arXiv:2603.03368v1 [math.NT] 2 Mar 2026

有限域上的置换三项式与完全置换多项式：基于纤维判据

CHAHRAZADE BOUYACOUB、ASMAE EL-BAZ 和 OMAR KIHEL

Abstract. 我们通过将验证归结为在一个三元素乘法子群上的显式计算，利用 Zieve纤维判据，为 Bousalmi、Bayad 和 Derbal 最近关于置换多项式的结果给出了简洁的新证明。在此基础上，我们结合 Zieve 定理与 AGW 判据，建立了一个通用框架，通过对单位根立方根进行纤维分解，在有限域上构造完全置换多项式。该判据的标量特例可导出易于构造和验证的多个族。我们通过具体例子展示这一构造，并通过反例说明其背后的算术条件是尖锐的。

1. Introduction

有限域上的置换多项式——在 $\mathbb{F}_q$ 上诱导双射的多项式 $f \in \mathbb{F}_q[X]$ ——自 Hermite 和 Dickson 在十九世纪的奠基性工作以来，一直备受关注。对它们的研究横跨数论、组合学和代数，并因其在编码理论、密码学以及伪随机序列设计中的应用而进一步受到推动。一个自然的强化概念是完全置换多项式 （CPP）：满足以下条件的多项式 f，其中 f 和 $f+X$ 都在 $\mathbb{F}_q$ 上构成置换。完全置换多项式所要求的条件严格得多，因此也相应地更难构造。

在证明置换性质方面，最有效的现代工具包括两种约化原理。第一种由 Zieve [5], 提出，适用于形如 $f(X) = X^r h\left(X^{(q-1)/d}\right)$ 的多项式，并将 $\mathbb{F}_q$ 上的置换问题归结为两个条件：对 r 的互素要求，以及在较小的乘法子群 μ_d上的置换检验。第二种是 Akbary、Ghioca 和 Wang [1], 提出的 AGW 判据，它提供了一个一般性的逐纤维框架：将有限集上的双射分解为纤维的置换，以及对每个单独纤维的双射性。这两种工具已经

Date：2026年3月5日。2020 *Mathematics Subject Classification.* 主要分类 11T06；次要分类 11T71、12E20。*Key words and phrases.* 置换多项式、完全置换多项式、有限域、Zieve 定理、AGW 判据。

成为构造新置换族的标准方法。在这一方向上，Ayad、Belghaba 和 Kihel [2, 3] 研究了有限域上的置换二项式$ax^n + x^m$，在关于参数 $d = \gcd(n-m, q-1)$ 的严格算术条件下建立了不存在性结果，并且仅根据 d 对基域的大小给出了界。

2021 年，Bousalmi、Bayad 和 Derbal [4]给出了形如 $X^r(X^{2(q-1)/3} + \alpha X^{(q-1)/3} + \beta)$ 的置换三项式的显式族，它们定义在 $\mathbb{F}_q$ 上，满足 $q \equiv 1$ （模 3），参数由单位根或满足简单算术条件的域元素给出（文献 [4] 中的定理 3 和 4）。他们的证明依赖直接求值和分类讨论。我们的首项贡献是通过系统地应用 Zieve 判据，为这些结果给出简短明晰的替代证明，并采用 $d = 3$：在每种情况下，验证都归结为在三元素群 μ_3 上进行显式计算。

我们的第二项也是主要贡献，涉及完全置换多项式。我们基于 AGW 框架，建立了一个一般判据，用于判定形如 $f(X) = X^r c(X^{(q-1)/3})$ 的多项式何时是 $\mathbb{F}_q$ 上的 CPP，其中 $q \equiv 1$（模 9）。该判据分解为四个可验证条件——互素与非消失假设、纤维单射性、诱导映射的良定义条件，以及在 μ_3 上的置换检验——并统一处理一系列三项式形式。随后，我们专门讨论一种标量纤维特化，它出现在 $r \equiv 1$ （模 $(q-1)/3$）时：在此情形下，纤维映射变为标量乘法，四个条件也简化为简单的非消失检验和置换检验。由此得到的族判据易于应用，并能构造出显式的 CPP 族。最后，我们通过具体反例表明，同余条件 $q \equiv 1$ （模 9）对于我们的构造至关重要；也就是说，若只假设 $q \equiv 1$ （模 3），自然的参数选择便会失效。

2. Preliminaries

2.1. 记号与常设假设。 全文中，$\mathbb{F}_q$ 表示一个阶为 q 的有限域，且 $q \equiv 1 \pmod 3$，并令

$$s := \frac{q-1}{3}.$$

乘法群 $\mathbb{F}_q^*$ 含有唯一的3阶子群，

$$\mu_3 := \{u \in \mathbb{F}_q^* : u^3 = 1\} = \{1, \omega, \omega^2\},$$

其中 ω 是一个固定的本原三次单位根，从而 $\omega^2 + \omega + 1 = 0$。映射 π: $\mathbb{F}_q^* \to \mu_3$ 由 $\pi(x) = x^s$ 定义，是一个满射群同态，其核为

$$K := \ker \pi = \{z \in \mathbb{F}_q^* : z^s = 1\},$$

一个阶为 s 的子群。对每个 $u \in \mu_3$，纤维 $\pi^{-1}(u) = tK$，其中 t 是 $\mathbb{F}_q^*$ 中任意满足 $t^s = u$ 的元素，是 K 的一个陪集，其基数为 s。三个纤维 $\pi^{-1}(1)$、$\pi^{-1}(\omega)$、$\pi^{-1}(\omega^2)$ 构成 $\mathbb{F}_q^*$ 的一个划分。

以下由 Zieve 提出的结果 [5]，将某些结构化多项式是否置换 $\mathbb{F}_q$ 的问题，归结为在小群 μ_d 上进行置换检验。

定理 2.1 (Zieve [5])。设 d 和 r 是满足 $d \mid q-1$ 的正整数，并设 $h \in \mathbb{F}_q[X]$。则

$$f(X) \;=\; X^r\, h\Big(X^{(q-1)/d}\Big)$$

是 $\mathbb{F}_q$ 上的置换多项式，当且仅当
(1) 最大公约数$\left(r,\ \dfrac{q-1}{d}\right) = 1$，且(2) 映射 $u \mapsto u^r\, h(u)^{(q-1)/d}$ 是 μ_d 的一个置换。

本文仅将定理 2.1 用于 $d = 3$，因此条件 (1) 变为最大公约数$(r,\ s) = 1$，而条件 (2) 则是在三元群 μ_3 上进行置换检验。

定理 2.2 (AGW 判据 [1, 引理 1。2])。设 A、S、S 为有限集，满足 $|S| = |S|$，并设 $g\colon A \to A$、$\bar{g}\colon S \to S$、$\lambda\colon A \to S$、$\lambda\colon A \to S$ 为满足以下条件的映射

$$\bar{\lambda} \circ g \;=\; \bar{g} \circ \lambda.$$

如果 λ 和 λ 均为满射，则以下条件等价：

（i） g 是 A上的双射；（ii） $\bar{g}$ 是从 S 到 $\bar{S}$的双射，并且对每个 $s \in S$，g 在 $\lambda^{-1}(s)$ 上是单射。

本文将 AGW 判据与 $A = \mathbb{F}_q^*$、$S = S = \mu_3$ 和$\lambda = \lambda = \pi$结合应用：$x \mapsto x^s$。

3. Short proofs of the Bousalmi–Bayad–Derbal theorems

本节通过将 Zieve 定理 2.1 与 $d = 3$直接结合应用，为 [4] 中的定理 3 和 4 给出新的证明。在每种情况下，验证都归结为对 $\mu_3 = \{1, \omega, \omega^2\}$进行显式计算。

定理 3.1 （中的定理 3）。设 $q \equiv 1$ （模 3），且设 r 为满足 最大公约数（r, $q-1$） $= 1$的正整数。
(1) 对于满足 $(3\delta^2+1)^s = 1$ 且属于 $\mathbb{F}_q$ 的每个 $\delta \in \mu_3$，多项式

$$f(X) \;=\; X^r\big(X^{2s} + \delta\, X^s + \delta^2 + 1\big)$$

是 $\mathbb{F}_q$ 上的置换多项式。
(2) 对于满足 $\binom{\gamma+2}{\gamma-1} = 1$ 且属于 $\mathbb{F}_q$ 的任意 $\gamma \in \mathbb{F}_q \setminus \{1, -2\}$，多项式

$$f(X) \;=\; X^r\big(X^{2s} + X^s + \gamma\big)$$

是 $\mathbb{F}_q$ 上的置换多项式。

证明。由于 $\gcd(r, q-1) = 1$ 蕴含 $\gcd(r, s) = 1$，定理 2.1 的条件 (1) 在两部分中均成立。剩下只需验证 $u \mapsto u^r h(u)^s$ 置换 μ_3，其中 h 是相应的二次多项式。

第（1）部分。定义 $h_\delta(X) = X^2 + \delta X + \delta^2 + 1$。我们利用关系 $1 + \omega + \omega^2 = 0$，在 μ_3 的每个元素上计算 h_δ。

如果 $\delta = 1$，那么

$$h_1(1) = 4, \qquad h_1(\omega) = \omega^2 + \omega + 2 = 1, \qquad h_1(\omega^2) = \omega + \omega^2 + 2 = 1.$$

如果 $\delta = \omega$，那么

$$h_\omega(1) = 1+\omega+\omega^2+1 = 1, \qquad h_\omega(\omega) = \omega^2+\omega^2+\omega^2+1 = 3\omega^2+1, \qquad h_\omega(\omega^2) = 1.$$

如果 $\delta = \omega^2$，那么

$$h_{\omega^2}(1) = 1, \qquad h_{\omega^2}(\omega) = 1, \qquad h_{\omega^2}(\omega^2) = 3\omega + 1.$$

在每种情况下，三个值中恰有一个等于 $3\delta^2+1$，其余两个等于 1。根据假设 $(3\delta^2 + 1)^s = 1$，因此对每个 $u \in \mu_3$，$h_\delta(u)^s = 1$。所以，对所有 $u \in \mu_3$，诱导映射满足 $u \mapsto u^r h_\delta(u)^s = u^r$。由于最大公约数 $(r, 3) = 1$（这是最大公约数 $(r, q-1) = 1$ 且 $3 \mid q-1$ 的结果），映射 $u \mapsto u^r$ 是循环群 μ_3 上的置换。根据定理 2.1，f 是 $\mathbb{F}_q$ 上的置换多项式。

第（2）部分。定义 $h_\gamma(X) = X^2 + X + \gamma$。在 μ_3 上求值：

$$h_\gamma(1) = 2 + \gamma, \qquad h_\gamma(\omega) = \omega^2 + \omega + \gamma = \gamma - 1, \qquad h_\gamma(\omega^2) = \gamma - 1.$$

$u \mapsto u^r h_\gamma(u)^s$ 在 μ_3 上的三个像因此为

$$(2+\gamma)^s, \qquad \omega^r(\gamma-1)^s, \qquad \omega^{2r}(\gamma-1)^s.$$

我们验证这三个值两两不同。假设 $\left(\frac{\gamma+2}{\gamma-1}\right)^s = 1$ 给出 $(2+\gamma)^s = (\gamma-1)^s$。三个两两比值为

$$\frac{(2+\gamma)^s}{\omega^r(\gamma-1)^s} = \frac{1}{\omega^r}, \qquad \frac{\omega^r(\gamma-1)^s}{\omega^{2r}(\gamma-1)^s} = \frac{1}{\omega^r}, \qquad \frac{(2+\gamma)^s}{\omega^{2r}(\gamma-1)^s} = \frac{1}{\omega^{2r}}.$$

由于最大公约数 $(r,3) = 1$，ω^r 和 ω^{2r} 都不等于 1，因此这三个比值都不等于 1。三个像两两不同，故 $u \mapsto u^r h_\gamma(u)^s$ 置换 μ_3。根据定理 2.1，f 是 $\mathbb{F}_q$ 上的置换多项式。□

定理3.2 ([4]的定理4)。设 $q \equiv 1$ (模 3)，设 $p =$ 特征$(\mathbb{F}_q)$，并设 r 为正整数，且 最大公约数 $(r, q-1) = 1$。

(1) 若 $q \equiv 1$（模 6），则 $f(X) = X^r\left(X^{2s} + X^s + \frac{p-1}{2}\right)$ 是 $\mathbb{F}_q$ 的置换多项式。（2）若 $p \equiv 1$（模 3）且 $q = p^{3k}$ 满足 $k \geq 1$，则 $f(X) = X^r$（$X^{2s}+X^s+2$）是 $\mathbb{F}_q$ 的置换多项式。（3）若 $p \geq 5$、$p \equiv -1$（模 3），且 $q = p^{2k}$ 满足 $k \geq 1$，则 $f(X) = X^r$（$X^{2s} + X^s + 2$）是 $\mathbb{F}_q$ 的置换多项式。

证明。 每一项都是定理 3.1(2)在 γ 取特定值时的特殊情形：只需验证在给定假设下 $\left(\frac{\gamma+2}{\gamma-1}\right)^s = 1$，随后定理 3.1(2)证明中的互异性论证即可原样适用。

项 *(1)*： $\gamma = (p-1)/2$， $q \equiv 1$ (模 6)。我们计算

$$\frac{\gamma+2}{\gamma-1} = \frac{p+3}{p-3} \equiv \frac{3}{-3} = -1 \pmod{p}.$$

由于 $q \equiv 1$ (模 6)，整数 $s = (q-1)/3$ 是偶数，因此 $(-1)^s = 1$ 属于 $\mathbb{F}_q$。

项 *(2)*： $\gamma = 2$， $p \equiv 1$ (模 3)， $q = p^{3k}$。这里 $(\gamma+2)/(\gamma-1) = 4$。我们证明 $p-1 \mid s$。写作

$$\frac{q-1}{p-1} = 1 + p + \cdots + p^{3k-1},$$

这个和有 $3k$ 项，每项模 3 同余于 1（因为 $p \equiv 1$ (模 3)），所以该和能被 3 整除。因此 $s = (q-1)/3$ 能被 $p-1$ 整除。由于 $4 \in \mathbb{F}_p^*$ 且 $\mathbb{F}_p^*$ 的阶为 $p-1$，我们得到 $4^s = 1$。

第 *(3)* 项： $\gamma = 2$， $p \geq 5$， $p \equiv -1$ (模 3)， $q = p^{2k}$。再次，$(\gamma+2)/(\gamma-1) = 4$，我们证明 $p-1 \mid s$。其和

$$\frac{q-1}{p-1} = 1 + p + \cdots + p^{2k-1}$$

有 $2k$ 项，余数交替为 1， -1， 1， -1，.....模 3（因为 $p \equiv -1$ (模 3)）。这些项两两配对，每对的和为 $1 + (-1) = 0$(模 3)，因此总和能被 3 整除。于是 $p-1 \mid s$ 且 $4^s = 1$。□

4. A general criterion for index-3 complete permutation polynomials

在第 3 节中，我们已经证明 Zieve 判据为检验 $f(X) = X^r c(X^s)$ 的置换性质提供了一种高效方法。现在我们转向一个要求更高的问题：何时 f 是一个完全置换多项式，也就是说，何时 $F(X) = f(X) + X$ 也能置换 $\mathbb{F}_q$? F的结构使得无法直接应用 Zieve 定理，因为加法项 X破坏了乘法形式 $X^r h(X^s)$。因此，我们采用 AGW 判据（定理 2.2），将 F在 $\mathbb{F}_q^*$ 上的双射性分解为对 μ_3 的置换检验，以及投影 $\pi\colon x \mapsto x^s$的每个纤维上的单射性。

定理 4.1. 设 $q \equiv 1 \pmod 3$，设 $s = (q-1)/3$，且设 r 为一个正整数。设 $c\colon \mu_3 \to \mathbb{F}_q^*$ 是一个函数，并通过 $c(x^s)$ 将其延拓至 $\mathbb{F}_q^*$，定义

$$f(X) = X^r\, c(X^s), \qquad F(X) = f(X) + X.$$

假设以下条件成立：

(G1) $\gcd(r, s) = 1$，$\gcd(r, 3) = 1$，且 $c(u)^s = 1$ 对所有 $u \in \mu_3$。

(G2) 对于每个 $u \in \mu_3$ 以及每个满足 $t^s = u$ 的 $t \in \mathbb{F}_q^*$，定义 $\beta_u := c(u)\, t^{r-1}$，该映射

$$\varphi_u \colon K \longrightarrow \mathbb{F}_q^*, \qquad z \longmapsto z\big(1 + \beta_u\, z^{r-1}\big)\,,$$

是单射。

(G3) 对于每个 $u \in \mu_3$，其值

$$v(u) := \big(1 + \beta_u\, z^{r-1}\big)^s$$

与 $z \in K$ 的选择无关，且属于 μ_3。

(G4) 映射 $\psi(u) := u\mu_3 v(u)$ 是 μ_3 的一个置换。

那么 f 是 $\mathbb{F}_q$ 上的完全置换多项式。

证明。由 (G1)，对所有 $u \in \mu_3$，有 $\gcd(r, s) = 1$，且 $c(u)^s = 1$，因此映射 $u \mapsto u^r c(u)^s = u^r$ 是 μ_3 的一个置换（因为 $\gcd(r,3) = 1$）。由 Zieve 定理 2.1，取 $d = 3$，可得 f 是 $\mathbb{F}_q$ 上的置换多项式。

我们利用 AGW 判据（定理 2.2）及以下数据证明 F 将 $\mathbb{F}_q^*$ 置换：

$$A = \mathbb{F}_q^*, \quad S = \bar{S} = \mu_3, \quad \lambda = \bar{\lambda} = \pi, \quad g = F, \quad \bar{g} = \bar{\psi}.$$

由于 $\pi\colon \mathbb{F}_q^* \to \mu_3$ 是一个满射群同态，关于 λ 和 $\bar{\lambda}$ 的满射性假设成立。接下来只需证明交换性 $\pi \circ F = \psi \circ \pi$ 以及条件 (ii) 的两个要求。

固定 $u \in \mu_3$，并选择满足 $t^s = u$ 的 $t \in \mathbb{F}_q^*$。纤维 $\pi^{-1}(u) = tK$ 中的每个元素都可唯一地写成 $x = tz$，其中 $z \in K$，直接计算可得

$$F(tz) = (tz)^r c((tz)^s) + tz = t^r z^r c(u) + tz = tz\big(1 + \beta_u\, z^{r-1}\big),$$

其中 $\beta_u := c(u)\, t^{r-1} \neq 0$。对两边应用 π：

$$\pi\big(F(tz)\big) = (tz)^s\big(1 + \beta_u\, z^{r-1}\big)^s = u \cdot \big(1 + \beta_u\, z^{r-1}\big)^s. \tag{1}$$

由 (G3)，因子 $(1 + \beta_u\, z^{r-1})^s = v(u)$ 与 $z \in K$ 无关，因此得到 (1)

$$\pi\big(F(x)\big) = u \cdot v(u) = \bar{\psi}(u) = \bar{\psi}\big(\pi(x)\big)$$

对每个 $x \in \pi^{-1}(u)$ 都成立。由于 $u \in \mu_3$ 是任意的，交换性 $\pi \circ F = \bar{\psi} \circ \pi$ 在整个 $\mathbb{F}_q^*$ 上成立。

由 (G4)，$\psi\colon \mu_3 \to \mu_3$ 是一个双射。对于纤维上的单射性，注意到 $F(tz) = t \cdot \varphi_u(z)$，其中 $\varphi_u(z) = z(1 + \beta_u\, z^{r-1})$。由于 $t \neq 0$，等式 $F(tz_1) = F(tz_2)$ 可推出 $\varphi_u(z_1) = \varphi_u(z_2)$，因此由 (G2) 得 $z_1 = z_2$。于是，对每个 $u \in \mu_3$，F 在 $\pi^{-1}(u)$ 上是单射的。

定理 2.2 中条件 (ii) 的两个要求均得到满足，因此 F 是 $\mathbb{F}_q^*$ 上的双射。由于 $F(0) = 0$，映射 F 置换了 $\mathbb{F}_q$。□

注记 4.2. 条件 (G2) 和 (G3) 涉及为纤维 $\pi^{-1}(u)$ 选择一个代表元 t，但这两个条件都不依赖于这一选择。事实上，将 t 替换为满足 $z_0 \in K$ 的 $t' = tz_0$，会将 β_u 替换为 $\beta'_u = \beta_u\, z_0^{r-1}$，而

映射 $\varphi_u(z)$ 会变为映射 $\varphi_u(z_0^{-1}z')$，后者是单射当且仅当 φ_u 是单射。同样，当 z 遍历 K 时，乘积 $z_0^{r-1}z^{r-1}$ 遍历的集合与 z^{r-1} 遍历的集合相同，因此 (G3) 中的不变性得以保持。

注记 4.3. 当 $r \equiv 1$（模 s）时，记 $r-1 = ks$。于是对每个 $z \in K$，我们有 $z^{r-1} = (z^s)^k = 1$，因此条件 (G3) 在 $v(u) = (1+\beta_u)^s$ 下自动成立，而 (G2) 归结为 $1+\beta_u \neq 0$（一个简单的非消失）。这一特殊化是下一节的主题。

5. The scalar fiber specialization

当 $r \equiv 1$（模 s）时，定理 4.1 的一般判别准则大为简化：纤维映射变为标量乘法，四个条件 (G1)–(G4) 归结为初等的非消失与置换检验。这一特殊化是该判别准则最实用的形式，也是我们在第6节例子中所采用的形式。

定理5.1（标量纤维完全置换多项式定理）。设 $q \equiv 1$（模 9），设 $s = (q-1)/3$，并将 $r = 1+ks$ 写作某个正整数 k。设 $c\colon \mu_3 \to \mathbb{F}_q^*$是一个函数，满足对所有 $u \in \mu_3$都有 $c(u)^s = 1$，并定义

$$f(X) = X^r\, c(X^s), \qquad F(X) = f(X) + X.$$

对于每个 $u \in \mu_3$，令 $\tau(u) := 1 + c(u)\, u^k$以及 $v(u) := \tau(u)^s$。假设：

（H1） $\tau(u) \neq 0$ 对所有 $u \in \mu_3$均成立。（H2） 由 $\psi(u) = u \cdot v(u)$ 定义的映射 $\psi\colon \mu_3 \to \mu_3$ 是 μ_3上的置换。

那么，f 是 $\mathbb{F}_q$上的完全置换多项式。

证明。由于 $q \equiv 1$（模 9），我们有 $3 \mid s$，因此 $r = 1+ks \equiv 1$（模 3），从而 $\gcd(r, 3) = 1$。此外，$\gcd(r, s) = \gcd(1+ks, s) = 1$。结合假设对所有 $u \in \mu_3$均有 $c(u)^s = 1$，我们看到，映射 $u \mapsto u^r c(u)^s = u^r$ 是 μ_3 上的恒等映射（因为 $r \equiv 1$（模 3）），因此是一个置换。Zieve 定理 2.1 随即推出，f 是 $\mathbb{F}_q$上的置换多项式。

我们验证 F 满足定理 4.1 的条件。固定 $u \in \mu_3$ 和 $t \in \mathbb{F}_q^*$，使得 $t^s = u$。对于任意 $z \in K$，恒等式 $z^{r-1} = z^{ks} = (z^s)^k = 1$ 将纤维表达式化简为

$$F(tz) = tz\big(1 + c(u)\, t^{r-1}\big).$$

由于 $t^{r-1} = t^{ks} = (t^s)^k = u^k$，标量 $\tau(u) = 1 + c(u)\, u^k$ 与 z 及代表元 t 的选取均无关，并且根据 (H1) 它非零。因此

$$F(tz) = \tau(u) \cdot tz$$

对于每个 $z \in K$：映射 F 在纤维 $\pi^{-1}(u)$ 上的作用是乘以非零常数 $\tau(u)$，显然是单射。这就验证了 (G2)。

$z^{r-1} = 1$ 在 K 上的恒等式使得 (G3) 自动成立：对于每个 $z \in K$，

$$\big(1 + \beta_u\, z^{r-1}\big)^s = \big(1 + c(u)\, u^k\big)^s = \tau(u)^s = v(u),$$

它与 z 无关，且属于 μ_3。

¯最后，条件(G4)要求 $\psi(u) = u \cdot v(u)$是 μ_3的一个置换，这恰好就是(H2)。根据定理 4.1， F 是 $\mathbb{F}_q$上的置换多项式。□

注记 5.2。 假设 $q \equiv 1 \pmod 9$ 仅用于确保$3 \mid s$，进而保证 gcd(r，3) $= 1$。如果 $q \equiv 1 \pmod 3$ 但 $q \not\equiv 1 \pmod 9$，那么 $3 \nmid s$，而同余 $r \equiv 1 \pmod s$ 不再能推出 $r \equiv 1 \pmod 3$。第 6 节中的反例表明，在这种情况下，这一构造确实可能失效。

推论 5.3。 在定理 5.1的假设下，设 $v(u) = \tau(u)^s$ 对所有 $u \in \mu_3$都取常值 $\alpha \in \mu_3$ 。则条件 (H1)和 (H2) 均成立，并且 $f(X) = X^r c(X^s)$ 是 $\mathbb{F}_q$ 上的完全置换多项式。

证明。 由于 $\alpha = \tau(u)^s \neq 0$，标量 $\tau(u)$ 对每个 $u \in \mu_3$，¯都非零，这就是 (H1)。诱导映射为 $\psi(u) = u \cdot \alpha = \alpha u$，是循环群 μ_3 上的旋转，因此是双射。这验证了 (H2)，结论由定理5.1得出。□

6. Examples and counterexamples

本节将通过明确的完全置换多项式构造来说明族判据（推论 5.3），然后通过反例证明，同余 $q \equiv 1 \pmod 9$ 对我们的方法至关重要。

在全文中，我们固定 $\delta \in \mathbb{F}_q$，使其满足 $\delta^2 + \delta + 1 = 0$，并取 $c(u) = u^2 + \delta u + \delta^2 + 1$，从而使 δ 扮演 ω 和 $\mu_3 = \{1, \delta, \delta^2\}$ 的角色。根据定理 3.1(1) 的证明，

$$c(1) = 1, \qquad c(\delta^2) = 1, \qquad c(\delta) = 3\delta^2 + 1,$$

并且当（$3\delta^2 + 1$）$^s = 1$时，对所有 $u \in \mu_3$ 均有 c（u）$^s = 1$。我们研究标量纤维情形 $r = 1 + ks$，并定义 f（X）$= X^r c$（X^s）以及 F（X）$= f$（X）$+ X$。对每个 $u \in \mu_3$，我们按定理5.1 中的定义，记 τ（u）$= 1 + c$（u）u^k，以及 v（u）$= \tau$（u）^{s}。

6.1. 完全置换多项式示例。 对于每个示例，我们验证对所有 ¯$u \in \mu_3$ 均有 τ（u）$\neq 0$，且 v（u）在 μ_3 上为常数，因此 ψ（u）$= u\, v$（u）是 μ_3 的旋转（推论 5.3）。

(a) $q = 109$, $s = 36$, $\delta = 63$, $k = 2$ ($r = 73$)。 可以验证 $63^2 + 63 + 1 = 4033 = 37 \times 109 \equiv 0$，从而确认 $\delta \in \mu_3$，其中 $\delta^2 \equiv 45$ （模 109）。我们计算 c（δ）$= 3 \cdot 45 + 1 \equiv 27$ （模 109），并验证 $27^{36} \equiv 1$ （模 109），因此对所有 $u \in \mu_3$ 均有 c（u）$^s = 1$。

由于 $k = 2$，单位根的立方满足 $1^2 = 1$、$\delta^2 \equiv 45$，$(\delta^2)^2 = \delta^4 = \delta \equiv 63$，因此：

$$\begin{aligned} \tau(1) &= 1 + c(1) \cdot 1^2 = 1 + 1 = 2, \\ \tau(\delta) &= 1 + c(\delta) \cdot \delta^2 = 1 + 27 \cdot 45 \equiv 1 + 16 = 17 \pmod{109}, \\ \tau(\delta^2) &= 1 + c(\delta^2) \cdot \delta = 1 + 63 = 64. \end{aligned}$$

这三个值均非零，从而验证了 (H1)。直接计算可得，对于每个 $u \in \mu_3$，$v(u) = \tau(u)^{36} \equiv 1 \pmod{109}$，因此 $\bar{\psi}(u) = u \cdot 1 = u$ 是 μ_3 上的恒等映射。根据推论 5.3，$f(X) = X^{73} c(X^{36})$ 是 $\mathbb{F}_{109}$ 上的完全置换多项式。

(b) $q = 163$, $s = 54$, $\delta = 58$, $k = 3$ ($r = 163$)。我们有 $58^2 + 58 + 1 = 3423 = 21 \times 163 \equiv 0$，其中 $\delta^2 \equiv 104 \pmod{163}$。计算 $c(\delta) = 3 \cdot 104 + 1 \equiv 150 \pmod{163}$，并验证 $150^{54} \equiv 1 \pmod{163}$。

由于对所有 $u \in \mu_3$，$k = 3$ 且 $u^3 = 1$，因此对于每个 u，我们有 $\tau(u) = 1 + c(u)$：

$$\tau(1) = 1 + c(1) = 2,$$
$$\tau(\delta) = 1 + c(\delta) = 1 + 150 = 151,$$
$$\tau(\delta^2) = 1 + c(\delta^2) = 2.$$

这三个值均非零。直接计算可得，对于每个 $u \in \mu_3$，$v(u) = \tau(u)^{54} \equiv 104 \equiv \delta^2 \pmod{163}$。由于 v 是常数，其值为 $\delta^2 \in \mu_3$，映射 $\bar{\psi}(u) = \delta^2 u$ 是 μ_3的一个非平凡旋转：

$$\bar{\psi}(1) = \delta^2, \qquad \bar{\psi}(\delta) = \delta^3 = 1, \qquad \bar{\psi}(\delta^2) = \delta^4 = \delta.$$

根据推论 5.3，$f(X) = X^{163} c(X^{54})$ 是 $\mathbb{F}_{163}$的完全置换多项式。

(c) $q = 199$, $s = 66$, $\delta = 106$, $k = 3$ ($r = 199$)。我们有 $106^2 + 106 + 1 = 11343 = 57 \times 199 \equiv 0$，其中 $\delta^2 \equiv 92 \pmod{199}$。计算 $c(\delta) = 3 \cdot 92 + 1 \equiv 78 \pmod{199}$，并验证 $78^{66} \equiv 1 \pmod{199}$。

同样，$k = 3$ 和 $u^3 = 1$，因此 $\tau(u) = 1 + c(u)$：

$$\tau(1) = 2,$$
$$\tau(\delta) = 1 + 78 = 79,$$
$$\tau(\delta^2) = 2.$$

这三个值都不为零。直接计算可得，对于每个 $u \in \mu_3$，$v(u) = \tau(u)^{66} \equiv 106 \equiv \delta \pmod{199}$。由于 v 是常数，值为 $\delta \in \mu_3$，¯映射 $\psi(u) = \delta u$ 是一个非平凡旋转：

$$\bar{\psi}(1) = \delta, \qquad \bar{\psi}(\delta) = \delta^2, \qquad \bar{\psi}(\delta^2) = \delta^3 = 1.$$

根据推论 5.3，$f(X) = X^{199} c(X^{66})$ 是 $\mathbb{F}_{199}$ 的完全置换多项式。

6.2. **模 $q \equiv 1 \pmod 9$ 之外的反例。** 我们证明，当 $q \equiv 1 \pmod 3$ 但 $q \not\equiv 1 \pmod 9$ 时，这种构造可能失效，即使 r 满足所有互素条件也是如此。在每种情况下，我们都使用相同的结构形式 $F(X) = X^r(X^{2s} + \delta X^s + \delta^2 + 1) + X$，其中 $\delta^2 + \delta + 1 = 0$。

反例 1： $q = 7$。这里 $7 \equiv 1 \pmod 3$，但 $7 \not\equiv 1 \pmod 9$。我们有 $s = 2$ 和 $\delta = 2$（因为 $4 + 2 + 1 = 7 \equiv 0$），因此得到 $\delta^2 + 1 \equiv 5 \pmod 7$。取 $r = 1$（它满足 $\gcd(1,6) = 1$）：

$$F(X) = X(X^4 + 2X^2 + 5) + X = X^5 + 2X^3 + 6X = X(X^4 + 2X^2 + 6).$$

对于 $x \in \{3,4\}$，我们有 $x^2 \equiv 2$ （模 7），所以内因子的值为 $4+4+6 = 14 \equiv 0$（模 7）。因此 $F(0) = F(3) = F(4) = 0$：三个不同的元素映射到 0，而 F 不是 $\mathbb{F}_7$的置换。

反例 2： $q = 31$。这里 $31 \equiv 4$ （模 9），因此 $31 \not\equiv 1$ （模 9）。我们有 $s = 10$ 和 $\delta = 25$（因为 $625 + 25 + 1 = 651 = 21 \times 31 \equiv 0$），且$\delta^2 \equiv 5$ 和 $\delta^2+1 \equiv 6$ （模 31）。取 $r = 7$，它满足 gcd(7，30) $= 1$、gcd(7，10) $= 1$，以及 gcd(7，3) $= 1$:

$$F(X) = X^7(X^{20} + 25X^{10} + 6) + X.$$

由于 $2^5 = 32 \equiv 1$ （模 31）且 $8 = 2^3$，我们有 $8^5 = 2^{15} =$ $(2^5)^3 \equiv 1$，因此 $8^{10} \equiv 1$和 $8^{20} \equiv 1$。$x = 8$ 处的内因子计算结果为 $1+25+6 = 32 \equiv 1$ （模 31），所以

$$F(8) = 8^7 \cdot 1 + 8.$$

现在 $8^7 = 8^5 \cdot 8^2 \equiv 1 \cdot 64 \equiv 2$（模 31），得到 $F(8) \equiv 2+8 = 10$（模 31）。

对于 $x = 5$：我们计算得 $5^2 = 25, 5^4 \equiv 625 \equiv 5$ （模 31），因此 $5^{10} = (5^5)^2 = (5^4 \cdot 5)^2 = 25^2 \equiv 5$ 且 $5^{20} = (5^{10})^2 = 25$ （模 31）。内因子的值为 $25 + 25 \cdot 5 + 6 = 156 \equiv 1$（模 31），并且 $5^7 = 5^4 \cdot 5^2 \cdot 5 = 5 \cdot 25 \cdot 5 = 625 \equiv 5$（模 31）。因此 $F(5) = 5 \cdot 1 + 5 = 10$。

由于 $F(5) \equiv F(8) \equiv 10$ 且 $5 \not\equiv 8$，映射 F 不是单射。

这些反例并不声称在 $q \equiv 1$（模 9）之外不存在完全置换多项式；它们表明，我们构造中采用的自然参数选择在该范围内可能失效，而且我们的判据确实用到了同余 $q \equiv 1$ （模 9）。

References

[1] A. Akbary、D. Ghioca 和 Q. Wang, *On constructing permutations of finite fields*, Finite Fields Appl. **17** （2011），第 1 期，51–67。[2] M. Ayad、K. Belghaba 和 O. Kihel, *On permutation binomials over finite fields*, Bull. Aust. Math. Soc. **89** （2014），第 1 期，112–124。[3] M. Ayad、K. Belghaba 和 O. Kihel, *On permutation binomials*, Rocky Mountain J. Math. **45** （2015），第 2 期，389–399。[4] B. Bousalmi、A. Bayad 和 A. Derbal, *Explicit classes of permutation and complete permutation polynomials over finite fields* **31** 2021 , Adv. Stud. Contemp. Math.（），第 1 期，89–98。[5] M. E. Zieve, *On some permutation polynomials over $\mathbb{F}_q$ of the form $x^r h\,(x^{(q-1)/d})$* , Proc. Amer. Math. Soc. **137** （2009），第 7 期，2209–2216。

Chahrazade Bouyacoub，数学系，LA3C实验室电子邮件：chahrazadelamia.bouloudene@usthb.edu.dz

Asmae El-Baz，拉瓦尔大学数学与统计系，魁北克省，魁北克市 QC G1V 0A6，加拿大电子邮件：asmae.el-baz.1@ulaval.ca

Omar Kihel，布鲁克大学数学系，加拿大安大略 L2S 3A1

电子邮件：okihel@brocku.ca