpha_1 = \alpha_1 - \alpha_2$, 从而得到 $\alpha_1 = \alpha_2$. 与假设矛盾. 故 $\alpha_1 - \alpha_2 \notin \mathbb{F}_q^*$, 从而方程 (2.15) 无解.

综上所述, 置换码 C_5 的极小汉明距离为 $q^2 - 1$. 故 C_5 是一个 $(q^2 - 1, q^2 - q, q^2 - 1)$ - 置换码. 证毕.

4 参数分析

本文共构造了五类置换码, 值得强调的是, 这些构造均基于置换多项式方法 (如第 3 节所述). 相较于文献 [11] 中采用的圈搜索、贪婪算法等构造方法, 置换多项式构造法的核心优势在于: 其生成的置换码字序列可由统一的函数形式显式表示, 从而简化了计算置换码的关键参数的过程. 本文构造的五类置换码的具体参数信息见表 1 (其中 Z^+ 表示正整数).

表 1 五类置换码参数表

置换码	码长 n	码字数量 $M(n, d)$	极小汉明距离 d	q 的限制条件
定理 1	$q^3 - 1$	$q^3 - q$	$q^3 - 1$	$q = 2^m, m \in Z^+$
定理 2	$q^2 - 1$	$q^2 - q$	$q^2 - 1$	$q \equiv 0 \pmod{3}$
定理 3	$q^2 - 1$	$2(q^2 - q)$	$q^2 - q - 2$	$q \equiv 5 \pmod{6}$
定理 4	$q^2 - 1$	$2(q^2 - q)$	$q^2 - q - 2$	$q \equiv 2 \pmod{6}$
定理 5	$q^2 - 1$	$q^2 - q$	$q^2 - 1$	$q = 5^n$

表 1 所列的五类置换码均具有接近最大值的极小汉明距离 (其中定理 3.1、定理 3.2 和定理 3.5 构造的置换码的极小汉明距离达到其最大值). 为了具体分析本文构造的置换码, 我们选取定理 3.1 构造的置换码作为代表案例进行详细考察. 分析过程将借助置换码码字数量的理论上界 (定理 4.1) 作为参照.

定理 4.1 ^[18, Theorem 1] 对于一个码长为 n 的置换码, 若其最小汉明距离为 d , 则该置换码的码字数量 $M(n, d)$ 满足上界: $M(n, d) \leq \frac{n!}{(d-1)!}$.

本文在定理 3.1 中构造的置换码为 $(2^{3m}-1, 2^{3m}-2^m, 2^{3m}-1)$ - 置换码, 由定理 3.6 知, 若一个置换码的码长为 $2^{3m}-1$, 且其极小汉明距离为 $2^{3m}-1$, 则该置换码的码字数量 $M(n, d)$ 满足上界: $M(n, d) \leq \frac{(2^{3m}-1)!}{(2^{3m}-2^m)!} = 2^{3m}-1$. 这个理论上界大于 $(2^{3m}-1, 2^{3m}-2^m, 2^{3m}-1)$ - 置换码的码字数量 $2^{3m}-2^m$, 注意到当 m 趋近无穷大时, 有 $\lim_{m \rightarrow \infty} \frac{2^{3m}-1}{2^{3m}-2^m} = 1$, 这说明本文构造的置换码的码字数量渐近地达到了理论上界. 另一方面, 其极小汉明距离 $2^{3m}-1$ 等于最大可能值 $2^{3m}-1$ (码长). 由于置换码的纠错能力 $t = (d-1)/2$, 这说明 $(2^{3m}-1, 2^{3m}-2^m, 2^{3m}-1)$ - 置换码具有良好的纠错能力. 往往置换码的码字数量与纠错能力难以兼顾, 我们构造的五类置换码接近最大可能值的极小汉明距离, 而其码字数量还存在提升空间. 如何在保持优秀纠错能力的同时, 进一步提升置换码的码字数量, 或者寻找在码字数量和距离之间取得更好平衡的构造方法, 仍然是极具挑战性的研究方向.

5 结论

本文研究了五类置换码的构造, 确定了所构造置换码的参数——码长、码字数量与极小汉明距离. 所构造的置换码是基于五类置换二项式簇构造的. 所做工作的主要贡献在于:

1、通过分析每一类置换二项式簇中置换二项式的系数条件, 确定了置换二项式簇中所包含的置换二项式的数目, 从而确定了所构造置换码的码字数量;

2、通过研究有限域上特定方程存在解的条件, 从而确定了所构造置换码的极小距离;

3、本文构造的五类置换码具有较好的纠错能力, 部分置换码的极小距离达到了最大值 (等于码字长度), 且码字数量渐近地达到了上界 (定理 3.1, 3.2, 3.5);

后续我们将寻找其他置换多项式簇来探索置换码的构造, 以期设计出更多性能优异的置换码并研究它们在通信系统中的应用.

参 考 文 献

- [1] Smith D H, Montemanni R. A new table of permutation codes [J]. Designs, Codes and Cryptography, 2012, 63(2): 241–253.
- [2] Ian F B. Permutation codes for discrete channels [J]. IEEE Trans. Inf. Theory, 1974, 20(1): 138–140.
- [3] Pavlidou N, Vinck A H, Yazdani J, Honary B. Powerline communications: state of the art and future trends [J]. IEEE Commun. Mag., 2003, 41(7): 34–40.
- [4] Colbourn C J, Klove T, Ling A C. Permutation arrays for powerline communication and mutually orthogonal latin squares [J]. IEEE Transactions on Information Theory, 2004, 50(6): 1289–1291.
- [5] Barg A, Mazumdar A. Codes in permutations and error correction for rank modulation [J]. IEEE Transactions on Information Theory, 2010, 13: (854–858).
- [6] Slepian D. Permutation modulation [J]. Proc. IEEE, 1965, 53(3): 228–236.

- [7] Wadayama T, AJ H. A multilevel construction of permutation codes [J]. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, 2001, 84: 2518–2522.
- [8] Dukes P, Sawchuck N. Bounds on permutation codes of distance four [J]. *Journal of Algebraic Combinatorics*, 2010, 31(1): 143–158.
- [9] Frankl P, Deza M. On the maximum number of permutations with given maximal or minimal distance [J]. *Journal of Combinatorial Theory*, 1977, 22(3): 352–360.
- [10] Cameron P J. Permutation codes [J]. *European Journal of Combinatorics*, 2010, 31(2): 482–490.
- [11] Chu W, Colbourn C J, Dukes P. Constructions for permutation codes in powerline communications [J]. *Designs Codes and Cryptography*, 2004, 32(1): 51–64.
- [12] Wang Q. Polynomials over finite fields: an index approach [C]. *Combinatorics and finite fields: Difference sets, polynomials, pseudorandomness and applications*, 2019, 23: 319–48.
- [13] Tarnanen H. Upper bounds on permutation codes via linear programming[J]. *European Journal of Combinatorics*, 1999, 20(1): 101–114.
- [14] Cao X, Hu L, Zha Z. Constructing permutation polynomials from piecewise permutations[J]. *Finite Fields and Their Applications*, 2014, 26: 162–174.
- [15] Bartoli D, Giulietti M. Permutation polynomials, fractional polynomials, and algebraic curves [J]. *Finite Fields and Their Applications*, 2018, 51: 1–16.
- [16] 林东岱. 代数学基础与有限域 (第二版)[M]. 北京: 高等教育出版社, 2022.
- [17] Lidl R. Introduction to finite fields and their applications[M]. Cambridge: Cambridge University Press, 1997.
- [18] Vinck A H, Haering J, Wadayama T. Coded M-FSK for power line communications[C]. *Proceedings of the 2000 IEEE International Symposium on Information Theory*. Sorrento, Italy, 2000: 137.
- [19] Sharma R K, Gupta Rohit. Determination of a type of permutation binomials and trinomials [J]. *Applicable Algebra in Engineering Communication and Computing*, 2020, 31(1): 65–86.

CONSTRUCTION AND PARAMETER ANALYSIS OF FIVE CLASSES OF PERMUTATION CODES FROM PERMUTATION POLYNOMIAL CLUSTERS

YE Na, XIA Yong-bo

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

Abstract: This paper investigates the construction of permutation codes based on the permutation polynomials over finite fields. By utilizing some permutation polynomials of the form $f(x) = \alpha x^m + \beta x$ (where m is a positive integer) over finite fields, five classes of permutation codes are constructed. Employing some techniques of solving equations over finite fields, the parameters of these codes are determined, including the code length, cardinality, and minimum Hamming distance. The obtained results enrich the theory about the construction of permutation codes.

Keywords: permutation polynomial; permutation code; minimum Hamming distance; cardinality; Finite field

2010 MR Subject Classification: 11T06; 94B60; 94A24