arXiv:2304.03992v2 [math.NT] 4 Oct 2023

关于次数为 2、3、4 的稳定多项式

Tong Lin[1] Qiang Wang[1]

摘要

设 q 为一个素数幂。根据 Capelli 引理，我们构造了有限域 $\mathbb{F}_q$ 上形如 $b^{m-1}(x+a)^m + c(x+a) + d$ 的稳定多项式，其中 $m = 2$为 3、4。当$m = 3$ 且 q 为偶数时，我们证实了 Ahmadi 和 Monsef-Shokri 的猜想 [2]，即多项式 $f(x) = x^3 + x^2 + 1$ 在 $\mathbb{F}_2$上稳定。此外，当 $m = 2$且 $q \equiv 1 \pmod 4$时，我们改进了 Gom´ez-P´erez 和 Nicol´as 关于二次稳定多项式数量的下界 [4]。

1 引言

设 $\mathbb{K}$ 是一个域。若多项式 $t(x) \in \mathbb{K}[x]$ 在 $\mathbb{K}$ 上稳定，则对每个 $n \in \mathbb{N}$，n 次迭代 $t^{(n)}(x) = t(t(\ldots t(t(x))))$ 都是 t 在 $\mathbb{K}$上的不可约多项式。关于域上多项式稳定性的问题可以追溯到20世纪80年代。当时，Odoni [8, 命题 4.1], 受一个涉及非线性递推关系的素因子的数论问题启发，发现了一个在 $\mathbb{Q}$上稳定的多项式 $t_1(x) = x^2 - x + 1$。另一方面，对于任意素数 p 和整数 $n \geq 3$，Odoni 在 [9, 推论 1.6] 中证明， n 次迭代 $t_2(x) = x^p - x - 1$ 在素域 $\mathbb{F}_p$上可约。此后，人们对各种域上的多项式稳定性，尤其是低次数多项式的稳定性，进行了广泛研究。例如，Ahmadi 等人在 [1, 定理 4、推论 11] 中表明，在 $\mathbb{Z}[x]$ 中的几乎所有首一二次多项式在$\mathbb{Q}$ 上稳定，并且在特征 2 的有限域上不存在稳定二次多项式。2010年，Gom´ez-P´erez 和 Nicol´as 首次估计了奇特征有限域上稳定二次多项式的数量，见 [4, 定理 1]。他们还与 Ostafe 和 Sardonil 一起，在 2014 [5, 定理 5.5]中估计了奇特征有限域上任意次数 $d \in \mathbb{N}$ 的稳定多项式的数量。2012年，Jones 和 Boston 给出了二次多项式在有限域上稳定的充要条件（以所谓的调整后的临界轨道来表述）

[1]数学与统计学院，卡尔顿大学，1125 Colonel By Drive，渥太华，安大略省 K1S 5B6，加拿大。作者获得加拿大自然科学与工程研究理事会资助（RGPIN-2023-04673）。电子邮箱：tonglin4@cmail.carleton.ca（T. Lin），wang@math.carleton.ca （Q. Wang）。数学主题分类：11T06 (11B37)。关键词：有限域；不可约多项式；稳定性；非线性递推关系；有限域上的序列。

奇特征有限域 [6, 命题 2。3] （另见 [7] 勘误）。根据他们的结果，Ostafe 和 Shparlinski 估计了在奇特征有限域上检验二次多项式稳定性的复杂度 [10, 推论 2]。

对于次数大于 2 的多项式，确定此类多项式是否在某个域上稳定仍然颇具挑战性，迄今已知的次数为 ≥ 3 的稳定多项式示例并不多。例如，根据 [5, 定理 4.3]，形如 $ax^3 + bx + c$ 的多项式在 $\mathbb{F}_{3^k}$ 上均不稳定。至于 $\mathbb{F}_{2^k}$ 上的三次多项式，Ahmadi 和 Monsef-Shokri 提出，$f(x) = x^3 + x^2 + 1$ 在 $\mathbb{F}_2$ [2, 猜想 14]中是稳定的。受该猜想启发，我们提出了若干次数小于或等于 4 的新稳定多项式类，从而证实了 Ahmadi 和 Monsef-Shokri 的猜想。

本文其余部分的组织如下。第 2 节中，我们介绍一类新的多项式，并对其应用 [2] 中提出的稳定性判定。基于该判定，形如

$$f(x) = b^{m-1}(x + a)^m + c(x + a) + d$$

其中 $m \in \{2, 3, 4\}$分别在第 3、4 和 5节中构造。在第 3节中，我们还改进了 [4, 定理 1] 中给出的关于 $\mathbb{F}_q$ 在 $q \equiv 1$（模 4）时稳定二次多项式数量的下界。在第 4节中，我们验证了 Ahmadi 和 Monsef-Shokri 提出的上述猜想 [2, 猜想 14]，该猜想是我们构造的一个特殊情形。在第 5节中，我们还给出了一个显式结果，用于描述形如 $x^4 + cx + d$ 在$\mathbb{F}_{3^m}$上的多项式的因式分解模式。在第 6节中，我们作出总结性评论。

我们需要以下记号。设 q 为素数幂，且 $m \in \mathbb{N}$。对于满足 $d \mid m$的每个$d \in \mathbb{N}$，从 $\mathbb{F}_{q^m}$ 到 $\mathbb{F}_{q^d}$ 的迹映射定义为

$$\mathrm{Tr}_d^m(x) = \sum_{j=0}^{\frac{m}{d}-1} x^{q^{jd}}$$

当 $d = 1$时，我们将 Tr_d^m记为 Tr_m。

2 基于数列的稳定性判定

本节围绕以下 Capelli 引理所给出的稳定性判定展开 a.

引理 2.1 ([2, 引理 13], [3, 引理 1])。设 q 为任意素数幂，且 $f(x) \in \mathbb{F}_q[x]$是一个次数为 $d \in \mathbb{N}$的不可约多项式。若 $f^{(n)}(x)$ 在 $\mathbb{F}_q$上不可约，则 $f^{(n+1)}(x)$ 在 $\mathbb{F}_q$上不可约，当且仅当存在 $\mathbb{F}_{q^{d^n}}$中 $f^{(n)}(x)$ 的某个根 α，使得 $f(x) - \alpha$在 $\mathbb{F}_{q^{d^n}}$上不可约。

注 2.2。Capelli 引理揭示了一个权衡：在较小的域上使用较高次数的多项式（即 $\left(f^{(n)}(x)\right)_{n\geq 1}$），与在较大的域上使用较低次数的多项式（即 $(f(x) - \alpha_n)_{n\geq 1}$，其中 $\alpha_n \in \mathbb{F}_{q^{d^n}}$和 $f^{(n)}(\alpha_n) = 0$）。

接下来，我们定义一类新的多项式（称为抗移位多项式），并通过反复运用 Capelli 引理来研究其稳定性。

定义 2.3. 若多项式 $f(x)$ 满足 $\deg(f) = d$，且对于任意 $r \in \mathbb{N}$ 和任意 $a \in \mathbb{F}_{q^r}$，$f(x) - a$ 在 $\mathbb{F}_{q^{dr}}$ 中都有一个根，则称其为 $SR(q,d)$-多项式（其中 SR 表示抗移位）。

例 2.4. 每个二次多项式都是一个 $SR(q,2)$-多项式。事实上，若$f(x)$ 是二次的，则 $f(x) - a$要么在 $\mathbb{F}_{q^r}$中有一个根，要么在 $\mathbb{F}_{q^r}$上不可约。后一种情况下，$f(x) - a$在其分裂域 $\mathbb{F}_{q^{2r}}$中有一个根。类似地，每个三次多项式都是一个 $SR(q,3)$-多项式。

例 2.5. 每个四次多项式都是一个 $SR(q,4)$-多项式。事实上，假设 $f(x)$ 是四次的。若 $f(x) - a$在 $\mathbb{F}_{q^r}$中有一个根，则结论显然成立。否则，有两种可能。如果 $f(x) - a$在 $\mathbb{F}_{q^r}$上不可约，则它在其分裂域 $\mathbb{F}_{q^{4r}}$中有一个根。如果 $f(x) - a$在 $\mathbb{F}_{q^r}$上分解为两个不可约二次因子的乘积，则它在 $\mathbb{F}_{q^{2r}} \subset \mathbb{F}_{q^{4r}}$中有一个根。

例 2.6. 五次多项式 $f(x) = \left(x^2 + x + 1\right)\left(x^3 + x + 1\right)$ 不是$SR(2,5)$ 多项式，因为它在 $\mathbb{F}_{2^2} \setminus \mathbb{F}_2$ 中有 2 个根，在 $\mathbb{F}_{2^3} \setminus \mathbb{F}_2$中有 3 个根，因此它的根都不在 $\mathbb{F}_{2^5}$中。

令 $f(x)$ 为任意 $SR(q,d)$-多项式。令 $\alpha_0 = 0$。对于每个 $n \in \mathbb{N}$，令 α_n为 $f(x) - \alpha_{n-1}$在 $\mathbb{F}_{q^{d^n}}$中的一个根。于是很容易看出，

$$f^{(n)}(\alpha_n) = f^{(n-1)}(f(\alpha_n)) = f^{(n-1)}(\alpha_{n-1}) = \cdots = f(\alpha_1) = \alpha_0 = 0$$

换句话说，α_n 是 $\mathbb{F}_{q^{d^n}}$ 中 $f^{(n)}(x)$ 的一个根。然后对于每个 $n \in \mathbb{N}_0 = \mathbb{N} \cup \{0\}$，令

$$f_n(x) = f(x) - \alpha_n$$

采用上述记号，以下结果是 Capelli 引理的另一种表述。

命题 2.7. 设 $f(x)$ 是任意一个 $SR(q,d)$-多项式，且设 $n \in \mathbb{N}_0$。假设 $f^{(n)}(x)$ 在 $\mathbb{F}_q$ 上不可约。那么，$f^{(n+1)}(x)$ 在 $\mathbb{F}_q$ 上不可约，当且仅当 $f_n(x)$ 在 $\mathbb{F}_{q^{d^n}}$ 上不可约。

注意到 $\alpha_0 = 0$ 是 $f^{(0)}(x) = x$ 在 $\mathbb{F}_q$ 中的一个根，并且 $f_0(x) = f(x)$。因此，命题 2.7 在 $n = 0$ 时显然成立。利用上述结果，可以得到 $SR(q,d)$-多项式的稳定性判定。

推论 2.8. 设 $f(x)$ 是任意一个 $SR(q,d)$-多项式。那么，$f(x)$ 在 $\mathbb{F}_q$ 上稳定，当且仅当对每个 $n \in \mathbb{N}_0$，$f_n(x)$ 在 $\mathbb{F}_{q^{d^n}}$ 上不可约。

证明 若 $f(x)$ 在 $\mathbb{F}_q$ 上稳定，则对每个 $n \in \mathbb{N}_0$，$f^{(n)}(x)$ 在 $\mathbb{F}_q$ 上不可约。由命题 2.7，$f_n(x)$ 对每个 $n \in \mathbb{N}_0$ 都在 $\mathbb{F}_{q^{d^n}}$ 上不可约。反之，若对每个 $n \in \mathbb{N}_0$，$f_n(x)$ 在 $\mathbb{F}_{q^{d^n}}$ 上不可约，则 $f_0(x) = f(x)$ 在 $\mathbb{F}_q$ 上不可约，且 $f_1(x)$ 在 $\mathbb{F}_{q^d}$ 上不可约。由命题 2.7，$f^{(2)}(x)$ 在 $\mathbb{F}_q$ 上不可约。又由于 $f_2(x)$ 在 $\mathbb{F}_{q^{d^2}}$ 上不可约，根据命题 2.7，$f^{(3)}(x)$ 在 $\mathbb{F}_q$ 上不可约。以此类推可知，对每个 $n \in \mathbb{N}$，$f^{(n)}(x)$ 在 $\mathbb{F}_q$ 上不可约。因此，$f(x)$ 在 $\mathbb{F}_q$ 上稳定。□

下文将给出次数为 $d = 2$、3、4 的稳定 $SR(q,d)$-多项式示例。

3 稳定 $SR(q, 2)$-多项式（$q \equiv 1 \pmod 4$）

设 q 为奇素数幂。本节研究 $\mathbb{F}_q$ 上的二次多项式的稳定性，其形式如下:

$$f(x) = b(x+a)^2 + c(x+a) - a + \frac{c^2 - 2c}{4b}$$

其中 $b \neq 0$。

定理 3.1. 若 $a, b, c \in \mathbb{F}_q$, $b \neq 0$ 和 $4ab + 2c$ 是 $\mathbb{F}_q$中的非平方数，则

$$f(x) = b(x+a)^2 + c(x+a) - a + \frac{c^2 - 2c}{4b}$$

在 $\mathbb{F}_q$ 上稳定，当且仅当 $q \equiv 1 \pmod 4$。

证明 沿用第 2 节引入的思路，我们构造一个数列 $(\alpha_n)_{n\geq 0}$，其中 $\alpha_0 = 0$ 且 $f(\alpha_n) = \alpha_{n-1}$ $(n \in \mathbb{N})$。对于每个 $n \in \mathbb{N}_0$，令

$$f_n(x) = f(x) - \alpha_n = b(x+a)^2 + c(x+a) - (\alpha_n + a) + \frac{c^2 - 2c}{4b}$$

由推论 2.8，$f(x)$ 在 $\mathbb{F}_q$ 上稳定，当且仅当 $f_n(x)$ 在 $\mathbb{F}_{q^{2^n}}$ 上对每个$n \in \mathbb{N}_0$均不可约。变量替换 $y = b(x+a)$ 表明，后一个断言成立当且仅当

$$g_n(y) = y^2 + cy - \beta_n$$

在 $\mathbb{F}_{q^{2^n}}$ 上对每个 $n \in \mathbb{N}_0$ 均不可约，其中

$$\beta_n = b(\alpha_n + a) - \frac{c^2 - 2c}{4}$$

等价地，$f(x)$ 在 $\mathbb{F}_q$ 上稳定，当且仅当

$$\Delta_n = c^2 + 4\beta_n$$

对每个 $n \in \mathbb{N}_0$，它在 $\mathbb{F}_{q^{2^n}}$ 中都是非平方数。只需验证该断言对所有 $n \in \mathbb{N}$ 均成立，因为根据假设，$\Delta_0 = 4ab + 2c$ 在 $\mathbb{F}_q$ 中是非平方数。对于每个$n \in \mathbb{N}$，由于 $f(\alpha_n) = \alpha_{n-1}$，我们有 $g_{n-1}\left(\beta_n + \frac{c^2-2c}{4}\right) = 0$，即

$$\left(\beta_n + \frac{c^2 - 2c}{4}\right)^2 + c\left(\beta_n + \frac{c^2 - 2c}{4}\right) = \beta_{n-1}$$

这意味着

$$\left(\frac{\Delta_n - c^2}{4} + \frac{c^2 - 2c}{4}\right)^2 + c\left(\frac{\Delta_n - c^2}{4} + \frac{c^2 - 2c}{4}\right) + \frac{c^2}{4} = \frac{\Delta_{n-1} - c^2}{4} + \frac{c^2}{4}$$

由此可得

$$\Delta_n^2 = 4\Delta_{n-1} \tag{1}$$

情形 1: $q \equiv 3$ （模 4）

在此情况下， $q+1 \equiv 0$ （模 4）。如果 γ 是 $\mathbb{F}_{q^2}$中的本原元，那么 $\mathbb{F}_q = \langle \gamma^{q+1} \rangle$。因此， $\mathbb{F}_q$ 中的每个元素都是 $\mathbb{F}_{q^2}$中的四次幂。所以 Δ_1^2 （$\overset{1)}{=} 4\Delta_0 = s^4$ 对于某个 $s \in \mathbb{F}_{q^2}$，这意味着 $\Delta_1 = (st)^2 \in \mathbb{F}_{q^2}$ 对于某个四次单位根 $t \in \mathbb{F}_{q^2}$。因此， $g_1(x)$ 在 $\mathbb{F}_{q^2}$ 上可约，而 $f(x)$ 在 $\mathbb{F}_q$ 上不稳定。

情形 2: $q \equiv 1$ （模 4）

在此情形下，我们证明对于每个 $n \in \mathbb{N}$， Δ_n a是 $\mathbb{F}_{q^{2^n}}$ 中的非平方数。反设该断言不成立。于是存在一个最小的 $n_0 \in \mathbb{N}$，使得 Δ_{n_0} 是 $\mathbb{F}_{q^{2^{n_0}}}$ 中的平方。如果 $n_0 - 1 = 0$，那么 $\Delta_{n_0-1} = \Delta_0$ 是 $\mathbb{F}_q$中的非平方数。如果 $n_0 - 1 \geq 1$，那么根据 n_0 的最小性， Δ_{n_0-1} 再次是 $\mathbb{F}_{q^{2^{n_0-1}}}$ 中的非平方数。在这两种情况下，我们都有

$$\mathbb{F}_{q^{2^{n_0}}} \cong \mathbb{F}_{q^{2^{n_0-1}}}[x] / \left\langle x^2 - \Delta_{n_0-1} \right\rangle \cong \left\{ u + vx_0 : \ u, v \in \mathbb{F}_{q^{2^{n_0-1}}} \right\}$$

其中 $x_0 \in \mathbb{F}_{q^{2^{n_0}}}$和 $x_0^2 = \Delta_{n_0-1}$。由于 Δ_{n_0} 是 $\mathbb{F}_{q^{2^{n_0}}}$中的平方， $\Delta_{n_0} = (u + vx_0)^2$ 对某个 u、 $v \in \mathbb{F}_{q^{2^{n_0-1}}}$ 成立。由于 $4x_0^2 = 4\Delta_{n_0-1}$ $\overset{1)}{=} \Delta_{n_0}^2$，存在一个 $\epsilon \in \{\pm 1\}$ 使得

$$2x_0 = \epsilon \Delta_{n_0} = \epsilon (u + vx_0)^2 = \epsilon \left(u^2 + v^2 \Delta_{n_0-1} \right) + 2\epsilon uvx_0$$

这表明

$$\begin{cases} \epsilon \left(u^2 + v^2 \Delta_{n_0-1} \right) & = 0 \\ 2\epsilon uv & = 2 \end{cases}$$

第二个方程意味着 $v \neq 0$，结合第一个方程可知 $\Delta_{n_0-1} = -u^2 v^{-2}$。由于 $q \equiv 1 \pmod 4$， -1 是 $\mathbb{F}_q$中的一个平方。因此， Δ_{n_0-1} 是 $\mathbb{F}_{q^{2^{n_0-1}}}$中的一个平方，这与 n_0 的最小性矛盾。因此，不存在这样的 n_0 ，这证明 $f(x)$在 $\mathbb{F}_q$上是稳定的。□

在 [4, 定理 1], Gom´ez-P´erez 和 Nicol´as 证明，对于每个奇素数幂 q，在 $\mathbb{F}_q$上（不一定是首一的）稳定二次多项式的数量至少为 $(q-1)_4^{\ 2}$。当 $q \equiv 1 \pmod 4$ 时，我们可以改进这~~个下界~~。设 $f(x)$ 如定理 3.1中所述。注意，如果 $\delta = 4ab + 2c$，那么

$$f(x) = bx^2 + \left(\frac{\delta}{2} \right) x + \frac{\delta^2 - 4\delta}{16b} \tag{2}$$

并且 $f(x)$的判别式为 δ。因此， $f(x)$ 只取决于 b（对于它，作为 $b \neq 0$ 有 $q-1$ 种选择）以及 δ（如果我们希望 $f(x)$ 在 $\mathbb{F}_q$ 上稳定，它必须是 $\mathbb{F}_q$ 中 $\frac{q+1}{2}$ 个非平方数之一）。这些观察得出了以下结果。

推论 3.2. 如果 q 是素数幂且 $q \equiv 1$ （模 4），那么

$$S_q \geq \frac{q^2 - 1}{2}$$

其中， S_q 是 $\mathbb{F}_q$ 上（可能是非首一的）稳定二次多项式的数量。

我们没有在定理 $f(x)$ 的证明中将其改写为等式 (2)，是因为这样做的话，变量替换 $y = b(x+a)$ 就不会那么显而易见。不过，定理 3.1 现在可以重新表述如下。

定理 3.3。设 q 是一个素数幂，使得 $q \equiv 1$ （模 4）。如果 b， $\eta \in \mathbb{F}_q^*$ 一个 d

$$f(x) = bx^2 + \left(\frac{\delta}{2}\right)x + \frac{\delta^2 - 4\delta}{16b}$$

那么 $f(x)$ 在 $\mathbb{F}_q$ 上稳定，当且仅当 δ 是 $\mathbb{F}_q$ 中的非平方数。此外，上述形式的稳定多项式有 $\frac{q^2-1}{2}$ 个。

4 稳定 $SR(2^m,3)$-多项式

设 $m \in \mathbb{N}$。本节研究 $\mathbb{F}_{2^m}$ 上形如.....的三次多项式的稳定性

$$f(x) = b^2(x+a)^2 + x$$

其中 $a, b \neq 0$。为此，需要以下结果。

命题 4.1（[11, 定理 7.20]）。若 $m \in \mathbb{N}$, $a, b, c \in \mathbb{F}_{2^m}$ 且 $a \neq 0$，则在 $\mathbb{F}_{2^m}$ 中，方程 $ax^2 + bx + c = 0$ 有

$$\begin{cases} a \text{ unique solution}, & \text{if } b = 0; \\ \text{two distinct solutions}, & \text{if } b \neq 0 \text{ and } Tr_m\left(acb^{-2}\right) = 0; \\ \text{no solution}, & \text{if } b \neq 0 \text{ and } Tr_m\left(acb^{-2}\right) = 1. \end{cases}$$

引理 4.2。若 $m \in \mathbb{N}, u, v \in \mathbb{F}_{2^m}^*$ 且 $u^3 + u = v$，则 $\mathbf{Tr}_m\left(u^{-1}\right) = \mathbf{Tr}_m\left(v^{-1}\right)$。

证明 我们注意到 $x^2 + (u+1)x + u = (x+u)(x+1)$，且 $u \neq 1$ （否则 $v = 0$）。因此

$$\mathrm{Tr}_m\left(u\left(u^2+1\right)^{-1}\right) = \mathrm{Tr}_m\left(u\left(u+1\right)^{-2}\right) = 0 \tag{3}$$

其中最后一步由命题 4.1 得出。由于 $v = u^3 + u = u\left(u^2+1\right)$,

$$u^{-1} + u\left(u^2+1\right)^{-1} = \left(u\left(u^2+1\right)\right)^{-1}\left(\left(u^2+1\right) + u^2\right) = v^{-1} \tag{4}$$

对 Tr 应用$_m$ 于等式（4）可得

$$\begin{aligned} \mathrm{Tr}_m\left(u^{-1}\right) &\overset{(3)}{=} \mathrm{Tr}_m\left(u^{-1}\right) + \mathrm{Tr}_m\left(u\left(u^2+1\right)^{-1}\right) \\ &= \mathrm{Tr}_m\left(u^{-1} + u\left(u^2+1\right)^{-1}\right) \\ &\overset{(4)}{=} \mathrm{Tr}_m\left(v^{-1}\right) \end{aligned}$$

如所需。 □

下面的定理讨论了 $\mathbb{F}_{2^m}$ 上三次三项式的因式分解模式，在证明我们的主要结果中起着关键作用。

定理 4.3 ([12, 定理 1])。设 $m \in \mathbb{N}$。若 a，$b \in \mathbb{F}_{2^m}$，$b \neq 0$ 且 t_1，t_2 是 x^2+bx+a^3的两个根，那么在 $\mathbb{F}_{2^m}$上，多项式 x^3+ax+b
(1) 完全分解为一次因子，当且仅当 $\mathrm{Tr}_m\left(a^3b^{-2}\right)=\mathrm{Tr}_m(1)$，且 t_1、t_2 在 $\mathbb{F}_{2^m}$ 中都是立方数（若 m 为偶数），或在 $\mathbb{F}_{2^{2m}}$ 中都是立方数（若 m 为奇数）；(2) 分解为一个一次因子和一个二次因子，当且仅当 $\mathrm{Tr}_m\left(a^3b^{-2}\right)\neq\mathrm{Tr}_m(1)$；(3) 不可约，当且仅当 $\mathrm{Tr}_m\left(a^3b^{-2}\right)=\mathrm{Tr}_m(1)$，且 t_1、t_2 在 $\mathbb{F}_{2^m}$ 中都不是立方数（若m为偶数），或在 $\mathbb{F}_{2^{2m}}$ 中都不是立方数（若 m 为奇数）。

完成所有准备工作后，我们现在陈述本节的主要结果。

定理 4.4. 若 $m \in \mathbb{N}$、a、$b \in \mathbb{F}_{2^m}^*$ 以及 $\mathrm{Tr}_m\left((ab)^{-1}\right)=\mathrm{Tr}_m(1)$，则

$$f(x)=b^2(x+a)^3+x$$

在$\mathbb{F}_{2^m}$ 上稳定，当且仅当它在$\mathbb{F}_{2^m}$上不可约。

证明 我们只证明不可约性蕴含稳定性，因为反向结论显然成立。不失一般性，我们只需考虑 m为偶数的情形，另一种情形可以用同样的方法证明。令 $q=2^m$。遵循第 2 节提出的思路，我们构造一个数列 $(\alpha_n)_{n\geq 0}$，使得 $\alpha_0=0$，并且$f(\alpha_n)=\alpha_{n-1}$ $(n\in\mathbb{N})$。对于每个 $n\in\mathbb{N}_0$，令

$$f_n(x)=f(x)+\alpha_n=b^2(x+a)^3+(x+a)+(\alpha_n+a)$$

根据推论 2.8，$f(x)$ 在 $\mathbb{F}_q$ 上稳定，当且仅当 $f_n(x)$ 在 $\mathbb{F}_{q^{3^n}}$ 上不可约，对每个$n\in\mathbb{N}_0$ 均如此。变量替换 $y=b(x+a)$ 意味着，后一个结论成立当且仅当

$$g_n(y)=y^3+y+\beta_n$$

对每个 $n\in\mathbb{N}_0$，在$\mathbb{F}_{q^{3^n}}$ 上不可约，其中

$$\beta_n=b(\alpha_n+a)$$

由于对每个 $n\in\mathbb{N}$，$f(\alpha_n)=\alpha_{n-1}$，因此我们有 $g_{n-1}(\beta_n)=0$，即

$$\beta_n^3+\beta_n=\beta_{n-1} \tag{5}$$

由于 $\beta_0=ab\neq 0$，利用公式（5）很容易验证 $\beta_n\notin 0$，对每个 $n\in\mathbb{N}$均为 1。此外，公式（5）表明，任何包含 β_n的域也包含 β_j（$0\leq j\leq n-1$）。结合反复使用引理 4.2，可得

$$\mathrm{Tr}_{3^nm}\left(\beta_n^{-1}\right)=\mathrm{Tr}_{3^nm}\left(\beta_{n-1}^{-1}\right)=\cdots=\mathrm{Tr}_{3^nm}\left(\beta_0^{-1}\right) \tag{6}$$

接下来我们注意到

$$\mathrm{Tr}_{3^nm}\left(\beta_0^{-1}\right)=\mathrm{Tr}_m\left(\mathrm{Tr}_m^{3^nm}\left((ab)^{-1}\right)\right)=\mathrm{Tr}_m\left((ab)^{-1}\right)=\mathrm{Tr}_m(1)=\mathrm{Tr}_{3^nm}(1)$$

其中最后一步由 $3^nm\equiv m$ （模 2）可知成立。于是我们由式（6）推得

$$\mathrm{Tr}_{3^nm}\left(\beta_n^{-1}\right)=\mathrm{Tr}_{3^nm}(1) \tag{7}$$

由于 m 是偶数，式（7）和命题 4.1 意味着 $x^2+\beta_n x+1$ 总是在 $\mathbb{F}_{q^{3^n}}=\mathbb{F}_{2^{3^n m}}$ 中有一个根。

反设 $f(x)$ 在 $\mathbb{F}_{2^m}$ 上不稳定。那么，对于某个 $n\in\mathbb{N}_0$，$g_n(x)$ 在 $\mathbb{F}_{q^{3^n}}$ 上可约。由于根据假设，$f_0(x)=f(x)$ 在 $\mathbb{F}_q$ 上不可约，我们知道 $g_0(x)$ 在 $\mathbb{F}_q$ 上不可约。因此，存在最小的 $n_0\in\mathbb{N}$，使得 $g_{n_0}(x)$ 在 $\mathbb{F}_{q^{3^{n_0}}}$ 上可约。

应用定理4.3 于 $g_{n_0}(x)$，由等式（7）可推得，t_1，t_2这两个 $x^2+\beta_{n_0}x+1$ 的根都是 $\mathbb{F}_{q^{3^{n_0}}}$ 中的立方数。如果 $t_1=w^3$ 对于某个 $w\in\mathbb{F}^*_{q^{3^{n_0}}}$，那么根据韦达公式，$t_2=t_1^{-1}=w^{-3}$ 以及

$$w^3+w^{-3}=t_1+t_2=\beta_{n_0} \tag{8}$$

设 u 是 $\mathbb{F}_{q^{3^{n_0-1}}}$ 中 $x^2+\beta_{n_0-1}x+1$ 的一个根。根据韦达公式，u^{-1} 是另一个根。此外，我们知道

$$w^9+w^{-9}=\left(w^3+w^{-3}\right)^3+\left(w^3+w^{-3}\right)\overset{(8)}{=}\beta_{n_0}^3+\beta_{n_0}\overset{(5)}{=}\beta_{n_0-1} \tag{9}$$

将等式（9）两边乘以 w^9，可知 w^9 是 $x^2+\beta_{n_0-1}x+1$的一个根。因此 $w^9=u$ 或 u^{-1}。无论哪种情况，$w^9\in\mathbb{F}_{q^{3^{n_0-1}}}$。令 $d=q^{3^{n_0-1}}$，则有

$$\begin{aligned} w\in\mathbb{F}^*_{q^{3^{n_0}}}=\mathbb{F}^*_{d^3} &\Rightarrow w^{d^3-1}=1 &&\Rightarrow w^{\left(d^2+d+1\right)(d-1)}=1\\ w^9\in\mathbb{F}^*_{q^{3^{n_0-1}}}=\mathbb{F}^*_{d} &\Rightarrow \left(w^9\right)^{(d-1)}=1 &&\Rightarrow \left(w^3\right)^{3(d-1)}=1 \end{aligned} \tag{10}$$

接着我们注意到 $d^2+d+1\equiv 0$（模 3），因为当 m 为偶数时，

$$d\equiv(2^m)^{3^{n_0-1}}\equiv((-1)^m)^{3^{n_0-1}}\equiv 1\pmod 3$$

我们还注意到，对每个 $j\in\mathbb{N}$，都有 $j^2+j+1\not\equiv 0$（模 9）。因此，对于满足 $3\nmid r$ 的某个 $r\in\mathbb{N}$，有 $d^2+d+1=3r$。由等式（10），$\left(w^3\right)^{r(d-1)}=w^{\left(d^2+d+1\right)(d-1)}=1$，这意味着 w^3 在 $\mathbb{F}^*_{d^3}$ 中的阶整除 $\gcd(r(d-1),3(d-1))=d-1$。特别地，$w^3\in\mathbb{F}^*_d=\mathbb{F}^*_{q^{3^{n_0-1}}}$。由于 $u=\left(w^3\right)^3$、$u^{-1}=\left(w^{-3}\right)^3$，或反之，$x^2+\beta_{n_0-1}x+1$ 的两个根 u、u^{-1} 都是 $\mathbb{F}_{q^{3^{n_0-1}}}$ 中的立方数。由等式（7）和定理 4.3，$g_{n_0-1}(x)$ 在 $\mathbb{F}_{q^{3^{n_0-1}}}$ 上可约。由于 n_0 是使得 $g_{n_0}(x)$ 在 $\mathbb{F}_{q^{3^{n_0}}}$ 上可约的最小正整数，因此有 $n_0-1=0$。然而，如前所示，$g_0(x)$ 在 $\mathbb{F}_q$ 上不可约。因此，不存在这样的 n_0，结论得证。□

当 $a=b=1$ 时，完全相同的证明可得出以下结果。

推论 4.5。多项式 $f(x)=x^3+x+1$ 在 $\mathbb{F}_{2^m}$ 上稳定，当且仅当 $3\nmid m$。

根据推论4.5，当 $m=1$时，我们得到 [2, 猜想 14]。

5 奇素数幂 $SR(q,4)$ 的稳定多项式

本节中，我们给出 $\mathbb{F}_q$ 上稳定四次多项式的例子，其中 q 是奇素数幂。首先，我们回顾以下结果。

定理 5.1 ([2, 定理 8])。设 q 是一个奇素数幂，并设 $f(x)$ 是一个次数为 d 的多项式，它是 r 个两两不同的不可约多项式在 $\mathbb{F}_q$ 上的乘积。那么 $r \equiv d$ (模 2) 当且仅当 f 的判别式是 $\mathbb{F}_q$中的平方数。

以下结论是定理 5.1的直接推论。

命题 5.2. 若 q 是素数幂，且 $q \equiv 1$ (模 4)，则 $f(x) = x^4 - a$ 在 $\mathbb{F}_q$ 上不可约，当且仅当 a是 $\mathbb{F}_q$中的非平方数。

证明 由于 $4 \mid q-1$, -1 是 $\mathbb{F}_q$ 中的平方数。如果 $f(x)$ 在 $\mathbb{F}_q$ 上不可约，那么根据定理 5.1， $f(x)$ 的判别式，即 $D(f) = 256(-a)^3 = (-1)(16a)^2 a$ 是 $\mathbb{F}_q$ 中的非平方数，而这要求 a 是 $\mathbb{F}_q$ 中的非平方数。

反之，如果 a 是 $\mathbb{F}_q$中的非平方数，那么 $D(f)$ 也是如此。根据定理 5.1， $f(x)$ 要么在 $\mathbb{F}_q$ 上不可约，要么在 $\mathbb{F}_q$上分解为两个一次因子与一个不可约二次因子的乘积。后一种情况不可能发生。事实上，假设

$$\begin{aligned} x^4 - a &= \left(x^2 + rx + s\right)\left(x^2 + tx + u\right) \\ &= x^4 + (r+t)x^3 + (rt + s + u)x^2 + (ru + st)x + su \end{aligned}$$

其中 $r, s, t, u \in \mathbb{F}_q$。比较对应项的系数，可得

$$\begin{cases} r + t & = 0 \\ rt + s + u & = 0 \\ ru + st & = 0 \\ su & = -a \end{cases} \Rightarrow \begin{cases} t & = -r \\ s + u & = r^2 \\ r(-s + u) & = 0 \\ su & = -a \end{cases}$$

如果 $r = 0$，那么 $u = -s$。因此 $a = -su = s^2$。如果 $r \neq 0$，那么 $u = s$。因此 $a = (-1)s^2$。在这两种情况下， a 都是 $\mathbb{F}_q$ 中的平方数，这是不可能的。因此 $f(x)$ 是不可约的。 □

基于命题 5.2，可以得到一类稳定四次多项式。

定理 5.3。设 q 为素数幂，使得 $q \equiv 1$ （模 4）。如果 a、 $b \in \mathbb{F}_q^*$，则 n

$$f(x) = b^3(x + a)^4 - a$$

当且仅当 ab 是 $\mathbb{F}_q$ 中的非平方数时，在 $\mathbb{F}_q$ 上稳定。

证明 假设 $q = p^m$ ，其中 $m \in \mathbb{N}$ 且 p 为奇素数。我们只给出 $p = 8k + 1$ 情形的证明，因为其他情形（即 $p \equiv 3$、5、7 (mod 8)）也可以用相同的方法证明。

如果 $f(x)$ 在 $\mathbb{F}_q$上稳定，那么它在 $\mathbb{F}_q$上不可约。因此，我们知道$bf(x) = (b($ $x + a))^4 - ab$ 在 $\mathbb{F}_q$上不可约。变量替换 $y = b(x + a)$ 因而表明 $y^4 - ab$ 在 $\mathbb{F}_q$上不可约。由命题 5.2，我们推知 ab 是 $\mathbb{F}_q$中的非平方数。

反过来，假设 ab 是 $\mathbb{F}_q$中的非平方数。和之前一样，按照第 2节提出的思路，我们构造一个数列 $(\alpha_n)^{n\geq 0}$，使得 $\alpha_0 = 0$ 并且$f(\alpha_n) = \alpha_{n-1}$ $(n \in \mathbb{N})$。对于每个 $n \in \mathbb{N}_0$，令

$$f_n(x) = f(x) - \alpha_n = b^3(x+a)^4 - (\alpha_n + a).$$

根据推论 2.8， $f(x)$ 在 $\mathbb{F}_q$ 上稳定，当且仅当 $f_n(x)$ 在 $\mathbb{F}_{q^{4^n}}$ 上不可约，对每个$n \in \mathbb{N}_0$均成立。由变量替换 $y = b(x+a)$ 可知，后一结论成立当且仅当

$$g_n(y) = y^4 - \beta_n$$

对每个 $n \in \mathbb{N}_0$，在 $\mathbb{F}_{q^{4^n}}$ 上不可约，其中

$$\beta_n = b(\alpha_n + a)$$

根据命题 5.2， $f(x)$ 在 $\mathbb{F}_q$上稳定，当且仅当 β_n 在 $\mathbb{F}_{q^{4^n}}$ 中对每个 $n \in \mathbb{N}_0$都是非平方数。只需对 $n \in \mathbb{N}$ 验证后一结论，因为根据假设我们知道$\beta_0 = ab$ 在 $\mathbb{F}_q$中是非平方数。反设该结论不成立，则存在最小的 $n_0 \in \mathbb{N}$，使得 β_{n_0} 在 $\mathbb{F}_{q^{4^{n_0}}}$中是平方。

若 $n_0 - 1 = 0$，则 $\beta_{n_0-1} = \beta_0$ 在 $\mathbb{F}_q$中是非平方数。若 $n_0 - 1 \geq 1$，则由n_0的最小性可知， β_{n_0-1} 在 $\mathbb{F}_{q^{4^{n_0-1}}}$中仍是非平方数。根据命题 5.2， $g_{n_0-1}(x)$ 在 $\mathbb{F}_{q^{4^{n_0-1}}}$上不可约。若 x_0 是 $g_{n_0-1}(x)$ 在 $\mathbb{F}_{q^{4^{n_0}}}$ 中的一个根，则 $x_0^4 = \beta_{n_0-1}$ 并且

$$\mathbb{F}_{q^{4^{n_0}}} \cong \mathbb{F}_{q^{4^{n_0-1}}}[x]/\langle g_{n_0-1}(x)\rangle \cong \left\{ r + sx_0 + tx_0^2 + ux_0^3 : \ r,s,t,u \in \mathbb{F}_{q^{4^{n_0-1}}} \right\}$$

根据假设， β_{n_0}是 $\mathbb{F}_{q^{4^{n_0}}}$ 中的一个平方。因此，存在 r、 s、 t、 $u \in \mathbb{F}_{q^{4^{n_0-1}}}$使得 $\beta_{n_0} = \left(r + sx_0 + tx_0^2 + ux_0^3\right)^2$。由于对每个 $n \in \mathbb{N}$， $f(\alpha_n) = \alpha_{n-1}$，我们有

$$\beta_n^4 = \beta_{n-1} \tag{11}$$

特别地，我们知道

$$\left(r + sx_0 + tx_0^2 + ux_0^3\right)^8 = \beta_{n_0}^4 = \beta_{n_0-1} = x_0^4 \tag{12}$$

由此可得

$$\left(r + sx_0 + tx_0^2 + ux_0^3\right)^2 = \epsilon x_0 \tag{13}$$

其中 $\epsilon \in \mathbb{F}_q$是一个四次单位根。容易看出，以下各项中至少有三项 r、 s、 t、 u不为零。事实上，若其中两项（例如 r 和 s ）为 0，则由式（13）可得，

$$t^2\beta_{n_0-1} + 2tu\beta_{n_0-1}x_0 + u^2\beta_{n_0-1}x_0^2 = \epsilon x_0$$

因此 $t^2\beta_{n_0-1} = u^2\beta_{n_0-1} = 0$。然而，由式（11），对每个 $n \in \mathbb{N}$，都有 $\beta_n \neq 0$，因为 $\beta_0 \neq 0$。于是， $t = u = 0$，这意味着 $\beta_{n_0} = 0$，这是不可能的。其余情形可用同样的方法证明。

与此同时，回顾一下 $p = 8k+1$。因此，式（12）意味着

$$\left(r + sx_0 + tx_0^2 + ux_0^3\right)^{8k+1} = \beta_{n_0-1}^k \left(r + sx_0 + tx_0^2 + ux_0^3\right)$$

化简后可得

$$r^p + s^p\beta_{n_0-1}^{2k}x_0 + t^p\beta_{n_0-1}^{4k}x_0^2 + u^p\beta_{n_0-1}^{6k}x_0^3 = \beta_{n_0-1}^k\left(r + sx_0 + tx_0^2 + ux_0^3\right)$$

比较对应项的系数，我们便得到

$$\begin{cases} r^p & = r\beta_{n_0-1}^k \\ s^p\beta_{n_0-1}^{2k} & = s\beta_{n_0-1}^k \end{cases} \tag{14}$$

先前的讨论表明， r 和 s 中必有一个非零。不失一般性，我们只需考虑 $r \neq 0$ 的情形，因为另一种情形的证明同样成立。由于 $r \neq 0$, $\beta_{n_0-1}^k = r^{p-1} = r^{8k}$。因此，对于某个$k$次单位根 $v \in \overline{\mathbb{F}_q}$，有 $\beta_{n_0-1} = vr^8$ 。由于 $2k \mid (8k+1)^m - 1 = q-1$， $\mathbb{F}_q$ 包含所有 $2k$次单位根（因而也包含所有 k次单位根），设为 $\pm v_j$ $(1 \leq j \leq k)$，其中当 $j_1 \neq j_2$时，$v_{j_1} \neq \pm v_{j_2}$ 。因此，所有 k次单位根都是 $\mathbb{F}_q$ 中的平方，因为它们恰好是 $v_j^2 (1 \leq j \leq k)$。特别地， β_{n_0-1} 是 $\mathbb{F}_{q^{4^{n_0-1}}}$中的平方，而这正如前文所示是不可能的。因此，不存在这样的 n_0 ，这证明 $f(x)$在 $\mathbb{F}_q$上稳定。□

接下来，令 $q = 3^m$。我们研究 $\mathbb{F}_q$ 上如下形式的多项式的稳定性

$$f(x) = b^3(x+a)^4 + c(x+a) - a$$

其中 a、b、$c \in \mathbb{F}_q$和 b、$c \neq 0$。与之前一样，我们构造一个数列 $(\alpha_n)_{n\geq 0}$，使得 $\alpha_0 = 0$ ，并且 $f(\alpha_n) = \alpha_{n-1}$ $(n \in \mathbb{N})$。对于每个 $n \in \mathbb{N}_0$，令

$$f_n(x) = f(x) - \alpha_n = b^3(x+a)^4 + c(x+a) - (\alpha_n + a)$$

由推论 2.8， $f(x)$ 在 $\mathbb{F}_q$ 上稳定，当且仅当 $f_n(x)$ 在 $\mathbb{F}_{q^{4^n}}$ 上不可约，对每个$n \in \mathbb{N}_0$均成立。变量替换 $y = b(x+a)$ 表明，后一个断言成立，当且仅当

$$g_n(y) = y^4 + cy - \beta_n$$

对每个 $n \in \mathbb{N}_0$，在 $\mathbb{F}_{q^{4^n}}$ 上不可约，其中

$$\beta_n = b(\alpha_n + a)$$

接下来，我们证明一个定理，用以描述多项式 $g_n(x)$ 在 $\mathbb{F}_{3^m}$上的因式分解模式。

定理 5.4. 设 $q = 3^m$且 $c \in \mathbb{F}_q^*$。若 $g(x) = x^3 - dx - c^2$且 $h(x) = x^4 + cx + d$，则有以下结论。

(1) $h(x)$ 在 $\mathbb{F}_q$ 上完全分解为一次因子，当且仅当对于某些两两不同的 r_1、r_2、$r_3 \in \mathbb{F}_q$， $-r_j^2 \pm cr_j^{-1} (1 \leq j \leq 3)$ 是 $\mathbb{F}_q$ 中的平方；

(2) $h(x)$ 在 $\mathbb{F}_q$ 上可分解为两个不可约二次因子的乘积，当且仅当 $g(u_j) = 0$ ($1 \leq j \leq 3$)，其中存在一组两两不同的 u_1、u_2、$u_3 \in \mathbb{F}_q$，使得 u_1、u_2 在 $\mathbb{F}_q$ 中为非平方数，并且对于某个 $r \in \mathbb{F}_q$，有 $u_3 = r^2$ ，其中 $-r^2 \pm cr^{-1}$ 在 $\mathbb{F}_q$ 中为非平方数；

(3) $h(x)$ 有唯一的根 $\mathbb{F}_q$，当且仅当 $g(x)$ 在 $\mathbb{F}_q$ 上不可约；(4) $h(x)$ 在 $\mathbb{F}_q$ 中恰有两个根，当且仅当 $g(x)$ 有唯一的根 $r^2 \in \mathbb{F}_q$，其中 $r \in \mathbb{F}_q$，且 $r^4 - c^2 r^{-2}$ 在 $\mathbb{F}_q$ 中为非平方数；(5) $h(x)$ 在 $\mathbb{F}_q$ 上不可约，当且仅当 $g(x)$ 有唯一的根，且该根在 $\mathbb{F}_q$ 中为非平方数。

证明 首先，我们注意到，如果 $h(x)$ 在 $\mathbb{F}_q$ 上可分解为两个（可能可约的）二次因子的乘积，即

$$\begin{aligned} x^4 + cx + d &= \left(x^2 + rx + s\right)\left(x^2 + tx + u\right) \\ &= x^4 + (r+t)x^3 + (rt + s + u)x^2 + (ru + st)x + su \end{aligned}$$

那么我们有

$$\begin{cases} r + t & = 0 \\ rt + s + u & = 0 \\ ru + st & = c \\ su & = d \end{cases} \Rightarrow \begin{cases} t & = -r \\ s + u & = r^2 \\ r(-s + u) & = c \\ su & = d \end{cases}$$

根据第三个方程，$r \neq 0$。由第二个和第三个方程解出 s, u，可得 $s = cr^{-1} - r^2$，$u = -cr^{-1} - r^2$。这些结果与第四个方程一起推出 $r^4 - c^2 r^{-2} = su = d$。因此，$g\left(r^2\right) = r^6 - dr^2 - c^2 = 0$。所以，$h(x)$ 能在 $\mathbb{F}_q$ 上分解为两个二次因子的乘积，当且仅当存在一个 $r \in \mathbb{F}_q$ 使得

$$f(x) = \left(x^2 + rx + cr^{-1} - r^2\right)\left(x^2 - rx - cr^{-1} - r^2\right) \tag{15}$$

且后一结论成立，当且仅当 $g(x)$ 有一个在 $\mathbb{F}_q$ 中为平方的根。我们还注意到，式（15）中第一个二次因子的判别式为 $-r^2 - cr^{-1}$，第二个二次因子的判别式为 $-r^2 + cr^{-1}$。

首先，我们证明条目（1）。显然，h（x）在 $\mathbb{F}_q$上是可分的。假设 h（x）具有四个两两不同的根。那么容易验证，这些根恰好产生三种两两不同的、形如式（15）的分解，并且在每一种分解中，两个二次因子在 $\mathbb{F}_q$上都是可约的。因此，条目（1）由关于式（15）的注记可得。

接下来，我们证明第 (2) 项。若 $h(x)$可分解为两个不可约二次因子的乘积，则存在满足式 (15) 的 $r \in \mathbb{F}_q$，使得 $r^2 \in \mathbb{F}_q$ 是 $g(x)$的一个根，并且 $-r^2 \pm cr^{-1}$ 在 $\mathbb{F}_q$中均为非平方数。此外，由于 $h(x)$在 $\mathbb{F}_q$上恰有两个不同的不可约因子，定理 5.1 表明，$h(x)$的判别式，即 $D(h) = 256d^3$，是 $\mathbb{F}_q$中的一个平方数。因此，d 是 $\mathbb{F}_q$中的一个平方数。根据 [12, 定理2]，$g(x)$要么在 $\mathbb{F}_q$ 中有三个根，要么在 $\mathbb{F}_q$上不可约。后一种情况不可能，因为我们已经证明 $g(x)$在 $\mathbb{F}_q$中有一个根。因此，$g(x)$在 $\mathbb{F}_q$ 中还有另外两个根，它们必定是 $\mathbb{F}_q$ 中的非平方数（因为如果其中一个是平方数，那么由式 (15) 可得 $h(x)$在 $\mathbb{F}_q$ 上的另一种不可约因子分解）。反过来的方向是显然的。

然后我们证明第 (3) 项。若 $h(x)$可分解为一个一次因子与一个不可约三次因子的乘积，则与前面的证明类似，定理 5.1 和 [12,定理 2] 表明， $g(x)$要么在 $\mathbb{F}_q$ 中有三个根 u_1、u_2、u_3，要么在 $\mathbb{F}_q$上不可约。在前一种情况下，根据韦达公式可知 $u_1u_2u_3 = c^2$。如果 u_1、u_2、u_3 在 $\mathbb{F}_q$中全都不是平方数，那么 c^2也不是平方数，这不可能。因此，其中一个必定是 $\mathbb{F}_q$中的平方数，从而可由式 (15) 将 $h(x)$分解为两个二次因子。既然这不可能， g 必定在 $\mathbb{F}_q$上不可约。反过来的方向是显然的。

现在我们证明第 (4)项。如果 $h(x)$分解为两个一次因子和一个不可约二次因子的乘积，那么存在一个满足方程 (15)的 $r \in \mathbb{F}_q$，使得 r^2 是 $g(x)$ 的一个根，并且 $-r^2 \pm cr^{-1}$ 中恰有一个是 $\mathbb{F}_q$ 中的平方数。同时，定理 5.1 蕴含 $h(x)$ 的判别式是 $\mathbb{F}_q$ 中的非平方数。因此，根据[12, 定理 2]， d 是 $\mathbb{F}_q$ 中的非平方数，且 $g(x)$ 在 $\mathbb{F}_q$ 中没有其他根。反之亦然。

最后，我们证明第 5项。如果 $h(x)$ 在 $\mathbb{F}_q$上不可约，那么如同前面的证明，定理 5.1 和 [12, 定理 2] 表明 $g(x)$ 有唯一的根 u 在 $\mathbb{F}_q$ 中。由于没有 $r \in \mathbb{F}_q$ 满足方程 (15)，u 在 $\mathbb{F}_q$ 中是非平方数。□

设 a、b、c 以及 $(\beta_n)_{n\geq 0}$ 如前所述。定理 5.4 导出以下结果。

推论 5.5. 多项式 $f(x) = b^3(x+a)^4 + c(x+a) - a$ 在 $\mathbb{F}_{3^m}$上稳定，当且仅当对每个 $n \in \mathbb{N}_0$， $x^3 - \beta_n x - c^2$ 在 $\mathbb{F}_{3^{4^n m}}$ 中有唯一一个非平方数根。

6 结论

本文通过反复运用 Capelli 引理，构造了若干类次数为 2、3 和 4 的稳定抗平移多项式。因此，我们证实了 Ahmadi 和 Monsef-Shokri 的猜想 [2]，即多项式 $f(x) = x^3+x^2+1$在 $\mathbb{F}_2$上稳定。当 q 为素数幂且 $q \equiv 1$ （模 4）时，我们得到了 $\mathbb{F}_q$ 上稳定二次多项式数量下界的改进。对于任意次数 d 的有限域上的稳定多项式数量，目前似乎尚未建立下界（尽管已有研究利用特征和给出了上界，见[4, 定理 1] 和 [5, 定理 5。5] 展望未来，我们希望基于第 2 节中的稳定性判定，在 $\mathbb{F}_q$ 上构造稳定二次多项式（当 $q \equiv 3$ （模 4）时），并找到次数为 ≥ 5 的稳定多项式实例。此外，我们正致力于为有限域上稳定多项式的数量建立更好的估计。

placeholder

[1] O. Ahmadi, F. Luca, A. Ostafe, I.E. Shparlinski, 《稳定二次多项式》, Glasgow Mathematical Journal. 54(2): 359–369, 2012.

[2] O. Ahmadi, K. Monsef-Shokri, 《有限域上三项式稳定性札记》, 《有限域及其应用》. 63: 101649, 2020.[3] S. Cohen, 《有限域中某些类型的不可约多项式》, 剑桥哲学学会数学会刊 66(2), 335–344, 1969.[4] D. Gom´ez-P´erez, A.P. Nicol´as, 《稳定二次多项式数量的估计》, 《有限域及其应用》. 16(6), 401–405, 2010.[5] D. Gom´ez-P´erez, A.P. Nicol´as, A. Ostafe, D. Sardonil, 《有限域上的稳定多项式》, Revista Matem´atica Iberoamericana. 30(2), 523–535, 2014.[6] R. Jones, N. Boston, 《有限域上的定型多项式》, 《美国数学会会刊》. 140(6): 1849–1863, 2012.[7] R. Jones, N. Boston, 《〈有限域上的定型多项式〉勘误》, 《美国数学会会刊》 148(2), 913–914, 2020.[8] R.W.K. Odoni, 《数列的素因子》 $w_{n+1} = 1 + w_1 \dots w_n$, 《伦敦数学会杂志》. (Ser. 2) 32(1), 1–11, 1985.[9] R.W.K. Odoni, 《多项式迭代与复合的伽罗瓦理论》, 《伦敦数学会会刊》. (Ser. 3) 51(3) 385–414, 1985.[10] A. Ostafe, I.E. Shparlinski, 《稳定二次多项式临界轨道长度》, 《美国数学会会刊》. 138(8), 2653— 2656, 2010.[11] Z.-X. Wan, 《有限域与伽罗瓦环讲义》. 世界科学出版公司, 2003.[12] K.S. Williams, 关于 GF (2^n) 和 GF (3^n) 上三次多项式的札记, 《数论杂志》 7, 361–365, 1975.