March 2023

# Rational Functions of Degree Five That Permute the Projective Line Over a Finite Field

Christopher Sze
*University of South Florida*

# Rational Functions of Degree Five That Permute the Projective Line Over a Finite Field

by

Christopher Sze

A dissertation submitted in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
Department of Mathematics and Statistics
College of Arts and Sciences
University of South Florida

Major Professor: Xiang-dong Hou, Ph.D.
Brian Curtin, Ph.D.
Giacomo Micheli, Ph.D.
Dmytro Savchuk, Ph.D.
Qiang Wang, Ph.D.

Date of Approval:
March 28, 2023

Keywords: absolutely irreducible, Carlitz's formula, Hasse-Weil bound, permutation polynomial, power sum

## DEDICATION

In loving memory of my mother, Virginia Sze.

## ACKNOWLEDGMENTS

I would first like to thank my advisor, Dr. Xiang-dong Hou, for his guidance, support, and patience. Without him, this work would not be a success and I would not be here in the United States pursuing a doctorate. I am forever indebted to him.

I would like to thank my committee members Dr. Brian Curtin, Dr. Giacomo Micheli, and Dr. Dmytro Savchuk for taking the time to read this dissertation and providing their input. I am grateful to Dr. Qiang Wang for accepting to be the chairperson of my defense and for offering valuable feedback.

I would also like to thank Dr. Rimbey and Dr. Savchuk for entrusting me to be the instructor of record for multiple classes during my stay here at the University of South Florida.

I am thankful to Munna and Roderico de Armas for their company, friendship, and comfort in times of need. Warm appreciation to Evelyn Nonepara for the friendship and for adopting my cats back home in the Philippines.

I would like to express my deepest gratitude to my father Wing Sheun, and my siblings Nelson and Jennylyn, for their love, support, and encouragement.

## TABLE OF CONTENTS

## LIST OF TABLES

## LIST OF FIGURES

## ABSTRACT

Rational functions over a finite field $\mathbb{F}_q$ induce mappings from the projective line $\mathbb{P}^1(\mathbb{F}_q)$ to itself. Rational functions that permute the projective line are called permutation rational functions (PRs). The notion of permutation rational functions is a natural extension of the permutation polynomials which have been studied for over a century. Recently, PRs of degrees up to four have been determined. This dissertation is a project aimed at determining PRs of degree five.

Rational functions of degree five (excluding those that are equivalent to polynomials) are divided into five cases according to the factorization of their denominators. Our main results can be summarized as follows:

1. We showed that in Cases I and II, there are no PRs, whenever $q$ is sufficiently large.

2. In Case III, we completely determined all PRs. When $q$ is odd, there is an infinite family; when $q$ is even, there are two infinite families.

3. In Case IV, we determined all PRs under an additional condition. There is an infinite family each for odd $q$ and for even $q$.

Our approach is based on a combination of two methods. One uses the Carlitz power sum formula, which is a new technique that is particularly effective for PRs of low degrees. The other method relies on the Hasse-Weil bound on the number of zeros of an absolutely irreducible polynomial in two variables. This is a well-known technique that allows people to relate permutation properties of a rational function with the factorization of an associated polynomial.

# CHAPTER 1:
# INTRODUCTION

Let $\mathbb{F}_q$ denote the finite field with $q$ elements whose algebraic closure is denoted by $\overline{\mathbb{F}_q}$. A polynomial $f(X) \in \mathbb{F}_q[X]$ is called a *permutation polynomial* (PP) of $\mathbb{F}_q$ if the induced mapping $x \mapsto f(x)$ is a permutation of $\mathbb{F}_q$. Let $\mathbb{P}^1(\mathbb{F}_q) = \mathbb{F}_q \cup \{\infty\}$ be the projective line over $\mathbb{F}_q$. A rational function $f(X) \in \mathbb{F}_q(X)$ defines a mapping from $\mathbb{P}^1(\mathbb{F}_q)$ to itself; the rational function is called a *permutation rational function* (PR) of $\mathbb{P}^1(\mathbb{F}_q)$ if it permutes $\mathbb{P}^1(\mathbb{F}_q)$. Let $\mathbb{F}$ be any field. For $0 \neq f(X) = P(X)/Q(X) \in \mathbb{F}(X)$, where $P, Q \in \mathbb{F}[X]$ and $\gcd(P, Q) = 1$, we define the *degree* of the rational function to be $\deg f = \max\{\deg P, \deg Q\}$, which is the degree of the extension of $\mathbb{F}(X)$ over $\mathbb{F}(f(X))$.

PPs were first studied by Hermite [15], Jordan [24], and Serret [40] on prime finite fields. Dickson [8] started the classification of low degree PPs over arbitrary finite fields. PPs of degree $\leq 7$, including degree 8 in characteristic 2, have been classified [8, 11, 12, 28, 41]. Modern treatments of the subject can be found in [27], [33, Chapter 7] and [34, Chapter 8]; also see [19] for a survey on the study of PPs over finite fields up to 2015. The interest in this subject has been rekindled multiple times throughout history because of the applications of PPs in many areas of mathematics. The recent surge of research activities in PPs is driven by a variety of mathematical questions arising from cryptography, computer science, and information theory.

A unique feature of finite fields is that every function from $\mathbb{F}_q$ to itself is representation by a polynomial in $\mathbb{F}_q[X]$; such a representation is unique modulo $X^q - X$. The polynomial representation of any permutation of $\mathbb{F}_q$ is given by the Lagrange interpolation. However,

the study of PPs of finite fields is not about constructions of arbitrary permutations of finite fields, but about permutations either with simple algebraic form or with additional properties. For example, permutation binomials and low degree permutation rational functions are of great interest but they are difficult to determine. While PPs have been extensively studied, the study of PRs is still in its infancy. Recently, PRs of degree 3 were determined by Ferraguti and Micheli [13] and PRs of degree 4 were determined by Hou [20]. For the classification of PRs of degree 4 by a different approach, see Ding and Zieve [10].

Let $\mathbb{F}_q^*$ denote the multiplicative group of $\mathbb{F}_q$. PRs of subgroups of $\mathbb{F}_q^*$ play a central role in the study of certain types of PPs. More precisely, we have the following result which can be traced to multiple sources and is considered folklore [38, 44, 52]:

**Theorem 1.1.** *Let $h \in \mathbb{F}_q[X]$ and $r$, $d$ be positive integers such that $d \mid q-1$. Then $X^r h(X^{(q-1)/d})$ is a PP of $\mathbb{F}_q$ if and only if $\gcd(r,(q-1)/d)=1$ and $X^r h(X)^{(q-1)/d}$ permutes the multiplicative group $\mu_d := \{x \in \mathbb{F}_q^* : x^d = 1\}$.*

In the above theorem, $X^r h(X)^{(q-1)/d}$ is a polynomial of high degree. However, it can be represented by a rational function of low degree. The study of low degree rational functions, as a function on $\mu_d$, that permute subgroups of $\mathbb{F}_q^*$ has led to the construction of many new PPs. There is a vast literature of works based on this approach; we only sample a few: [4, 22, 21, 29, 30, 39, 51]. For additional references on PPs and PRs, we refer the reader to [3, 17, 9, 14, 23, 31, 32, 42, 45, 43, 47, 48, 49, 50].

For any field $\mathbb{F}$, let $\mathbb{P}^1(\mathbb{F}) = \mathbb{F} \cup \{\infty\}$ be the projective line over $\mathbb{F}$. Each $f(X) \in \mathbb{F}(X)$ induces a function $\bar{f} : \mathbb{P}^1(\mathbb{F}) \mapsto \mathbb{P}^1(\mathbb{F})$, where $\overline{f \circ g} = \bar{f} \circ \bar{g}$. Let $G(\mathbb{F}) = \{\phi \in \mathbb{F}(X) : \deg \phi = 1\}$. $G(\mathbb{F})$ is a group under composition of functions and is isomorphic to the projective general linear group $\mathrm{PGL}(2,\mathbb{F})$, or the automorphism group $\mathrm{Aut}(\mathbb{F}(X)/\mathbb{F})$ of $\mathbb{F}(X)$ over $\mathbb{F}$. For each $f(X) \in G(\mathbb{F})$, there exists $g \in \mathbb{F}(X)$ such that $g \circ f = f \circ g = X$, hence $\bar{g} \circ \bar{f} = \bar{f} \circ \bar{g} = \mathrm{id}_{\mathbb{P}^1(\mathbb{F})}$. Therefore elements of $G(\mathbb{F})$, which are the degree one rational functions over $\mathbb{F}$, permute $\mathbb{P}^1(\mathbb{F})$. Observe that the set of PRs of $\mathbb{P}^1(\mathbb{F})$ is closed under composition, i.e. if $f, g$ are PRs of $\mathbb{P}^1(\mathbb{F})$, then $f \circ g$ is also a PR of $\mathbb{P}^1(\mathbb{F})$. We can then define equivalence between two

rational functions in the following manner. We say that $f, g \in \mathbb{F}(X)$ are *equivalent* if there exist $\phi, \psi \in G(\mathbb{F})$ such that $f = \phi \circ g \circ \psi$.

We then ask the following question. Are there rational functions of higher degree that permute $\mathbb{P}^1(\mathbb{F})$? The answer depends on $\mathbb{F}$. For example, the answer is positive if $\mathbb{F} = \mathbb{R}$ $(f(X) = X^3)$ or $\operatorname{char}\mathbb{F} = p > 0$ $(f(X) = X^p)$. The answer could be negative as shown in the following proposition.

**Proposition 1.2.** *If $\mathbb{F} = \mathbb{Q}$ or $\mathbb{F}$ is algebraically closed with $\operatorname{char}\mathbb{F} = 0$, then there are no rational functions of degree $> 1$ that permute $\mathbb{P}^1(\mathbb{F})$.*

*Proof.* Assume to the contrary that there exists $f \in \mathbb{F}(X)$ with $\deg f = d > 1$ such that $f$ permutes $\mathbb{P}^1(\mathbb{F})$.

First, assume that $\mathbb{F}$ is algebraically closed with $\operatorname{char}\mathbb{F} = 0$. Write $f = P(X)/Q(X)$, where $P, Q \in \mathbb{F}[X]$, $\gcd(P, Q) = 1$, and $\deg P < \deg Q = d$. Since $f$ takes the value $\infty$ exactly once, we may assume that $Q(X) = X^d$. We may replace $Q$ with $Q + aP$ for any $a \in \mathbb{F}^*$ (the multiplicative group of $\mathbb{F}$). Then $Q + aP = (X + u(a))^d$ for some $u(a) \in \mathbb{F}^*$. Consequently,

$$P = a^{-1}((X + u(a))^d - X^d) = \sum_{i=0}^{d-1} \binom{d}{i} a^{-1} u(a)^{d-i} X^i.$$

It follows that

$$u(a) = \frac{a^{-1}u(a)^d}{a^{-1}u(a)^{d-1}}$$

is independent of $a$ for all $a \in \mathbb{F}^\times$. This is clearly impossible.

Next, assume that $\mathbb{F} = \mathbb{Q}$. We may write $f = P(X)/Q(X)$, where $P, Q \in \mathbb{Z}[X]$, $\gcd(P, Q) = 1$ (in $\mathbb{Q}[X]$), and $\deg P < \deg Q = d$. We may assume $\deg P > 0$. (Otherwise, $f$ is equivalent to a polynomial $f_1 = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_0$, and we may assume $a_{d-1} \neq 0$. Simply consider $f_1(1/x) - a_d$.) By a suitable transformation $X \mapsto rX$, we may assume that $Q$ is monic. There exist $\alpha, \beta \in \mathbb{Z}[X]$ such that

$$\alpha P + \beta Q = k \in \mathbb{Z} \setminus \{0\}.$$

Thus for each $u \in \mathbb{Z}$, $\gcd(P(u), Q(u)) \mid k$. For each $0 \neq a \in \mathbb{Z}$, there exists $u = u(a) \in \mathbb{Q}$ such that $P(u)/Q(u) = a$, i.e., $Q(u) - aP(u) = 0$. Since $Q - aP \in \mathbb{Z}[X]$ is monic, $u \in \mathbb{Z}$. The map $a \mapsto u$ is one-to-one. Moreover, $\gcd(Q(u), P(u)) = P(u) \mid k$. Since $|P(x)| \to \infty$ as $x \to \infty$, there are only finitely many $u \in \mathbb{Z}$ such that $P(u) \mid k$. This is a contradiction. $\square$

It appears to be a nontrivial question to describe all fields $\mathbb{F}$ such that only rational functions of degree one permute $\mathbb{P}^1(\mathbb{F})$, although this is not a direction that we pursue in this dissertation.

A polynomial $f(X) \in \mathbb{F}_q[X]$ permutes $\mathbb{P}^1(\mathbb{F}_q)$ if and only if $f(X)$ is a PP of $\mathbb{F}_q$. Since PPs of low degrees are known, we only consider rational functions which are not equivalent to a polynomial. Let $f(X) \in \mathbb{F}_q(X)$ which is not equivalent to a polynomial. Write $f(X) = P(X)/Q(X)$, where $P, Q \in \mathbb{F}_q[X]$ and $\gcd(P, Q) = 1$. If $\deg P = \deg Q$, then $f(X)$ is equivalent to $P_1(X)/Q(X)$, for some $P_1 \in \mathbb{F}_q[X]$ with $\deg P_1 < \deg Q$. If $\deg P < \deg Q$, then $f(X)$ is equivalent to $Q/P$. Therefore, up to equivalence, we may assume $\deg P > \deg Q$.

The main objective of this dissertation is to determine PRs of degree 5. Let $f(X)$ be a PR of $\mathbb{P}^1(\mathbb{F}_q)$ of degree 5 which is not equivalent to a polynomial. Then $f(X)$ is equivalent to $P(X)/Q(X)$, where $P, Q \in \mathbb{F}_q[X], \gcd(P, Q) = 1, \deg Q < \deg P = 5$, and $Q$ has no roots in $\mathbb{F}_q$. Hence up to equivalence, we may assume that $f(X)$ is one of the following forms.

**Case I.**

$$f(X) = X^3 + aX^2 + bX + \frac{cX + d}{Q(X)},$$

where $a, b, c, d \in \mathbb{F}_q$, $(c, d) \neq (0, 0)$, and $Q(X)$ is a monic irreducible quadratic over $\mathbb{F}_q$.

**Case II.**

$$f(X) = X^2 + aX + \frac{bX^2 + cX + d}{Q(X)},$$

where $a, b, c, d \in \mathbb{F}_q$, $(b, c, d) \neq (0, 0, 0)$, and $Q(X)$ is a monic irreducible cubic over $\mathbb{F}_q$.

**Case III.**

$$f(X) = X + \frac{aX^3 + bX^2 + cX + d}{Q(X)^2},$$

where $a, b, c, d \in \mathbb{F}_q$, $(a, b, c, d) \neq (0, 0, 0, 0)$, and $Q(X)$ is a monic irreducible quadratic over $\mathbb{F}_q$.

**Case IV.**

$$f(X) = X + \frac{aX + b}{Q_1(X)} + \frac{cX + d}{Q_2(X)},$$

where $a, b, c, d \in \mathbb{F}_q$, $(a, b) \neq (0, 0)$, $(c, d) \neq (0, 0)$, $Q_1(X)$ and $Q_2(X)$ are different monic irreducible quadratics over $\mathbb{F}_q$.

**Case V.**

$$f(X) = X + \frac{aX^3 + bX^2 + cX + d}{Q(X)},$$

where $a, b, c, d \in \mathbb{F}_q, (a, b, c, d) \neq (0, 0, 0, 0)$, and $Q(X)$ is a monic irreducible quartic over $\mathbb{F}_q$.

Here is a summary of our results. In Case I and II, we found that there are no PRs when $q$ is sufficiently large (Theorems 2.1, 2.2, 3.1). In Case III, we determined all PRs and obtained an infinite family of PRs when $q$ is odd (Theorem 4.1), and two infinite families of PRs when $q$ is even (Theorem 4.6). Case IV is partially resolved, where we determined all PRs under an additional condition and obtained one infinite family of PRs for odd $q$ (Theorem 5.1) and one infinite family of PRs for even $q$ (Theorem 5.4). Case V is currently unresolved. Our approach is based on a novel combination of the Carlitz power sum and the Hasse-Weil bound which make a seemly theoretic question "computable". Our proof entails heavy computations which are handled by *Mathematica* [46].

### 1.1 Preliminaries and Outline of Approach

In this section, we present the tools that we will use and also provide a general overview of our approach to the question. The following theorem provides a useful criterion for PPs and PRs.

**Theorem 1.3** (**Permutation Criterion [33]**). *A list of elements $a_1, a_2, \ldots, a_q \in \mathbb{F}_q$ are distinct if and only if*

$$\sum_{i=1}^{q} a_i^t = \begin{cases} 0 & \text{if } 1 \le t \le q-2, \\ -1 & \text{if } t = q-1. \end{cases}$$

(Note: The above theorem is equivalent to the Hermite's Criterion [33, Theorem 7.4] which is stated in terms of congruences modulo $X^q - X$.) We prove the following general version of Theorem 1.3, which was first proved by Akbary and Wang in [1, Lemma 2.1].

**Lemma 1.4** (**Exercise 2.10 [18]**). *Let $\mathbb{F}$ be any field and let $A$ be a finite subgroup of $\mathbb{F}^*$ (the multiplicative group of $\mathbb{F}$) of order $l$. Let $a_1, \ldots, a_l \in A$. Then $a_1, \ldots, a_l$ are distinct if and only if*

$$\sum_{j=1}^{l} a_j^s = 0 \quad \text{for all} \quad 1 \le s \le l-1.$$

*Proof.* We first note that $A$ is cyclic and char $\mathbb{F}$ does not divide $l$. Let

$$f(X) = \sum_{j=1}^{l} \sum_{i=0}^{l-1} (a_j^{-1} X)^i = \sum_{i=0}^{l-1} \left( \sum_{j=1}^{l} a_j^{-1} \right) X^i \in \mathbb{F}[X].$$

Since

$$\sum_{i=0}^{l-1} \alpha^i = \begin{cases} 0 & \text{if } \alpha \in A \setminus \{1\}, \\ l & \text{if } \alpha = 1, \end{cases}$$

we have

$$\sum_{i=0}^{l-1} (a_j^{-1} x)^i = \begin{cases} 0 & \text{if } x \in A \setminus \{a_j\}, \\ l & \text{if } x = a_j. \end{cases}$$

Now $a_1, \ldots, a_l$ are distinct if and only if $f(\alpha) = l$, for all $\alpha \in A$. But since $\deg f \le l-1$, this happens if and only if $f$ is the constant polynomial $l$. Now $f = l$ if and only if

$$\sum_{j=1}^{l} a_j^{-i} = 0 \quad \text{for all} \quad 1 \le i \le l-1.$$

□

Let $f(X) \in \mathbb{F}_q(X)$ be such that $f(\mathbb{F}_q) \subset \mathbb{F}_q$ and $f(\infty) = \infty$, which is true for the rational functions in all Cases I – V. For integer $k \geq 0$, let

$$S(f,k) := \sum_{x \in \mathbb{F}_q} f(x)^k$$

denote the $k$-th *power sum* of $f$. Then by the permutation criterion $f(X)$ is a PR of $\mathbb{P}^1(\mathbb{F}_q)$ if and only if

$$S(f,k) = \begin{cases} 0 & \text{if } \ 1 \leq k \leq q-2, \\ -1 & \text{if } \ k = q-1. \end{cases} \tag{1.1}$$

Write $f(X) = P(X)/Q(X), \gcd(P,Q) = 1$, where $Q(X)$ is a product of monic irreducible polynomials over $\mathbb{F}_q$. Each irreducible factor $Q_i$ of $Q(X)$ can be written as $(X-r)(X-r^q)\cdots(X-r^{q^{d_i-1}})$, where $r \in \mathbb{F}_{q^{d_i}}, d_i = \deg Q_i$. Hence, the partial fraction decomposition of $f(X)^k$, for $k \geq 1$, is of the form

$$f(X)^k = \sum_{i=0}^{m} \alpha_i X^i + \sum_{i=1}^{n} \frac{\beta_i}{(X-r_i)^{s_i}}, \tag{1.2}$$

where $\alpha_0, \ldots, \alpha_m \in \mathbb{F}_q, \beta_1, \ldots, \beta_n \in \overline{\mathbb{F}_q}, r_1, \ldots, r_n \in \overline{\mathbb{F}_q} \setminus \mathbb{F}_q$, and $s_1, \ldots, s_n$ are positive integers. The following formula by Carlitz plays a key role in our approach; it allows us to compute the power sum $S(f,k)$ explicitly.

**Lemma 1.5 (Carlitz's Formula [7, 16, 17]).** *We have*

$$\sum_{x \in \mathbb{F}_q} \frac{1}{(x-X)^k} = \frac{1}{(X^q - X)^k}, \quad 1 \leq k \leq q.$$

Throughout this dissertation, *the numerator of a rational function* refers to the numerator of the rational function in lowest terms.

Now by taking the summation of (1.2) as $x$ runs through the elements of $\mathbb{F}_q$, we have

$$S(f,k) = \sum_{i=0}^{m} \left( \alpha_i \sum_{x \in \mathbb{F}_q} x^i \right) + \sum_{i=1}^{n} \sum_{x \in \mathbb{F}_q} \frac{\beta_i}{(x - r_i)^{s_i}}.$$

If $0 \leq i \leq q-2$, then by the permutation criterion, we have $\sum_{x \in \mathbb{F}_q} x^i = 0$. If $s_i \leq q$, then by Carlitz's Formula we have

$$\sum_{x \in \mathbb{F}_q} \frac{\beta_i}{(x - r_i)^{s_i}} = \frac{\beta_i}{(r_i^q - r_i)^{s_i}}.$$

Therefore

$$S(f,k) = \sum_{i=1}^{n} \frac{\beta_i}{(r_i^q - r_i)^{s_i}}, \tag{1.3}$$

whenever $m \leq q-2$, and $s_i \leq q$ for all $1 \leq i \leq n$. Let

$$s(f,k) := \text{the numerator of } S(f,k).$$

If we assume that $f$ is a PR of $\mathbb{P}^1(\mathbb{F}_q)$, then by the permutation criterion,

$$s(f,k) = 0, \tag{1.4}$$

whenever $q \geq \max\{k, m\} + 2$, where $m$ is the degree of the polynomial part in (1.2). We will refer to these equations as the power sum conditions. In Appendix A, we list down the formulas of $s(f,k)$, for small values of $k$, where $f(X)$ is one of the rational functions in Cases I, III and IV. (The calculation of the power sums in Cases II and V is not included since we did not use them in our proof for Case II, while Case V is still unresolved.) It is our belief that the power sums hold the ultimate secret about PRs.

Another tool that we used in our approach is the Hasse-Weil bound for the number of zeros of an absolutely irreducible polynomial over finite fields. We first look at the following

definitions. A polynomial $F \in \mathbb{F}_q[X_1, \ldots, X_n]$ is said to be *absolutely irreducible* if $F$ is irreducible in $\overline{\mathbb{F}_q}[X_1, \ldots, X_n]$. For a polynomial $F(X_1, \ldots, X_n) \in \mathbb{F}_q[X_1, \ldots, X_n]$, define

$$V_{\mathbb{F}_q^n}(F) = \{(x_1, \ldots, x_n) \in \mathbb{F}_q^n : F(x_1, \ldots, x_n) = 0\}.$$

For a homogeneous polynomial $F(X_0, \ldots, X_n) \in \mathbb{F}_q[X_0, \ldots, X_n]$, define

$$V_{\mathbb{P}^n(\mathbb{F}_q)}(F) = \{(x_0 : \ldots : x_n) \in \mathbb{P}^n(\mathbb{F}_q) : F(x_0, \ldots, x_n) = 0\}.$$

Let $F(X, Y, Z) \in \mathbb{F}_q[X, Y, Z]$ be a homogeneous polynomial of degree $d$ that is absolutely irreducible. By Aubry and Perret's [2] version of the Hasse-Weil bound, we have

$$\left||V_{\mathbb{P}^2(\mathbb{F}_q)}(F)| - (q+1)\right| \leq (d-1)(d-2)q^{1/2}. \tag{1.5}$$

We will use the following lemma by Hou [20], which is an optimized version of the Hasse-Weil bound that is applicable to the circumstances of this dissertation.

**Lemma 1.6.** *Let $F(X, Y, Z) \in \mathbb{F}_q[X, Y, Z]$ be an absolutely irreducible homogeneous polynomial of degree $d$. Let $d_1 = \deg_X F, d_2 = \deg_Y F, d_3 = \deg_Z F$, and assume that $1 \leq d_1 \leq d_2 \leq d_3$. Then*

$$|V_{\mathbb{P}^2(\mathbb{F}_q)}(F)| \geq q + 1 - 2(d_1 - 1)(d_2 - 1)q^{1/2} - \frac{1}{2}(d_2 - 1)(d - 1)(d - 2).$$

We are now ready to discuss the outline of our approach. First, we compute the power sum conditions $s(f, k) = 0$, for small $k$. If the parameters of $f$ cause the power sum conditions to fail, then $f$ is not a PR. If the parameters of $f$ either satisfy the power sum conditions or is inconclusive, we further investigate the functions $F$ and $G$, which are defined below. Let

$$F(X, Y) = \text{the numerator of } \frac{f(X) - f(Y)}{X - Y}.$$

Clearly, $f$ is a PR if and only if $F$ has no roots $(x, y) \in \mathbb{F}_q^2$ with $x \neq y$. Since $F(X, Y)$ is a symmetric function, we can write $F(X, Y) = G(X + Y, XY)$, where $G \in \mathbb{F}_q[X, Y]$.

**Case 1.** Assume that $G(X, Y)$ is not absolutely irreducible. Then this condition together with some of the power conditions $s(f, k) = 0$, impose restrictions on the parameters of $f$. Using the factorization of $G(X, Y)$ in $\overline{\mathbb{F}_q}[X, Y]$, we find all the roots of $G(X, Y)$ in $\mathbb{F}_q^2$ if possible. Using Lemma 1.10 in Section 1.2, we are able to show in some of the cases we considered, that the corresponding roots in the symmetric polynomial $F(X, Y)$ are not elements of $\mathbb{F}_q^2$. Therefore, $f(X)$ is a PR of $\mathbb{P}^1(\mathbb{F}_q)$.

**Case 2.** Assume that $G(X, Y)$ is absolutely irreducible. Using Corollary 1.9 in Section 1.2, we are able to show in some of the cases we considered, that $F(X, Y)$ has an absolutely irreducible factor in $\mathbb{F}_q[X, Y]$. Hence, by the Hasse-Weil bound, there exists $(x, y) \in \mathbb{F}_q^2$, with $x \neq y$, such that $F(x, y) = 0$, whenever $q$ is sufficiently large. Therefore, this shows that $f(X)$ is not a PR of $\mathbb{P}^1(\mathbb{F}_q)$.

The outline is illustrated in Figure 1. The power sum conditions alone allow us to solve Case I. For Case II, we provide a theoretic result; no computation is needed. For Case III $q$ odd case, we make use of the power sum conditions and the Hasse-Weil bound. To use the Hasse-Weil bound, the existence of an absolutely irreducible factor of $F(X, Y)$ over $\mathbb{F}_q$ has to be established. For Case III $q$ even case, the power sum conditions alone allow us to solve the problem completely because we are able to factor the power sums effectively modulo 2. For Case IV, in the situation that we considered, unfortunately power sum conditions alone will not allow us to determine the PRs because equations $s(f, k)$ are very long even for small values of $k$, and *Mathematica* is unable to find a factorization for $s(f, k)$; we have to use the combination of power sums and absolute irreducibility of $G(X, Y)$.

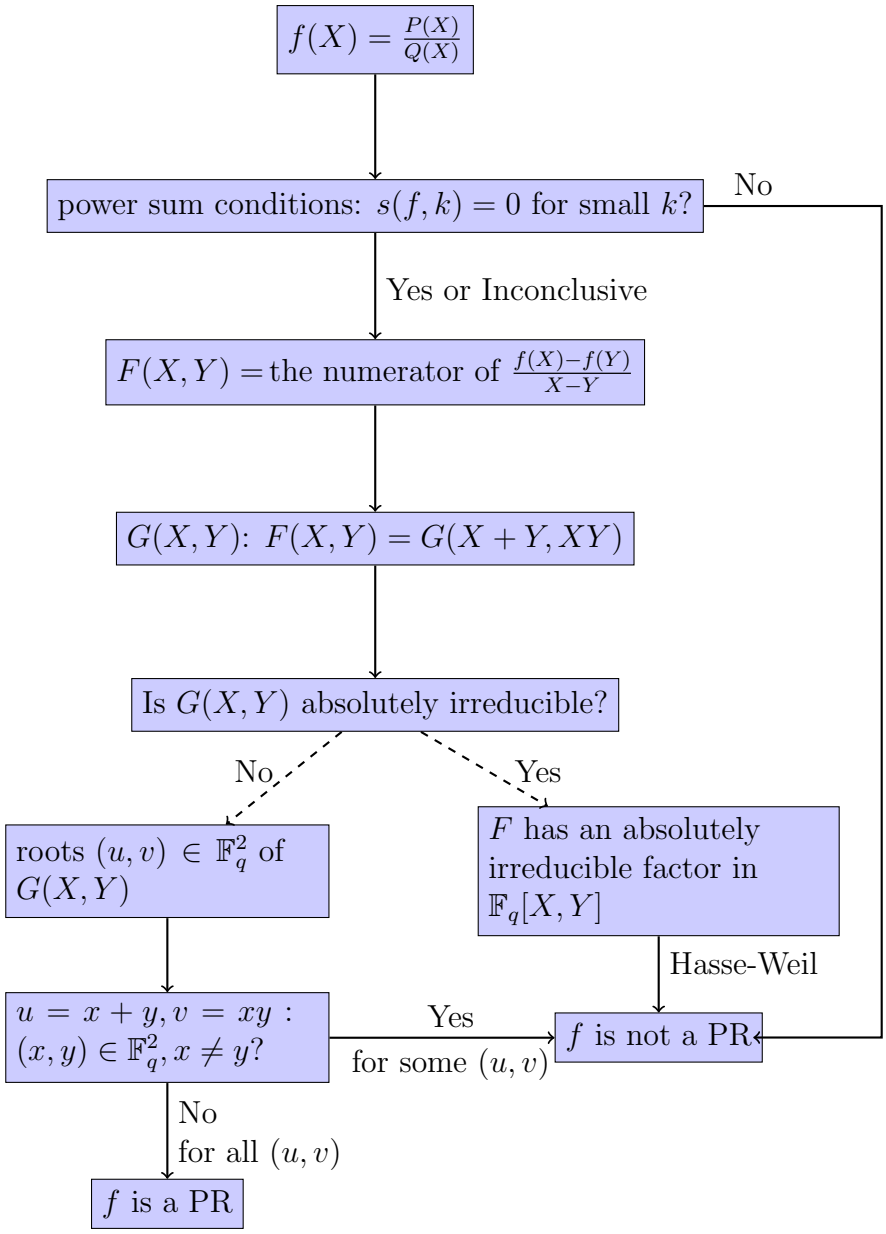


**Figure 1.** Outline of Approach

**Note.** A dashed arrow is an implication that is not logically sound in general but true in the cases we considered.

## 1.2 Propositions and Lemmas

Throughout this dissertation, the automorphism $\sigma$ always denotes the Frobenius of $\overline{\mathbb{F}_q}/\mathbb{F}_q$ which is defined by $\sigma(\cdot) = (\cdot)^q$.

**Proposition 1.7.** *Let $\mathbb{F}$ be a field. Let $F(X,Y) \in \mathbb{F}[X,Y]$ be symmetric such that $F(X,Y) = G(X+Y, XY)$, where $G \in \mathbb{F}[X,Y]$ is irreducible. Then one of the following occurs.*

*(i)* $F(X,Y)$ *is irreducible.*

*(ii)* $F(X,Y) = \epsilon H(X,Y)H(Y,X)$, *where* $H(X,Y) \in \mathbb{F}[X,Y]$ *is irreducible,* $\epsilon \in \mathbb{F}^*$, *and* $\gcd(H(X,Y), H(Y,X)) = 1$.

*(iii)* $\operatorname{char}\mathbb{F} \neq 2$ *and* $F(X,Y) = \epsilon(X-Y)^2$, *where* $\epsilon \in \mathbb{F}^*$.

*Proof.* Assume that $F(X,Y)$ is not irreducible. Let $H(X,Y) \in \mathbb{F}[X,Y]$ be an irreducible factor of $F(X,Y)$. Then we also have $H(Y,X) \mid F(X,Y)$. If $\gcd(H(X,Y), H(Y,X)) = 1$, then $H(X,Y)H(Y,X)$ is a symmetric factor of $F(X,Y)$, hence $F(X,Y) = \epsilon H(X,Y)H(Y,X)$ for some $\epsilon \in \mathbb{F}^*$. If $\gcd(H(X,Y), H(Y,X)) \neq 1$, then $H(Y,X) = \delta H(X,Y)$ for some $\delta \in \mathbb{F}^*$. Since $H(X,Y) = \delta H(Y,X) = \delta^2 H(X,Y)$, we have $\delta = \pm 1$. If $\delta = 1$, then $H(X,Y)$ is a nontrivial symmetric factor of $F(X,Y)$; this is impossible since $G(X,Y)$ is irreducible. So $\operatorname{char}\mathbb{F} \neq 2$ and $H(Y,X) = -H(X,Y)$. Then $H(X,X) = -H(X,X)$, i.e., $H(X,X) = 0$. Thus $X - Y \mid H(X,Y)$, and hence $X - Y \mid F(X,Y)$. Let $F_1(X,Y) = F(X,Y)/(X-Y)$. Then $F_1(X,Y) = -F_1(Y,X)$, whence $X - Y \mid F_1(X,Y)$. Therefore, $(X-Y)^2 \mid F(X,Y)$. Since $G(X,Y)$ is irreducible, we have $F(X,Y) = \epsilon(X-Y)^2$ for some $\epsilon \in \mathbb{F}^*$. □

**Proposition 1.8.** *Assume that $F(X,Y) = H(X,Y)H(Y,X) \in \mathbb{F}_q[X,Y]$, where $H(X,Y) \in \overline{\mathbb{F}}_q[X,Y]$ is irreducible and $\gcd(H(X,Y), H(Y,X)) = 1$. Then one of the following occurs.*

*(i)* $H(X,Y) = aH_1(X,Y)$, *where* $H_1(X,Y) \in \mathbb{F}_q[X,Y]$, $a \in \mathbb{F}_{q^2}^*$, $a^2 \in \mathbb{F}_q$.

*(ii)* $H(X,Y) \in \mathbb{F}_{q^2}[X,Y]$ *and* $\sigma(H(X,Y)) = \pm H(Y,X)$. *If* $\sigma(H(X,Y)) = H(Y,X)$, *then*

$$H(X,Y) = \sum_{i<j} (a_{ij} X^i Y^j + \sigma(a_{ij}) Y^i X^j) + \sum_i a_{ii} X^i Y^i, \tag{1.6}$$

*where* $a_{ij} \in \mathbb{F}_{q^2}$ *and* $a_{ii} \in \mathbb{F}_q$. *If* $\sigma(H(X,Y)) = -H(Y,X)$, *then*

$$H(X,Y) = \sum_{i<j} (a_{ij} X^i Y^j - \sigma(a_{ij}) Y^i X^j) + \sum_i a_{ii} X^i Y^i, \tag{1.7}$$

*where* $a_{ij} \in \mathbb{F}_{q^2}$ *and* $\mathrm{Tr}_{q^2/q}(a_{ii}) = 0$.

**Note.** In (1.6), write $a_{ii} = b_i + \sigma(b_i)$, $b_i \in \mathbb{F}_{q^2}$. Then

$$H(X,Y) = U(X,Y) + \sigma(U(Y,X)), \text{ where } U(X,Y) = \sum_{i<j} a_{ij} X^i Y^j + \sum_i b_i X^i Y^i.$$

In (1.7), write $a_{ii} = b_i - \sigma(b_i)$, $b_i \in \mathbb{F}_{q^2}$. Then

$$H(X,Y) = V(X,Y) - \sigma(V(Y,X)), \text{ where } V(X,Y) = \sum_{i<j} a_{ij} X^i Y^j + \sum_i b_i X^i Y^i.$$

*Proof of Proposition 1.8.* Recall that $\sigma \in \mathrm{Aut}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ is defined by $\sigma(\cdot) = (\cdot)^q$. Then $\sigma(H(X,Y)) \mid F(X,Y)$. Hence there exists $\epsilon \in \overline{\mathbb{F}}_q^*$ such that $\sigma(H(X,Y)) = \epsilon H(X,Y)$ or $\epsilon H(Y,X)$.

First assume that $\sigma(H(X,Y)) = \epsilon H(X,Y)$. Write $H(X,Y) = aH_1(X,Y)$, where $a \in \overline{\mathbb{F}}_q^*$ and at least one of the coefficients of $H_1(X,Y)$ is 1. Since

$$\sigma(a)\sigma(H_1(X,Y)) = \sigma(H(X,Y)) = \epsilon H(X,Y) = \epsilon a H_1(X,Y),$$

we have $\sigma(H_1(X,Y)) = H_1(X,Y)$, i.e., $H_1(X,Y) \in \mathbb{F}_q[X,Y]$. Since $a^2 H_1(X,Y) H_1(Y,X) = F(X,Y) \in \mathbb{F}_q[X,Y]$, we have $a^2 \in \mathbb{F}_q$.

Next, assume that $\sigma(H(X,Y)) = \epsilon H(Y,X)$. Then

$$H(X,Y)H(Y,X) = \sigma(H(X,Y)H(Y,X)) = \sigma(H(X,Y))\sigma(H(Y,X)) = \epsilon^2 H(X,Y)H(Y,X).$$

Hence $\epsilon = \pm 1$. Therefore $\sigma^2(H(X,Y)) = H(X,Y)$, whence $H(X,Y) \in \mathbb{F}_{q^2}[X,Y]$. The remaining claims are obvious. □

The following corollary is a direct result of Propositions 1.7 and 1.8 and will be used repeatedly in some of our main theorems.

**Corollary 1.9.** *Let $F(X,Y) \in \mathbb{F}_q[X,Y]$ be symmetric such that $F(X,Y) = G(X+Y, XY)$, where $G$ is absolutely irreducible. Suppose* $\operatorname{char} \mathbb{F}_q = 2$ *or $F(X,Y) \neq \epsilon(X-Y)^2$ for all $\epsilon \in \overline{\mathbb{F}_q}^*$. If $F(X,Y)$ does not have an absolutely irreducible factor in $\mathbb{F}_q[X,Y]$, then $F(X,Y) = H(X,Y)H(Y,X)$, where $H(X,Y) \in \mathbb{F}_{q^2}[X,Y]$ is absolutely irreducible and $\sigma(H(X,Y)) = \pm H(Y,X)$.*

*Proof.* Since $F(X,Y)$ is not absolutely irreducible, then by taking $\mathbb{F} = \overline{\mathbb{F}_q}$ in Proposition 1.7, we have $F(X,Y) = H(X,Y)H(Y,X)$, where $H(X,Y) \in \overline{\mathbb{F}_q}[X,Y]$ is irreducible, and $\gcd(H(X,Y), H(Y,X)) = 1$. If $H(X,Y) = aH_1(X,Y)$, for some $a \in \overline{\mathbb{F}_q}, H_1(X,Y) \in \mathbb{F}_q[X,Y]$, then $H_1(X,Y)$ is an absolutely irreducible factor of $F(X,Y) \in \mathbb{F}_q[X,Y]$, which is a contradiction. Therefore, the conclusion follows from Proposition 1.8. □

**Lemma 1.10.** *Let $f(X) \in \mathbb{F}_q(X)$ and $F(X,Y) = G(X+Y, XY)$ be the numerator of $\big((f(X) - f(Y)\big)/(X-Y)$. Suppose for all $(x,y) \in \mathbb{F}_q^2$ such that $G(x,y) = 0$, one of the following conditions is satisfied.*

*(i)* $\operatorname{char} \mathbb{F}_q$ *is odd and $x^2 - 4y$ is either 0 or non-square element in $\mathbb{F}_q$.*

*(ii)* $\operatorname{char} \mathbb{F}_q = 2$ *and either $\operatorname{Tr}_{q/2}(y/x^2) = 1$ or $x = 0$.*

*Then $f$ is a PR of $\mathbb{P}^1(\mathbb{F}_q)$.*

*Proof.* Suppose to the contrary that there exists $(u, v) \in \mathbb{F}_q^2, u \neq v$ such that $F(u, v) = G(u+v, uv) = 0$. Let $x = u + v, y = uv$. Then $u, v$ are precisely the roots of $X^2 - xX + y \in \mathbb{F}_q[X]$. If char $\mathbb{F}_q$ is odd, then $x^2 - 4y$ is a nonzero square in $\mathbb{F}_q$. If char $\mathbb{F}_q = 2$, then $x \neq 0$ and $\mathrm{Tr}_{q/2}(y/x^2) = 0$. □

**Lemma 1.11.** *Let $F(X_1, \ldots, X_n) = F_k + F_{k+1} + \ldots + F_l \in \mathbb{F}_q[X_1, \ldots, X_n]$, where each $F_i \in \mathbb{F}_q[X_1, \ldots, X_n]$ is homogeneous of degree $i$ and $F_k F_l \neq 0$. If there exists absolutely irreducible $h \in \mathbb{F}_q[X_1, \ldots, X_n]$ such that either $h \mid F_k$, $h^2 \nmid F_k$, or $h \mid F_l$, $h^2 \nmid F_l$, ($h$ has to be homogeneous), then $F$ has an absolutely irreducible factor in $\mathbb{F}_q[X_1, \ldots, X_n]$.*

*Proof.* Let $h \in \mathbb{F}_q[X_1, \ldots, X_n]$ be absolutely irreducible such that $h \mid F_k$, $h^2 \nmid F_k$. Let $g = g_i + g_{i+1} + \ldots \in \overline{\mathbb{F}_q}[X_1, \ldots, X_n]$ be an irreducible factor of $F$, where each $g_j$ is homogeneous of degree $j$, $h \mid g_i$ and at least one of the coefficients of $g_i$ is 1.

We claim that $g \in \mathbb{F}_q[X_1, \ldots, X_n]$. Otherwise, there exists $\tau \in \mathrm{Aut}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ such that $\tau(g) \neq g$. Since $F \in \mathbb{F}_q[X_1, \ldots, X_n]$, then $\tau(F) = F$, whence $\tau(g) \mid F$. Since a coefficient of $g_i$ is 1, $\gcd(\tau(g), g) = 1$, whence $g\tau(g) \mid F$. Since $h \in \mathbb{F}_q[X_1, \ldots, X_n]$, then $\tau(h) = h$, whence $h \mid \tau(g_i)$. Now $g\tau(g) = g_i\tau(g_i) + (\text{terms of higher degree})$. Therefore, $h^2 \mid g_i\tau(g_i) \mid F_k$, which is a contradiction.

The proof for the case when $h \mid F_l$, $h^2 \nmid F_l$ is identical. □

## CHAPTER 2:

## CASE I, QUADRATIC DENOMINATOR

Assume that

$$f(X) = X^3 + aX^2 + bX + \frac{cX + d}{Q(X)},$$

where $a, b, c, d \in \mathbb{F}_q, (c, d) \neq (0, 0)$ and $Q(X)$ is a monic irreducible quadratic over $\mathbb{F}_q$.

If $q$ is odd, then by a suitable substitution $X \mapsto X + u, u \in \mathbb{F}_q$, up to equivalence, we may assume that

$$f(X) = X^3 + aX^2 + bX + \frac{cX + d}{X^2 - r},$$

where $a, b, c, d \in \mathbb{F}_q, (c, d) \neq (0, 0)$ and $r$ is a non-square element in $\mathbb{F}_q$.

If $q$ is even, then $Q(X) = X^2 + u_1X + u_0 \in \mathbb{F}_q[X]$ is irreducible over $\mathbb{F}_q$ if and only if $u_1 \neq 0$ and $\mathrm{Tr}_{q/2}(u_0/u_1^2) = 1$, where $\mathrm{Tr}_{q/2}$ is the trace map from $\mathbb{F}_q$ to $\mathbb{F}_2$. By a suitable substitution $X \mapsto uX, u \in \mathbb{F}_q^*$, then up to equivalence, we may assume that

$$f(X) = X^3 + aX^2 + bX + \frac{cX + d}{X^2 + X + t},$$

where $a, b, c, d, t \in \mathbb{F}_q$, and $\mathrm{Tr}_{q/2}(t) = 1$.

## 2.1 Case I, $q$ Odd

Assume that $q$ is odd and

$$f(X) = X^3 + aX^2 + bX + \frac{cX + d}{X^2 - r},$$

where $a, b, c, d \in \mathbb{F}_q, (c, d) \neq (0, 0)$ and $r$ is a non-square element in $\mathbb{F}_q$.

We illustrate the method of computing and simplifying the power sum $S(f, 1)$ to the form given in (1.3). Let $X^2 - r = (X - r_1)(X - r_2)$, where $r_1, r_2 \in \mathbb{F}_{q^2}$. We have

$$\begin{aligned} S(f,1) &= \sum_{x \in \mathbb{F}_q} \left( (x^3 + ax^2 + bx + \frac{cx + d}{(x - r_1)(x - r_2)} \right) \qquad (2.1) \\ &= \sum_{x \in \mathbb{F}_q} \left( \frac{d + cr_1}{(r_1 - r_2)(x - r_1)} + \frac{-d - cr_2}{(r_1 - r_2)(x - r_2)} \right) \quad \text{(Permutation Criterion)} \\ &= \left( \frac{d + cr_1}{(r_1 - r_2)(r_2 - r_1)} + \frac{-d - cr_2}{(r_1 - r_2)(r_1 - r_2)} \right) \quad \text{(Carlitz's Formula)} \\ &= \frac{-2d - cr_1 - cr_2}{(r_1 - r_2)^2} = \frac{-2d}{(r_1 - r_2)^2}, \end{aligned}$$

whenever $q \geq m + 2 = 5$, where $m$ is the degree of the polynomial part inside the summation in (2.1).

Suppose $f$ is a PR of $\mathbb{P}^1(\mathbb{F}_q)$. From the above result, we have $s(f, 1) = -2d$. Note that the condition $q \geq \max\{k, m\} + 2$ is needed in order for the power sum conditions given in (1.4) to hold. So if $q \geq 5$, we have

$$d = 0.$$

Setting $d = 0$ in $s(f, k)$ for $k = 2, 3, 4, 6$, we obtain the following power sum conditions. See Appendix A.1 for the formulas for $s(f, k)$. If $q \geq 8$, then

$$-2cr(c + 8br + 8r^2) = 0. \qquad (2.2)$$

If $q \geq 11$, then

$$-24acr^3(5c + 8br + 8r^2) = 0. \tag{2.3}$$

If $q \geq 14$ then

$$\begin{aligned} &2cr^2(3c^3 - 32bc^2r - 480b^2cr^2 - 352c^2r^2 - 256b^3r^3 - 864a^2cr^3 - 1728bcr^3 - 768a^2br^4 \\ &\quad - 768b^2r^4 - 1248cr^4 - 768a^2r^5 - 768br^5 - 256r^6) = 0. \end{aligned} \tag{2.4}$$

If $q \geq 20$, then

$$\begin{aligned} &-4cr^3(5c^5 - 72bc^4r + 600b^2c^3r^2 + 168c^4r^2 + 14080b^3c^2r^3 + 11160a^2c^3r^3 + 22320bc^3r^3 \\ &\quad + 17280b^4cr^4 + 111360a^2bc^2r^4 + 111360b^2c^2r^4 + 39000c^3r^4 + 3072b^5r^5 + 149760a^2b^2cr^5 \\ &\quad + 99840b^3cr^5 + 211200a^2c^2r^5 + 211200bc^2r^5 + 30720a^2b^3r^6 + 15360b^4r^6 + 32640a^4cr^6 \\ &\quad + 391680a^2bcr^6 + 195840b^2cr^6 + 113920c^2r^6 + 15360a^4br^7 + 92160a^2b^2r^7 + 30720b^3r^7 \\ &\quad + 241920a^2cr^7 + 161280bcr^7 + 15360a^4r^8 + 92160a^2br^8 + 30720b^2r^8 + 48000cr^8 \\ &\quad + 30720a^2r^9 + 15360br^9 + 3072r^{10}) = 0. \end{aligned} \tag{2.5}$$

Since $d = 0$, we have $c \neq 0$, otherwise $f(X)$ is not a degree 5 rational function. Hence by (2.2), $c = -8r(b + r)$. Substituting this into (2.3), (2.4), (2.5), we get

$$(2^{11})(3)(ar^5)(b + r)^2 = 0, \tag{2.6}$$

$$(2^{15})(r^7)(b + r)^2(-3a^2 + 7b + 7r) = 0, \tag{2.7}$$

$$(2^{19})(3)(5)(r^{10})(b+r)^2(-a^2b^2+23b^3+a^4r-25a^2br+97b^2r-24a^2r^2+125br^2+51r^3) = 0. \tag{2.8}$$

Since $c \neq 0$, then $b + r \neq 0$. Hence by (2.7),

$$-3a^2 + 7b + 7r = 0. \tag{2.9}$$

If char $\mathbb{F}_q = 3$, then (2.9) implies $b + r = 0$, which is a contradiction. Therefore char $\mathbb{F}_q \neq 3$, whence $a = 0$ by (2.6). By (2.9), $7(b + r) = 0$. Thus char $\mathbb{F}_q = 7$. Hence by (2.8), we have

$$-a^2b^2 + 23b^3 + a^4r - 25a^2br + 97b^2r - 24a^2r^2 + 125br^2 + 51r^3 = 0. \tag{2.10}$$

Setting $a = 0$ in (2.10) and reducing modulo 7 gives $2(b + r)^3 = 0$, which is a contradiction. We have the following result.

**Theorem 2.1.** *Let $q$ be odd and*

$$f(X) = X^3 + aX^2 + bX + \frac{cX + d}{X^2 - r}, \tag{2.11}$$

*where $a, b, c, d \in \mathbb{F}_q, (c, d) \neq (0, 0)$ and $r$ is a non-square element in $\mathbb{F}_q$. Then $f(X)$ is not a PR of $\mathbb{P}^1(\mathbb{F}_q)$ when $q \geq 23$.*

Using *Mathematica* to search for PRs when $q < 23$, we determined all rational functions of the form given in (2.11) that permute $\mathbb{P}^1(\mathbb{F}_q)$. The complete list is given in Appendix B.1.

### 2.2 Case I, $q$ Even

Assume that $q$ is even and

$$f(X) = X^3 + aX^2 + bX + \frac{cX + d}{X^2 + X + t},$$

where $a, b, c, d, t \in \mathbb{F}_q$, and $\mathrm{Tr}_{q/2}(t) = 1$.

Suppose $f$ is a PR of $\mathbb{P}^1(\mathbb{F}_q)$. Since $s(f, 1) = c$, then if $q \geq 5$, we have

$$c = 0.$$

Setting $c = 0$ in $s(f, k)$ for $k = 3, 5, 9$, we obtain the following conditions. If $q \geq 11$, then

$$d(1 + a^2 + b^2 + ad + bd + dt + t^2) = 0. \tag{2.12}$$

If $q \geq 17$, then

$$d(1 + a + b + t)(1 + a + b + d + t)(1 + a^2 + b^2 + d + ad + bd + d^2 + dt + t^2) = 0. \tag{2.13}$$

If $q \geq 29$, then

$$\begin{aligned} d(1 + a + b + t)(1 + a + b + d + t)(1 + a + a^2 + a^3 + b + a^2b + b^2 + ab^2 + b^3 + d^2 + ad^2 + bd^2 \\ + d^3 + t + a^2t + b^2t + d^2t + t^2 + at^2 + bt^2 + t^3)(1 + a + a^2 + a^3 + b + a^2b + b^2 + ab^2 + b^3 \\ + d + a^2d + b^2d + d^3 + t + a^2t + b^2t + t^2 + at^2 + bt^2 + dt^2 + t^3) = 0. \end{aligned} \tag{2.14}$$

Since $c = 0$, we have $d \neq 0$. By (2.12), we have

$$1 + a^2 + b^2 + ad + bd + dt + t^2 = 0. \tag{2.15}$$

If $t = 1 + a + b$ or $1 + a + b + d$, then by (2.15), $d = 0$, which is a contradiction. Therefore by (2.13) and (2.14), $L_1 = L_2 = 0$, where

$$\begin{aligned} L_1 &= 1 + a^2 + b^2 + d + ad + bd + d^2 + dt + t^2, \\ L_2 &= (1 + a + a^2 + a^3 + b + a^2b + b^2 + ab^2 + b^3 + d^2 + ad^2 + bd^2 + d^3 + t + a^2t + b^2t + d^2t \\ &\quad + t^2 + at^2 + bt^2 + t^3)(1 + a + a^2 + a^3 + b + a^2b + b^2 + ab^2 + b^3 + d + a^2d + b^2d + d^3 \\ &\quad + t + a^2t + b^2t + t^2 + at^2 + bt^2 + dt^2 + t^3). \end{aligned}$$

Let $\mathrm{Res}(L_1, L_2; t)$ denote the *resultant of* $L_1$ *and* $L_2$ *with respect to* $t$. We have $\mathrm{Res}(L_1, L_2; t) = d^{12}$, hence $d = 0$, which is a contradiction. We have the following result.

**Theorem 2.2.** *Let $q$ be even and*

$$f(X) = X^3 + aX^2 + bX + \frac{cX + d}{X^2 + X + t}, \tag{2.16}$$

*where $a, b, c, d, t \in \mathbb{F}_q, (c, d) \neq (0, 0)$ and $\mathrm{Tr}_{q/2}(t) = 1$. Then $f(X)$ is not a PR of $\mathbb{P}^1(\mathbb{F}_q)$ when $q \geq 2^5$.*

Using *Mathematica* to search for PRs when $q < 2^5$, we determined all rational functions of the form given in (2.16) that permute $\mathbb{P}^1(\mathbb{F}_q)$. The complete list is given in Appendix B.2.

# CHAPTER 3:

# CASE II, CUBIC DENOMINATOR

Assume that

$$f(X) = X^2 + aX + \frac{bX^2 + cX + d}{Q(X)}, \tag{3.1}$$

where $a, b, c, d \in \mathbb{F}_q$, $b, c, d \neq (0, 0, 0)$, and $Q(X)$ is a monic irreducible cubic over $\mathbb{F}_q$.

**Theorem 3.1.** *Let $f(X)$ be given in* (3.1). *Then $f(X)$ is not a PR of $\mathbb{P}^1(\mathbb{F}_q)$ when $q \geq 919$.*

In fact Theorem 3.1 is a special case of the following result with $n = 5$.

**Theorem 3.2.** *Let $f(X) = P(X)/Q(X) \in \mathbb{F}_q(X)$, where $P, Q \in \mathbb{F}_q[X]$, $\gcd(P, Q) = 1$, $\deg P = n = \deg Q + 2$, and $q > (2n-4)(2n-5)q^{1/2} + 2n - 1$. Assume that $f(X)$ is not of the form $g(X)^p$ ($p$ has to be 2), where $p = \operatorname{char} \mathbb{F}_q$ and $g(X) \in \mathbb{F}_q(X)$. Then $f(X)$ is not a PR of $\mathbb{P}^1(\mathbb{F}_q)$.*

*Proof.* Up to equivalence, we may assume that $Q(X) = X^{n-2} + \cdots$ and

$$f(X) = X^2 + aX + \frac{P_1(X)}{Q(X)},$$

where $a \in \mathbb{F}_q^*$, $b \in \mathbb{F}_q$, $P_1 \in \mathbb{F}_q[X]$, $\deg P_1 < n - 2$. Then

$$\begin{aligned} \frac{f(X) - f(Y)}{X - Y} &= (X + Y) + a + \frac{1}{Q(X)Q(Y)} \frac{P_1(X)Q(Y) - P_1(Y)Q(X)}{X - Y} \\ &= \frac{F(X, Y)}{Q(X)Q(Y)}, \end{aligned}$$

where $F(X,Y) \in \mathbb{F}_q[X,Y]$ and

$$F(X,Y) = X^{n-2}Y^{n-2}(X+Y) + \text{terms of lower degree.}$$

By Lemma 1.11, $F(X,Y)$ has an absolutely irreducible factor $h \in \mathbb{F}_q[X,Y]$. By the Hasse-Weil bound,

$$|V_{\mathbb{F}_q^2}(F)| \geq |V_{\mathbb{F}_q^2}(h)| \geq q + 1 - (2n-4)(2n-5)q^{1/2} - 3 = q - (2n-4)(2n-5)q^{1/2} - 2,$$

where 3 is the number of zeros of $F(X,Y)$ at infinity.

Let $f'$ denote the formal derivative of $f$. If $f'(X) = 0$, then $Q(X)P'(X) - P(X)Q'(X) = 0$. We have $\gcd(P,Q) = 1$, so $P \mid P', Q \mid Q'$, hence $P' = Q' = 0$. Therefore $P = (P_1)^p, Q = (Q_1)^p$ where $P_1, Q_1 \in \mathbb{F}_q[X]$, which is a contradiction since $f(X)$ is not of the form $g(X)^p, g \in \mathbb{F}_q(X)$. Thus, $f'(X) \neq 0$.

We claim that $F(X,X) \neq 0$. In fact, we have

$$(f(Y) - f(X))Q(X)Q(Y) = (Y - X)F(X,Y).$$

Applying $\partial/\partial Y$ to the above equation gives

$$Q(X)\big[f'(Y)Q(Y) + (f(X) - f(Y))Q'(Y)\big] = F(X,Y) + (Y-X)\frac{\partial F(X,Y)}{\partial Y}.$$

Setting $Y = X$ gives

$$Q(X)^2 f'(X) = F(X,X),$$

hence the claim. Therefore, $|V_{\mathbb{F}_q}(F(X,X))| \leq \deg F(X,X) \leq 2n-3$. Since $q \geq$, we have

$$|V_{\mathbb{F}_q^2}(F)| \geq q - (2n-4)(2n-5)q^{1/2} - 2 > 2n - 3 \geq |V_{\mathbb{F}_q}(F(X,X))|.$$

Hence there exists $(x, y) \in \mathbb{F}_q^2$ with $x \neq y$ such that $F(x, y) = 0$, whence $f(X)$ is not a PR of $\mathbb{P}^1(\mathbb{F}_q)$. □

Theorem 3.2 can be generalized as follows.

**Theorem 3.3.** *Let $f(X) = P(X)/Q(X) \in \mathbb{F}_q(X)$, where $P, Q \in \mathbb{F}_q[X]$, $\gcd(P, Q) = 1$, $Q(X)$ has no roots in $\mathbb{F}_q$, $\deg P = m$, $\deg Q = n$, $m \neq n$. Assume that $f(X)$ is not of the form $g(X)^p$, where $p = \operatorname{char} \mathbb{F}_q$ and $g(X) \in \mathbb{F}_q(X)$. Let $d = |m - n|$ and assume that* (i) *$d = 2$, or* (ii) *$p \nmid d$ and $\gcd(d, q-1) > 1$. Then $f(X)$ is not a PR of $\mathbb{F}_q$ when $q$ is sufficiently large.*

*Proof.* Let $u = \min\{m, n\}$. Then

$$\frac{f(X) - f(Y)}{X - Y} = \frac{F(X, Y)}{Q(X)Q(Y)},$$

where $F(X, Y) \in \mathbb{F}_q[X, Y]$ and

$$F(X, Y) = aX^u Y^u \frac{X^d - Y^d}{X - Y} + \text{terms of lower degree}, \quad a \in \mathbb{F}_q^*.$$

Under condition (i) or (ii), $(X^d - Y^d)/(X - Y)$ has a linear factor of multiplicity 1 in $\mathbb{F}_q[X, Y]$. By Lemma 1.11, $F(X, Y)$ has an absolutely irreducible factor in $\mathbb{F}_q[X, Y]$. Since $f(X)$ is not of the form $g(X)^p$, $f'(X) \neq 0$. It follows that $F(X, X) \neq 0$. Thus by the Hasse-Weil bound, when $q$ is sufficiently large, $F(X, Y)$ has a root $(x, y) \in \mathbb{F}_q^2$ with $x \neq y$. Therefore $f(X)$ is a not a PR of $\mathbb{F}_q$. □

If $G$ (defined in Theorem 3.4) is absolutely irreducible and $f$ is a PR of $\mathbb{F}_q$, then the degrees of the numerator and the denominator of $f$ are subject to rather stringent restrictions.

**Theorem 3.4.** *Let $f(X) = P(X)/Q(X) \in \mathbb{F}_q(X)$, where $P, Q \in \mathbb{F}_q[X]$, $\gcd(P, Q) = 1$, $Q(X)$ has no roots in $\mathbb{F}_q$, $\deg P = m$, $\deg Q = n$, $m \neq n$. Assume that $f(X)$ is not of the form $g(X)^p$, where $p = \operatorname{char} \mathbb{F}_q$ and $g(X) \in \mathbb{F}_q(X)$. Let $F(X, Y)$ be the numerator of*

$(f(X)-f(Y))/(X-Y)$ *and write* $F(X,Y)=G(X+Y,XY)$*, where* $G\in\mathbb{F}_q[X,Y]$*. Assume that* $G$ *is absolutely irreducible. Let* $d=|m-n|$*,* $u=\min\{m,n\}$*. Write* $d=p^el$*, where* $e\in\mathbb{N}$*,* $l\in\mathbb{Z}^+$*,* $p\nmid l$*. If* $f$ *is an exceptional PR of* $\mathbb{F}_q$ *(i.e.,* $f$ *is a PR of* $\mathbb{F}_{q^k}$ *for infinitely many* $k\in\mathbb{Z}^+$*), then the following conditions are satisfied.*

*(i)* $u$ *is even.*

*(ii)* $d$ *is odd, i.e., both* $p^e$ *and* $l$ *are odd.*

*(iii) If* $l>1$*, then the order of* $q$ *in* $\mathbb{Z}_l^\times$ *is* $2s$*, where* $s$ *is odd. Moreover,* $\gcd(l,q^s-1)=1$*, equivalently,* $\gcd(l,q^{s_1}-1)=1$ *for all positive odd integers* $s_1$*.*

*Proof.* We have

$$F(X,Y)=F_0(X,Y)+\text{terms of lower degree},$$

where

$$F_0(X,Y)=\alpha X^uY^u\frac{X^d-Y^d}{X-Y},\quad \alpha\in\mathbb{F}_q^*.$$

Let $\zeta\in\overline{\mathbb{F}}_q$ be a primitive $l$-th root of unity. Then

$$\begin{aligned}F_0(X,Y)&=\alpha X^uY^u\frac{(X^l-Y^l)^{p^e}}{X-Y}=\alpha X^uY^u\frac{(\prod_{i=0}^{l-1}(X-\zeta^iY))^{p^e}}{X-Y}\\&=\alpha X^uY^u(X-Y)^{p^e-1}\prod_{i=1}^{l-1}(X-\zeta^iY)^{p^e}.\end{aligned}$$

We claim that $F(X,Y)$ does not have an absolutely irreducible factor in $\mathbb{F}_q[X,Y]$. Otherwise, by the Hasse-Weil bound, $f(X)$ is not a PR of $\mathbb{F}_{q^r}$, for all $r\geq r'$, where $r'$ is sufficiently large. This contradicts the assumption that $f(X)$ is an exceptional PR of $\mathbb{F}_q$. Hence the claim is proved. By Propositions 1.7 and 1.8, we have

$$F(X,Y)=H(X,Y)H(Y,X),$$

where $H(X,Y) \in \mathbb{F}_{q^2}[X,Y]$ is absolutely irreducible, $\gcd(H(X,Y),H(Y,X)) = 1$, and $\sigma(H(X,Y)) = (-1)^t H(Y,X)$, where $t \in \{0,1\}$. Let $h(X,Y)$ be the homogeneous part of $H(X,Y)$ of the highest degree and write

$$h(X,Y) = \epsilon X^a Y^b (X-Y)^c \prod_{i=1}^{l-1} (X-\zeta^i Y)^{d_i}, \quad \epsilon \in \mathbb{F}_{q^2}^*.$$

Then

$$\begin{aligned} h(Y,X) &= \epsilon Y^a X^b (Y-X)^c \prod_{i=1}^{l-1} (Y-\zeta^i X)^{d_i} \\ &= \epsilon (-1)^c X^b Y^a (X-Y)^c \prod_{i=1}^{l-1} (-\zeta^i (X-\zeta^{-i} Y))^{d_i} \\ &= \epsilon (-1)^{c+\sum_{i=1}^{l-1} d_i} \zeta^{\sum_{i=1}^{l-1} i d_i} X^b Y^a (X-Y)^c \prod_{i=1}^{l-1} (X-\zeta^i X))^{d_{l-i}}. \end{aligned}$$

We also have

$$\begin{aligned} h(Y,X) &= (-1)^t \sigma(h(X,Y)) = \epsilon^q (-1)^t X^a Y^b (X-Y)^c \prod_{i=1}^{l-1} (X-\zeta^{qi} Y)^{d_i} \\ &= \epsilon^q (-1)^t X^a Y^b (X-Y)^c \prod_{i=1}^{l-1} (X-\zeta^i Y)^{d_{q'i}}, \end{aligned}$$

where $q' \in \mathbb{Z}_l^\times$ is such that $q'q \equiv 1 \pmod{l}$ and the subscript of $d_{q'i}$ is taken in $\mathbb{Z}_l$.

From the above we have

$$h(X,Y)h(Y,X) = \epsilon^2 (-1)^{c+\sum_{i=1}^{l-1} d_i} \zeta^{\sum_{i=1}^{l-1} i d_i} X^{a+b} Y^{a+b} (X-Y)^{2c} \prod_{i=1}^{l-1} (X-\zeta^i X))^{d_i + d_{l-i}}$$

and

$$h(X,Y)h(Y,X) = \epsilon^{q+1} (-1)^t X^{2a} Y^{2b} (X-Y)^{2c} \prod_{i=1}^{l-1} (X-\zeta^i Y)^{d_i + d_{q'i}}.$$

Since $F_0(X,Y) = h(X,Y)h(Y,X)$, we have

$$\epsilon^2(-1)^{c+\sum_{i=1}^{l-1} d_i}\zeta^{\sum_{i=1}^{l-1} id_i} = \alpha, \tag{3.2}$$

$$a + b = u, \tag{3.3}$$

$$2c = p^e - 1 \tag{3.4}$$

$$d_i + d_{l-i} = p^e, \quad 1 \le i \le l-1, \tag{3.5}$$

and

$$\epsilon^{q+1}(-1)^t = \alpha, \tag{3.6}$$

$$2a = 2b = u, \tag{3.7}$$

$$2c = p^e - 1 \tag{3.8}$$

$$d_i + d_{q'i} = p^e, \quad 1 \le i \le l-1. \tag{3.9}$$

It follows immediately that $u$ is even and $p^e$ is odd. If $l$ is even, then by (3.5), $d_{l/2}+d_{l/2} = p^e$, which is a contradiction. So $l$ is odd.

Assume $l > 1$. Let $\tau$ be the order of $q$ in $\mathbb{Z}_l^\times$. If $\tau$ is odd, the by (3.9), $d_{q'^\tau 1} = p^e - d_1$, i.e., $2d_1 = p^e$, which is a impossible. If $\tau = 4s$, then $q'^{2s} \equiv -1 \pmod{l}$. It follows from (3.9) that $d_{l-1} = d_{q'^{2s}1} = d_1$. Then by (3.5), $p^e = d_1 + d_{l-1} = 2d_1$, which is impossible. Therefore $\tau = 2s$, where $s$ is odd. If $\gcd(l, q^s - 1) = v > 1$, let $s_1$ be the order of $q$ in $\mathbb{Z}_v^\times$. Then $s_1 \mid s$, whence $s_1$ is odd. By (3.9), $d_{q'^{s_1}l/v} = p^e - d_{l/v}$. On the other hand, $d_{q'^{s_1}l/v} = d_{l/v}$ (since $q'^{s_1} \equiv 1 \pmod{v}$). Thus $2d_{l/v} = p^e$, which is impossible. Hence $\gcd(l, q^s - 1) = 1$. □

**Remark.** If conditions (i) – (iii) are satisfied, there exist $\epsilon, t, a, b, c$, and $d_i$ $(1 \le i \le l-1)$ satisfying (3.2) – (3.9). First, since $u$ is even and $p^e$ is odd, we can choose $a = b = u/2$ and $c = (p^e - 1)/2$.

If $l = 1$, (3.5) and (3.9) are vacuously satisfied. Assume that $l$ is odd and greater than 1. Let $\langle q \rangle < \mathbb{Z}_l^\times$ act on $\mathbb{Z}_l \setminus \{0\}$ by multiplication. (Recall that $|\langle q \rangle| = 2s$, where $s$ is odd.) We

claim that every orbit of this action has even length. Let $i \in \mathbb{Z}_l \setminus \{0\}$ and let $w$ be the length of the $\langle q \rangle$-orbit of $i$. Let $l' = \gcd(i, l)$. Then $(l/l') \mid q^w - 1$. Assume to the contrary that $w$ is odd. Then $w \mid s$, whence $(l/l') \mid q^s - 1$, which is a contradiction to (iii). So the claim is proved. For each $\langle q \rangle$-orbit $\{i, q'i, \ldots, q'^{2k-1}i\}$ ($k$ odd), choose $d_i = d_{q'^2 i} = \cdots = d_{q'^{2(k-1)}i}$ and $d_{q'i} = d_{q'^3 i} = \cdots = d_{q'^{2k-1}i} = p^e - d_i$. Then (3.9) is satisfied. We have $q'^k i \equiv -i \pmod{l}$, so $d_{l-i} = d_{q'^k i}$. Since $k$ is odd, we have $d_{q'^k i} = p^e - d_i$. Thus (3.5) is satisfied.

In (3.2),

$$\left(\zeta^{\sum_{i=1}^{l-1} i d_i}\right)^{q+1} = \zeta^{\sum_{i=1}^{l-1} q i d_i + \sum_{i=1}^{l-1} i d_i} = \zeta^{\sum_{i=1}^{l-1} i d_{q'i} + \sum_{i=1}^{l-1} i d_i}$$
$$= \zeta^{\sum_{i=1}^{l-1} i(d_{q'i} + d_i)} = \zeta^{p^e \sum_{i=1}^{l-1} i} = \zeta^{p^e l(l-1)/2} = 1.$$

Let $\gamma$ be a primitive element of $\mathbb{F}_{q^2}$ and write $\alpha = \gamma^{x(q+1)}$, $(-1)^{c+\sum_{i=1}^{l-1} d_i} \zeta^{\sum_{i=1}^{l-1} i d_i} = \gamma^{y(q-1)}$ and $\epsilon = \gamma^z$, where $x, y, z \in \mathbb{Z}$. Then (3.2) becomes

$$2z \equiv x(q+1) - y(q-1) \pmod{q^2 - 1} \tag{3.10}$$

and (3.6) becomes

$$(q+1)z \equiv x(q+1) + \frac{1}{2}(q^2 - 1)t \pmod{q^2 - 1},$$

i.e.,

$$z \equiv x + \frac{1}{2}(q-1)t \pmod{q-1}. \tag{3.11}$$

Choose $z = x + \frac{1}{2}(q-1)t$. Then (3.10) becomes

$$2x + t(q-1) \equiv x(q+1) - y(q-1) \pmod{q^2 - 1},$$

i.e.,

$$(q-1)(-x + t + y) \equiv 0 \pmod{q^2 - 1}.$$

We choose $t = x - y$.

# CHAPTER 4:

# CASE III, QUADRATIC SQUARE DENOMINATOR

Assume that

$$f(X) = X + \frac{aX^3 + bX^2 + cX + d}{Q(X)^2},$$

where $a, b, c, d \in \mathbb{F}_q, (a, b, c, d) \neq (0, 0, 0, 0)$ and $Q(X)$ is a monic irreducible quadratic over $\mathbb{F}_q$. If $q$ is odd, we may assume $Q(X) = X^2 - r$, where $r$ is a non-square element in $\mathbb{F}_q$. If $q$ is even, we may assume $Q(X) = X^2 + X + t$, where $t \in \mathbb{F}_q$ and $\mathrm{Tr}_{q/2}(t) = 1$.

## 4.1 Case III, $q$ Odd

Assume that $q$ is odd and

$$f(X) = X + \frac{aX^3 + bX^2 + cX + d}{(X^2 - r)^2},$$

where $a, b, c, d \in \mathbb{F}_q, (a, b, c, d) \neq (0, 0, 0, 0)$, $r$ is a non-square element in $\mathbb{F}_q$, and $X^2 - r$ does not divide $aX^3 + bX^2 + cX + d$.

In this section, we will use the power sum conditions $s(f, k) = 0$ with $k = 1, 2, \ldots, 5$. See Appendix A.3 for the formulas for $s(f, k)$. Assume that $f$ is a PR of $\mathbb{P}^1(\mathbb{F}_q)$. First, since $s(f, 1) = 3d - br$, we have

$$b = 3d/r. \tag{4.1}$$

Setting $b = 3d/r$ in $s(f, k)$ for $k = 2, \ldots, 5$, we get the following conditions. If $q \geq 4$, then

$$32d^2 - 5c^2r + 6acr^2 - 5a^2r^3 - 32cr^3 - 160ar^4 = 0. \tag{4.2}$$

If $q \geq 5$,

$$3d(2d^2 - acr^2 + a^2r^3 + 4cr^3 - 12ar^4 - 128r^5) = 0. \tag{4.3}$$

If $q \geq 6$, then

$$\begin{aligned} 4608d^4 - 1440c^2d^2r + 99c^4r^2 + 1728acd^2r^2 - 180ac^3r^3 - 1440a^2d^2r^3 - 9216cd^2r^3 + 210a^2c^2r^4 \\ + 896c^3r^4 + 15360ad^2r^4 - 180a^3cr^5 - 1920ac^2r^5 - 49152d^2r^5 + 99a^4r^6 + 2688a^2cr^6 \\ + 4608c^2r^6 - 2688a^3r^7 - 15360acr^7 - 142848a^2r^8 - 81920cr^8 - 147456ar^9 = 0. \end{aligned} \tag{4.4}$$

If $q \geq 7$, then

$$\begin{aligned} 5d(160d^4 - 22c^2d^2r - 60acd^2r^2 + 11ac^3r^3 + 58a^2d^2r^3 + 192cd^2r^3 - 21a^2c^2r^4 - 36c^3r^4 \\ - 576ad^2r^4 + 21a^3cr^5 + 180ac^2r^5 + 1536d^2r^5 - 11a^4r^6 - 300a^2cr^6 - 384c^2r^6 + 252a^3r^7 \\ + 1536acr^7 - 2688a^2r^8 - 3072cr^8 - 72704ar^9 - 32768r^{10}) = 0. \end{aligned} \tag{4.5}$$

Let $p = \text{char } \mathbb{F}_q$. From (4.3), $d(2d^2 - acr^2 + a^2r^3 + 4cr^3 - 12ar^4 - 128r^5) = 0$ provided that $p \neq 3$. In the proof of the next theorem we consider $p = 3$ and $p \neq 3$ as separate cases.

**Theorem 4.1.** *Let $q$ be odd and*

$$f(X) = X + \frac{aX^3 + bX^2 + cX + d}{(X^2 - r)^2}, \tag{4.6}$$

*where $a, b, c, d \in \mathbb{F}_q$, $(a, b, c, d) \neq (0, 0, 0, 0)$, $r$ is a non-square element in $\mathbb{F}_q$, and $X^2 - r$ does not divide $aX^3 + bX^2 + cX + d$. If $q \geq 457$, then $f$ is a PR of $\mathbb{P}^1(\mathbb{F}_q)$ if and only if $b = 3d/r, c = 3ar - 32r^2$ and $d^2 = a^2r^3 - 16ar^4 + 128r^5$. The condition is sufficient for all $q$.*

*Proof.* We prove that the given conditions on $a, b, c, d$ are necessary for $f$ to be a PR of $\mathbb{P}^1(\mathbb{F}_q)$. The sufficiency of these conditions is proved in Lemma 4.4. Throughout the proof

we will make use of further additional lemmas (4.2, 4.3, 4.5) which will appear after the main body of the proof.

We have

$$\frac{f(X)-f(Y)}{X-Y}=\frac{F(X,Y)}{(X^2-r)^2(Y^2-r)^2},$$

where

$$\begin{aligned}F(X,Y)&=cr^2+r^4+2drX+br^2X+ar^2X^2-2r^3X^2-dX^3+r^2X^4+2drY+br^2Y\\&\quad+2crXY+ar^2XY-dX^2Y-cX^3Y+ar^2Y^2-2r^3Y^2-dXY^2-cX^2Y^2\\&\quad-2arX^2Y^2+4r^2X^2Y^2-bX^3Y^2-2rX^4Y^2-dY^3-cXY^3-bX^2Y^3-aX^3Y^3\\&\quad+r^2Y^4-2rX^2Y^4+X^4Y^4. \qquad (4.7)\end{aligned}$$

Moreover, $F(X,Y)=G(X+Y,XY)$, where

$$\begin{aligned}G(X,Y)&=cr^2+r^4+2drX+br^2X+ar^2X^2-2r^3X^2-dX^3+r^2X^4+2crY-ar^2Y\\&\quad+4r^3Y+2dXY-cX^2Y-4r^2X^2Y+cY^2-2arY^2+6r^2Y^2-bXY^2-2rX^2Y^2\\&\quad-aY^3+4rY^3+Y^4. \qquad (4.8)\end{aligned}$$

Suppose that $f$ is a PR of $\mathbb{P}^1(\mathbb{F}_q)$ and $q\geq 457$.

We first consider the case when $\mathrm{char}\,\mathbb{F}_q=3$. Then one of the conditions (i) – (iii) in Lemma 4.2 holds. If (i) or (ii) holds, then by Lemma 4.3, $G(X,Y)$ is absolutely irreducible. By Lemma 4.5, $F(X,Y)$ has an absolutely irreducible factor in $\mathbb{F}_q[X,Y]$. Now since $F(X,X)\neq 0$, then $|V_{\mathbb{F}_q}(F(X,X))|\leq 8$. Since $F(X,Y)=X^4Y^4+$ (terms of lower degree), the number of $\mathbb{F}_q$-rational points at infinity is 2. Let $\hat{F}(X,Y,Z)$ be the homogenization of $F(X,Y)$. Then by Lemma 1.6, we have

$$\begin{aligned}|V_{\mathbb{F}_q^2}(F(X,Y))|+2=|V_{\mathbb{P}^2(\mathbb{F}_q)}(\hat{F})|&\geq q+1-2(4-1)(4-1)q^{1/2}-\frac{1}{2}(4-1)(8-1)(8-2)\\&=q-18q^{1/2}-62.\end{aligned}$$

Hence,

$$|V_{\mathbb{F}_q^2}(F(X,Y))| \geq q - 18q^{1/2} - 64 > 8 \geq |V_{\mathbb{F}_q}(F(X,X))|.$$

Thus there exists $(x,y) \in \mathbb{F}_q^2$ with $x \neq y$ such that $F(x,y) = 0$. Therefore $f(X)$ is not a PR of $\mathbb{P}^1(\mathbb{F}_q)$. Hence (iii) holds and $b, c, d$ satisfy $b = 3d/r, c = 3ar - 32r^2$, and $d^2 = a^2r^3 - 16ar^4 + 128r^5$. Note that in this case, $X^2 - r$ does not divide $aX^3 + bX^2 + cX + d$.

Throughout the remainder of the proof, we assume char $\mathbb{F}_q \neq 3$. Suppose $G$ is not absolutely irreducible. By Lemma 4.5, $F(X,Y)$ has an absolutely irreducible factor in $\mathbb{F}_q[X,Y]$. Then by the same argument as above, $f(X)$ is not a PR of $\mathbb{P}^1(\mathbb{F}_q)$.

Suppose now that $G$ is absolutely irreducible.

**Case 1.** Assume $d = 0$. Then $b = 0$. We have

$$\begin{aligned} G(X,Y) = {} & cr^2 + r^4 + ar^2X^2 - 2r^3X^2 + r^2X^4 + 2crY - ar^2Y + 4r^3Y - cX^2Y - 4r^2X^2Y \\ & + cY^2 - 2arY^2 + 6r^2Y^2 - 2rX^2Y^2 - aY^3 + 4rY^3 + Y^4. \end{aligned} \tag{4.9}$$

Let $G_1(X,Y) = G(X, Y - r)$. Then

$$G_1(X,Y) = crX^2 + ar^2X^2 + r^2X^4 - cX^2Y + cY^2 + arY^2 - 2rX^2Y^2 - aY^3 + Y^4. \tag{4.10}$$

Write $G_1(X,Y) = h_2 + h_3 + h_4$, where

$$\begin{aligned} h_2 &= (c + ar)(rX^2 + Y^2), \\ h_3 &= -Y(cX^2 + aY^2), \\ h_4 &= (rX^2 - Y^2)^2. \end{aligned}$$

If $c + ar = 0$, then $aX^3 + bX^2 + cX + d = aX(X^2 - r)$, which is a contradiction since $X^2 - r$ does not divide $aX^3 + bX^2 + cX + d$. Thus, $h_2 \neq 0$. Let $D(X,Y) = h_3^2 - 4h_2h_4$. Since $\gcd(h_2, h_3, h_4) = 1$, $G_1(X,Y)$ is not absolutely irreducible if and only if $D$ is a square in

$\overline{\mathbb{F}_q}[X,Y]$. Since $D(X,Y)$ is homogeneous, we have that $D(X,Y)$ is a square in $\overline{\mathbb{F}_q}[X,Y]$ if and only if $D(1,Y)$ is a square in $\overline{\mathbb{F}_q}[X,Y]$. We have

$$D(1,Y) = -4r^3(c+ar) + (c^2+4cr^2+4ar^3)Y^2 + 2(ac+2cr+2ar^2)Y^4 + (a^2-4c-4ar)Y^6.$$

**Case 1.1.** Assume $a^2-4c-4ar \neq 0$. Let $(a^2-4c-4ar)^{-1}D(1,Y) = (A_0+A_1Y+A_2Y^2+Y^3)^2$, where $A_0, A_1, A_2 \in \overline{\mathbb{F}_q}$. Comparing the coefficients of $Y^0, Y^3, Y^5$ in this equation, we get the following equations:

$$\begin{aligned} &-a^2A_0^2 + 4A_0^2c + 4aA_0^2r - 4cr^3 - 4ar^4 = 0,\\ &A_0 + A_1A_2 = 0,\\ &A_2 = 0. \end{aligned}$$

The last two equations imply $A_0 = 0$, and from the first equation we get $c + ar = 0$, which is a contradiction as seen earlier.

**Case 1.2.** Assume $a^2 - 4c - 4ar = 0$. Then $c = (a^2 - 4ar)/4$. Hence,

$$D(1,Y) = -a^2r^3 + \frac{1}{16}a^2(a^2 - 8ar + 32r^2)Y^2 + \frac{1}{2}a^2(a-2r)Y^4.$$

Note that we must have $a \neq 0$, otherwise $a = b = c = d = 0$, which is a contradiction.

**Case 1.2.1.** Assume $a = 2r$. Then $c = -r^2$. We have

$$D(1,Y) = -4r^5 + 5r^4Y^2.$$

Let $D(1,Y) = (A_0 + A_1Y)^2$, where $A_0, A_1 \in \overline{\mathbb{F}_q}$. Comparing the coefficients of $Y^0, Y^1, Y^2$ in this equation, we get the following equations:

$$\begin{aligned} A_0^2 + 4r^5 &= 0, \\ A_0A_1 &= 0, \\ -A_1^2 + 5r^4 &= 0. \end{aligned}$$

If $A_0 = 0$, then $4r^5 = 0$, which is a contradiction since $p$ is odd. Thus, $A_1 = 0$, whence $5r^4 = 0$. Therefore, $p = 5$. We have $d^2 = a^2r^3 - 16ar^4 + 128r^5, c = 3ar - 32r^2$. Note that $X^2 - r$ does not divide $aX^3 + bX^2 + cX + d = rX(2X^2 - r)$.

**Case 1.2.2.** Assume $a \neq 2r$. Let $2\big(a^2(a-2r)\big)^{-1}D(1,Y) = (A_0 + A_1Y + Y^2)^2$, where $A_0, A_1 \in \overline{\mathbb{F}_q}$. Comparing the coefficients of $Y^0, Y^2, Y^3$ in this equation, we get the following equations:

$$\begin{aligned} &aA_0^2 - 2A_0^2r + 2r^3 = 0, \\ &-a^2 + 16aA_0 + 8aA_1^2 + 8ar - 32A_0r - 16A_1^2r - 32r^2 = 0, \\ &A_1 = 0. \end{aligned}$$

Now $A_1 = 0$ together with the second equation gives $A_0 = \big(16(a-2r)\big)^{-1}(a^2-8ar+32r^2)$, and substituting this into the first equation we get $a^2-16ar+128r^2 = 0$. Hence, $a = 8(1+i)r$ and $c = 8(-1+3i)r^2$, where $i \in \mathbb{F}_q$ is such that $i^2 = -1$. Therefore, $d^2 = a^2r^3-16ar^4+128r^5$ and $c = 3ar-32r^2$. Note that $X^2-r$ does not divide $aX^3+bX^2+cX+d = 8rX(X^2+iX^2-r+3ir)$.

**Case 2.** Assume $d \neq 0$. Setting $b = 3d/r$ and $G_1(X,Y) = rG(X, Y-r)$, we have

$$\begin{aligned} G_1(X,Y) = {} & cr^2X^2 + ar^3X^2 - drX^3 + r^3X^4 + 8drXY - crX^2Y + crY^2 + ar^2Y^2 - 3dXY^2 \\ & - 2r^2X^2Y^2 - arY^3 + rY^4. \end{aligned}$$

Write $G_1(X,Y) = h_2 + h_3 + h_4$, where

$$\begin{aligned} h_2 &= r(crX^2 + ar^2X^2 + 8dXY + cY^2 + arY^2), \\ h_3 &= -drX^3 - crX^2Y - 3dXY^2 - arY^3, \\ h_4 &= r(rX^2 - Y^2)^2. \end{aligned}$$

Since $d \neq 0$, we have $h_2 \neq 0$. Let $D(X,Y) = h_3^2 - 4h_2h_4$. We have $\gcd(h_2, h_3, h_4) = 1$, so as in Case 1, $D(1,Y)$ must be a square in $\overline{\mathbb{F}_q}[X,Y]$. We have

$$\begin{aligned} D(1,Y) = {} & r^2(d^2 - 4cr^3 - 4ar^4) + 2dr^2(c - 16r^2)Y + r(6d^2 + c^2r + 4cr^3 + 4ar^4)Y^2 \\ & + 2dr(3c + ar + 32r^2)Y^3 + (9d^2 + 2acr^2 + 4cr^3 + 4ar^4)Y^4 + 2d(3a - 16r)rY^5 \\ & + r^2(a^2 - 4c - 4ar)Y^6. \end{aligned} \tag{4.11}$$

**Case 2.1.** Assume $a^2 - 4c - 4ar \neq 0$.

Let $\big(r^2(a^2 - 4c - 4ar)\big)^{-1} D(1,Y) = (A_0 + A_1Y + A_2Y^2 + Y^3)^2$, where $A_0, A_1, A_2 \in \overline{\mathbb{F}_q}$. Comparing the coefficients of $Y^0, Y^1, \ldots, Y^5$ in this equation we get the following equations:

$$a^2A_0^2 - 4A_0^2c - d^2 - 4aA_0^2r + 4cr^3 + 4ar^4 = 0, \tag{4.12}$$

$$a^2A_0A_1 - 4A_0A_1c - cd - 4aA_0A_1r + 16dr^2 = 0, \tag{4.13}$$

$$6d^2 - a^2A_1^2r - 2a^2A_0A_2r + 4A_1^2cr + 8A_0A_2cr + c^2r + 4aA_1^2r^2 + 8aA_0A_2r^2 + 4cr^3 + 4ar^4 = 0, \tag{4.14}$$

$$3cd - a^2A_0r - a^2A_1A_2r + 4A_0cr + 4A_1A_2cr + adr + 4aA_0r^2 + 4aA_1A_2r^2 + 32dr^2 = 0, \tag{4.15}$$

$$9d^2 - 2a^2A_1r^2 - a^2A_2^2r^2 + 2acr^2 + 8A_1cr^2 + 4A_2^2cr^2 + 8aA_1r^3 + 4aA_2^2r^3 + 4cr^3 + 4ar^4 = 0, \tag{4.16}$$

$$-3ad + a^2A_2r - 4A_2cr + 16dr - 4aA_2r^2 = 0. \tag{4.17}$$

Solving (4.15)−(4.17) for $A_0, A_1, A_2$, we get

$$\begin{aligned}
A_0 = {} & \big(1/(r^3(a^2-4c-4ar)^3)\big)(54acd^3-90a^2d^3r-288cd^3r-12a^2c^2dr^2+48c^3dr^2 \\
& +864ad^3r^2+a^5dr^3-10a^3cdr^3+72ac^2dr^3-2048d^3r^3+18a^4dr^4-160a^2cdr^4 \\
& +384c^2dr^4-184a^3dr^5+768acdr^5+384a^2dr^6), \\
A_1 = {} & \big(1/(r^2(a^2-4c-4ar)^2)\big)(-18cd^2+30ad^2r+a^3cr^2-4ac^2r^2-128d^2r^2-2a^2cr^3 \\
& -8c^2r^3+2a^3r^4-16acr^4-8a^2r^5), \\
A_2 = {} & \big(1/(r(a^2-4c-4ar)\big)(3ad-16dr).
\end{aligned}$$

Substituting $A_0, A_1, A_2$ into (4.12)−(4.14), we obtain $L_1 = L_2 = L_3 = 0$, where

$$\begin{aligned}
L_1 = {} & 729a^2c^2d^6-2430a^3cd^6r-7776ac^2d^6r-324a^3c^3d^4r^2+1296ac^4d^4r^2+2025a^4d^6r^2 \\
& +36288a^2cd^6r^2+20736c^2d^6r^2+27a^6cd^4r^3+270a^4c^2d^4r^3+1512a^2c^3d^4r^3-6912c^4d^4r^3 \\
& -38880a^3d^6r^3-179712acd^6r^3+36a^4c^4d^2r^4-288a^2c^5d^2r^4+576c^6d^2r^4-45a^7d^4r^4+792a^5cd^4r^4 \\
& -11304a^3c^2d^4r^4+20736ac^3d^4r^4+278784a^2d^6r^4+294912cd^6r^4-6a^7c^2d^2r^5+84a^5c^3d^2r^5 \\
& -672a^3c^4d^2r^5+1728ac^5d^2r^5-378a^6d^4r^5-4680a^4cd^4r^5+69888a^2c^2d^4r^5-104448c^3d^4r^5 \\
& -884736ad^6r^5-87a^6c^2d^2r^6+1192a^4c^3d^2r^6-5168a^2c^4d^2r^6+9472c^5d^2r^6+15032a^5d^4r^6 \\
& -56576a^3cd^4r^6-18432ac^2d^4r^6+1048576d^6r^6+14a^9d^2r^7-250a^7cd^2r^7+3224a^5c^2d^2r^7 \\
& -17984a^3c^3d^2r^7+33536ac^4d^2r^7-115200a^4d^4r^7+440320a^2cd^4r^7-393216c^2d^4r^7-51a^8d^2r^8 \\
& +344a^6cd^2r^8-4832a^4c^2d^2r^8+8704a^2c^3d^2r^8+36864c^4d^2r^8+354304a^3d^4r^8-786432acd^4r^8 \\
& +a^{10}cr^9-20a^8c^2r^9+160a^6c^3r^9-640a^4c^4r^9+1280a^2c^5r^9-1024c^6r^9-1304a^7d^2r^9 \\
& +18432a^5cd^2r^9-80384a^3c^2d^2r^9+147456ac^3d^2r^9-393216a^2d^4r^9+a^{11}r^{10}-40a^9cr^{10} \\
& +480a^7c^2r^{10}-2560a^5c^3r^{10}+6400a^3c^4r^{10}-6144ac^5r^{10}+11600a^6d^2r^{10}-100096a^4cd^2r^{10} \\
& +221184a^2c^2d^2r^{10}-20a^{10}r^{11}+480a^8cr^{11}-3840a^6c^2r^{11}+12800a^4c^3r^{11}-15360a^2c^4r^{11} \\
& -35072a^5d^2r^{11}+147456a^3cd^2r^{11}+160a^9r^{12}-2560a^7cr^{12}+12800a^5c^2r^{12}-20480a^3c^3r^{12}
\end{aligned}$$

$$+ 36864a^4d^2r^{12} - 640a^8r^{13} + 6400a^6cr^{13} - 15360a^4c^2r^{13} + 1280a^7r^{14} - 6144a^5cr^{14} - 1024a^6r^{15},$$

$$\begin{aligned}
L_2 = {} & -486ac^2d^4 + 1620a^2cd^4r + 2592c^2d^4r + 27a^4c^2d^2r^2 - 432c^4d^2r^2 - 1350a^3d^4r^2 - 15552acd^4r^2 \\
& - 54a^5cd^2r^3 - 108a^3c^2d^2r^3 + 432ac^3d^2r^3 + 18720a^2d^4r^3 + 36864cd^4r^3 - 6a^5c^3r^4 + 48a^3c^4r^4 \\
& - 96ac^5r^4 + 15a^6d^2r^4 + 264a^4cd^2r^4 + 1776a^2c^2d^2r^4 - 5376c^3d^2r^4 - 86016ad^4r^4 + a^6c^2r^5 \\
& + 20a^4c^3r^5 - 16a^2c^4r^5 - 320c^5r^5 + 116a^5d^2r^5 - 1776a^3cd^2r^5 - 2816ac^2d^2r^5 + 131072d^4r^5 \\
& + 16a^7cr^6 - 218a^5c^2r^6 + 1008a^3c^3r^6 - 1952ac^4r^6 - 2688a^4d^2r^6 + 14592a^2cd^2r^6 - 16384c^2d^2r^6 \\
& + 9a^8r^7 - 304a^6cr^7 + 2192a^4c^2r^7 - 4864a^2c^3r^7 + 512c^4r^7 + 12032a^3d^2r^7 - 32768acd^2r^7 \\
& - 114a^7r^8 + 1776a^5cr^8 - 6080a^3c^2r^8 + 2048ac^3r^8 - 16384a^2d^2r^8 + 512a^6r^9 - 3776a^4cr^9 \\
& + 3072a^2c^2r^9 - 928a^5r^{10} + 2048a^3cr^{10} + 512a^4r^{11},
\end{aligned}$$

$$\begin{aligned}
L_3 = {} & 81a^2cd^4 + 81c^2d^4 - 135a^3d^4r - 1134acd^4r - 27a^3c^2d^2r^2 + 108ac^3d^2r^2 + 2241a^2d^4r^2 \\
& + 3456cd^4r^2 + 18a^4cd^2r^3 + 90a^2c^2d^2r^3 - 216c^3d^2r^3 - 11904ad^4r^3 + a^4c^3r^4 - 8a^2c^4r^4 \\
& + 16c^5r^4 + 37a^5d^2r^4 - 416a^3cd^2r^4 + 568ac^2d^2r^4 + 20480d^4r^4 + 2a^5c^2r^5 - 24a^3c^3r^5 + 64ac^4r^5 \\
& - 462a^4d^2r^5 + 2680a^2cd^2r^5 - 2560c^2d^2r^5 - 11a^4c^2r^6 + 40a^2c^3r^6 + 80c^4r^6 + 1896a^3d^2r^6 \\
& - 5120acd^2r^6 - a^7r^7 + 18a^5cr^7 - 104a^3c^2r^7 + 320ac^3r^7 - 2560a^2d^2r^7 + 13a^6r^8 - 152a^4cr^8 \\
& + 480a^2c^2r^8 - 56a^5r^9 + 320a^3cr^9 + 80a^4r^{10}.
\end{aligned}$$

We have $d \neq 0$, so by (4.3),

$$2d^2 - acr^2 + a^2r^3 + 4cr^3 - 12ar^4 - 128r^5 = 0. \tag{4.18}$$

Taking the resultant of (4.18) and (4.2) with respect to $d$, we get

$$4r^2(c - 3ar + 32r^2)^2(5c - 7ar - 64r^2)^2 = 0.$$

Therefore, either $c - 3ar + 32r^2 = 0$ or $5c - 7ar - 64r^2 = 0$.

**Case 2.1.1.** Assume $c - 3ar + 32r^2 = 0$. Then by (4.18), $d^2 = a^2r^3 - 16ar^4 + 128r^5$.

**Case 2.1.2.** Assume $5c - 7ar - 64r^2 = 0$.

**Case 2.1.2.1.** Assume $p \neq 5$. Then by (4.18), $d^2 = (a^2r^3+48ar^4+192r^5)/5$. Substituting $d^2$ and $c = (7ar + 64r^2)/5$ into equations $L_1 = L_2 = L_3 = 0$, we obtain

$$(a - 28r)M_1 = (a - 28r)M_2 = (a - 28r)M_3 = 0,$$

where

$$\begin{aligned}
M_1 &= 3125a^{10} - 111500a^9r - 2624400a^8r^2 + 76303616a^7r^3 + 1191918848a^6r^4 \\
&\quad - 17626513408a^5r^5 - 259406970880a^4r^6 - 861392076800a^3r^7 + 35664166912a^2r^8 \\
&\quad + 2394712702976ar^9 - 1292785156096r^{10}, \\
M_2 &= 375a^7 - 11560a^6r - 140928a^5r^2 + 1329472a^4r^3 + 36695296a^3r^4 + 205918208a^2r^5 \\
&\quad + 253231104ar^6 - 381681664r^7, \\
M_3 &= 325a^6+3500a^5r-328432a^4r^2-2239616a^3r^3-7824128a^2r^4-55148544ar^5-155451392r^6.
\end{aligned}$$

If $a = 28r$, then $d^2 = 464r^5 = a^2r^3 - 16ar^4 + 128r^5$ and $c = 52r^2 = 3ar - 32r^2$.

Now assume $a \neq 28r$. We have

$$\begin{aligned}
\mathrm{Res}(M_1, M_2; a) &= (2^{194})(5^{32})(7)(13^{23})(29^3)(9473)r^{70}, \\
\mathrm{Res}(M_2, M_3; a) &= (2^{110})(5^{20})(13^{13})(19)(29)(157)(283)(12923)r^{42},
\end{aligned}$$

where $\mathrm{Res}(M_1, M_2; a)$ denotes the resultant of $M_1$ and $M_2$ with respect to $a$.

Since $p$ is odd and $p \neq 5$, we have $p = 13$ or 29. Now using the conditions for $a, c$ and $d$, (4.4) implies

$$3a^3 + 88a^2r - 2384ar^2 - 12096r^3 = 0. \tag{4.19}$$

By taking the resultant of $L_3$ and (4.19) with respect to $a$, we get

$$(2^{39})(5^{12})(7)(149)(373)(1543)r^{18} = 0,$$

which is a contradiction. Therefore, $p = 5$.

**Case 2.1.2.2.** Assume $p = 5$. Then $a = -64r/7 = 3r$. By (4.18), $d^2 = 2cr^3$. Then from equations $L_2 = L_3 = 0$ we get

$$(c + 3r^2)(c^4 + 3c^2r^4 + 4cr^6 + 3r^8) = 0,$$
$$(c + 3r^2)(c^4 + 2c^3r^2 + 4c^2r^4 + 4r^8) = 0.$$

Assume $c + 3r^2 \neq 0$. Then $c^4 + 3c^2r^4 + 4cr^6 + 3r^8 = 0$ and $c^4 + 2c^3r^2 + 4c^2r^4 + 4r^8 = 0$. By taking the resultant of these two equations with respect to $c$, we get $4r^{32} = 0$, which is a contradiction since $p$ is odd. Therefore, $c = 2r^2$ which implies $d^2 = 4r^5$. Hence, $r$ is a square in $\mathbb{F}_q$, which is a contradiction.

**Case 2.2.** Assume $a^2 - 4c - 4ar = 0$. Then $c = (a^2 - 4ar)/4$. Since $D(1, Y)$ in (4.11) is a square, we must have $3a - 16r = 0$. Clearly, $p \neq 3$, whence $a = 16r/3$. Thus, equations (4.2)$-$(4.4) imply

$$81d^2 - 2560r^5 = 0, \tag{4.21}$$
$$27d^2 - 2240r^5 = 0, \tag{4.22}$$
$$6561d^4 - 18144d^2r^5 - 7659520r^{10} = 0. \tag{4.23}$$

By taking the resultant of (4.21) and (4.22) with respect to $d$, we get

$$(2^{12})(3^6)(5^2)(13^2)r^{10} = 0,$$

and from the resultant of (4.21) and (4.23) with respect to $d$, we get

$$(2^{26})(3^{16})(5^2)(41^2)r^{20} = 0.$$

Therefore, we must have $p = 5$. We now have

$$D(1, Y) = r^2(d^2 + r^5) + dr^4Y + d^2rY^2 + 2dr^3Y^3 + 4d^2Y^4.$$

Let $D(1, Y) = (A_0+A_1+2dY^2)^2$, where $A_0, A_1 \in \overline{\mathbb{F}_q}$. Comparing the coefficients of $Y^0, Y^1, Y^3$ in this equation, we get

$$\begin{aligned} -A_0^2 + d^2r^2 + r^7 &= 0, \\ -2A_0A_1 + dr^4 &= 0, \\ -2d(2A_1 - r^3) &= 0. \end{aligned}$$

The last two equations give $A_0 = dr$, and so the first equation becomes $r^7 = 0$, which is a contradiction. □

**Lemma 4.2.** *Let char $\mathbb{F}_q = 3$ and $f(X)$ be given in (4.6). If $f$ is a PR of $\mathbb{P}^1(\mathbb{F}_q)$ and $q \geq 3^2$, then one of the following conditions holds.*

*(i)* $a = r, b = c = d = 0$.

*(ii)* $a = b = d = 0, c = -r^2$.

*(iii)* $b = 0, c = r^2, d^2 = a^2r^3 - ar^4 - r^5$.

*Proof.* By (4.1) $b = 0$. Hence (4.2), (4.4), (4.5) imply

$$d^2 + 2c^2r + 2a^2r^3 + 2cr^3 + ar^4 = 0, \tag{4.24}$$

$$cr^4(c^2 + 2r^4) = 0, \tag{4.25}$$

$$d(d^4 + 2c^2d^2r + 2ac^3r^3 + a^2d^2r^3 + a^4r^6 + ar^9 + r^{10}) = 0. \tag{4.26}$$

**Case 1.** Assume $c = 0$. The resultant of (4.24) and (4.26) with respect to $d$ is $2ar^{19}(a + 2r)^5$. Note that $a \neq 0$, otherwise $a = b = c = d = 0$. Therefore we must have $a = r$. It follows that $d = 0$.

**Case 2.** Assume $c \neq 0$. Then $c = r^2$ or $-r^2$.

If $c = -r^2$, then the resultant of (4.24) and (4.26) with respect to $d$ is $2ar^{23}(a + 2r)$. If $a = r$, then $d = 0$, whence $X^2 - r$ divides $aX^3 + bX^2 + cX + d = rX^3 - r^2X$ which is a contradiction. Therefore $a = 0$, and so $d = 0$.

If $c = r^2$, then (4.24) becomes $d^2 = a^2r^3 - ar^4 - r^5$. □

**Lemma 4.3.** *Let* char $\mathbb{F}_q = 3$ *and* $f(X), G(X, Y)$ *be given in* (4.6), (4.8), *respectively. If*

*(i)* $a = r, b = c = d = 0$ *or*

*(ii)* $a = b = d = 0, c = -r^2$,

*then* $G(X, Y)$ *is absolutely irreducible.*

*Proof.* Let $G_1(X, Y) = G(X, Y - r)$. Then $G_1(X, Y) = h_2 + h_3 + h_4$, where

$$h_2 = crX^2 + ar^2X^2 + 2dXY + 2brXY + cY^2 + arY^2,$$
$$h_3 = 2(dX^3 + cX^2Y + bXY^2 + aY^3),$$
$$h_4 = (rX^2 - Y^2)^2.$$

In either case, $h_2 \neq 0$ and $\gcd(h_2, h_3, h_4) = 1$. Let $D(X, Y) = h_3^2 - 4h_2h_4$. Suppose $G(X, Y)$ is not absolutely irreducible. Then $D(1, Y)$ is a square in $\overline{\mathbb{F}_q}[Y]$.

If $a = r, b = c = d = 0$, then $D(1, Y) = r^3(2r^2 + rY^2 + Y^4)$. Let $2r^2 + rY^2 + Y^4 = (A_0 + A_1Y + Y^2)^2$, where $A_0, A_1 \in \overline{\mathbb{F}_q}$. Comparing the coefficients of $Y^0, Y^2, Y^3$, we get

$$2(A_0^2 + r^2) = 0,$$
$$A_0 + 2A_1^2 + r = 0,$$
$$A_1 = 0.$$

Simultaneously solving the equations gives $r^2 = 0$, which is a contradiction.

If $a = b = d = 0, c = -r^2$, then $D(1, Y) = r^2(r^3 + 2rY^4 + Y^6)$. Let $r^3 + 2rY^4 + Y^6 = (A_0 + A_1Y + A_2Y^2 + Y^3)^2$, where $A_0, A_1, A_2 \in \overline{\mathbb{F}_q}$. Comparing the coefficients of $Y^3, Y^5$, we get

$$A_0 + A_1A_2 = 0,$$
$$A_2 = 0.$$

Hence $A_0 = 0$, which is a contradiction. □

**Lemma 4.4.** *Let $f(X)$ be given in (4.6). If $b = 3d/r, c = 3ar - 32r^2$ and $d^2 = a^2r^3 - 16ar^4 + 128r^5$, then $f$ is a PR of $\mathbb{P}^1(\mathbb{F}_q)$.*

*Proof.* Let $F(X, Y), G(X, Y)$ be as in (4.7), (4.8), respectively. Let $G_1(X, Y) = rG(X, Y - r)$ and write $G_1(X, Y) = h_2 + h_3 + h_4$, where

$$h_2 = -4r(-ar^2X^2 + 8r^3X^2 - 2dXY - arY^2 + 8r^2Y^2),$$
$$h_3 = -drX^3 - 3ar^2X^2Y + 32r^3X^2Y - 3dXY^2 - arY^3,$$
$$h_4 = r(rX^2 - Y^2)^2.$$

If $a - 8r = 0$, then $d^2 = 64r^5$, which is a contradiction since $r$ is a non-square in $\mathbb{F}_q$. Hence, $h_2 \neq 0$. Let $D = h_3^2 - 4h_2h_4$. We have

$$\begin{aligned} D = {} & r^2(d^2 - 16ar^4 + 128r^5)X^6 + 6d(a - 16r)r^3X^5Y + r(6d^2 + 9a^2r^3 - 176ar^4 + 896r^5)X^4Y^2 \\ & + 4d(5a - 32r)r^2X^3Y^3 + (9d^2 + 6a^2r^3 - 48ar^4 - 128r^5)X^2Y^4 + 2d(3a - 16r)rXY^5 \\ & + r^2(a^2 - 16ar + 128r^2)Y^6. \end{aligned}$$

Let $r = s^2$. It can be easily verified that

$$D = \left(\frac{1}{s}(ar^3X^3 - 16r^4X^3 + 3drX^2Y + 3ar^2XY^2 - 16r^3XY^2 + dY^3)\right)^2.$$

Therefore, $G_1(X,Y)$ is not absolutely irreducible and we can write

$$G_1 = \frac{1}{4h_4}(2h_4 + h_3 + \delta)(2h_4 + h_3 - \delta),$$

where $\delta^2 = D$. Hence, we have the following factorization of $G_1$:

$$\begin{aligned} G_1(X,Y) =& \big(-1/(4r^2)\big)\big(-ar^2X + 16r^3X - dY - 4r^2XY + s(dX - 2r^2X^2 + arY - 2rY^2)\big) \\ & \big(-ar^2X + 16r^3X - dY - 4r^2XY - s(dX - 2r^2X^2 + arY - 2rY^2)\big). \end{aligned}$$

Let $(x,y) \in \mathbb{F}_q^2$ be a root of $G_1(X,Y)$. Since $s \notin \mathbb{F}_q$, we must have $\phi_1 = \phi_2 = 0$, where

$$\phi_1 = -ar^2x + 16r^3x - dy - 4r^2xy, \tag{4.27}$$

$$\phi_2 = dx - 2r^2x^2 + ary - 2ry^2. \tag{4.28}$$

We have

$$\mathrm{Res}(\phi_1, \phi_2; x) = 32r^5y(-4ar^2 + 64r^3 + ary - 40r^2y + 8ry^2 - y^3). \tag{4.29}$$

Assume $(x,y) \neq (0,0)$.

If $y = 0$, then from (4.27), (4.28), $r^2x(-a + 16r) = x(d - 2r^2x) = 0$. Hence $a = 16r$ and $x = d/(2r^2)$. Therefore, $x^2 = d^2/(4r^4) = 32r$.

If $y \neq 0$, then by (4.29),

$$-4ar^2 + 64r^3 + ary - 40r^2y + 8ry^2 - y^3 = 0. \tag{4.30}$$

Now

$$\begin{aligned} & d\phi_1 - (-ar^2 + 16r^3 - 4r^2y)\phi_2 \\ &= -2r^4x^2(a - 16r + 4y) - y(d^2 - a^2r^3 + 16ar^4 - 2ar^3y - 32r^4y + 8r^3y^2) \\ &= -2r^4x^2(a - 16r + 4y) - 2r^3y(64r^2 - ay - 16ry + 4y^2). \end{aligned}$$

If $a - 16r + 4y = 0$, then it follows that $-64r^2 + ay + 16ry - 4y^2 = -64r^2 = 0$, which is a contradiction. Hence,

$$x^2 = \frac{y(-64r^2 + ay + 16ry - 4y^2)}{r(a - 16r + 4y)}.$$

Using (4.30) we can simplify $x^2$ as

$$\begin{aligned} x^2 &= \frac{y(-64r^2 + ay + 16ry - 4y^2) - 8(-4ar^2 + 64r^3 + ary - 40r^2y + 8ry^2 - y^3)}{r(a - 16r + 4y)} \\ &= \frac{32r^2 - 8ry + y^2}{r}. \end{aligned}$$

Since $G(X, Y) = (1/r)G_1(X, Y + r)$, we have that the roots of $G(X, Y)$ are $(x, y - r)$, where $(x, y)$ is a root of $G_1(X, Y)$. We have

$$x^2 - 4(y - r) = \begin{cases} 4r & \text{if } x = 0, y = 0, \\ 36r & \text{if } x \neq 0, y = 0, \\ \dfrac{(6r - y)^2}{r} & \text{if } x \neq 0, y \neq 0. \end{cases}$$

Therefore, $x^2 - 4(y - r)$ is either 0 or a non-square in $\mathbb{F}_q$. By Lemma 1.10, $f$ is a PR of $\mathbb{P}^1(\mathbb{F}_q)$. □

**Lemma 4.5.** *Let $F(X, Y), G(X, Y)$ be given in (4.7), (4.8), respectively. If $G(X, Y)$ is absolutely irreducible, then $F(X, Y)$ has an absolutely irreducible factor in $\mathbb{F}_q[X, Y]$.*

*Proof.* We have

$$\begin{aligned} F(X, Y) = {} & r^2(c + r^2) + r(2d + br)(X + Y) + r(arX^2 - 2r^2X^2 + 2cXY + arXY + arY^2 \\ & - 2r^2Y^2) - d(X + Y)(X^2 + Y^2) + (r^2X^4 - cX^3Y - cX^2Y^2 - 2arX^2Y^2 \\ & + 4r^2X^2Y^2 - cXY^3 + r^2Y^4) - bX^2Y^2(X + Y) - X^2Y^2(2rX^2 + aXY + 2rY^2) \\ & + X^4Y^4. \end{aligned}$$

Assume to the contrary that $F(X,Y)$ does not have an absolutely irreducible factor in $\mathbb{F}_q[X,Y]$. By Corollary 1.9, $F(X,Y) = H(X,Y)H(Y,X)$, where $H(X,Y) \in \mathbb{F}_{q^2}[X,Y]$ is absolutely irreducible and $\sigma(H(X,Y)) = \pm H(Y,X)$.

Let $H = h_0 + h_1 + h_2 + h_3 + h_4$, where $h_i$ is homogeneous of degree $i$. Since $h_4(X,Y)h_4(Y,X) = X^4Y^4$ and $\sigma(h_4(X,Y)) = \pm h_4(Y,X)$, we must have $h_4(X,Y) = \pm X^2Y^2$. We may assume $h_4(X,Y) = X^2Y^2$. Hence, $\sigma(H(X,Y)) = H(Y,X)$.

We have $h_0^2 = r^2(c+r^2)$. Since $0 = h_3(X,Y)h_4(Y,X) + h_3(Y,X)h_4(X,Y) = (h_3(X,Y) + h_3(Y,X))X^2Y^2$, we have $h_3(X,Y) = -h_3(Y,X)$. Since $-X^2Y^2(2rX^2 + aXY + 2rY^2) = h_2(X,Y)h_4(Y,X) + h_3(X,Y)h_3(Y,X) + h_2(Y,X)h_4(X,Y)$, we have $XY \mid h_3(X,Y)$. Since $\sigma(H(X,Y)) = H(Y,X)$, it follows that

$$\begin{aligned} h_1(X,Y) &= A_1X + A_2Y, \\ h_2(X,Y) &= B_1X^2 + BXY + B_2Y^2, \\ h_3(X,Y) &= CXY(X-Y), \end{aligned}$$

where $A_2 = A_1^q, B_2 = B_1^q, B \in \mathbb{F}_q$, and $C^q = -C$. Comparing the coefficients of $X^iY^j$ in the equation $F(X,Y) = H(X,Y)H(Y,X)$, we get the following.

$$h_0^2 - cr^2 - r^4 = 0, \tag{4.31}$$

$$A_1h_0 + A_2h_0 - 2dr - br^2 = 0, \tag{4.32}$$

$$A_1^2 + A_2^2 + 2Bh_0 - 2cr - ar^2 = 0, \tag{4.33}$$

$$BB_1 + BB_2 + c - A_1C + A_2C = 0, \tag{4.34}$$

$$A_1A_2 + B_1h_0 + B_2h_0 - ar^2 + 2r^3 = 0, \tag{4.35}$$

$$A_1B + A_2B + A_1B_1 + A_2B_2 + d = 0, \tag{4.36}$$

$$B^2 + B_1^2 + B_2^2 + c + 2A_1C - 2A_2C + 2h_0 + 2ar - 4r^2 = 0, \tag{4.37}$$

$$B_1 + B_2 - C^2 + 2r = 0, \tag{4.38}$$

$$A_2B_1 + A_1B_2 + d = 0, \tag{4.39}$$

$$BB_1 + BB_2 + c - A_1C + A_2C = 0, \tag{4.40}$$

$$A_1 + A_2 + b + B_1C - B_2C = 0, \tag{4.41}$$

$$a + 2B + 2C^2 = 0, \tag{4.42}$$

$$B_1B_2 - r^2 = 0, \tag{4.43}$$

$$(B_1 - B_2)C = 0, \tag{4.44}$$

$$B_1 + B_2 - C^2 + 2r = 0. \tag{4.45}$$

We first assume that $C = 0$. Then from $(4.41), (4.42), (4.45)$, we have

$$A_2 = -A_1 - b, \tag{4.46}$$

$$B = -a/2, \tag{4.47}$$

$$B_2 = -B_1 - 2r. \tag{4.48}$$

By (4.43),

$$B_1 = -r. \tag{4.49}$$

Substituting $(4.46) - (4.49)$ into (4.39),(4.40) gives $d = -br, c = -ar$. Then $aX^3 + bX^2 + cX + d$ is divisible by $X^2 - r$, which is a contradiction.

We now assume $C \neq 0$. By (4.44), $B_2 = B_1$. By (4.41),(4.42), $A_2 = -A_1 - b, B = (-a - 2C^2)/2$, whence $A_1 = (2c - 2bC - aC^2 - 2C^4 + 2ar + 4C^2r)/(4c)$ by (4.40). By (4.45), $B_1 = (C^2 - 2r)/2$, whence $C^2(C^2 - 4r) = 0$ by (4.43). But $C \neq 0$. Hence, $C^2 = 4r$. Therefore, from (4.39), we have $d = br$. So by (4.36),

$$b(a + 8r) = 0. \tag{4.50}$$

Now $h_0 = (-a^2 - 12c - 16ar + 8r^2)/8$, by (4.37).

If $b \neq 0$, then $a = -8r$. By (4.32), $c = 8r^2$. But by (4.35), $b^2/4 = 0$, which is a contradiction. Therefore, $b = 0$. By (4.31), (4.33), (4.35), we have

$$a^4 + 24a^2c + 144c^2 + 32a^3r + 384acr + 240a^2r^2 - 256cr^2 - 256ar^3 = 0, \tag{4.51}$$

$$c^2 + a^3r + 10acr + 25a^2r^2 + 64cr^2 + 128ar^3 = 0, \tag{4.52}$$

$$c^2 - 2acr + 5a^2r^2 + 32cr^2 + 96ar^3 = 0. \tag{4.53}$$

From (4.51) and (4.53), we have

$$a(a + 8r)^2(a^5 + 96a^4r + 3456a^3r^2 + 60416a^2r^3 + 532480ar^4 + 1245184r^5) = 0. \tag{4.54}$$

From (4.52) and (4.53), we have

$$ar^2(a + 8r)^2(a^3 + 48a^2r + 512ar^2 + 1024r^3) = 0. \tag{4.55}$$

If $a(a + 8r) \neq 0$, then (4.54) and (4.55) give $2^{48}r^{15} = 0$, which is a contradiction. Therefore, either $a = 0$ or $a = -8r$. If $a = 0$, then (4.52), (4.53) become

$$c(c + 64r^2) = 0,$$

$$c(c + 32r^2) = 0.$$

Thus, $c = 0$, whence $a = b = c = d = 0$, which is a contradiction. Now if $a = -8r$, then (4.51), (4.52), (4.53) give

$$9c^2 + 272cr^2 + 2112r^4 = 0, \tag{4.56}$$

$$c^2 + 144cr^2 + 3136r^4 = 0, \tag{4.57}$$

$$c^2 + 16cr^2 + 1088r^4 = 0. \tag{4.58}$$

But (4.56), (4.57) imply $(2^{26})(353)r^8 = 0$, and (4.57), (4.58) imply $(2^{20})(17)r^8 = 0$, which is a contradiction. □

## 4.2 Case III, $q$ Even

Assume that $q$ is even and

$$f(X) = X + \frac{aX^3 + bX^2 + cX + d}{(X^2 + X + t)^2},$$

where $a, b, c, d, t \in \mathbb{F}_q$, $(a, b, c, d) \neq (0, 0, 0, 0)$, $\mathrm{Tr}_{q/2}(t) = 1$ and $X^2 + X + t$ does not divide $aX^3 + bX^2 + cX + d$.

In the succeeding theorem, the useful power sum conditions $s(f, k) = 0$ are when $k = 1, 3, 5, 9, 11$. Suppose $f$ is a PR of $\mathbb{P}^1(\mathbb{F}_q)$. Since $s(f, 1) = b + c + at$, if $q \geq 3$, we have

$$c = b + at. \tag{4.59}$$

Setting $c = b + at$ in $s(f, k)$ for $k = 3, 5, 9, 11$, we get the following conditions. If $q \geq 5$, then

$$b + b^2 + ab^2 + d + a^2d + d^2 + at + bt + a^2bt + a^2t^2 + b^2t^2 = 0. \tag{4.60}$$

If $q \geq 7$, then

$$b + b^4 + d + d^4 + at + bt + a^4t^4 + b^4t^4 = 0. \tag{4.61}$$

If $q \geq 11$, then

$$b + b^8 + d + d^8 + at + bt + a^8t^8 + b^8t^8 = 0. \tag{4.62}$$

If $q \geq 13$, then

$$\begin{aligned} & b + b^8 + ab^8 + d + a^2d + b^2d + d^8 + ad^8 + at + bt + a^2bt + b^2t + b^3t + b^8t + d^2t + d^8t + a^3t^2 \\ & + bt^2 + b^2t^2 + ab^2t^2 + dt^2 + a^2dt^2 + d^2t^2 + at^3 + a^2t^3 + bt^3 + a^2bt^3 + b^2t^3 + a^2t^4 + bt^4 \\ & + ab^2t^4 + dt^4 + a^2dt^4 + d^2t^4 + at^5 + bt^5 + a^2bt^5 + a^2t^6 + b^2t^6 + a^8t^8 + a^9t^8 + b^8t^8 \\ & + ab^8t^8 + a^8t^9 + b^8t^9 = 0. \end{aligned} \tag{4.63}$$

**Theorem 4.6.** *Let $q$ be even and*

$$f(X) = X + \frac{aX^3 + bX^2 + cX + d}{(X^2 + X + t)^2}, \tag{4.64}$$

*where $a, b, c, d, t \in \mathbb{F}_q$, $(a, b, c, d) \neq (0, 0, 0, 0)$, $\mathrm{Tr}_{q/2}(t) = 1$ and $X^2 + X + t$ does not divide $aX^3 + bX^2 + cX + d$. If $q \geq 2^4$, then $f$ is a PR of $\mathbb{P}^1(\mathbb{F}_q)$ if and only if one of the following conditions holds.*

*(i)* $a = 1/t, b = d = 0, c = 1, t \neq 1$.

*(ii)* $a = b = c = 0, d = 1$.

*The condition is sufficient for all $q$.*

*Proof.* ($\Rightarrow$) Suppose $f$ is a PR of $\mathbb{P}^1(\mathbb{F}_q)$.

**Case 1.** Assume $a \neq 0$. By a suitable substitution $X \mapsto X + u, u \in \mathbb{F}_q$, up to equivalence we may assume $b = 0$. Therefore, $c = at$ by (4.59). From (4.61) and (4.62), we have

$$\begin{aligned} d + d^4 + at + a^4t^4 = 0, \\ d + d^8 + at + a^8t^8 = 0. \end{aligned}$$

Hence, $(d + d^2 + at + a^2t^2)^4 = 0$, whence $(d + at)(d + at + 1) = 0$. If $d = at$, then by (4.60), $a^3t = 0$, which is a contradiction. Thus, $d = at + 1$. By (4.60), $a^2(1 + at) = 0$. Therefore, $a = 1/t, b = d = 0$ and $c = 1$. Note that $X^2 + X + t$ divides $(1/t)X^3 + 1$ if and only if $t = 1$.

**Case 2.** Assume $a = 0$. Then by (4.59), $b = c$. From (4.60) and (4.61), we have

$$b + b^2 + d + d^2 + bt + b^2t^2 = 0,$$
$$b + b^4 + d + d^4 + bt + b^4t^4 = 0.$$

Hence, $(b+b^2+d+d^2+bt+b^2t^2)^2 = 0$, whence $(b+d+bt)(b+d+bt+1) = 0$. If $d = b+bt$, then by (4.63), $b^3 = 0$. Hence, $a = b = c = d = 0$, which is a contradiction. Thus, $d = b + bt + 1$. By (4.63), $b^2(1 + b) = 0$. If $b = 1$, then $aX^3 + bX^2 + cX + d = X^2 + X + t$, which is a contradiction. Therefore, $b = 0$ and $a = 0, c = 0, d = 1$.

($\Leftarrow$) We have

$$\frac{f(X) - f(Y)}{X - Y} = \frac{F(X, Y)}{(X^2 + X + t)^2(Y^2 + Y + t)^2},$$

where

$$\begin{aligned} F(X,Y) = {} & ct^2 + t^4 + dX + bt^2X + t^2X^2 + at^2X^2 + dX^3 + t^2X^4 + dY + bt^2Y + cXY \\ & + at^2XY + dX^2Y + cX^3Y + t^2Y^2 + at^2Y^2 + dXY^2 + X^2Y^2 + aX^2Y^2 + cX^2Y^2 \\ & + bX^3Y^2 + X^4Y^2 + dY^3 + cXY^3 + bX^2Y^3 + aX^3Y^3 + t^2Y^4 + X^2Y^4 + X^4Y^4. \end{aligned}$$

Then $F(X, Y) = G(X + Y, XY)$, where

$$\begin{aligned} G(X,Y) = {} & ct^2 + t^4 + dX + bt^2X + t^2X^2 + at^2X^2 + dX^3 + t^2X^4 + cY + at^2Y \\ & + cX^2Y + Y^2 + aY^2 + cY^2 + bXY^2 + X^2Y^2 + aY^3 + Y^4. \end{aligned}$$

**Case 1.** Assume $a = 1/t, b = d = 0, c = 1, t \neq 1$. Then

$$G(X,Y) = \frac{1}{t}(t^3 + t^5 + t^2X^2 + t^3X^2 + t^3X^4 + tY + t^2Y + tX^2Y + Y^2 + tX^2Y^2 + Y^3 + tY^4).$$

Let $G_1(X,Y) = tG(X+1, Y+t) = t^3X^4 + tX^2Y + Y^2 + tX^2Y^2 + Y^3 + tY^4$. It can be easily verified that

$$G_1(X,Y) = \Big(tX^2 + Y + s(tX^2 + Y^2)\Big)\Big(Y + Y^2 + s(tX^2 + Y^2)\Big),$$

where $s^2 + s + t = 0$. Let $(x,y) \in \mathbb{F}_q^2$ be a root of $G_1(X,Y)$. Since $s \notin \mathbb{F}_q$, we have $tx^2 + y = tx^2 + y^2 = 0$, or $y + y^2 = tx^2 + y^2 = 0$. Therefore, $(x,y) = (0,0)$ or $(t^{-1/2}, 1)$. Hence the roots of $G(X,Y) = (1/t)G_1(X+1, Y+t)$ in $\mathbb{F}_q^2$ are $(1,t)$ or $(t^{-1/2}+1, t+1)$. But if $(x_0,y_0) = (1,t)$ or $(t^{-1/2}+1, t+1)$, then $\mathrm{Tr}_{q/2}(y_0/x_0^2) = \mathrm{Tr}_{q/2}(t) = 1$. Thus by Lemma 1.10, $f$ is a PR of $\mathbb{P}^1(\mathbb{F}_q)$.

**Case 2.** Assume $a = b = c = 0, d = 1$. Then

$$G(X,Y) = t^4 + X + t^2X^2 + X^3 + t^2X^4 + Y^2 + X^2Y^2 + Y^4.$$

Let $G_1(X,Y) = G(X+1, Y+t) = X^2 + X^3 + t^2X^4 + X^2Y^2 + Y^4$. Then

$$G_1(X,Y) = (X + tX^2 + Y^2 + sX^2)(X + X^2 + tX^2 + Y^2 + sX^2),$$

where $s^2 + s + t = 0$. Let $(x,y) \in \mathbb{F}_q^2$ be a root of $G_1(X,Y)$. Since $s \notin \mathbb{F}_q$, we have $x + tx^2 + y^2 = x^2 = 0$, or $x + x^2 + tx^2 + y^2 = x^2 = 0$. Therefore $(x,y) = (0,0)$. Hence the only root of $G(X,Y) = G_1(X+1, Y+t)$ in $\mathbb{F}_q^2$ is $(x_0,y_0) = (1,t)$. But $\mathrm{Tr}_{q/2}(y_0/x_0^2) = \mathrm{Tr}_{q/2}(t) = 1$. Thus by Lemma 1.10, $f$ is a PR of $\mathbb{P}^1(\mathbb{F}_q)$. □

# CHAPTER 5:

# CASE IV, TWO DISTINCT QUADRATICS IN THE DENOMINATOR

Assume that

$$f(X) = X + \frac{aX+b}{Q_1(X)} + \frac{cX+d}{Q_2(X)},$$

where $a, b, c, d \in \mathbb{F}_q$, $(a,b) \neq (0,0)$, $(c,d) \neq (0,0)$, $Q_1(X)$ and $Q_2(X)$ are different monic irreducible quadratics over $\mathbb{F}_q$.

If $q$ is odd, then we may assume

$$f(X) = X + \frac{aX+b}{X^2-u} + \frac{cX+d}{X^2+v_1X+v_0}, \tag{5.1}$$

where $a, b, c, d, v_1 \in \mathbb{F}_q$, $u, v_0 \in \mathbb{F}_q^*$, $(a,b) \neq (0,0)$, $(c,d) \neq (0,0)$, $(v_0, v_1) \neq (-u, 0)$, and $u, v_1^2 - 4v_0$ are non-square elements in $\mathbb{F}_q$.

If $q$ is even, then we may assume

$$f(X) = X + \frac{aX+b}{X^2+X+u} + \frac{cX+d}{X^2+v_1X+v_0}, \tag{5.2}$$

where $a, b, c, d \in \mathbb{F}_q$, $u, v_0, v_1 \in \mathbb{F}_q^*$, $(a,b) \neq (0,0)$, $(c,d) \neq (0,0)$, $(v_0, v_1) \neq (u, 1)$, and $\mathrm{Tr}_{q/2}(u) = \mathrm{Tr}_{q/2}(v_0/v_1^2) = 1$.

In this dissertation, we will consider the cases when $v_1 = 0$ in (5.1) and $v_1 = 1$ in (5.2).

## 5.1 Case IV, $q$ Odd

Assume $q$ is odd and let

$$f(X) = X + \frac{aX+b}{X^2-u} + \frac{cX+d}{X^2-v},$$

where $a, b, c, d \in \mathbb{F}_q$, $(a,b) \neq (0,0)$, $(c,d) \neq (0,0)$, $u, v$ distinct non-square elements in $\mathbb{F}_q$.

Suppose $f$ is a PR of $\mathbb{P}^1(\mathbb{F}_q)$. In the proof of the next theorem, we use the results on the power sum conditions $s(f,k) = 0$ up to $k = 4$, where the values of $s(f,k)$ are given in Appendix A.5. For $q \geq 3$, $s(f,1) = -8(du+bv)$, hence we have

$$du + bv = 0. \tag{5.3}$$

Since $u \neq v$, we have $u - v \neq 0$. Hence from the equations $s(f,k),\ k = 2,3,4$, we have the following conditions. If $q \geq 4$, then

$$3d^2u^2 + 8bduv - c^2u^2v + 3b^2v^2 - a^2uv^2 - 8au^2v^2 - 8cu^2v^2 = 0. \tag{5.4}$$

If $q \geq 5$, then

$$\begin{aligned} &5d^3u^4+18bd^2u^3v-5d^3u^3v-3c^2du^4v+24b^2du^2v^2-24bd^2u^2v^2-6bc^2u^3v^2-12acdu^3v^2+3c^2du^3v^2 \\ &\quad + 12cdu^4v^2+5b^3uv^3-18b^2duv^3-3a^2bu^2v^3+12abcu^2v^3+6a^2du^2v^3+12abu^3v^3-12cdu^3v^3 \\ &\quad + 24bu^4v^3 + 24du^4v^3 - 5b^3v^4 + 3a^2buv^4 - 12abu^2v^4 - 24bu^3v^4 - 24du^3v^4 = 0. \end{aligned} \tag{5.5}$$

If $q \geq 6$, then

$$35d^4u^6 + 160bd^3u^5v - 70d^4u^5v - \cdots - 256cu^4v^7 = 0, \tag{5.6}$$

where the left hand side of (5.6) is $s(f,4)/\left(512(u-v)^4\right)$ and $s(f,4)$ is given in Appendix A.5.

**Theorem 5.1.** *Let $q$ be odd and*

$$f(X) = X + \frac{aX+b}{X^2-u} + \frac{cX+d}{X^2-v}, \tag{5.7}$$

*where $a, b, c, d \in \mathbb{F}_q$, $(a,b) \neq (0,0)$, $(c,d) \neq (0,0)$, $u, v$ distinct non-square elements in $\mathbb{F}_q$. If $q \geq 457$, then $f$ is a PR of $\mathbb{P}^1(\mathbb{F}_q)$ if and only if $a = -4u(3+w), b = d = 0, c = -4u(7+3w)$, and $v = u(9+4w)$, where $w^2 = 5$. The condition is sufficient for all $q$.*

*Proof.* Since the proof is quite lengthy, we only prove the necessity here. The proof for the sufficiency is given in Lemma 5.2 following this proof. Also, a key argument on the proof of the necessity, the existence of an absolutely irreducible factor of $F$, defined below, over $\mathbb{F}_q$, is delegated to Lemma 5.3.

Assume $q \geq 457$ and $f$ is a PR of $\mathbb{P}^1(\mathbb{F}_q)$. We have

$$\frac{f(X)-f(Y)}{X-Y} = \frac{F(X,Y)}{(X^2-u)(X^2-v)},$$

where

$$\begin{aligned} F(X,Y) = {} & -cu^2v - auv^2 + u^2v^2 - du^2X - bv^2X + auvX^2 + cuvX^2 - u^2vX^2 - uv^2X^2 + duX^3 \\ & + bvX^3 + uvX^4 - du^2Y - bv^2Y - cu^2XY - av^2XY + duX^2Y + bvX^2Y + cuX^3Y \\ & + avX^3Y + auvY^2 + cuvY^2 - u^2vY^2 - uv^2Y^2 + duXY^2 + bvXY^2 - auX^2Y^2 + u^2X^2Y^2 \\ & - cvX^2Y^2 + 2uvX^2Y^2 + v^2X^2Y^2 - bX^3Y^2 - dX^3Y^2 - uX^4Y^2 - vX^4Y^2 + duY^3 \\ & + bvY^3 + cuXY^3 + avXY^3 - bX^2Y^3 - dX^2Y^3 - aX^3Y^3 - cX^3Y^3 + uvY^4 - uX^2Y^4 \\ & - vX^2Y^4 + X^4Y^4, \end{aligned} \tag{5.8}$$

and $F(X,Y) = G(X+Y, XY)$, where

$$G(X,Y) = -cu^2v - auv^2 + u^2v^2 - du^2X - bv^2X + auvX^2 + cuvX^2 - u^2vX^2 - uv^2X^2 + duX^3$$

$$+ bvX^3 + uvX^4 - cu^2Y - 2auvY - 2cuvY + 2u^2vY - av^2Y + 2uv^2Y - 2duXY - 2bvXY$$
$$+ cuX^2Y + avX^2Y - 4uvX^2Y - auY^2 - 2cuY^2 + u^2Y^2 - 2avY^2 - cvY^2 + 4uvY^2 + v^2Y^2$$
$$- bXY^2 - dXY^2 - uX^2Y^2 - vX^2Y^2 - aY^3 - cY^3 + 2uY^3 + 2vY^3 + Y^4. \tag{5.9}$$

Suppose $G$ is absolutely irreducible, then by Lemma 5.3, $F(X,Y)$ has an absolutely irreducible factor in $\mathbb{F}_q[X,Y]$. Since $F(X,X) \neq 0$, we have $|V_{\mathbb{F}_q}F(X,X)| \leq 8$. Since $F(X,Y) = X^4Y^4 +$ (terms of lower degree), the number of $\mathbb{F}_q$-rational points at infinity is 2. Let $\hat{F}(X,Y,Z)$ be the homogenization of $F(X,Y)$. Then by Lemma 1.6, we have

$$\begin{aligned} |V_{\mathbb{F}_q^2}(F(X,Y))| + 2 = |V_{\mathbb{P}^2(\mathbb{F}_q)}(\hat{F})| &\geq q + 1 - 2(4-1)(4-1)q^{1/2} - \frac{1}{2}(4-1)(8-1)(8-2) \\ &= q - 18q^{1/2} - 62. \end{aligned}$$

Hence,

$$|V_{\mathbb{F}_q^2}(F(X,Y))| \geq q - 18q^{1/2} - 64 > 8 \geq |V_{\mathbb{F}_q}(F(X,X))|.$$

Thus there exists $(x,y) \in \mathbb{F}_q^2$ with $x \neq y$ such that $F(x,y) = 0$. Therefore $f(X)$ is not a PR of $\mathbb{P}^1(\mathbb{F}_q)$, which is a contradiction.

Suppose $G$ is not absolutely irreducible. Let

$$G_1(X,Y) = G(X, Y - v). \tag{5.10}$$

Then $G_1(X,Y) = h_1 + h_2 + h_3 + h_4$, where $\deg h_i = i$. Let $h(X,Y,Z) = h_1Z^3 + h_2Z^2 + h_3Z + h_4$ be the homogenization of $G_1(X,Y)$. Let $G_2(Y,Z) = h(1,Y,Z)$. We have

$$\begin{aligned} G_2(Y,Z) = (u - Y^2)(v - Y^2) &+ (du + bv + cuY + avY - 2uvY + 2v^2Y - bY^2 - dY^2 - aY^3 \\ &- cY^3 + 2uY^3 - 2vY^3)Z + (u - v)(av - uv + v^2 - 2dY - aY^2 - 2cY^2 + uY^2 \\ &- vY^2)Z^2 - (u - v)^2(d + cY)Z^3. \end{aligned} \tag{5.11}$$

View $G_2$ as a polynomial in $Z$ over $\mathbb{F}_q(Y)$. Since $\deg_Z G_2 = 3$ and the gcd of the coefficients of $G_2$ is 1, $G_2$ has a linear factor in $Z$ over $\overline{\mathbb{F}_q}(Y)$. Suppose $g \in \overline{\mathbb{F}_q}[Y,Z] \setminus \mathbb{F}_q[Y,Z]$ is a linear factor in $Z$ of $G_2$. If $\sigma^2(g) \neq g$, then $G_2 = Ag\sigma(g)\sigma^2(g), A \in \overline{\mathbb{F}_q}$, and $\deg_Y g = \deg_Y \sigma(g) = \deg_Y \sigma^2(g)$. Thus, $3 \deg_Y g = \deg_Y G_2 = 4$, a contradiction. Hence $G_2 = g\sigma(g)g_1$, where $g_1 \in \mathbb{F}_q[Y,Z]$. Therefore $G_2$ has a root $\rho(Y) \in \mathbb{F}_q(Y)$ for $Z$. Since $u - Y^2$ and $v - Y^2$ are irreducible over $\mathbb{F}_q$, we have $\rho(Y) = \phi(Y)/(d + cY)$, where $\phi(Y) \in \mathbb{F}_q[Y], \deg \phi = 2$, and $\phi(Y) \mid (u - Y^2)(v - Y^2)$. If $\phi(Y) = A(Y + u_1)(Y + v_1)$, where $A \in \mathbb{F}_q^*, u_1^2 = u, v_1^2 = v$, then $\sigma(u_1) = v_1 = -u_1$, which is a contradiction since $u \neq v$. Therefore, $\rho(Y) = A(u - Y^2)/(d + cY)$ or $A(v - Y^2)/(d + cY)$, where $A \in \mathbb{F}_q^*$.

**Case 1.** $\rho(Y) = A(u - Y^2)/(d + cY)$. By setting the numerator of $G_2(Y, \rho(Y))$ equal to 0 and comparing the coefficients of $Y^i$, we obtain the following equations.

$$
\begin{aligned}
&- u(-Ad^2u + A^3u^4 - Abdv - d^2v - aA^2u^2v + A^2u^3v - 2A^3u^3v + aA^2uv^2 - 2A^2u^2v^2 \\
&\quad + A^3u^2v^2 + A^2uv^3) = 0, && (5.12)\\
&- u(-2Acdu + 2A^2du^2 - Abcv - aAdv - 2cdv + 2Aduv - 2A^2duv - 2Adv^2) = 0, && (5.13)\\
&- Abdu - d^2u - 2Ad^2u + Ac^2u^2 - aA^2u^3 - 2A^2cu^3 + A^2u^4 + 3A^3u^4 - Abdv - d^2v + aAcuv \\
&\quad + c^2uv - aA^2u^2v - 2Acu^2v + 2A^2cu^2v - 6A^3u^3v + 2aA^2uv^2 + 2Acuv^2 - 3A^2u^2v^2 \\
&\quad + 3A^3u^2v^2 + 2A^2uv^3 = 0, && (5.14)\\
&- Abcu - aAdu - 2cdu - 4Acdu + 2Adu^2 + 4A^2du^2 - Abcv - aAdv - 2cdv - 4A^2duv \\
&\quad - 2Adv^2 = 0, && (5.15)\\
&Abd + d^2 + Ad^2 - aAcu - c^2u - 2Ac^2u + 2aA^2u^2 + 2Acu^2 + 4A^2cu^2 - 2A^2u^3 - 3A^3u^3 \\
&\quad - aAcv - c^2v - aA^2uv - 4A^2cuv + 3A^2u^2v + 6A^3u^2v - aA^2v^2 - 2Acv^2 - 3A^3uv^2 \\
&\quad - A^2v^3 = 0, && (5.16)\\
&Abc + aAd + 2cd + 2Acd - 2Adu - 2A^2du + 2Adv + 2A^2dv = 0, && (5.17)\\
&- (-c + Au - Av)(aA + c + Ac - Au - A^2u + Av + A^2v) = 0. && (5.18)
\end{aligned}
$$

**Case 1.1.** Assume $-c + Au - Av = 0$. Then $A = c/(u - v)$. By (5.17), $c(bc + ad) = 0$. If $c = 0$, then by (5.16), $d = 0$, which is a contradiction. Therefore, $c \neq 0$ and $b = -ad/c$. By (5.16), $(-d^2 + c^2u)(-a + c + u - v) = 0$. But $u$ is not a square in $\mathbb{F}_q$, therefore we must have $a = c + u - v$. Then by (5.14), $-c(d^2 - c^2u) = 0$, whence $u$ is a square in $\mathbb{F}_q$, which is a contradiction.

**Case 1.2.** Assume $-c + Au - Av \neq 0$. Then $A + c + Ac - Au - A^2u + Av + A^2v = 0$. If $A = -1$, then from (5.18), $a(-c - u + v) = 0$, whence $a = 0$. Thus $b \neq 0$. Hence $c = 0$ by (5.17). But by (5.15), $d = 0$, which is a contradiction. Therefore $A \neq -1$, and so $c = (-aA + Au + A^2u - Av - A^2v)/(1 + A)$. Substituting $c$ into (5.17) gives $-A(aAb + ad + aAd - Abu - A^2bu + Abv + A^2bv)/(1 + A) = 0$, whence

$$aAb + ad + aAd - Abu - A^2bu + Abv + A^2bv = 0. \tag{5.19}$$

If $a = 0$, then (5.19) implies $b = 0$, a contradiction. Therefore $a \neq 0$ and solving for $d$ in (5.19) gives $d = -Ab(a - u - Au + v + Av)/(a(1 + A))$. Substituting $c, d$ into (5.13) gives $-2A^3bu(u-v)(-a+u+Au-v-Av)/(1+A)^2 = 0$. If $-a+u+Au-v-Av = 0$, then (5.12) becomes $-A^3u^2(u-v)^3 = 0$, whence $A = 0$, a contradiction. Therefore $-a+u+Au-v-Av \neq 0$ and so $b = 0$. Hence $d = 0$ by (5.3). By (5.12), $A^2u^2(u-v)(-Au^2+av-uv+Auv+v^2) = 0$, hence $a = (Au^2 + uv - Auv - v^2)/v$. By (5.14), $A^3u(u - v)^4(A^2u - v)/((1 + A)^2v^2) = 0$. Therefore $v = A^2u$. We have

$$\begin{aligned} a &= -\frac{(-1 + A)(1 + A)^2u}{A}, \\ b &= d = 0, \\ c &= -(-1 + A)^2(1 + A)u, \\ v &= A^2u. \end{aligned}$$

Substituting these values into (5.5) we obtain $-2(-1+A)A^2(1+A)(1+A^2)(-1-4A+A^2)u^5 = 0$. Since $u \neq v$, we have $A^2 \neq 1$. Thus $(1+A^2)(-1-4A+A^2) = 0$.

**Case 1.2.1** Assume $-1-4A+A^2 = 0$. Then $A = 2+w$, where $w \in \mathbb{F}_q, w^2 = 5$. We have $a = -4u(3+w), b = d = 0, c = -4u(7+3w), v = u(9+4w)$, where $w^2 = 5$.

**Case 1.2.2** Assume $1+A^2 = 0$. Then by (5.6), $512(-3+4A)u^{12} = 0$, whence $A = 3/4$. It follows that $0 = 1+A^2 = 25/16$. Therefore char $\mathbb{F}_q = 5$ and $A = 2$. We have $a = 3u, b = d = 0, c = 2u, v = -u$, which is the same conclusion in Case 1.2.1 with char $\mathbb{F}_q = 5$.

**Case 2.** $\rho(Y) = A(v-Y^2)/(d+cY)$. By setting the numerator of $G_2(Y, \rho(Y))$ equal to 0 and comparing the coefficients of $Y^i$, we obtain the following equations.

$$v(d^2u + Ad^2u + Abdv + aA^2uv^2 - A^2u^2v^2 - A^3u^2v^2 - aA^2v^3 + 2A^2uv^3 + 2A^3uv^3 - A^2v^4 - A^3v^4) = 0, \tag{5.20}$$

$$v(2cdu + 2Acdu + Abcv + aAdv - 2Aduv - 2A^2duv + 2Adv^2 + 2A^2dv^2) = 0, \tag{5.21}$$

$$-d^2u - Ad^2u - 2Abdv - d^2v - Ad^2v + c^2uv + Ac^2uv + aAcv^2 - 3aA^2uv^2 - 2Acuv^2 - 2A^2cuv^2 + 3A^2u^2v^2 + 3A^3u^2v^2 + 3aA^2v^3 + 2Acv^3 + 2A^2cv^3 - 6A^2uv^3 - 6A^3uv^3 + 3A^2v^4 + 3A^3v^4 = 0, \tag{5.22}$$

$$-2(cdu + Acdu + Abcv + aAdv + cdv + Acdv - 2Aduv - 2A^2duv + 2Adv^2 + 2A^2dv^2) = 0, \tag{5.23}$$

$$Abd + d^2 + Ad^2 - c^2u - Ac^2u - 2aAcv - c^2v - Ac^2v + 3aA^2uv + 4Acuv + 4A^2cuv - 3A^2u^2v - 3A^3u^2v - 3aA^2v^2 - 4Acv^2 - 4A^2cv^2 + 6A^2uv^2 + 6A^3uv^2 - 3A^2v^3 - 3A^3v^3 = 0, \tag{5.24}$$

$$Abc + aAd + 2cd + 2Acd - 2Adu - 2A^2du + 2Adv + 2A^2dv = 0, \tag{5.25}$$

$$-(-c + Au - Av)(aA + c + Ac - Au - A^2u + Av + A^2v) = 0. \tag{5.26}$$

**Case 2.1.** Assume $-c + Au - Av = 0$. Then $A = c/(u-v)$. By (5.25), $c(bc+ad) = 0$. If $c = 0$, then (5.24) implies $d = 0$, which is a contradiction. Hence, $c \neq 0$ and so $b = -ad/c$.

Then by (5.23), $-2cd(c+u-v)=0$. Now if $d=0$, then (5.20) implies $c^2v^3(a-c-u+v)=0$, whence $a=c+u-v$. But $b=-ad/c=0$, a contradiction. Therefore $d\neq 0$ and we have $c+u-v=0$. (5.20) then implies $av^2(-d^2+u^2v-2uv^2+v^3)=0$ and we have $v=(u-v)^2/d^2$, contradicting the assumption that $v$ is a non-square element in $\mathbb{F}_q$.

**Case 2.2.** Assume $-c+Au-Av\neq 0$. Then $aA+c+Ac-Au-A^2u+Av+A^2v=0$. If $A=-1$, then (5.25) and (5.26) imply $-bc-ad=0$ and $-a(c+u-v)=0$, respectively. Since $c+u-v\neq 0$, we have $a=0$, whence $c=0$. By (5.24), $bd=0$, which is a contradiction. Therefore $A\neq -1$ and we have $c=(-aA+Au+A^2u-Av-A^2v)/(1+A)$. Replacing $c$ in (5.25) gives

$$-A(aAb+ad+aAd-Abu-A^2bu+Abv+A^2bv)/(1+A)=0. \tag{5.27}$$

If $a=0$, then (5.27) implies $A^2b(u-v)=0$, whence $b=0$, a contradiction. Therefore $a\neq 0$, and solving for $d$ in (5.27) gives $d=(-aAb+Abu+A^2bu-Abv-A^2bv)/(a(1+A))$. Hence (5.21) implies $-2A^2bv(-u+v)(a-u-Au+v+Av)^2)/(a(1+A))=0$. Therefore either $b=0$ or $a-u-Au+v+Av=0$. If $b=0$, then $d=0$, and (5.20) becomes $-A^2v^3(-u+v)(a-u-Au+v+Av)=0$, whence $a=u+Au-v-Av$. But substituting $a$ into $c$ gives $c=(-aA+Au+A^2u-Av-A^2v)/(1+A)=0$, a contradiction. Therefore $b\neq 0$ and $a=u+Au-v-Av$. Replacing $a$ in $d=(-aAb+Abu+A^2bu-Abv-A^2bv)/(a(1+A))$ gives $d=0$, whence $b=0$ by (5.3), which is a contradiction. □

**Lemma 5.2.** *Let $f(X)$ be given in* (5.7). *If $a=-4u(3+w), b=d=0, c=-4u(7+3w)$, and $v=u(9+4w)$, where $w^2=5$, then $f$ is a PR of $\mathbb{P}^1(\mathbb{F}_q)$.*

*Proof.* Let $F(X,Y), G(X,Y), G_1(X,Y), G_2(Y,Z)$ be as in (5.8),(5.9),(5.10),(5.11), respectively. It can be easily verified the $G_2$ has the following factorization in $\overline{\mathbb{F}_q}$:

$$\begin{aligned} G_2(Y,Z) = \big(&-4u(7+3w)YZ-(2+w)(u-Y^2)\big)\big(-16u^2(9+4w)Z^2+4u(1+w)YZ \\ &-2u-uw-2Y^2+wY^2\big). \end{aligned}$$

Since $G_1(X,Y) = \overline{h}(X,Y,1)$ where $\overline{h}(X,Y,Z)$ is the homogenization of $G_2(Y,Z)$, we have

$$G_1(X,Y) = \big(-4u(7+3w)Y - (2+w)(uX^2 - Y^2)\big)\big(-16u^2(9+4w) + 4u(1+w)Y \\ - 2uX^2 - uwX^2 - 2Y^2 + wY^2\big).$$

Since $G(X,Y) = G_1(X, Y - u(9+4w))$, we have

$$G(X,Y) = \big(190u^2 + 85u^2w - 2uX^2 - uwX^2 + 48uY + 22uwY + 2Y^2 + wY^2\big)\big(10u^2 + 5u^2w \\ - 2uX^2 - uwX^2 + 8uY + 6uwY - 2Y^2 + wY^2\big). \tag{5.28}$$

Let $(x,y) \in \mathbb{F}_q^2$ be a root of $G(X,Y)$. We compute $x^2 - 4y$. If $190u^2 + 85u^2w - 2ux^2 - uwx^2 + 48uy + 22uwy + 2y^2 + wy^2 = 0$, then

$$x^2 = (1/u)(190u^2 + 85u^2w + 48uy + 22uwy + 2y^2 + wy^2)(w-2),$$

whence

$$x^2 - 4y = (1/u)(y + u(5+2w))^2.$$

If $10u^2 + 5u^2w - 2ux^2 - uwx^2 + 8uy + 6uwy - 2y^2 + wy^2 = 0$, then

$$x^2 = (1/u)(10u^2 + 5u^2w + 8uy + 6uwy - 2y^2 + wy^2)(w-2),$$

whence

$$x^2 - 4y = (1/u)(y + u(5+2w))^2.$$

Therefore $x^2 - 4y$ is either 0 or a non-square in $\mathbb{F}_q$ since $u$ is a non-square in $\mathbb{F}_q$. By Lemma 1.10, $f$ is a PR of $\mathbb{P}^1(\mathbb{F}_q)$. □

**Lemma 5.3.** *Let $F(X,Y), G(X,Y)$ be given in (5.8), (5.9), respectively. If $G(X,Y)$ is absolutely irreducible, then $F(X,Y)$ has an absolutely irreducible factor in $\mathbb{F}_q[X,Y]$.*

*Proof.* We have

$$\begin{aligned}F(X,Y) = &-uv(cu+av-uv)-(du^2+bv^2)(X+Y)+auvX^2+cuvX^2-u^2vX^2-uv^2X^2\\ &-cu^2XY-av^2XY+auvY^2+cuvY^2-u^2vY^2-uv^2Y^2+(du+bv)(X+Y)(X^2+Y^2)\\ &+uvX^4+cuX^3Y+avX^3Y-auX^2Y^2+u^2X^2Y^2-cvX^2Y^2+2uvX^2Y^2+v^2X^2Y^2\\ &+cuXY^3+avXY^3+uvY^4-(b+d)X^2Y^2(X+Y)-X^2Y^2(uX^2+vX^2+aXY\\ &+cXY+uY^2+vY^2)+X^4Y^4.\end{aligned}$$

As in the proof of Lemma 4.5, it follows that $F(X,Y) = H(X,Y)H(Y,X)$, and $H(X,Y) = h_0+h_1+h_2+h_3+h_4$ is given by

$$\begin{aligned}h_0^2(X,Y) &= -uv(cu+av-uv),\\ h_1(X,Y) &= A_1X+A_2Y,\\ h_2(X,Y) &= B_1X^2+BXY+B_2Y^2,\\ h_3(X,Y) &= CXY(X-Y),\\ h_4(X,Y) &= X^2Y^2.\end{aligned}$$

where $A_2 = A_1^q, B_2 = B_1^q, B \in \mathbb{F}_q$, and $C^q = -C$. Comparing the coefficients of $X^iY^j$ in the equation $F(X,Y) = H(X,Y)H(Y,X)$, we get the following.

$$h_0^2 + cu^2v + auv^2 - u^2v^2 = 0, \tag{5.29}$$

$$A_1h_0 + A_2h_0 + du^2 + bv^2 = 0, \tag{5.30}$$

$$A_1^2 + A_2^2 + 2Bh_0 + cu^2 + av^2 = 0, \tag{5.31}$$

$$A_1A_2 + B_1h_0 + B_2h_0 - auv - cuv + u^2v + uv^2 = 0, \tag{5.32}$$

$$A_1B + A_2B + A_1B_1 + A_2B_2 - du - bv = 0, \tag{5.33}$$

$$B^2 + B_1^2 + B_2^2 + 2A_1C - 2A_2C + 2h_0 + au - u^2 + cv - 2uv - v^2 = 0, \tag{5.34}$$

$$A_2B_1 + A_1B_2 - du - bv = 0, \tag{5.35}$$

$$BB_1 + BB_2 - A_1C + A_2C - cu - av = 0, \tag{5.36}$$

$$A_1 + A_2 + b + B_1C - B_2C + d = 0, \tag{5.37}$$

$$a + 2B + c + 2C^2 = 0, \tag{5.38}$$

$$B_1B_2 - uv = 0, \tag{5.39}$$

$$-(B_1 - B_2)C = 0, \tag{5.40}$$

$$B_1 + B_2 - C^2 + u + v = 0. \tag{5.41}$$

From (5.40), either $C = 0$ or $B_1 = B_2$. If $C = 0$, then $B_2 = -B_1 - u - v$ by (5.41), whence (5.39) becomes $-(B_1+u)(B_1+v) = 0$. If $B_1 = -u$, then $B_2 = -v$. But $-v = B_2 = B_1^q = -u$, which is a contradiction. Similarly, if $B_1 = -v$, we also get a contradiction. Therefore, $C \neq 0$ and $B_1 = B_2$. Equations (5.37), (5.38) become

$$A_2 = -A_1 - b - d, \tag{5.42}$$

$$B = (-a - c - 2C^2)/2. \tag{5.43}$$

Let $u = u_1^2, v = v_1^2$. Then by (5.39) and (5.41) we have

$$B_1 = u_1v_1, \tag{5.44}$$

$$C^2 = (u_1 + v_1)^2, \tag{5.45}$$

and by (5.35), (5.42) and (5.44) we have $-(u_1 + v_1)(du_1 + bv_1) = 0$, whence

$$d = -bv_1/u_1. \tag{5.46}$$

Solving for $A_1$ in (5.36) using (5.42), (5.43) gives

$$A_1 = (-bC - Cd - cu_1^2 - au_1v_1 - cu_1v_1 - 2C^2u_1v_1 - av_1^2)/(2C). \tag{5.47}$$

Using (5.42), (5.45), (5.47) and solving for $h_0$ in (5.34) we get

$$h_0 = (1/8)(-a^2 - 2ac - c^2 - 8au_1^2 + 4cu_1^2 + 4av_1^2 - 8cv_1^2 + 8u_1^2v_1^2). \tag{5.48}$$

Therefore (5.29), (5.30), (5.31), (5.32), (5.33) become

$$\begin{aligned} &a^4 + 4a^3c + 6a^2c^2 + 4ac^3 + c^4 + 16a^3u_1^2 + 24a^2cu_1^2 - 8c^3u_1^2 + 64a^2u_1^4 - 64acu_1^4 + 16c^2u_1^4 \\ &\quad - 8a^3v_1^2 + 24ac^2v_1^2 + 16c^3v_1^2 - 80a^2u_1^2v_1^2 + 128acu_1^2v_1^2 - 80c^2u_1^2v_1^2 - 128au_1^4v_1^2 \\ &\quad + 128cu_1^4v_1^2 + 16a^2v_1^4 - 64acv_1^4 + 64c^2v_1^4 + 128au_1^2v_1^4 - 128cu_1^2v_1^4 = 0, \end{aligned} \tag{5.49}$$

$$b(u_1 - v_1)(a^2 + 2ac + c^2 + 8au_1^2 - 4cu_1^2 - 8u_1^3v_1 - 4av_1^2 + 8cv_1^2 - 16u_1^2v_1^2 - 8u_1v_1^3) = 0, \tag{5.50}$$

$$\begin{aligned} &a^3u_1^2 + 4b^2u_1^2 + 3a^2cu_1^2 + 3ac^2u_1^2 + c^3u_1^2 + 10a^2u_1^4 + 8acu_1^4 + 2c^2u_1^4 + 16au_1^6 - 8b^2u_1v_1 \\ &\quad + 4a^2u_1^3v_1 + 16acu_1^3v_1 + 4c^2u_1^3v_1 + 32au_1^5v_1 + 4b^2v_1^2 + 2a^2u_1^2v_1^2 + 8acu_1^2v_1^2 + 10c^2u_1^2v_1^2 \\ &\quad + 16au_1^4v_1^2 + 16cu_1^4v_1^2 + 32cu_1^3v_1^3 + 16cu_1^2v_1^4 = 0, \end{aligned} \tag{5.51}$$

$$\begin{aligned} &b^2u_1^2 - c^2u_1^4 - 2b^2u_1v_1 - a^2u_1^3v_1 - 4acu_1^3v_1 - c^2u_1^3v_1 - 8au_1^5v1 + b^2v_1^2 - a^2u_1^2v_1^2 - 8au_1^4v_1^2 \\ &\quad - 8cu_1^4v_1^2 - 8cu_1^3v_1^3 = 0, \end{aligned} \tag{5.52}$$

$$b(u_1 - v_1)(a + c + 2u_1^2 + 4u_1v_1 + 2v_1^2) = 0. \tag{5.53}$$

By (5.53) either $b = 0$ or $a + c + 2u_1^2 + 4u_1v_1 + 2v_1^2 = 0$.

**Case 1.** Assume $b = 0$. Then $d = 0$ by (5.46) so (5.49), (5.51), (5.52) imply $L_1 = L_2 = L_3 = 0$, where

$$L_1 = -c^2u_1^2 - a^2u_1v_1 - 4acu_1v_1 - c^2u_1v_1 - 8au_1^3v_1 - a^2v_1^2 - 8au_1^2v_1^2 - 8cu_1^2v_1^2 - 8cu_1v_1^3, \tag{5.54}$$

$$\begin{aligned} L_2 = {} & a^3 + 3a^2c + 3ac^2 + c^3 + 10a^2u_1^2 + 8acu_1^2 + 2c^2u_1^2 + 16au_1^4 + 4a^2u_1v_1 + 16acu_1v_1 + 4c^2u_1v_1 \\ & + 32au_1^3v_1 + 2a^2v_1^2 + 8acv_1^2 + 10c^2v_1^2 + 16au_1^2v_1^2 + 16cu_1^2v_1^2 + 32cu_1v_1^3 + 16cv_1^4, \end{aligned} \tag{5.55}$$

$$L_3 = a^4 + 4a^3c + 6a^2c^2 + 4ac^3 + c^4 + 16a^3u_1^2 + 24a^2cu_1^2 - 8c^3u_1^2 + 64a^2u_1^4 - 64acu_1^4 + 16c^2u_1^4$$

$$- 8a^3v_1^2 + 24ac^2v_1^2 + 16c^3v_1^2 - 80a^2u_1^2v_1^2 + 128acu_1^2v_1^2 - 80c^2u_1^2v_1^2 - 128au_1^4v_1^2 + 128cu_1^4v_1^2$$
$$+ 16a^2v_1^4 - 64acv_1^4 + 64c^2v_1^4 + 128au_1^2v_1^4 - 128cu_1^2v_1^4. \tag{5.56}$$

Let

$$\begin{aligned} L_4 &= L_2 + 4L_1 \\ &= a^3 + 3a^2c + 3ac^2 + c^3 + 10a^2u_1^2 + 8acu_1^2 - 2c^2u_1^2 + 16au_1^4 - 2a^2v_1^2 + 8acv_1^2 + 10c^2v_1^2 \\ &\quad - 16au_1^2v_1^2 - 16cu_1^2v_1^2 + 16cv_1^4. \end{aligned} \tag{5.57}$$

We have

$$\mathrm{Res}(L_3, L_4; c) = 4096a^2(a + 8u_1^2)(u_1 - v_1)^4(u_1 + v_1)^4M_1, \tag{5.58}$$
$$\mathrm{Res}(L_1, L_2; c) = -a^2(a + 8u_1^2)(u_1 - v_1)^3M_2, \tag{5.59}$$
$$\mathrm{Res}(L_1, L_3; c) = a^2(a + 8u_1^2)(u_1 - v_1)^3M_3, \tag{5.60}$$
$$\mathrm{Res}(L_2, L_4; c) = 256a^2(a + 8u_1^2)(u_1 - v_1)^3M_4, \tag{5.61}$$

where

$$M_1 = au_1^8 + 8u_1^{10} + 28au_1^6v_1^2 + 32u_1^8v_1^2 + 198au_1^4v_1^4 - 16u_1^6v_1^4 + 28au_1^2v_1^6 - 96u_1^4v_1^6 + av_1^8 + 72u_1^2v_1^8,$$
$$\begin{aligned} M_2 &= a^3u_1^3 + 12a^2u_1^5 + 36au_1^7 + 32u_1^9 - 3a^3u_1^2v_1 + 8a^2u_1^4v_1 + 160au_1^6v_1 + 256u_1^8v_1 + 3a^3u_1v_1^2 \\ &\quad - 32a^2u_1^3v_1^2 + 196au_1^5v_1^2 + 800u_1^7v_1^2 - a^3v_1^3 - 8a^2u_1^2v_1^3 - 64au_1^4v_1^3 + 1152u_1^6v_1^3 + 20a^2u_1v_1^4 \\ &\quad - 244au_1^3v_1^4 + 608u_1^5v_1^4 - 96au_1^2v_1^5 - 256u_1^4v_1^5 + 12au_1v_1^6 - 416u_1^3v_1^6 - 128u_1^2v_1^7, \end{aligned}$$
$$\begin{aligned} M_3 &= a^5u_1^5 + 24a^4u_1^7 + 192a^3u_1^9 + 512a^2u_1^{11} - 5a^5u_1^4v_1 - 56a^4u_1^6v_1 + 96a^3u_1^8v_1 + 2048a^2u_1^{10}v_1 \\ &\quad + 2048au_1^{12}v_1 + 10a^5u_1^3v_1^2 - 832a^3u_1^7v_1^2 + 12544au_1^{11}v_1^2 + 2048u_1^{13}v_1^2 - 10a^5u_1^2v_1^3 + 80a^4u_1^4v_1^3 \\ &\quad + 96a^3u_1^6v_1^3 - 6400a^2u_1^8v_1^3 + 25856au_1^{10}v_1^3 + 10240u_1^{12}v_1^3 + 5a^5u_1v_1^4 - 40a^4u_1^3v_1^4 + 832a^3u_1^5v_1^4 \\ &\quad - 2304a^2u_1^7v_1^4 + 16640au_1^9v_1^4 + 10240u_1^{11}v_1^4 - a^5v_1^5 - 24a^4u_1^2v_1^5 - 224a^3u_1^4v_1^5 + 6656a^2u_1^6v_1^5 \end{aligned}$$

$$
\begin{aligned}
&- 11008au_1^8v_1^5 - 30720u_1^{10}v_1^5 + 16a^4u_1v_1^6 - 192a^3u_1^3v_1^6 + 2560a^2u_1^5v_1^6 - 21760au_1^7v_1^6 \\
&- 92160u_1^9v_1^6 + 32a^3u_1^2v_1^7 - 2304a^2u_1^4v_1^7 - 14592au_1^6v_1^7 - 100352u_1^8v_1^7 - 768a^2u_1^3v_1^8 \\
&- 7424au_1^5v_1^8 - 51200u_1^7v_1^8 - 2304au_1^4v_1^9 - 10240u_1^6v_1^9, \\
M_4 = {} & a^5u_1^5+16a^4u_1^7+104a^3u_1^9+416a^2u_1^{11}+912au_1^{13}+1152u_1^{15}-5a^5u_1^4v_1-32a^4u_1^6v_1+216a^3u_1^8v_1 \\
&+ 1952a^2u_1^{10}v_1 + 7088au_1^{12}v_1 + 9600u_1^{14}v_1 + 10a^5u_1^3v_1^2-24a^4u_1^5v_1^2-176a^3u_1^7v_1^2+1056a^2u_1^9v_1^2 \\
&+ 17184au_1^{11}v_1^2 + 34048u_1^{13}v_1^2 - 10a^5u_1^2v_1^3 + 88a^4u_1^4v_1^3 - 1008a^3u_1^6v_1^3 - 3872a^2u_1^8v_1^3 \\
&+ 14944au_1^{10}v_1^3 + 64256u_1^{12}v_1^3 + 5a^5u_1v_1^4-32a^4u_1^3v_1^4 + 416a^3u_1^5v_1^4-5568a^2u_1^7v_1^4 - 720au_1^9v_1^4 \\
&+ 74112u_1^{11}v_1^4 - a^5v_1^5 - 48a^4u_1^2v_1^5 + 1088a^3u_1^4v_1^5 + 704a^2u_1^6v_1^5 - 15728au_1^8v_1^5 + 59520u_1^{10}v_1^5 \\
&+ 40a^4u_1v_1^6 - 464a^3u_1^3v_1^6 + 6464a^2u_1^5v_1^6 - 17984au_1^7v_1^6 + 32256u_1^9v_1^6 - 8a^4v_1^7 - 272a^3u_1^2v_1^7 \\
&+ 2368a^2u_1^4v_1^7-2752au_1^6v_1^7 + 4608u_1^8v_1^7 + 120a^3u_1v_1^8-2528a^2u_1^3v_1^8 + 5872au_1^5v_1^8-6272u_1^7v_1^8 \\
&- 24a^3v_1^9 - 1120a^2u_1^2v_1^9 - 1584au_1^4v_1^9 - 2432u_1^6v_1^9 + 160a^2u_1v_1^{10} - 5344au_1^3v_1^{10} - 768u_1^5v_1^{10} \\
&- 32a^2v_1^{11}-1952au_1^2v_1^{11}-3328u_1^4v_1^{11}+80au_1v_1^{12}-3456u_1^3v_1^{12}-16av_1^{13}-1152u_1^2v_1^{13}.
\end{aligned}
$$

**Case 1.1.** Assume $a+8u_1^2=0$. Then by (5.54), $-cu_1(cu_1+cv_1-32u_1^2v_1+8u_1v_1^2+8v_1^3)=0$. Since $d=0$, we have $c\neq 0$, whence $c=8v_1(4u_1^2-u_1v_1-v_1^2)/(u_1+v_1)$. Therefore (5.55), (5.56) imply

$$512u_1^2(u_1-v_1)v_1(4u_1^2-u_1v_1-v_1^2)(2u_1^3-7u_1^2v_1+v_1^3)=0, \tag{5.62}$$

$$4096u_1^4(u_1-v_1)v_1^2(4u_1^2-u_1v_1-v_1^2)(25u_1^3-13u_1^2v_1-5u_1v_1^2+v_1^3)=0. \tag{5.63}$$

Note that $4u_1^2-u_1v_1-v_1^2\neq 0$ since $c\neq 0$. Therefore

$$2u_1^3-7u_1^2v_1+v_1^3=0, \tag{5.64}$$

$$25u_1^3-13u_1^2v_1-5u_1v_1^2+v_1^3=0. \tag{5.65}$$

Computing the resultant of (5.64),(5.65) with respect to $u_1$ gives $-512v_1^9 = 0$, which is a contradiction.

**Case 1.2.** Assume $a + 8u_1^2 \neq 0$. Since $b = 0$, we have $a \neq 0$. Hence by (5.58) − (5.61), we have $M_1 = M_2 = M_3 = M_4 = 0$. Now

$$\mathrm{Res}(M_1, M_2; a) = 128u_1^2v_1(u_1 + v_1)^6(u_1^4 - 18u_1^2v_1^2 + v_1^4)N_1, \tag{5.66}$$

$$\mathrm{Res}(M_2, M_3; a) = -8388608u_1^{10}(u_1 - v_1)^{15}v_1^3(u_1 + v_1)^{15}(u_1^4 - 18u_1^2v_1^2 + v_1^4)N_2, \tag{5.67}$$

$$\mathrm{Res}(M_2, M_4; a) = -524288u_1^2(u_1 - v_1)^{15}v_1(u_1 + v_1)^{13}(u_1^4 - 18u_1^2v_1^2 + v_1^4)N_3, \tag{5.68}$$

where

$$\begin{aligned}
N_1 &= 8u_1^{20} - 28u_1^{19}v_1 + 61u_1^{18}v_1^2 - 628u_1^{17}v_1^3 - 1465u_1^{16}v_1^4 - 6656u_1^{15}v_1^5 - 20604u_1^{14}v_1^6 - 36448u_1^{13}v_1^7 \\
&\quad - 96820u_1^{12}v_1^8 - 56472u_1^{11}v_1^9 - 178698u_1^{10}v_1^{10} + 120344u_1^9v_1^{11} + 16434u_1^8v_1^{12} - 19040u_1^7v_1^{13} \\
&\quad + 18772u_1^6v_1^{14} - 1344u_1^5v_1^{15} + 180u_1^4v_1^{16} + 276u_1^3v_1^{17} - 11u_1^2v_1^{18} - 4u_1v_1^{19} - v_1^{20}, \\
N_2 &= 392u_1^{13} + 3083u_1^{12}v_1 + 3964u_1^{11}v_1^2 - 41646u_1^{10}v_1^3 - 216852u_1^9v_1^4 - 454895u_1^8v_1^5 - 432104u_1^7v_1^6 \\
&\quad - 78868u_1^6v_1^7 + 138592u_1^5v_1^8 + 47357u_1^4v_1^9 - 19796u_1^3v_1^{10} - 3294u_1^2v_1^{11} + 1516u_1v_1^{12} - 121v_1^{13}, \\
N_3 &= 15488u_1^{25} + 71104u_1^{24}v_1 - 458064u_1^{23}v_1^2 - 6922192u_1^{22}v_1^3 - 44051424u_1^{21}v_1^4 - 184156420u_1^{20}v_1^5 \\
&\quad - 543588777u_1^{19}v_1^6 - 1149458273u_1^{18}v_1^7 - 1733476245u_1^{17}v_1^8 - 1812491081u_1^{16}v_1^9 \\
&\quad - 1199148100u_1^{15}v_1^{10} - 313343860u_1^{14}v_1^{11} + 262844732u_1^{13}v_1^{12} + 375112356u_1^{12}v_1^{13} \\
&\quad + 251346002u_1^{11}v_1^{14} + 118934322u_1^{10}v_1^{15} + 45906554u_1^9v_1^{16} + 15630370u_1^8v_1^{17} + 4705052u_1^7v_1^{18} \\
&\quad + 1181004u_1^6v_1^{19} + 228684u_1^5v_1^{20} + 31176u_1^4v_1^{21} + 2511u_1^3v_1^{22} + 39u_1^2v_1^{23} - 13u_1v_1^{24} - v_1^{25}.
\end{aligned}$$

**Case 1.2.1.** Assume $u_1^4 - 18u_1^2v_1^2 + v_1^4 \neq 0$, then by (5.66)−(5.68), $N_1 = N_2 = N_3 = 0$. Now

$$\begin{aligned}
\mathrm{Res}(N_1, N_2; u_1) &= (2^{243})(17)(1531)(428251)(1643867)(389734167619) \\
&\quad (1074932332649424741960607 87)v_1^{260},
\end{aligned}$$

$$\mathrm{Res}(N_2, N_3; u_1) = (2^{247})(1667)(13716649)(25799351)(283014359)(35375129563)$$
$$(1944177462643649)(19445282751402604082227845826188610789427951 3)v_1^{325},$$

where the coefficients on the right hand side are written as a product of primes. Therefore we get a contradiction.

**Case 1.2.2.** Assume $u_1^4 - 18u_1^2v_1^2 + v_1^4 = 0$. Since $u^2 - 18uv + v^2 = 0$, we have $u^2 + 14uv + v^2 \neq 0$, otherwise $32uv = 0$ gives a contradiction. Therefore, solving for $a$ in the equation $M_1 = 0$, we get $a = -8u(u^2 + 2uv - 3v^2)^2/(u^2 + 14uv + v^2)^2$. Now since $u^2 - 18uv + v^2 = 0$, we have $v = u(9 + 4w)$, where $w^2 = 5$. Hence $a = -4u(3 + w)$. Now

$$\mathrm{Res}(L_3, L_4; a) = 4096c^2(u-v)^4(c+8v)(cu^4 + 28cu^3v + 72u^4v + 198cu^2v^2 - 96u^3v^2 + 28cuv^3$$
$$- 16u^2v^3 + cv^4 + 32uv^4 + 8v^5). \tag{5.69}$$

**Case 1.2.2.1.** Assume $c + 8v = 0$. Then by replacing $a, c$ in (5.54)$-$(5.56) we obtain the equations $-64u_1^3v_1K_1 = 0,\ -128u_1^2K_2 = 0,\ 1024u_1^4K_3 = 0$, where

$K_1 = 2u_1^2 + 2u_1v_1 + 6v_1^2 + u_1^2w + u_1v_1w + 2v_1^2w,$
$K_2 = 20u_1^4 - 4u_1^3v_1 + 34u_1^2v_1^2 - 12u_1v_1^3 + 12v_1^4 + 9u_1^4w - 2u_1^3v_1w + 15u_1^2v_1^2w - 4u_1v_1^3w + 4v_1^4w,$
$K_3 = 36u_1^4 + 116u_1^2v_1^2 + 98v_1^4 + 16u_1^4w + 53u_1^2v_1^2w + 41v_1^4w.$

We have

$$\mathrm{Res}(K_1, K_2; u_1) = 32v_1^8(95015 + 42492w),$$
$$\mathrm{Res}(K_2, u_1^4 - 18u_1^2v_1^2 + v_1^4; u_1) = 8192v_1^{16}(7207317 + 3223210w).$$

Hence $95015 + 42492w = 7207317 + 3223210w = 0$. Since $\gcd(95015, 42492) = \gcd(7207317, 3223210) = 1$, char $\mathbb{F}_q$ does not divide 42492 and 3223210. Since $w^2 = 5$,

we have

$$\left(-\frac{95015}{42492}\right)^2 - 5 = -\frac{(5)(19)}{42492^2} = 0,$$
$$\left(-\frac{7207317}{3223210}\right)^2 - 5 = \frac{(11)(31)(71)(199)}{3223210^2} = 0,$$

which is a contradiction.

**Case 1.2.2.2.** Assume $c + 8v \neq 0$. Since $d = 0$, we have $c \neq 0$. By (5.69),

$$cu^4 + 28cu^3v + 72u^4v + 198cu^2v^2 - 96u^3v^2 + 28cuv^3 - 16u^2v^3 + cv^4 + 32uv^4 + 8v^5 = 0. \tag{5.70}$$

We have seen that $u^2 + 14uv + v^2 \neq 0$, hence solving for $c$ in (5.70) gives $c = -8v(-3u^2 + 2uv + v^2)^2/(u^2 + 14uv + v^2)^2$. Since $v = u(9 + 4w)$, where $w^2 = 5$, we have $c = -4u(7 + 3w)$. But in the proof of Lemma 5.2, (5.28) gives a factorization of $G(X, Y)$. Hence $G(X, Y)$ is not absolutely irreducible, contradicting our assumption that $G(X, Y)$ is absolutely irreducible.

**Case 2.** Assume $b \neq 0$. Then $c = -a - 2u_1^2 - 4u_1v_1 - 2v_1^2$ and (5.49)−(5.51) become

$$16(u_1 - v_1)(u_1 + v_1)(a + u_1^2 + 2u_1v_1 + v_1^2)J_1 = 0, \tag{5.71}$$
$$12b(u_1 - v_1)^2(u_1 + v_1)(a + u_1^2 + 2u_1v_1 + v_1^2) = 0, \tag{5.72}$$
$$4(u_1 - v_1)^2J_2 = 0, \tag{5.73}$$

where

$$J_1 = 9au_1^2 + 9u_1^4 + 30u_1^3v_1 - 9av_1^2 + 8u_1^2v_1^2 - 6u_1v_1^3 - 9v_1^4, \tag{5.74}$$
$$J_2 = b^2 + a^2u_1^2 + 2au_1^4 + 4au_1^3v_1 + 2au_1^2v_1^2. \tag{5.75}$$

**Case 2.1.** Assume $a + u_1^2 + 2u_1v_1 + v_1^2 = 0$. By (5.73), $J_2 = 0$, and substituting $a$ into this equation we get

$$(b - u_1^3 - 2u_1^2v_1 - u_1v_1^2)(b + u_1^3 + 2u_1^2v_1 + u_1v_1^2) = 0.$$

Thus, $b = \pm u_1(u_1 + v_1)^2$. Now $c = -a - 2u_1^2 - 4u_1v_1 - 2v_1^2$ implies $c + a = -2(u_1 + v_1)^2$, whence $(u_1 + v_1)^2 \in \mathbb{F}_q$. But $u_1 \notin \mathbb{F}_q$, therefore $b \notin \mathbb{F}_q$ gives a contradiction.

**Case 2.2.** Assume $a + u_1^2 + 2u_1v_1 + v_1^2 \neq 0$. Then by (5.72), $12 = 0$, whence $\mathrm{char}\ \mathbb{F}_q = 3$. Now by (5.71), $J_1 = 0$. Hence, $2u_1^2v_1^2 = 0$, which is a contradiction. □

## 5.2 Case IV, $q$ Even

Assume $q$ is even and let

$$f(X) = X + \frac{aX + b}{X^2 + X + u} + \frac{cX + d}{X^2 + X + v},$$

where $a, b, c, d, u, v \in \mathbb{F}_q, (a, b) \neq (0, 0), (c, d) \neq (0, 0), u \neq v, \mathrm{Tr}_{q/2}(u) = \mathrm{Tr}_{q/2}(v) = 1$.

Suppose $f$ is a PR of $\mathbb{P}^1(\mathbb{F}_q)$. We will be using the power sum conditions $s(f, k) = 0$, for $k = 1, 3, 5, 7$. We have $s(f, 1) = a + c$. Hence, if $q \geq 3$, then

$$c = a. \tag{5.76}$$

Setting $c = a$ in $s(f, k)$ for $k = 3, 5, 7$, we obtain the following conditions. If $q \geq 5$, then

$$a^2b + ab^2 + a^2d + ad^2 + a^3u + bu + b^2u + du + d^2u + au^2 + a^2u^2 + a^3v + bv + b^2v + dv + d^2v + av^2 + a^2v^2 = 0. \tag{5.77}$$

If $q \geq 7$, then

$$a^4b + ab^4 + a^4d + ad^4 + a^5u + a^5u^2 + a^4bu^2 + ab^4u^2 + a^4du^2 + ad^4u^2 + a^5u^3 + bu^3 + b^4u^3 + du^3 + d^4u^3 + au^4 + a^4u^4 + a^5u^4 + au^5 + a^4u^5 + a^5v + a^5u^2v + bu^2v + b^4u^2v + du^2v + d^4u^2v + au^4v + a^4u^4v + a^5v^2 + a^4bv^2 + ab^4v^2 + a^4dv^2 + ad^4v^2 + a^5uv^2 + buv^2 + b^4uv^2 + duv^2 + d^4uv^2 + a^5v^3 + bv^3 + b^4v^3 + dv^3 + d^4v^3 + av^4 + a^4v^4 + a^5v^4 + auv^4 + a^4uv^4 + av^5 + a^4v^5 = 0. \quad (5.78)$$

If $q \geq 9$, then

$$a^2b^5 + ab^6 + a^2b^4d + \cdots + a^4v^8 = 0. \quad (5.79)$$

The entirety of (5.79) is given in Appendix C.

**Theorem 5.4.** *Let $q$ be even and*

$$f(X) = X + \frac{aX + b}{X^2 + X + u} + \frac{cX + d}{X^2 + X + v}, \quad (5.80)$$

*where $a, b, c, d, u, v \in \mathbb{F}_q, (a, b) \neq (0, 0), (c, d) \neq (0, 0), u \neq v, \mathrm{Tr}_{q/2}(u) = \mathrm{Tr}_{q/2}(v) = 1$. If $q \geq 2^9$, then $f$ is a PR of $\mathbb{P}^1(\mathbb{F}_q)$ if and only if $a = c = 0, b^2 + b + 1 = 0, d = b + 1, v = u + 1$. The condition is sufficient for all $q$.*

*Proof.* We prove the necessity here. The proof for the sufficiency is given in the lemma that follows after this theorem.

Suppose $q \geq 2^9$ and $f$ is a PR of $\mathbb{P}^1(\mathbb{F}_q)$. Using (5.76), we have

$$\frac{f(X) - f(Y)}{X - Y} = \frac{F(X, Y)}{(X^2 + X + u)(X^2 + X + v)(Y^2 + Y + u)(Y^2 + Y + v)},$$

where

$$F(X, Y) = du^2 + au^2v + bv^2 + auv^2 + u^2v^2 + duX + du^2X + bvX + u^2vX + bv^2X + uv^2X$$

$$
\begin{aligned}
&+ uvX^2 + u^2vX^2 + uv^2X^2 + duX^3 + bvX^3 + uvX^4 + duY + du^2Y + bvY + u^2vY \\
&+bv^2Y + uv^2Y + bXY + dXY + auXY + u^2XY + au^2XY + avXY + v^2XY + av^2XY \\
&+ uX^2Y + duX^2Y + u^2X^2Y + vX^2Y + bvX^2Y + v^2X^2Y + bX^3Y + dX^3Y + auX^3Y \\
&+ avX^3Y + uX^4Y + vX^4Y + uvY^2 + u^2vY^2 + uv^2Y^2 + uXY^2 + duXY^2 + u^2XY^2 \\
&+ vXY^2 + bvXY^2 + v^2XY^2 + X^2Y^2 + bX^2Y^2 + dX^2Y^2 + auX^2Y^2 + u^2X^2Y^2 + avX^2Y^2 \\
&+ v^2X^2Y^2 + bX^3Y^2 + dX^3Y^2 + X^4Y^2 + uX^4Y^2 + vX^4Y^2 + duY^3 + bvY^3 + bXY^3 \\
&+ dXY^3 + auXY^3 + avXY^3 + bX^2Y^3 + dX^2Y^3 + uvY^4 + uXY^4 + vXY^4 + X^2Y^4 \\
&+ uX^2Y^4 + vX^2Y^4 + X^4Y^4, \qquad (5.81)
\end{aligned}
$$

and $F(X,Y) = G(X+Y, XY)$, where

$$
\begin{aligned}
G(X,Y) = {} & du^2 + au^2v + bv^2 + auv^2 + u^2v^2 + duX + du^2X + bvX + u^2vX + bv^2X + uv^2X \\
&+ uvX^2 + u^2vX^2 + uv^2X^2 + duX^3 + bvX^3 + uvX^4 + bY + dY + auY + u^2Y + au^2Y \\
&+ avY + v^2Y + av^2Y + uXY + u^2XY + vXY + v^2XY + bX^2Y + dX^2Y + auX^2Y \\
&+ avX^2Y + uX^3Y + vX^3Y + Y^2 + bY^2 + dY^2 + auY^2 + u^2Y^2 + avY^2 + v^2Y^2 + bXY^2 \\
&+ dXY^2 + uXY^2 + vXY^2 + X^2Y^2 + uX^2Y^2 + vX^2Y^2 + Y^4. \qquad (5.82)
\end{aligned}
$$

Suppose $G$ is absolutely irreducible. Then by Lemma 5.6, $F(X,Y)$ has an absolutely irreducible factor in $\mathbb{F}_q[X,Y]$. Since $F(X,X) \neq 0$, we have $|V_{\mathbb{F}_q}F(X,X)| \leq 8$. Since $F(X,Y) = X^4Y^4 +$ (terms of lower degree), the number of $\mathbb{F}_q$-rational points at infinity is 2. Let $\hat{F}(X,Y,Z)$ be the homogenization of $F(X,Y)$. Then by Lemma 1.6, we have

$$
\begin{aligned}
|V_{\mathbb{F}_q^2}(F(X,Y))| + 2 = |V_{\mathbb{P}^2(\mathbb{F}_q)}(\hat{F})| &\geq q + 1 - 2(4-1)(4-1)q^{1/2} - \frac{1}{2}(4-1)(8-1)(8-2) \\
&= q - 18q^{1/2} - 62.
\end{aligned}
$$

Hence,

$$|V_{\mathbb{F}_q^2}(F(X,Y))| \geq q - 18q^{1/2} - 64 > 8 \geq |V_{\mathbb{F}_q}(F(X,X))|.$$

Thus there exists $(x,y) \in \mathbb{F}_q^2$ with $x \neq y$ such that $F(x,y) = 0$. Therefore $f(X)$ is not a PR of $\mathbb{P}^1(\mathbb{F}_q)$, which is a contradiction.

Suppose $G$ is not absolutely irreducible. Let

$$G_1(X,Y) = G(X+1, Y+u). \tag{5.83}$$

Then

$$\begin{aligned} G_1(X,Y) = (u+v)^2(bX+aY) + (u+v)(bX^2+auX^2+u^2X^2+uvX^2+uXY+vXY+aY^2+uY^2 \\ + vY^2) + X(duX^2+u^2X^2+bvX^2+uvX^2+bXY+dXY+uXY+auXY+vXY \\ + avXY + bY^2 + dY^2 + uY^2 + vY^2) + (uX^2+XY+Y^2)(vX^2+XY+Y^2). \end{aligned}$$

Let $h(X,Y,Z)$ be the homogenization of $G_1(X,Y)$, and let $G_2(Y,Z) = h(1,Y,Z)$. We have

$$\begin{aligned} G_2 = (u+Y+Y^2)(v+Y+Y^2) + (du+u^2+bv+uv+bY+dY+uY+auY+vY+avY \\ + bY^2+dY^2+uY^2+vY^2)Z + (u+v)(b+au+u^2+uv+uY+vY+aY^2+uY^2+vY^2)Z^2 \\ + (u+v)^2(b+aY)Z^3. \end{aligned} \tag{5.84}$$

View $G_2$ as a polynomial in $Z$ over $\mathbb{F}_q(Y)$. Since $\deg_Z G_2 = 3$ and the gcd of the coefficients of $G_2$ is 1, $G_2$ has a linear factor in $Z$ over $\overline{\mathbb{F}_q}(Y)$. Suppose $g \in \overline{\mathbb{F}_q}[Y,Z] \setminus \mathbb{F}_q[Y,Z]$ is a linear factor in $Z$ of $G_2$. If $\sigma^2(g) \neq g$, then $G_2 = Ag\sigma(g)\sigma^2(g), A \in \overline{\mathbb{F}_q}$, and $\deg_Y g = \deg_Y \sigma(g) = \deg_Y \sigma^2(g)$. Thus, $3\deg_Y g = \deg_Y G_2 = 4$, a contradiction. Hence $G_2 = g\sigma(g)g_1$, where $g_1 \in \mathbb{F}_q[Y,Z]$. Therefore $G_2$ has a root $\rho(Y) \in \mathbb{F}_q(Y)$ for $Z$. Since $u+Y+Y^2$ and $v+Y+Y^2$ are irreducible over $\mathbb{F}_q$, we have $\rho(Y) = \phi(Y)/(b+aY)$, where $\phi(Y) \in \mathbb{F}_q[Y], \deg\phi = 2$, and $\phi(Y) \mid (u+Y+Y^2)(v+Y+Y^2)$. If $\phi(Y) = A(Y+u_1)(Y+v_1)$, where $A \in \mathbb{F}_q^*, u_1^2+u_1+u =$

$v_1^2 + v_1 + v = 0$, then $\sigma(u_1) = v_1 = u_1 + 1$, whence $v_1^2 + v_1 + u = 0$, which is a contradiction since $u \neq v$. Therefore, $\rho(Y) = A(u + Y + Y^2)/(b + aY)$ or $A(u + Y + Y^2)/(b + aY)$, where $A \in \mathbb{F}_q^*$.

**Case 1.** $\rho(Y) = A(u+Y+Y^2)/(b+aY)$. Let $G_2(Y, \rho(Y)) = \psi(Y)(u+Y+Y^2)/(b+aY)^2$, where $\psi(Y) \in \mathbb{F}_q[Y]$. Comparing the coefficients of $Y^i$ in the equation $\psi(Y) = 0$, we obtain the following.

$$Abdu + Abu^2 + A^2bu^2 + aA^2u^3 + A^2u^4 + A^3u^4 + b^2v + Ab^2v + Abuv + A^2buv + aA^2u^2v + A^2u^2v^2 + A^3u^2v^2 = 0, \tag{5.85}$$

$$b^2 + Ab^2 + Abd + Abu + aAbu + A^2bu + aAdu + aAu^2 + aA^2u^2 + Abv + A^2bv + aAuv + aA^2uv = 0, \tag{5.86}$$

$$aAb + b^2 + Ab^2 + aAd + Abd + aAu + a^2Au + Abu + A^2bu + A^2u^2 + A^3u^2 + a^2v + aAv + a^2Av + Abv + A^2bv + A^2v^2 + A^3v^2 = 0, \tag{5.87}$$

$$a(a + Ab + Ad + Au + A^2u + Av + A^2v) = 0, \tag{5.88}$$

$$a^2 + aA^2u + A^2u^2 + A^3u^2 + aA^2v + A^2v^2 + A^3v^2 = 0. \tag{5.89}$$

If $a = 0$, then (5.89) becomes $A^2(1 + A)(u + v)^2 = 0$, whence $A = 1$. By (5.86), $bd = 0$, which is a contradiction since $a = c = 0$. Therefore $a \neq 0$, and by (5.88),

$$a + Ab + Ad + Au + A^2u + Av + A^2v = 0. \tag{5.90}$$

Taking the resultant of (5.89) and (5.90) with respect to A, we get

$$a^2(b + d)^2(a + b + d)(u + v)^2 = 0. \tag{5.91}$$

Hence either $b + d = 0$ or $a + b + d = 0$.

**Case 1.1.** Assume $d = b$. Then (5.86), (5.87), (5.90) become

$$b^2 + Abu + A^2bu + aAu^2 + aA^2u^2 + Abv + A^2bv + aAuv + aA^2uv = 0, \tag{5.92}$$

$$b^2 + aAu + a^2Au + Abu + A^2bu + A^2u^2 + A^3u^2 + a^2v + aAv + a^2Av + Abv + A^2bv + A^2v^2 + A^3v^2 = 0, \tag{5.93}$$

$$a + Au + A^2u + Av + A^2v = 0. \tag{5.94}$$

Adding equations (5.92) and (5.93) gives

$$aAu + a^2Au + aAu^2 + A^2u^2 + aA^2u^2 + A^3u^2 + a^2v + aAv + a^2Av + aAuv + aA^2uv + A^2v^2 + A^3v^2 = 0. \tag{5.95}$$

Now the resultant of (5.94) and (5.95) with respect to $A$ is $a^5(u+v)^4$, which is a contradiction since $a \neq 0$.

**Case 1.2.** Assume $b + d \neq 0$. Then $d = a + b$ and by (5.90),

$$(1 + A)(a + Au + Av) = 0. \tag{5.96}$$

If $A = 1$, then (5.89) implies $a(a+u+v) = 0$, whence $a+u+v = 0$. Setting $d = b+a, a = u+v$ in (5.77) gives $(u+v)^2 = 0$, which is a contradiction. Therefore $A \neq 1$ and $a + Au + Av = 0$, whence $A = a/(u + v)$. Hence equations (5.85), (5.86) become

$$ab + b^2 + a^2u = 0, \tag{5.97}$$

$$a^3 + ab + b^2 + a^2v = 0. \tag{5.98}$$

Adding equations (5.97) and (5.98) gives $a^2(a + u + v)$, whence $a = u + v$, which is a contradiction since $A \neq 1$.

**Case 2.** $\rho(Y) = A(v+Y+Y^2)/(b+aY)$. Let $G_2(Y, \rho(Y)) = \psi(Y)(v+Y+Y^2)/(b+aY)^2$, where $\psi(Y) \in \mathbb{F}_q[Y]$. Comparing the coefficients of $Y^i$ in the equation $\psi(Y) = 0$, we obtain the following.

$$b^2u + Abdu + Abu^2 + Ab^2v + Abuv + A^2buv + aA^2u^2v + A^2u^3v + A^2bv^2 + aA^2uv^2 + A^3u^2v^2 + A^2uv^3 + A^3v^4 = 0, \tag{5.99}$$

$$b^2 + Ab^2 + Abd + Abu + aAbu + A^2bu + aAdu + aAu^2 + aA^2u^2 + A^2u^3 + Abv + A^2bv + aAuv + aA^2uv + A^2u^2v + A^2uv^2 + A^2v^3 = 0, \tag{5.100}$$

$$aAb + b^2 + Ab^2 + aAd + Abd + a^2u + aAu + a^2Au + Abu + A^2bu + A^2u^2 + aA^2u^2 + A^3u^2 + A^2u^3 + aAv + a^2Av + Abv + A^2bv + A^2u^2v + A^2v^2 + aA^2v^2 + A^3v^2 + A^2uv^2 + A^2v^3 = 0, \tag{5.101}$$

$$a(a + Ab + Ad + Au + A^2u + Av + A^2v) = 0, \tag{5.102}$$

$$a^2 + aA^2u + A^2u^2 + A^3u^2 + aA^2v + A^2v^2 + A^3v^2 = 0. \tag{5.103}$$

**Case 2.1.** Assume $a = 0$. By (5.103), $A^2(1 + A)(u + v)^2 = 0$, whence $A = 1$. Then (5.100) becomes $bd + u^3 + u^2v + uv^2 + v^3 = 0$, whence $d = (u + v)^3/b$. Hence (5.99) implies

$$b^2 + bu + u^3 + bv + u^2v + uv^2 + v^3 = 0. \tag{5.104}$$

Now (5.77) implies

$$(b^2 + u^3 + u^2v + uv^2 + v^3)(b + b^2 + u^3 + u^2v + uv^2 + v^3) = 0. \tag{5.105}$$

If $b^2 + u^3 + u^2v + uv^2 + v^3 = 0$, then this equation added to (5.104) gives $b(u + v) = 0$, which is a contradiction. If $b^2 + u^3 + u^2v + uv^2 + v^3 \neq 0$, then $b + b^2 + u^3 + u^2v + uv^2 + v^3 = 0$, and when the latter equation is added to (5.104) we get $b(1 + u + v) = 0$. Therefore $v = u + 1$. Now (5.99) becomes $b^2 + b + 1 = 0$ and $d = 1/b = b + 1$.

**Case 2.2.** Assume $a \neq 0$. Then by (5.102),

$$a + Ab + Ad + Au + A^2u + Av + A^2v = 0. \tag{5.106}$$

Computing the resultant of (5.103) and (5.106) with respect to $A$ gives

$$a^2(b+d)^2(a+b+d)(u+v)^2 = 0. \tag{5.107}$$

Thus either $b + d = 0$ or $a + b + d = 0$.

If $d = b$, then (5.106) becomes

$$a + Au + A^2u + Av + A^2v = 0. \tag{5.108}$$

Adding equations (5.100) and (5.101) gives

$$\begin{aligned} &a^2u + aAu + a^2Au + aAu^2 + A^2u^2 + A^3u^2 + aAv + a^2Av + aAuv + aA^2uv + A^2v^2 \\ &\quad + aA^2v^2 + A^3v^2 = 0. \end{aligned} \tag{5.109}$$

Computing the resultant of (5.108) and (5.109) with respect to $A$ gives $a^5(u+v)^4 = 0$, which is a contradiction.

Therefore, $d \neq b$ so $d = b + a$. By (5.106), we have $(1 + A)(a + Au + Av)$. If $A = 1$, then (5.103) becomes $a(a + u + v) = 0$. Thus $a + u + v = 0$. Substituting $d = b + a, v = u + a$ into (5.77), we get $a^2 = 0$, which is contradiction. Hence $A \neq 1$, and so $A = a/(u+v)$. By (5.100), $ab+b^2+a^2v = 0$. This implies $b$ is a root of $X^2+aX+a^2v$. But $\mathrm{Tr}_{q/2}(a^2v/a^2) = \mathrm{Tr}_{q/2}(v) = 1$, hence $b \notin \mathbb{F}_q$, a contradiction. □

**Lemma 5.5.** *Let $f(X)$ be given in* (5.80). *If $a = c = 0, b^2 + b + 1 = 0, d = b + 1, v = u + 1$, then $f$ is a PR of $\mathbb{P}^1(\mathbb{F}_q)$.*

*Proof.* Let $F(X,Y), G(X,Y), G_1(X,Y), G_2(X,Y)$ be as in (5.81), (5.82), (5.83), (5.84), respectively. Then $G_2$ has the following factorization.

$$\begin{aligned} G_2(Y,Z) &= u + u^2 + Y + Y^4 + bZ + bZ^2 + uZ^2 + YZ^2 + Y^2Z^2 + bZ^3 \\ &= (1 + u + Y + Y^2 + bZ)(u + Y + Y^2 + bZ + Z^2). \end{aligned}$$

Since $G_1(X,Y) = \overline{h}(X,Y,1)$ where $\overline{h}(X,Y,Z)$ is the homogenization of $G_2(Y,Z)$, we have

$$G_1(X,Y) = (bX + X^2 + uX^2 + XY + Y^2)(1 + bX + uX^2 + XY + Y^2).$$

Since $G(X,Y) = G_1(X+1, Y+u)$, we have

$$\begin{aligned} G(X,Y) = (1 + b + u^2 + bX + uX + X^2 + uX^2 + Y + XY + Y^2)(1 + b + u^2 + bX + uX \\ + uX^2 + Y + XY + Y^2). \end{aligned} \tag{5.110}$$

Let $(x,y) \in \mathbb{F}_q^2$ be a root of $G(X,Y)$ and suppose $x \neq 0$. Then by (5.110), either

$$u + 1 = \frac{1 + b + u^2 + bx + ux + y + xy + y^2}{x^2},$$

or

$$u = \frac{1 + b + u^2 + bx + ux + y + xy + y^2}{x^2}.$$

Now

$$\begin{aligned} \mathrm{Tr}_{q/2}\left(\frac{1+b+u^2+bx+ux+y+xy+y^2}{x^2}\right) &= \mathrm{Tr}_{q/2}\left(\frac{(b+u+y)^2 + (b+u+y)x + y}{x^2}\right) \\ &= \mathrm{Tr}_{q/2}\left(\left(\frac{b+u+y}{x}\right)^2 + \frac{b+u+y}{x}\right) + \mathrm{Tr}_{q/2}\left(\frac{y}{x^2}\right) \\ &= \mathrm{Tr}_{q/2}\left(\frac{y}{x^2}\right). \end{aligned}$$

Hence, $\mathrm{Tr}_{q/2}(y/x^2) = \mathrm{Tr}_{q/2}(u+1)$ or $\mathrm{Tr}_{q/2}(u)$. But $b^2+b+1=0, b \in \mathbb{F}_q$ implies $q = 2^n$ where $n$ is even, whence $\mathrm{Tr}_{q/2}(1) = 0$. Therefore in either case, $\mathrm{Tr}_{q/2}(y/x^2) = \mathrm{Tr}_{q/2}(u) = 1$. By Lemma 1.10, $f$ is a PR of $\mathbb{P}^1(\mathbb{F}_q)$. □

In Lemmas 4.5 and 5.3 where we showed that $F(X,Y)$ has an absolutely irreducible factor in $\mathbb{F}_q[X,Y]$, we only used the assumption that $G(X,Y)$ is absolutely irreducible. In the proof of the succeeding lemma, we have to make the further assumption that $f$ is a PR of $\mathbb{P}^1(\mathbb{F}_q)$ and use the power sum conditions up to $k=7$ in order to arrive at the desired contradiction.

**Lemma 5.6.** *Let $f(X), F(X,Y), G(X,Y)$ be given in* (5.80), (5.81), (5.82), *respectively. If $f$ is a PR of $\mathbb{P}^1(\mathbb{F}_q)$, $q \geq 9$, and $G(X,Y)$ is absolutely irreducible, then $F(X,Y)$ has an absolutely irreducible factor in $\mathbb{F}_q[X,Y]$.*

*Proof.* Write $F(X,Y) = F_0 + F_1 + \cdots + F_8$, where $F_i$ is homogeneous of degree $i$. We have

$$F_0 = du^2 + au^2v + bv^2 + auv^2 + u^2v^2,$$

$$F_1 = (du + du^2 + bv + u^2v + bv^2 + uv^2)(X+Y),$$

$$F_2 = uvX^2 + u^2vX^2 + uv^2X^2 + bXY + dXY + auXY + u^2XY + au^2XY + avXY + v^2XY + av^2XY + uvY^2 + u^2vY^2 + uv^2Y^2,$$

$$F_3 = (X+Y)(duX^2 + bvX^2 + uXY + u^2XY + vXY + v^2XY + duY^2 + bvY^2),$$

$$F_4 = uvX^4 + bX^3Y + dX^3Y + auX^3Y + avX^3Y + X^2Y^2 + bX^2Y^2 + dX^2Y^2 + auX^2Y^2 + u^2X^2Y^2 + avX^2Y^2 + v^2X^2Y^2 + bXY^3 + dXY^3 + auXY^3 + avXY^3 + uvY^4,$$

$$F_5 = XY(X+Y)(uX^2 + vX^2 + bXY + dXY + uXY + vXY + uY^2 + vY^2),$$

$$F_6 = (1+u+v)X^2Y^2(X+Y)^2,$$

$$F_7 = 0,$$

$$F_8 = X^4Y^4.$$

Assume to the contrary that $F(X,Y)$ does not have an absolutely irreducible factor in $\mathbb{F}_q[X,Y]$. By Corollary 1.9, $F(X,Y) = H(X,Y)H(Y,X)$, where $H(X,Y) \in \mathbb{F}_{q^2}[X,Y]$ is absolutely irreducible and $\sigma(H(X,Y)) = H(Y,X)$.

Let $H = h_0 + h_1 + h_2 + h_3 + h_4$, where $h_i$ is homogeneous of degree $i$. Since $h_4(X,Y)h_4(Y,X) = X^4Y^4$ and $\sigma(h_4(X,Y)) = h_4(Y,X)$, we have $h_4(X,Y) = X^2Y^2$.

We have $h_0^2 = du^2 + au^2v + bv^2 + auv^2 + u^2v^2$. Since $F_7 = h_3(X,Y)h_4(Y,X) + h_3(Y,X)h_4(X,Y) = (h_3(X,Y) + h_3(Y,X))X^2Y^2$, we have $h_3(X,Y) = h_3(Y,X)$. Since $F_6 = h_2(X,Y)h_4(Y,X) + h_3(X,Y)h_3(Y,X) + h_2(Y,X)h_4(X,Y)$, then $XY \mid h_3(X,Y)$. Since $\sigma(H(X,Y)) = H(Y,X)$, it follows that

$$\begin{aligned} h_1(X,Y) &= A_1X + A_2Y, \\ h_2(X,Y) &= B_1X^2 + BXY + B_2Y^2, \\ h_3(X,Y) &= CXY(X+Y), \end{aligned}$$

where $A_2 = A_1^q, B_2 = B_1^q, B, C \in \mathbb{F}_q$. Comparing the coefficients of $X^iY^j$ in the equation $F(X,Y) = H(X,Y)H(Y,X)$, we obtain the following equations.

$$h_0^2 + du^2 + au^2v + bv^2 + auv^2 + u^2v^2 = 0, \tag{5.111}$$

$$A_1h_0 + A_2h_0 + du + du^2 + bv + u^2v + bv^2 + uv^2 = 0, \tag{5.112}$$

$$A_1A_2 + B_1h_0 + B_2h_0 + uv + u^2v + uv^2 = 0, \tag{5.113}$$

$$A_2B_1 + A_1B_2 + du + bv = 0, \tag{5.114}$$

$$B_1B_2 + uv = 0, \tag{5.115}$$

$$A_1^2 + A_2^2 + b + d + au + u^2 + au^2 + av + v^2 + av^2 = 0, \tag{5.116}$$

$$A_1B + A_2B + A_1B_1 + A_2B_2 + u + du + u^2 + v + bv + v^2 = 0, \tag{5.117}$$

$$b + BB_1 + BB_2 + A_1C + A_2C + d + au + av = 0, \tag{5.118}$$

$$B_1C + B_2C + u + v = 0, \tag{5.119}$$

$$1 + b + B^2 + B_1^2 + B_2^2 + d + au + u^2 + av + v^2 = 0, \tag{5.120}$$

$$A_1 + A_2 + b + B_1C + B_2C + d = 0. \tag{5.121}$$

$$1 + B_1 + B_2 + C^2 + u + v = 0. \tag{5.122}$$

By (5.122),

$$B_2 = 1 + B_1 + C^2 + u + v. \tag{5.123}$$

Then (5.115) and (5.119) become

$$B_1 + B_1^2 + B_1C^2 + B_1u + B_1v + uv = 0, \tag{5.124}$$

$$(1 + C)(C^2 + C + u + v) = 0. \tag{5.125}$$

If $C = 1$, then by (5.124), $(B_1+u)(B_1+v) = 0$. But if $B_1 = u$, then $B_2 = 1+B_1+1+u+v = v$. Hence $v = B_2 = B_1^q = u$, gives a contradiction. Similarly, if $B_1 = v$, we also get a contradiction. Therefore $C \neq 1$ and

$$C^2 + C + u + v = 0. \tag{5.126}$$

Note that in the succeeding computations, we perform reduction modulo $C^2 + C + u + v$ whenever possible. Substituting $B_2$ in (5.121), we get

$$A_2 = A_1 + b + d + u + v. \tag{5.127}$$

Replacing $A_2, B_2$ in (5.113) and solving for $h_0$ gives

$$h_0 = (A_1^2 + A_1b + A_1d + A_1u + A_1v + uv + u^2v + uv^2)/(1 + C). \tag{5.128}$$

Substituting (5.127) and (5.128) into (5.111), (5.112), (5.116), we have

$$A_1^4+A_1^2b^2+A_1^2d^2+A_1^2u^2+du^2+Cdu^2+du^3+au^2v+aCu^2v+du^2v+au^3v+A_1^2v^2+bv^2+bCv^2$$
$$+auv^2+buv^2+aCuv^2+Cu^2v^2+u^3v^2+u^4v^2+bv^3+auv^3+u^2v^3+u^2v^4=0, \quad (5.129)$$

$$A_1^2b+A_1b^2+A_1^2d+A_1d^2+A_1^2u+du+Cdu+A_1u^2+du^2+Cdu^2+A_1^2v+bv+bCv+buv$$
$$+duv+bu^2v+Cu^2v+du^2v+u^3v+A_1v^2+bv^2+bCv^2+buv^2+Cuv^2+duv^2$$
$$+uv^3=0, \quad (5.130)$$

$$a(u+v)(u+v+1)+(b+d)(b+d+1)=0. \quad (5.131)$$

**Case 1.** Assume $u+v+1=0$. Then by (5.131), $(b+d)(1+b+d)=0$.

**Case 1.1** Assume $b+d=0$. Setting $v=u+1, d=b$, then (5.114), (5.117) become

$$A_1+b+B_1+A_1C=0,$$
$$1+A_1+b+B+B_1+C+A_1C=0.$$

Adding these two equations give $B=C+1$, whence (5.120) becomes $1+a+C+C^2=0$. Then by (5.126), we have $a=0$. Replacing $h_0, A_2$ in (5.111), (5.112), we obtain the following equations.

$$(A_1^2+A_1^4+bC+Cu^2+Cu^4)/C=0, \quad (5.132)$$

$$(A_1+A_1^2+u+Cu+u^2+Cu^2)/(1+C)=0. \quad (5.133)$$

Now

$$\mathrm{Res}(A_1^2+A_1^4+bC+Cu^2+Cu^4, A_1+A_1^2+u+Cu+u^2+Cu^2; A_1)=b^2(1+C),$$

whence $b=0$, which is a contradiction since $a=0$.

**Case 1.2** Assume $b+d+1=0$. Setting $v=u+1, d=b+1$ in (5.77) gives $a^3=0$, whence $a=0$. Then from (5.111), (5.114), we have

$$(A_1^4+bC+Cu^4)/C=0,$$
$$A_1+b+A_1C+u=0.$$

Now

$$\mathrm{Res}(A_1^4+bC+Cu^4, A_1+b+A_1C+u; A_1)=b(1+b)(1+b+b^2).$$

Since $a=0$, we have $b\neq 0$. Since $c=0$, we have $d\neq 0$, whence $b\neq 1$. Therefore $1+b+b^2=0$. We now have the same conditions on the parameters of $f$ in Lemma 5.5. In the proof of the lemma, (5.110) gives a factorization of $G(X,Y)$. This contradicts our assumption that $G(X,Y)$ is absolutely irreducible.

**Case 2.** Assume $u+v+1\neq 0$. Then

$$a=\frac{(b+d)(1+b+d)}{(u+v)(1+u+v)}. \tag{5.134}$$

Hence from (5.114), (5.118) we get

$$A_1=\frac{-bB_1-B_1d-B_1u-du-bv-B_1v}{1+C}, \tag{5.135}$$
$$B=\frac{-b^2-bC-Cd-d^2-bu-Cu-bCu-du-Cdu-Cu^2-bv-Cv-bCv-dv-Cdv-Cv^2}{(1+C)(1+u+v)}. \tag{5.136}$$

Substituting these into (5.117),(5.120) gives

$$(b+d)(1+b+d)L_1=0, \tag{5.137}$$
$$(b+d)(1+b+d)L_2=0, \tag{5.138}$$

where

$$L_1 = 1 + b + C + bC + d + Cd + u + u^2 + v + v^2,$$
$$L_2 = b + b^2 + d + d^2 + u + Cu + Cu^2 + u^3 + v + Cv + u^2v + Cv^2 + uv^2 + v^3.$$

**Case 2.1.** Assume $b + d = 0$. Then $a = 0$. Setting $a = 0, d = b$ in (5.79) gives

$$b(1 + b)(u + v)^6(b + b^2 + u + v) = 0.$$

Since $a = 0$, we have $b \neq 0$. Hence $(1 + b)(b + b^2 + u + v) = 0$.

**Case 2.1.1.** Assume $b = 1$. Then (5.112) and (5.124) imply

$$1 + C + u + B_1u^2 + B_1^2u^2 + B_1Cu^2 + v + u^3v + B_1v^2 + B_1^2v^2 + B_1Cv^2 + uv^3 = 0, \quad (5.139)$$
$$B_1 + B_1^2 + B_1C + uv = 0. \quad (5.140)$$

Taking the resultant of (5.139) and (5.140) with respect to $B_1$, we get $1+C+u+u^2+v+v^2 = 0$, whence $0 = C^2 + C + u + v = (u + v)^4$, which is a contradiction.

**Case 2.1.2.** Assume $b \neq 1$. Then $b + b^2 + u + v = 0$. Setting $v = b^2 + b + u$, we have $C^2 + C + u + v = (b + C)(1 + b + C)$.

Suppose $C = b$. Substituting this and (5.135) into (5.129), (5.130), (5.124) gives the following equations.

$$1 + b^3 + b^4 + bB_1^2 + b^3B_1^2 + bB_1^4 + b^3u^2 + b^5u^2 + bu^4 = 0, \quad (5.141)$$
$$1 + b^2 + b^3 + bB_1 + b^2B_1 + bB_1^2 + b^2u + b^3u + bu^2 = 0, \quad (5.142)$$
$$B_1 + bB_1 + B_1^2 + bu + b^2u + u^2 = 0. \quad (5.143)$$

Taking the resultant of (5.141), (5.142) and the resultant of (5.141), (5.143), both with respect to $B_1$, gives $(1 + b^3 + b^4)^2 = 0$ and $(1 + b^2 + b^3)^2 = 0$, respectively. Therefore, $b + b^2 = 0$, whence $b = 0$ or 1, which is a contradiction.

Now suppose $C = b + 1$. Then (5.129), (5.124) imply

$$b^5 + b^2B_1^2 + b^4B_1^2 + B_1^4 + b^2B_1^4 + b^2u^2 + b^6u^2 + u^4 + b^2u^4 = 0, \tag{5.144}$$

$$bB_1 + B_1^2 + bu + b^2u + u^2 = 0. \tag{5.145}$$

Taking the resultant of (5.144), (5.145) with respect to $B_1$ yields $b^{10} = 0$, which is a contradiction.

**Case 2.2.** Assume $1 + b + d = 0$. Then substituting $d = b + 1$ and (5.135) into (5.130) and (5.124) gives

$$\begin{aligned} B_1 + B_1^2 + B_1C + bu^2 + b^2u^2 + B_1u^2 + B_1^2u^2 + B_1Cu^2 + uv + u^3v + bv^2 + b^2v^2 + B_1v^2 \\ + B_1^2v^2 + B_1Cv^2 + uv^3 = 0, \end{aligned} \tag{5.146}$$

$$B_1 + B_1^2 + B_1C + uv = 0. \tag{5.147}$$

Taking the resultant of (5.146), (5.147) with respect to $B_1$ yields $b^2(1 + b)^2(u + v)^4 = 0$. Therefore $b = 1$, so $d = 0$. But $c = a = 0$, a contradiction.

**Case 2.3.** Assume $(b + d)(b + d + 1) \neq 0$. Then $L_1 = L_2 = 0$. We have

$$\mathrm{Res}(L_1, L_2; C) = (1+b+d+u+v)(b+b^2+d+d^2+bu+du+u^3+bv+dv+u^2v+uv^2+v^3).$$

**Case 2.3.1.** Assume $1 + b + d + u + v = 0$. Substituting $d = b + u + v + 1$ and (5.136), (5.123) into (5.120) gives $C + u + v = 0$. Since $C^2 + C + u + v = 0$, we have $u + v = 0$, which is a contradiction.

**Case 2.3.2.** Assume $1 + b + d + u + v \neq 0$. Then

$$b + b^2 + d + d^2 + bu + du + u^3 + bv + dv + u^2v + uv^2 + v^3 = 0. \tag{5.148}$$

Substituting (5.134) into (5.77) yields

$$\begin{aligned} &b^3 + b^4 + b^2d + bd^2 + d^3 + d^4 + b^3u + b^2du + bd^2u + d^3u + bu^2 + b^2u^2 + du^2 + d^2u^2 + bu^3 \\ &\quad + du^3 + u^4 + u^6 + b^3v + b^2dv + bd^2v + d^3v + bu^2v + du^2v + bv^2 + b^2v^2 + dv^2 + d^2v^2 \\ &\quad + buv^2 + duv^2 + u^4v^2 + bv^3 + dv^3 + v^4 + u^2v^4 + v^6 = 0. \end{aligned} \tag{5.149}$$

Taking the resultant of (5.148), (5.149) with respect to $b$ gives $(u + v)^7(1 + u + v)^4 = 0$, which is a contradiction. □

# CHAPTER 6:
# CONCLUSION AND FUTURE WORK

This dissertation is a research project aimed at determining rational functions of degree five that permute the projective line over a finite field. Out of five cases of rational functions of degree five, we have resolved the first three cases completely and partially in Case IV. We have determined five infinite families of PRs; three in Case III and two in Case IV. The result indicates that the permutation property of rational functions is profoundly related to the coefficients in a subtle way through polynomial equations. In our approach we used the combination of two methods, power sums and Hasse-Weil bound. Our work demonstrated that these two complement each other.

There are numerous questions to be considered for future work. First and foremost, we will work on the remaining part of Case IV and move on to Case V. The question that we face is essentially the same, to find the conditions on the coefficients so that the polynomial $G(X, Y)$ factors. The number of undetermined coefficients in these cases increases by one. We hope that the power sums combined with other considerations can provide useful constraints on the coefficients.

In this dissertation, our focus has been the determination of the PRs of degree 5. We have found several families of such PRs. We will investigate possible equivalences among such PRs and hopefully classify them up to equivalence.

This work has potential applications to coding theory and cryptography. When $q = 2^n$, permutations of $\mathbb{F}_q$ are used in cryptography in various encryption schemes. Let $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be a permutation. We identify $\mathbb{F}_{2^n}$ with $\mathbb{F}_2^n$ using a basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$. Then $f$ can

be treated as a function $\bar{f} : \mathbb{F}_2^n \to \mathbb{F}_2^n$. The *algebraic degree* of $f$ is defined as follows: First represent $f$ by a polynomial of degree $\leq 2^n - 1$: $f = \sum_{i=0}^{2^n-1} a_i x^i$. For each $0 \leq i \leq 2^n - 1$, let $\mathrm{wt}(i)$ be the base 2 wright of $i$, i.e., the sum of the base 2 digits of $i$. Then the algebraic degree of $f$ is $\max\{\mathrm{wt}(i) : a_i \neq 0\}$. One of the cryptographic criteria for Boolean functions is that cryptographic functions must have high algebraic degrees to resist the higher order differential attack [5, 6, 25, 26]. PRs low in rational degree usually have high algebraic degree. In our work, a PR of degree 5 is of the form $f = P(X)/Q(X)$, where $P, Q \in \mathbb{F}_{2^n}[X]$, $\deg P = 5$ and $\deg Q = d$ with $2 \leq d \leq 4$. As a function on $\mathbb{F}_{2^n}$, $f = P(X)Q(X)^{2^n-2}$, which has a high algebraic degree.

Another important security measure for cryptographic functions is their *differential uniformity*. The differential uniformity of a function $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is defined as follows: For $a \in \mathbb{F}_{2^n}^*$, the *derivative* of $f$ in the direction of $a$ is the function $D_a f(x) = f(x + a) + f(x)$, $x \in \mathbb{F}_{2^n}$. For $b \in \mathbb{F}_{2^n}$, let

$$\delta(a, b) = |\{x \in \mathbb{F}_{2^n} : D_a f(x) = b\}|.$$

The differential uniformity of $f$ is defined to be

$$\delta(f) = \max_{a \in \mathbb{F}_{2^n}^*, b \in \mathbb{F}_{2^n}} \delta(a, b).$$

The cryptographic functions are required to have low differential uniformity to resist the differential attack [35, 36, 37]. The lowest differential uniformity that a function $\mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ can achieve is 2, in which case, the function is called an *almost perfect nonlinear (APN)* function. Most existing work on differential uniformity deal with power functions and polynomial functions. It will be interesting to study the differential uniformity of low degree rational permutations of $\mathbb{F}_{2^n}$.

## REFERENCES


[1] A. Akbary, Q. Wang, *On polynomials of the form $x^r f(x^{(q-1)/l})$*, International Journal of Mathematics and Mathematical Sciences (2007), vol. 2007, Article ID 023408, 7 pages.

[2] Y. Aubry, M. Perret, *A Weil theorem for singular curves*, in: Arithmetic, Geometry and Coding Theory, Luminy, 1993, de Gruyter, Berlin, 1996, pp.1 – 7.

[3] D. Bartoli and X. Hou, *On a conjecture on permutation rational functions over finite fields*, Finite Fields Appl. **76** (2021), Paper No. 101904, 16 pp.

[4] X. Cao, X. Hou, J. Mi, S. Xu, *More permutation polynomials with Niho exponents which permute $\mathbb{F}_{p^2}$*, Finite Fields Appl. **62** (2020), Article 101626.

[5] C. Carlet, *Boolean functions for cryptography and error-correcting codes*, In: Y. Crama and P. Hammer (Eds.), Boolean Models and Methods in Mathematics, Computer Science, pp. 257 – 397, Cambridge University Press, 2010.

[6] C. Carlet, *Vectorial Boolean functions for cryptography*, In: Y. Crama and P. Hammer (Eds.), Boolean Models and Methods in Mathematics, Computer Science, and Engineering, pp. 398 – 470, Cambridge University Press, 2010.

[7] L. Carlitz, *On certain functions connected with polynomials in a Galois field*, Duke Math. J. **1** (1935), 137 – 168.

[8] L. E. Dickson, *The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group*, Ann. Math. **11** (1897), 65 – 120, 161 – 183.

[9] C. Ding, L. Qu, Q. Wang, J. Yuan, P. Yuan *Permutation trinomials over finite fields with even characteristic*, SIAM J. Discrete Math. **29** (2015), no. 1, 79–92.

[10] Z. Ding and M. E. Zieve *Low-degree permutation rational functions over finite fields*, Acta Arithmetica **202** (2022), 253 – 280.

[11] X. Fan, *A classification of permutation polynomials of degree 7 over finite fields*, arXiv:1812.02080.

[12] X. Fan, *Permutation polynomials of degree 8 over finite fields of characteristic 2*, arXiv:1903.10309.

[13] A. Ferraguti and G. Micheli, *Full Classification of permutation rational functions and complete rational functions of degree three over finite fields*, Designs, Codes and Cryptography **88** (2020) 867 – 886.

[14] T. Helleseth and V. Zinoviev, *New Kloosterman sums identities over $\mathbb{F}_{2^m}$ for all $m$*, Finite Fields Appl. **9** (2003), 187 – 193.

[15] C. Hermite *Sur les fonctions de sept 1ettres*, C. R . A cad. Sci. Paris **57**, 750 – 757 ( 1863); Oeuvres, vo1. 2, pp. 280 – 288, Gauthier-Villars, Paris, 1908.

[16] K. Hicks, X. Hou, G. L. Mullen, *Sums of reciprocals of polynomials over finite fields*, Amer. Math. Monthly **119** (2012), 313 – 317.

[17] X. Hou, *A power sum formula by Carlitz and its applications to permutation rational functions of finite fields*, Cryptogr. Commun. **13** (2021), 681 – 694.

[18] X. Hou, *Lectures on Finite Fields*, American Mathematical Soc., 2018.

[19] X. Hou, *Permutation polynomials over finite fields — a survey of recent advances*, Finite Fields Appl. **32** (2015), 82 – 119.

[20] X. Hou, *Rational functions of degree four that permute the projective line over a finite field*, Communications in Algebra **49** (2021), 3798–3809.

[21] X. Hou and V. P. Lavorante, *A general construction of permutation polynomials of* $\mathbb{F}_{q^2}$, Finite Fields Appl. to appear.

[22] X. Hou and V. P. Lavorante, *New results on permutation binomials*, Finite Fields Appl. to appear.

[23] X. Hou and C. Sze, *On a type of permutation rational functions over finite fields*, Finite Fields Appl. **68** (2020), Article 101758

[24] C. Jordan, *Traité des substitutions et des équations algebriques*, Gauthier-Villars, Paris, 1870.

[25] L. R. Knudsen, *Truncated and higher order differentials*, Proceedings of Fast Software Encryption, Second International Workshop, Lecture Notes in Computer Science 1008, pp. 196 – 211, 1995.

[26] X. Lai, *Higher order derivatives and differential cryptanalysis*, Proceedings of the Symposium on Communication, Coding and Cryptography, in honor of J. L. Massey on the occasion of his 60th birthday, 1994.

[27] H. Lausch and W. Nöbauer, *Algebra of Polynomials*, North-Holland, Amsterdam, 1973.

[28] J. Li, D. B. Chandler, Q. Xiang, *Permutation polynomials of degree* 6 *or* 7 *over finite fields of characteristic* 2, Finite Fields Appl. **16** (2010), 406 – 419.

[29] K. Li, L. Qu, X. Chen, C. Li, *Permutation polynomials of the form* $cx + Tr_{q^l/q}(x^a)$ *and permutation trinomials over finite fields with even characteristic*, Cryptogr. Commun. **10** (2018), 531 – 554.

[30] K. Li, L. Qu, C. Li, S. Fu, *New permutation trinomials constructed from fractional polynomials*, Acta Arith. **183** (2018), 101 – 116.

[31] L. Li, S. Wang, C. Li, X. Zeng, *Permutation polynomials* $(x^{p^m} - x + \delta)^{s_1} + (x^{p^m} - x + \delta)^{s_2} + x$ *over* $\mathbb{F}_{p^n}$, Finite Fields Appl. **51** (2018), 31 – 61.

[32] L. Li, Q. Wang, Y. Xu, X. Zeng, *Several classes of complete permutation polynomials with Niho exponents*, Finite Fields Appl. **72** (2021), Article 101831

[33] R. Lidl and H. Niederreiter, *Finite Fields*, Cambridge University Press, Cambridge, 1997.

[34] G. L. Mullen and D. Panario (eds), *Handbook of Finite Fields*, Discrete Mathematics and Its Applications, CRC Press, Boca Raton, FL, 2013.

[35] K. Nyberg, *Perfect nonlinear S-boxes*, Advances in cryptology - EUROCRYPT '91 (Brighton, 1991), 378 – 386, Lecture Notes in Comput. Sci. 547, Springer, Berlin, 1991.

[36] K. Nyberg, *Differentially uniform mappings for cryptography*, Advances in cryptology—EUROCRYPT '93 (Lofthus, 1993), 55 – 64, Lecture Notes in Comput. Sci., 765, Springer, Berlin, 1994.

[37] K. Nyberg and L. R. Knudsen, *Provable security against differential cryptanalysis*, Advances in cryptology - CRYPTO '92 (Santa Barbara, CA, 1992), 566 – 574, Lecture Notes in Comput. Sci. 740, Springer, Berlin, 1993.

[38] Y. H. Park and J. B. Lee, *Permutation polynomials and group permutation polynomials*, Bull. Austral. Math. Soc. **63** (2001), 67 – 74.

[39] X. Qin and L. Yan, *Constructing permutation trinomials via monomials on the subsets of* $\mu_{q+1}$, AAECC, Published on April 10, 2021, DOI:10.1007/s00200-021-00505-8.

[40] J.-A. Serret, *Cours d'algèbre supérieure*, 3rd ed., Gauthier-Villars, Paris, 1866.

[41] C. J. Shallue and I. M. Wanless, *Permutation polynomials and orthomorphism polynomials of degree six*, Finite Fields Appl. **20** (2013), 94 – 92.

[42] Z. Tu, X. Zeng, Y. Jiang, *Two classes of permutation polynomials having the form* $(x^{2^m} + x + \delta)^s + x$, Finite Fields Appl. **31** (2015), 12 – 24.

[43] Q. Wang, *A note on inverses of cyclotomic mapping permutation polynomials over finite fields*, Finite Fields Appl. **45** (2017), 422 – 427.

[44] Q. Wang, *Cyclotomic mapping permutation polynomials over finite fields*, in *Sequences, Subsequences, and Consequences*, S.W. Golomb, G. Gong, T. Helleseth, H.-Y. Song, (Eds.), pp. 119 – 128, Lecture Notes in Comput. Sci., vol. 4893, Springer, Berlin, 2007.

[45] Q. Wang, *Polynomials over finite fields: an index approach. Combinatorics and finite fields – difference sets, polynomials, pseudorandomness and applications*, Radon Ser. Comput. Appl. Math. **23** (2019), 319 – 346

[46] Wolfram Research, Inc., *Mathematica*, Version 13.2, Champaign, IL (2022).

[47] J. Yuan and C. Ding, *Four classes of permutation polynomials of* $\mathbb{F}_{2^m}$, Finite Fields Appl. **13** (2007), 869 – 876.

[48] J. Yuan, C. Ding, H. Wang, J. Pieprzyk, *Permutation polynomials of the form* $(x^p - x + \delta)^s + L(x)$, Finite Fields Appl. **14** (2008), 482 – 493.

[49] X. Zeng, X. Zhu, L. Hu, *Two new permutation polynomials with the form* $(x^{2^k} + x + \delta)^s + x$ *over* $\mathbb{F}_{2^n}$, Appl. Algebra Engrg. Comm. Comput. **21** (2010), 145 – 150.

[50] Z. Zha and L. Hu, *Some classes of permutation polynomials of the form* $(x^{p^m} - x + \delta)^s + x$ *over* $\mathbb{F}_{p^{2m}}$, Finite Fields Appl. **40** (2016), 150 – 162.

[51] D. Zheng, M. Yuan, L. Yu, *Two types of permutation polynomials with special forms*, Finite Fields Appl. **56** (2019), 1 – 16.

[52] 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), 2209 – 2216.

# APPENDIX A:
# MATHEMATICA CODES

Here we provide the Mathematica codes for computing $s(f,k) :=$ the numerator of $S(f,k)$, where $S(f,k) := \sum_{x\in\mathbb{F}_q} f(x)^k$, for the functions $f(X)$ in Case I, III and IV.

We also list the values of $s(f,k)$, for some small values of $k$. Note that if char $\mathbb{F}_q = 2$ and $k$ is even, then $s(f,k)$ is not useful since $S(f,2^i l) = S(f,l)^{2^i}$.

## A.1 Case I, $q$ Odd

$$f(X) = X^3 + aX^2 + bX + \frac{cX+d}{X^2-r}$$

```
Iodd[n_]:=Module[{f,fn,T1,T2,T3,T4},
f=X^3+a X^2+b X+(c X+d)/((X-r1)(X-r2));
fn=Apply[List,Apart[f^n]];
T1=Part[fn,(Length[fn]-2*n+1);;Length[fn]];
T2=T1/.{X-r1->r2-r1,X-r2->r1-r2};
T3=Numerator[Together[Total[T2]]];
T4=SymmetricReduction[T3,{r1,r2},{s1,s2}]/.{s1->0,s2->-r};
```

$$\begin{aligned}
s(f,1) &= -2d,\\
s(f,2) &= 2(3d^2 - c^2r - 8bcr^2 - 8adr^2 - 8cr^3),\\
s(f,3) &= -4(5d^3 - 3c^2dr + 12bcdr^2 + 6ad^2r^2 + 30ac^2r^3 + 24b^2dr^3 + 60cdr^3 + 48abcr^4 +\\
&\quad 24a^2dr^4 + 48bdr^4 + 48acr^5 + 24dr^5),\\
s(f,4) &= 2(35d^4 - 30c^2d^2r + 3c^4r^2 + 96bcd^2r^2 + 32ad^3r^2 - 32bc^3r^3 - 96ac^2dr^3 - 96b^2d^2r^3 -\\
&\quad 96cd^2r^3 - 480b^2c^2r^4 - 352c^3r^4 - 1920abcdr^4 - 480a^2d^2r^4 - 960bd^2r^4 - 256b^3cr^5 -\\
&\quad 864a^2c^2r^5 - 1728bc^2r^5 - 768ab^2dr^5 - 3456acdr^5 - 864d^2r^5 - 768a^2bcr^6 - 768b^2cr^6 -\\
&\quad 1248c^2r^6 - 256a^3dr^6 - 1536abdr^6 - 768a^2cr^7 - 768bcr^7 - 768adr^7 - 256cr^8),
\end{aligned}$$

$$
\begin{aligned}
s(f,5) = {} & -4(63d^5 - 70c^2d^3r + 15c^4dr^2 + 200bcd^3r^2 + 50ad^4r^2 - 120bc^3dr^3 - 180ac^2d^2r^3 - \\
& 160b^2d^3r^3 - 120cd^3r^3 + 50ac^4r^4 + 480b^2c^2dr^4 + 200c^3dr^4 + 960abcd^2r^4 + \\
& 160a^2d^3r^4 + 320bd^3r^4 + 3520abc^3r^5 + 3200b^3cdr^5 + 5280a^2c^2dr^5 + 10560bc^2dr^5 + \\
& 4800ab^2d^2r^5 + 10560acd^2r^5 + 1760d^3r^5 + 8640ab^2c^2r^6 + 9280ac^3r^6 + \\
& 640b^4dr^6 + 17280a^2bcdr^6 + 17280b^2cdr^6 + 13920c^2dr^6 + 2880a^3d^2r^6 + \\
& 17280abd^2r^6 + 2560ab^3cr^7 + 4160a^3c^2r^7 + 24960abc^2r^7 + 3840a^2b^2dr^7 + \\
& 2560b^3dr^7 + 24960a^2cdr^7 + 24960bcdr^7 + 12480ad^2r^7 + 2560a^3bcr^8 + \\
& 7680ab^2cr^8 + 16320ac^2r^8 + 640a^4dr^8 + 7680a^2bdr^8 + 3840b^2dr^8 + 10880cdr^8 + \\
& 2560a^3cr^9 + 7680abcr^9 + 3840a^2dr^9 + 2560bdr^9 + 2560acr^{10} + 640dr^{10}), \\
s(f,6) = {} & 4(231d^6 - 315c^2d^4r + 105c^4d^2r^2 + 840bcd^4r^2 + 168ad^5r^2 - 5c^6r^3 - 720bc^3d^2r^3 - \\
& 720ac^2d^3r^3 - 600b^2d^4r^3 - 360cd^4r^3 + 72bc^5r^4 + 360ac^4dr^4 + 2160b^2c^2d^2r^4 + \\
& 720c^3d^2r^4 + 2880abcd^3r^4 + 360a^2d^4r^4 + 720bd^4r^4 - 600b^2c^4r^5 - 168c^5r^5 - \\
& 4800abc^3dr^5 - 3840b^3cd^2r^5 - 3600a^2c^2d^2r^5 - 7200bc^2d^2r^5 - 3840ab^2d^3r^5 - \\
& 4800acd^3r^5 - 600d^4r^5 - 14080b^3c^3r^6 - 11160a^2c^4r^6 - 22320bc^4r^6 - \\
& 126720ab^2c^2dr^6 - 89280ac^3dr^6 - 9600b^4d^2r^6 - 126720a^2bcd^2r^6 - 126720b^2cd^2r^6 - \\
& 66960c^2d^2r^6 - 14080a^3d^3r^6 - 84480abd^3r^6 - 17280b^4c^2r^7 - 111360a^2bc^3r^7 - \\
& 111360b^2c^3r^7 - 39000c^4r^7 - 138240ab^3cdr^7 - 111360a^3c^2dr^7 - 668160abc^2dr^7 - \\
& 103680a^2b^2d^2r^7 - 69120b^3d^2r^7 - 334080a^2cd^2r^7 - 334080bcd^2r^7 - 111360ad^3r^7 - \\
& 3072b^5cr^8 - 149760a^2b^2c^2r^8 - 99840b^3c^2r^8 - 211200a^2c^3r^8 - 211200bc^3r^8 - \\
& 15360ab^4dr^8 - 199680a^3bcdr^8 - 599040ab^2cdr^8 - 633600ac^2dr^8 - 24960a^4d^2r^8 - \\
& 299520a^2bd^2r^8 - 149760b^2d^2r^8 - 211200cd^2r^8 - 30720a^2b^3cr^9 - 15360b^4cr^9 - \\
& 32640a^4c^2r^9 - 391680a^2bc^2r^9 - 195840b^2c^2r^9 - 113920c^3r^9 - 30720a^3b^2dr^9 - \\
& 61440ab^3dr^9 - 261120a^3cdr^9 - 783360abcdr^9 - 195840a^2d^2r^9 - 130560bd^2r^9 - \\
& 15360a^4bcr^{10} - 92160a^2b^2cr^{10} - 30720b^3cr^{10} - 241920a^2c^2r^{10} - 161280bc^2r^{10} - \\
& 3072a^5dr^{10} - 61440a^3bdr^{10} - 92160ab^2dr^{10} - 322560acdr^{10} - 40320d^2r^{10} - \\
& 15360a^4cr^{11} - 92160a^2bcr^{11} - 30720b^2cr^{11} - 48000c^2r^{11} - 30720a^3dr^{11} - \\
& 61440abdr^{11} - 30720a^2cr^{12} - 15360bcr^{12} - 15360adr^{12} - 3072cr^{13}), \\
s(f,7) = {} & -8(429d^7 - 693c^2d^5r + 315c^4d^3r^2 + 1764bcd^5r^2 + \ldots (139 \text{ terms}) \ldots + 7168dr^{15}), \\
s(f,8) = {} & 2(6435d^8 - 12012c^2d^6r + 6930c^4d^4r^2 + 29568bcd^6r^2 + \ldots (225 \text{ terms}) \ldots - \\
& 131072cr^{18}), \\
s(f,9) = {} & -4(12155d^9 - 25740c^2d^7r + 18018c^4d^5r^2 + 61776bcd^7r^2 + \ldots (320 \text{ terms}) \ldots + \\
& 294912dr^{20}), \\
s(f,10) = {} & 4(46189d^{10} - 109395c^2d^8r + 90090c^4d^6r^2 + 257400bcd^8r^2 + \\
& \ldots (470 \text{ terms}) \ldots - 1310720cr^{23}).
\end{aligned}
$$

## A.2 Case I, $q$ Even

$$f(X) = X^3 + aX^2 + bX + \frac{cX + d}{X^2 + X + t}$$

```
Ieven[n_]:=Module[{f,fn,T1,T2,T3,T4},
f=X^3+a X^2+b X+(c X+d)/((X-r1)(X-r2));
fn=Apply[List,Apart[f^n]];
T1=Part[fn,(Length[fn]-2*n+1);;Length[fn]];
T2=T1/.{X-r1->r2-r1,X-r2->r1-r2};
T3=PolynomialMod[Numerator[Together[Total[T2]]],2];
T4=SymmetricReduction[T3,{r1,r2},{s1,s2}]/.{s1->1,s2->t};
```

$$
\begin{aligned}
s(f,1) &= c,\\
s(f,3) &= c + a^2c + b^2c + ac^2 + c^3 + d + a^2d + b^2d + ad^2 + bd^2 + ct + a^2ct + b^2ct + c^2t + \\
&\quad bc^2t + d^2t + a^2ct^2 + c^2t^2 + dt^2 + ct^3,\\
s(f,5) &= c + a^4c + b^4c + c^5 + d + a^4d + b^4d + d^4 + ad^4 + bd^4 + ct + a^4ct + b^4ct + bc^4t + \\
&\quad d^4t + ct^2 + a^4ct^2 + b^4ct^2 + ac^4t^2 + bc^4t^2 + c^4t^3 + a^4ct^4 + dt^4 + ct^5 + ct^6,\\
s(f,7) &= c+a^2c+a^4c+a^6c+b^2c+a^4b^2c+b^4c+a^2b^4c+b^6c+ac^2+a^5c^2+ab^4c^2+c^3+a^4c^3+\\
&\quad b^4c^3+ac^4+ab^2c^4+c^5+c^7+d+a^2d+a^4d+a^6d+b^2d+a^4b^2d+b^4d+a^2b^4d+b^6d+\\
&\quad c^2d+a^4c^2d+b^4c^2d+c^4d+ad^2+a^5d^2+ab^4d^2+ac^4d^2+bc^4d^2+ad^4+ab^2d^4+b^3d^4+\\
&\quad a^2cd^4+b^2cd^4+c^2d^4+ct+a^2ct+a^4ct+a^6ct+b^2ct+a^4b^2ct+b^4ct+a^2b^4ct+b^6ct+\\
&\quad c^2t+a^4c^2t+bc^2t+a^4bc^2t+b^4c^2t+b^5c^2t+c^3t+a^4c^3t+b^4c^3t+c^4t+a^2bc^4t+b^2c^4t+\\
&\quad c^5t+bc^6t+d^2t+a^4d^2t+bd^2t+a^4bd^2t+b^4d^2t+b^5d^2t+c^4d^2t+d^4t+a^2bd^4t+b^2d^4t+\\
&\quad b^3d^4t+a^2ct^2+a^6ct^2+a^2b^4ct^2+c^2t^2+a^4c^2t^2+bc^2t^2+a^4bc^2t^2+b^4c^2t^2+b^5c^2t^2+\\
&\quad c^3t^2+a^4c^3t^2+b^4c^3t^2+c^4t^2+a^3c^4t^2+a^2bc^4t^2+b^2c^4t^2+c^5t^2+b^2c^5t^2+dt^2+a^4dt^2+\\
&\quad b^2dt^2+a^4b^2dt^2+b^4dt^2+b^6dt^2+d^2t^2+ad^2t^2+a^4d^2t^2+a^5d^2t^2+bd^2t^2+a^4bd^2t^2+\\
&\quad b^4d^2t^2+ab^4d^2t^2+b^5d^2t^2+d^4t^2+a^3d^4t^2+a^2bd^4t^2+b^2d^4t^2+cd^4t^2+ct^3+a^4ct^3+\\
&\quad b^2ct^3+a^4b^2ct^3+b^4ct^3+b^6ct^3+bc^2t^3+a^4bc^2t^3+b^5c^2t^3+a^2c^4t^3+bc^4t^3+b^3c^4t^3+\\
&\quad d^2t^3+a^4d^2t^3+b^4d^2t^3+a^2d^4t^3+bd^4t^3+ct^4+a^2ct^4+a^4b^2ct^4+b^4ct^4+a^2b^4ct^4+\\
&\quad c^2t^4+a^4c^2t^4+a^5c^2t^4+b^4c^2t^4+a^4c^3t^4+c^4t^4+ac^4t^4+a^2c^4t^4+a^3c^4t^4+bc^4t^4+\\
&\quad a^2bc^4t^4+b^2c^4t^4+c^5t^4+dt^4+a^6dt^4+a^4b^2dt^4+b^4dt^4+c^2dt^4+a^5d^2t^4+bd^2t^4+\\
&\quad a^4bd^2t^4+d^4t^4+ct^5+a^6ct^5+a^4b^2ct^5+b^4ct^5+a^4c^2t^5+a^4bc^2t^5+c^3t^5+c^4t^5+\\
&\quad a^2c^4t^5+bc^4t^5+a^4d^2t^5+bd^2t^5+a^6ct^6+a^4c^2t^6+bc^2t^6+c^3t^6+c^4t^6+a^4dt^6+b^2dt^6+\\
&\quad d^2t^6+ad^2t^6+bd^2t^6+a^4ct^7+b^2ct^7+bc^2t^7+d^2t^7+ct^8+a^2ct^8+c^2t^8+dt^8+ct^9,\\
s(f,9) &= c + a^8c + b^8c + c^9 + d + a^8d + b^8d + d^8 + ad^8 + bd^8 + ct + a^8ct + b^8ct + bc^8t + \\
&\quad d^8t + ct^2 + a^8ct^2 + b^8ct^2 + ac^8t^2 + bc^8t^2 + c^8t^3 + ct^4 + a^8ct^4 + b^8ct^4 + c^8t^4 + \\
&\quad ac^8t^4 + bc^8t^4 + c^8t^5 + a^8ct^8 + dt^8 + ct^9 + ct^{10} + ct^{12},\\
s(f,11) &= c + a^2c + a^8c + a^{10}c + \ldots (241 \text{ terms}) \ldots + ct^{15}.
\end{aligned}
$$

### A.3 Case III, $q$ Odd

$$f(X) = X + \frac{aX^3 + bX^2 + cX + d}{X^2 - r}$$

```
IIIodd[n_]:=Module[{f,fn,T1,T2,T3,T4},
f=X+(a X^3+b X^2+c X+d)/((X-r1)(X-r2))^2;
fn=Apply[List,Apart[f^n]];
T1=Part[fn,(Length[fn]-4*n+1);;Length[fn]];
T2=T1/.{X-r1->r2-r1,X-r2->r1-r2};
T3=Numerator[Together[Total[T2]]];
T4=SymmetricReduction[T3,{r1,r2},{s1,s2}]/.{s1->0,s2->-r};
```

$$\begin{aligned}
s(f,1) &= 2(3d - br),\\
s(f,2) &= 2(35d^2 - 5c^2r - 10bdr + 3b^2r^2 + 6acr^2 - 5a^2r^3 - 32cr^3 - 160ar^4),\\
s(f,3) &= 4(231d^3 - 63c^2dr - 63bd^2r + 21bc^2r^2 + 21b^2dr^2 + 42acdr^2 - 5b^3r^3 - 30abcr^3 - \\
&\quad 15a^2dr^3 - 240cdr^3 + 21a^2br^4 + 144bcr^4 + 144adr^4 - 240abr^5 - 384dr^5 - 1920br^6),\\
s(f,4) &= 2(6435d^4 - 2574c^2d^2r - 1716bd^3r + 99c^4r^2 + 1188bc^2dr^2 + 594b^2d^2r^2 + \\
&\quad 1188acd^2r^2 - 270b^2c^2r^3 - 180ac^3r^3 - 180b^3dr^3 - 1080abcdr^3 - 270a^2d^2r^3 - \\
&\quad 8064cd^2r^3 + 35b^4r^4 + 420ab^2cr^4 + 210a^2c^2r^4 + 896c^3r^4 + 420a^2bdr^4 + 5376bcdr^4 + \\
&\quad 2688ad^2r^4 - 270a^2b^2r^5 - 180a^3cr^5 - 1920b^2cr^5 - 1920ac^2r^5 - 3840abdr^5 - \\
&\quad 7680d^2r^5 + 99a^4r^6 + 2688ab^2r^6 + 2688a^2cr^6 + 4608c^2r^6 + 9216bdr^6 - \\
&\quad 2688a^3r^7 - 7680b^2r^7 - 15360acr^7 - 142848a^2r^8 - 81920cr^8 - 147456ar^9),\\
s(f,5) &= 4(46189d^5 - 24310c^2d^3r - 12155bd^4r + 2145c^4dr^2 + 12870bc^2d^2r^2 + \\
&\quad 4290b^2d^3r^2 + 8580acd^3r^2 - 715bc^4r^3 - 4290b^2c^2dr^3 - 2860ac^3dr^3 - 1430b^3d^2r^3 - \\
&\quad 8580abcd^2r^3 - 1430a^2d^3r^3 - 68640cd^3r^3 + 770b^3c^2r^4 + 1540abc^3r^4 + 385b^4dr^4 + \\
&\quad 4620ab^2cdr^4 + 2310a^2c^2dr^4 + 15840c^3dr^4 + 2310a^2bd^2r^4 + 47520bcd^2r^4 + \\
&\quad 15840ad^3r^4 - 63b^5r^5 - 1260ab^3cr^5 - 1890a^2bc^2r^5 - 7200bc^3r^5 - 1890a^2b^2dr^5 - \\
&\quad 1260a^3cdr^5 - 21600b^2cdr^5 - 21600ac^2dr^5 - 21600abd^2r^5 - 53760d^3r^5 + \\
&\quad 770a^2b^3r^6 + 1540a^3bcr^6 + 5600b^3cr^6 + 16800abc^2r^6 + 385a^4dr^6 + 16800ab^2dr^6 + \\
&\quad 16800a^2cdr^6 + 53760c^2dr^6 + 53760bd^2r^6 - 715a^4br^7 - 7200ab^3r^7 - 21600a^2bcr^7 - \\
&\quad 38400bc^2r^7 - 7200a^3dr^7 - 38400b^2dr^7 - 76800acdr^7 + 15840a^3br^8 + \\
&\quad 17920b^3r^8 + 107520abcr^8 + 53760a^2dr^8 + 122880cdr^8 - 161280a^2br^9 - \\
&\quad 204800bcr^9 - 204800adr^9 - 3809280abr^{10} - 819200dr^{10} - 1474560br^{11}),\\
s(f,6) &= 4(676039d^6 - 440895c^2d^4r - 176358bd^5r + 62985c^4d^2r^2 + \ldots(104\text{ terms})\ldots - \\
&\quad 40894464ar^{14}),\\
s(f,7) &= 8(5014575d^7 - 3900225c^2d^5r - 1300075bd^6r + 780045c^4d^3r^2 + \\
&\quad \ldots(155\text{ terms})\ldots - 40894464ar^{14}),\\
s(f,8) &= 2(300540195d^8 - 271455660c^2d^6r - 77558760bd^7r + 70204050c^4d^4r^2 + \\
&\quad \ldots(249\text{ terms})\ldots - 36507222016ar^{19}).
\end{aligned}$$

### A.4 Case III, $q$ Even

$$f(X) = X + \frac{aX^3 + bX^2 + cX + d}{X^2 + X + t}$$

```
IIIeven[n_]:=Module[{f,fn,T1,T2,T3,T4},
f=X+(a X^3+b X^2+c X+d)/((X-r1)(X-r2))^2;
fn=Apply[List,Apart[f^n]];
T1=Part[fn,(Length[fn]-4*n+1);;Length[fn]];
T2=T1/.{X-r1->r2-r1,X-r2->r1-r2};
T3=PolynomialMod[Numerator[Together[Total[T2]]],2];
T4=SymmetricReduction[T3,{r1,r2},{s1,s2}]/.{s1->1,s2->t};
```

$$s(f,1) = b + c + at,$$

$$s(f,3) = b+b^3+b^2c+c^2+ac^2+d+a^2d+d^2+at+b^2t+ab^2t+ct+a^2ct+c^2t+at^2+b^2t^2+a^2t^3,$$

$$\begin{aligned} s(f,5) = {} & b + b^5 + b^4c + c^4 + bc^4 + c^5 + d + d^4 + at + b^4t + ab^4t + ct + c^4t + ac^4t + at^2 + \\ & bt^2 + b^4t^2 + ct^2 + c^4t^2 + at^3 + a^4bt^4 + b^4t^4 + a^4ct^4 + a^4t^5 + a^5t^5 + a^4t^6, \end{aligned}$$

$$\begin{aligned} s(f,7) = {} & b+a^2b+b^7+b^6c+b^4c^2+ab^4c^2+c^4+ac^4+a^2c^4+a^3c^4+b^2c^4+d+b^4d+a^2b^4d+c^2d+ \\ & a^4c^2d+c^4d+bd^2+a^4bd^2+b^4d^2+cd^2+a^4cd^2+d^4+ad^4+at+a^3t+b^2t+b^6t+ab^6t+ \\ & ct+b^4ct+a^2b^4ct+b^4c^2t+c^3t+a^4c^3t+c^4t+a^2c^4t+c^5t+d^2t+ad^2t+a^4d^2t+a^5d^2t+ \\ & d^4t+at^2+a^3t^2+b^2t^2+b^6t^2+ct^2+dt^2+d^2t^2+a^4d^2t^2+a^2t^3+b^4t^3+a^2b^4t^3+ct^3+c^2t^3+ \\ & a^4c^2t^3+c^4t^3+at^4+a^2t^4+a^3t^4+b^2t^4+b^4t^4+ab^4t^4+a^4dt^4+a^2t^5+b^4t^5+a^4ct^5+a^4t^7, \end{aligned}$$

$$\begin{aligned} s(f,9) = {} & b+b^9+b^8c+c^8+bc^8+c^9+d+d^8+at+b^8t+ab^8t+ct+c^8t+ac^8t+at^2+bt^2+b^8t^2+ct^2+ \\ & c^8t^2+at^3+bt^4+b^8t^4+ct^4+c^8t^4+at^5+a^8bt^8+b^8t^8+a^8ct^8+a^8t^9+a^9t^9+a^8t^{10}+a^8t^{12}, \end{aligned}$$

$$\begin{aligned} s(f,11) = {} & b+b^3+b^{11}+b^{10}c+bc^2+b^8c^2+ab^8c^2+c^8+ac^8+b^3c^8+b^2c^9+c^{10}+ac^{10}+d+a^2d+ \\ & b^2d+b^8d+a^2b^8d+c^8d+a^2c^8d+b^8d^2+c^8d^2+d^8+ad^8+at+b^2t+ab^2t+b^{10}t+ab^{10}t+ \\ & ct+a^2ct+b^2ct+b^8ct+a^2b^8ct+ac^2t+b^8c^2t+c^8t+b^2c^8t+ab^2c^8t+c^9t+a^2c^9t+c^{10}t+ \\ & d^2t+d^8t+at^2+b^2t^2+ab^2t^2+b^3t^2+b^{10}t^2+ct^2+a^2ct^2+b^2ct^2+ac^2t^2+b^2c^8t^2+dt^2+ \\ & a^2dt^2+d^2t^2+a^2t^3+ab^2t^3+b^8t^3+a^2b^8t^3+ct^3+a^2ct^3+c^2t^3+c^8t^3+a^2c^8t^3+at^4+ \\ & a^2t^4+bt^4+b^2t^4+b^3t^4+b^8t^4+ab^8t^4+b^2ct^4+c^2t^4+ac^2t^4+c^8t^4+ac^8t^4+dt^4+a^2dt^4+ \\ & d^2t^4+at^5+a^2t^5+b^2t^5+ab^2t^5+b^8t^5+ct^5+a^2ct^5+c^2t^5+c^8t^5+at^6+b^2t^6+a^2t^7+ \\ & a^8b^3t^8+b^8t^8+ab^8t^8+a^8b^2ct^8+a^8c^2t^8+a^9c^2t^8+a^8dt^8+a^{10}dt^8+a^8d^2t^8+a^8b^2t^9+ \\ & a^9b^2t^9+b^8t^9+a^8ct^9+a^{10}ct^9+a^8c^2t^9+a^8b^2t^{10}+a^8t^{11}+a^{10}t^{11}+a^8t^{12}+a^9t^{12}+a^8t^{13}, \end{aligned}$$

$$\begin{aligned} s(f,13) = {} & b + a^4b + b^{13} + b^{12}c + b^8c^4 + b^9c^4 + b^8c^5 + c^8 + a^4c^8 + bc^8 + a^4bc^8 + b^4c^8 + c^9 + \\ & a^4c^9 + d + a^4d + bd^4 + a^8bd^4 + b^8d^4 + cd^4 + a^8cd^4 + d^8 + bd^8 + cd^8 + at + a^5t + b^4t + \\ & b^{12}t + ab^{12}t + ct + a^4ct + b^8c^4t + ab^8c^4t + c^8t + ac^8t + a^4c^8t + a^5c^8t + d^4t + ad^4t + \\ & a^8d^4t + a^9d^4t + d^8t + ad^8t + at^2 + a^5t^2 + bt^2 + a^4bt^2 + b^4t^2 + b^{12}t^2 + ct^2 + a^4ct^2 + \\ & b^8c^4t^2 + c^8t^2 + a^4c^8t^2 + d^4t^2 + a^8d^4t^2 + d^8t^2 + at^3 + a^5t^3 + a^4bt^4 + b^4t^4 + b^9t^4 + \\ & a^4b^9t^4 + b^{12}t^4 + ct^4 + a^4ct^4 + b^8ct^4 + a^4b^8ct^4 + bc^4t^4 + a^8bc^4t^4 + c^5t^4 + a^8c^5t^4 + \\ & bc^8t^4 + c^9t^4 + dt^4 + d^4t^4 + a^8d^4t^4 + a^4t^5 + a^5t^5 + b^8t^5 + ab^8t^5 + a^4b^8t^5 + a^5b^8t^5 + \\ & ct^5 + c^4t^5 + ac^4t^5 + a^8c^4t^5 + a^9c^4t^5 + c^8t^5 + ac^8t^5 + at^6 + a^4t^6 + bt^6 + b^8t^6 + a^4b^8t^6 + \\ & ct^6 + c^4t^6 + a^8c^4t^6 + c^8t^6 + at^7 + a^4t^8 + a^4bt^8 + b^4t^8 + b^8t^8 + b^9t^8 + a^4ct^8 + b^8ct^8 + \\ & a^4t^9 + a^5t^9 + b^8t^9 + ab^8t^9 + a^4t^{10} + b^8t^{10} + a^8bt^{12} + a^8ct^{12} + a^8t^{13} + a^9t^{13} + a^8t^{14}. \end{aligned}$$

### A.5 Case IV, $q$ Odd

$$f(X) = X + \frac{aX+b}{X^2-u} + \frac{cX+d}{X^2-v}$$

```
IVodd[n_]:=Module[{f,fn,T1,T2,T3,T4,T5},
f=X+(a X+b)/((X-u1)(X-u2))+(c X+d)/((X-v1)(X-v2));
fn=Apply[List,Apart[f^n]];
T1=Part[fn,(Length[fn]-4*n+1);;Length[fn]];
T2=T1/.{-u1+X->-u1+u2,-u2+X->-u2+u1,-v1+X->-v1+v2,-v2+X->-v2+v1};
T3=Numerator[Together[Total[T2]]];
T4=SymmetricReduction[T3,{u1,u2},{s1,s2}]/.{s1->0,s2->-u};
T5=SymmetricReduction[T4[[1]],{v1,v2},{t1,t2}]/.{t1->0,t2->-v};
```

$$\begin{aligned}
s(f,1) &= -8(du+bv),\\
s(f,2) &= 32(u-v)^2(3d^2u^2+8bduv-c^2u^2v+3b^2v^2-a^2uv^2-8au^2v^2-8cu^2v^2),\\
s(f,3) &= -256(u-v)^3(5d^3u^4+18bd^2u^3v-5d^3u^3v-3c^2du^4v+24b^2du^2v^2-\\
&\quad 24bd^2u^2v^2-6bc^2u^3v^2-12acdu^3v^2+3c^2du^3v^2+12cdu^4v^2+5b^3uv^3-\\
&\quad 18b^2duv^3-3a^2bu^2v^3+12abcu^2v^3+6a^2du^2v^3+12abu^3v^3-12cdu^3v^3+\\
&\quad 24bu^4v^3+24du^4v^3-5b^3v^4+3a^2buv^4-12abu^2v^4-24bu^3v^4-24du^3v^4),\\
s(f,4) &= 512(u-v)^4(35d^4u^6+160bd^3u^5v-70d^4u^5v-30c^2d^2u^6v+288b^2d^2u^4v^2-\\
&\quad 352bd^3u^4v^2+35d^4u^4v^2-96bc^2du^5v^2-96acd^2u^5v^2+60c^2d^2u^5v^2+3c^4u^6v^2+\\
&\quad 96cd^2u^6v^2+256b^3du^3v^3-768b^2d^2u^3v^3+256bd^3u^3v^3-96b^2c^2u^4v^3-384abcdu^4v^3+\\
&\quad 288bc^2du^4v^3-96a^2d^2u^4v^3+288acd^2u^4v^3-30c^2d^2u^4v^3+32ac^3u^5v^3-6c^4u^5v^3+\\
&\quad 384bcdu^5v^3+192ad^2u^5v^3-192cd^2u^5v^3-32c^3u^6v^3-96d^2u^6v^3+35b^4u^2v^4-\\
&\quad 352b^3du^2v^4+288b^2d^2u^2v^4-30a^2b^2u^3v^4+288ab^2cu^3v^4-96b^2c^2u^3v^4+\\
&\quad 288a^2bdu^3v^4-384abcdu^3v^4-96a^2d^2u^3v^4+3a^4u^4v^4+96ab^2u^4v^4+32a^3cu^4v^4-\\
&\quad 192b^2cu^4v^4-192a^2c^2u^4v^4+32ac^3u^4v^4+3c^4u^4v^4-384abdu^4v^4-384bcdu^4v^4-\\
&\quad 192ad^2u^4v^4+96cd^2u^4v^4-32a^3u^5v^4-96b^2u^5v^4-192a^2cu^5v^4+192ac^2u^5v^4+\\
&\quad 64c^3u^5v^4+192d^2u^5v^4-480a^2u^6v^4-768acu^6v^4-480c^2u^6v^4-256au^7v^4-70b^4uv^5+\\
&\quad 160b^3duv^5+60a^2b^2u^2v^5-96ab^2cu^2v^5-96a^2bdu^2v^5-6a^4u^3v^5-192ab^2u^3v^5+\\
&\quad 32a^3cu^3v^5+192b^2cu^3v^5+384abdu^3v^5+64a^3u^4v^5+192b^2u^4v^5+192a^2cu^4v^5-\\
&\quad 192ac^2u^4v^5-32c^3u^4v^5-96d^2u^4v^5+960a^2u^5v^5+1536acu^5v^5+960c^2u^5v^5+\\
&\quad 512au^6v^5-256cu^6v^5+35b^4v^6-30a^2b^2uv^6+3a^4u^2v^6+96ab^2u^2v^6-32a^3u^3v^6-\\
&\quad 96b^2u^3v^6-480a^2u^4v^6-768acu^4v^6-480c^2u^4v^6-256au^5v^6+512cu^5v^6-256cu^4v^7),\\
s(f,5) &= -4096(u-v)^5(63d^5u^8+350bd^4u^7v-189d^5u^7v-70c^2d^3u^8v+\\
&\quad \ldots(187\text{ terms})\ldots-640du^5v^9),\\
s(f,6) &= 16384(u-v)^6(231d^6u^{10}+1512bd^5u^9v-924d^6u^9v-315c^2d^4u^{10}v+\\
&\quad \ldots(447\text{ terms})\ldots-3072cu^6v^{12}),\\
s(f,7) &= -131072(u-v)^7(429d^7u^{12}+3234bd^6u^{11}v-2145d^7u^{11}v-693c^2d^5u^{12}v+\\
&\quad \ldots(769\text{ terms})\ldots-7168du^7v^{14}),\\
s(f,8) &= 131072(u-v)^8(6435d^8u^{14}+54912bd^7u^{13}v-38610d^8u^{13}v-12012c^2d^6u^{14}v+\\
&\quad \ldots(1465\text{ terms})\ldots-131072cu^8v^{17}).
\end{aligned}$$

### A.6 Case IV, $q$ Even

$$f(X) = X + \frac{aX+b}{X^2+X+u} + \frac{cX+d}{X^2+X+v}$$

```
IVeven[n_]:=Module[{f,fn,T1,T2,T3,T4,T5,T6},
f=X+(a X+b)/((X-u1)(X-u2))+(c X+d)/((X-v1)(X-v2));
fn=Apply[List,Apart[f^n]];
T1=Part[fn,(Length[fn]-4*n+1);;Length[fn]];
T2=T1/.{-u1+X->-u1+u2,-u2+X->-u2+u1};
T3=T2/.{-v1+X->-v1+v2,-v2+X->-v2+v1};
T4=PolynomialMod[Numerator[Together[Total[T3]]],2];
T5=SymmetricReduction[T4,{u1,u2},{s1,s2}]/.{s1->1,s2->u};
T6=SymmetricReduction[T5[[1]],{v1,v2},{t1,t2}]/.{t1->1,t2->v};
```

$$s(f,1) = a + c,$$

$$\begin{aligned} s(f,3) = {} & (u+v)^3(a^2c + b^2c + ac^2 + bc^2 + a^2d + ad^2 + au + a^3u + bu + b^2u + cu + a^2cu + \\ & c^3u + du + d^2u + au^2 + a^2u^2 + av + a^3v + bv + b^2v + cv + ac^2v + c^3v + dv + \\ & d^2v + auv + a^2uv + cuv + c^2uv + cv^2 + c^2v^2), \end{aligned}$$

$$\begin{aligned} s(f,5) = {} & (u+v)^5(a^4c + b^4c + ac^4 + bc^4 + a^4d + ad^4 + ac^4u + a^4cu^2 + b^4cu^2 + bc^4u^2 + \\ & a^4du^2 + ad^4u^2 + au^3 + a^5u^3 + bu^3 + b^4u^3 + cu^3 + a^4cu^3 + c^5u^3 + du^3 + d^4u^3 + \\ & au^4 + a^4u^4 + a^4cu^4 + au^5 + a^4u^5 + a^4cv + au^2v + a^5u^2v + bu^2v + b^4u^2v + cu^2v + \\ & ac^4u^2v + c^5u^2v + du^2v + d^4u^2v + au^3v + a^4u^3v + cu^3v + c^4u^3v + au^4v + a^4u^4v + \\ & b^4cv^2 + ac^4v^2 + bc^4v^2 + a^4dv^2 + ad^4v^2 + auv^2 + a^5uv^2 + buv^2 + b^4uv^2 + cuv^2 + \\ & a^4cuv^2 + c^5uv^2 + duv^2 + d^4uv^2 + au^2v^2 + a^4u^2v^2 + cu^2v^2 + a^4cu^2v^2 + c^4u^2v^2 + \\ & ac^4u^2v^2 + au^3v^2 + a^4u^3v^2 + cu^3v^2 + c^4u^3v^2 + av^3 + a^5v^3 + bv^3 + b^4v^3 + cv^3 + \\ & ac^4v^3 + c^5v^3 + dv^3 + d^4v^3 + auv^3 + a^4uv^3 + cuv^3 + c^4uv^3 + au^2v^3 + a^4u^2v^3 + \\ & cu^2v^3 + c^4u^2v^3 + cv^4 + c^4v^4 + ac^4v^4 + cuv^4 + c^4uv^4 + cv^5 + c^4v^5), \end{aligned}$$

$$\begin{aligned} s(f,7) = {} & (u+v)^7(a^6c+a^4b^2c+a^2b^4c+b^6c+a^5c^2+a^4bc^2+ab^4c^2+b^5c^2+a^2c^5+b^2c^5+ac^6+ \\ & bc^6+a^6d+a^4b^2d+a^2b^4d+a^2c^4d+b^2c^4d+a^5d^2+a^4bd^2+ab^4d^2+ac^4d^2+bc^4d^2+ \\ & a^2cd^4+b^2cd^4+ac^2d^4+bc^2d^4+a^2d^5+ad^6+a^5c^2u+ab^4c^2u+ac^6u+a^5d^2u+ac^4d^2u+ \\ & ac^2d^4u+a^4cu^2+a^6cu^2+a^4b^2cu^2+b^4cu^2+a^2b^4cu^2+b^6cu^2+a^4c^2u^2+b^4c^2u^2+ \\ & a^4c^3u^2+b^4c^3u^2+ac^4u^2+a^2c^4u^2+a^3c^4u^2+bc^4u^2+b^2c^4u^2+b^3c^4u^2+b^2c^5u^2+ \\ & ac^6u^2+a^4du^2+a^6du^2+a^4b^2du^2+b^4du^2+a^2b^4du^2+b^4c^2du^2+a^2c^4du^2+a^4d^2u^2+ \\ & b^4cd^2u^2+bc^4d^2u^2+a^4d^3u^2+ad^4u^2+a^2d^4u^2+a^3d^4u^2+bd^4u^2+a^2bd^4u^2+ab^2d^4u^2+ \\ & ac^2d^4u^2+bc^2d^4u^2+ad^6u^2+a^4c^2u^3+a^5c^2u^3+b^4c^2u^3+ab^4c^2u^3+a^4c^3u^3+b^4c^3u^3+ \\ & ac^4u^3+a^2c^4u^3+a^3c^4u^3+b^2c^4u^3+a^2c^5u^3+b^2c^5u^3+a^4d^2u^3+a^5d^2u^3+b^4d^2u^3+ \\ & a^4cd^2u^3+ac^4d^2u^3+ad^4u^3+a^2d^4u^3+b^2d^4u^3+a^2cd^4u^3+ac^2d^4u^3+a^2cu^4+a^4cu^4+ \\ & b^2cu^4+b^4cu^4+ac^2u^4+a^4c^2u^4+bc^2u^4+b^4c^2u^4+ac^4u^4+a^2c^4u^4+bc^6u^4+a^2du^4+ \\ & a^4du^4+b^2du^4+b^4du^4+a^4c^2du^4+ad^2u^4+a^4d^2u^4+bd^2u^4+a^4cd^2u^4+ac^4d^2u^4+ \\ & ad^4u^4+bd^4u^4+au^5+a^3u^5+a^7u^5+bu^5+a^2bu^5+a^4b^2u^5+b^4u^5+ab^4u^5+cu^5+ \\ & a^2cu^5+a^6cu^5+b^4cu^5+a^5c^2u^5+bc^2u^5+c^3u^5+a^4c^3u^5+c^7u^5+du^5+a^2du^5+c^2du^5+ \\ & ad^2u^5+a^4d^2u^5+c^4d^2u^5+d^4u^5+cd^4u^5+au^6+a^2u^6+a^3u^6+a^6u^6+b^2u^6+b^4u^6+ \end{aligned}$$

$$b^2cu^6+ac^2u^6+a^4c^2u^6+a^2du^6+a^4du^6+a^2u^7+a^3u^7+a^5u^7+bu^7+b^2u^7+a^2cu^7+$$
$$a^4cu^7+au^8+a^2u^8+a^4u^8+a^6cv+a^4b^2cv+a^2b^4cv+a^2c^5v+b^2c^5v+a^2cd^4v+a^4cu^2v+$$
$$a^6cu^2v+a^4b^2cu^2v+b^4cu^2v+a^2b^4cu^2v+a^4c^2u^2v+a^5c^2u^2v+b^4c^2u^2v+ab^4c^2u^2v+$$
$$a^4c^3u^2v+a^2c^4u^2v+a^3c^4u^2v+b^2c^4u^2v+ab^2c^4u^2v+b^2c^5u^2v+a^4d^2u^2v+a^5d^2u^2v+$$
$$b^4d^2u^2v+a^2d^4u^2v+a^3d^4u^2v+b^2d^4u^2v+a^2cd^4u^2v+a^4c^2u^3v+b^4c^2u^3v+a^2c^4u^3v+$$
$$b^2c^4u^3v+a^4d^2u^3v+a^2d^4u^3v+au^4v+a^3u^4v+a^7u^4v+bu^4v+a^2bu^4v+a^4b^2u^4v+$$
$$b^4u^4v+ab^4u^4v+cu^4v+a^4cu^4v+a^6cu^4v+b^2cu^4v+ac^2u^4v+a^5c^2u^4v+bc^2u^4v+$$
$$c^3u^4v+ac^6u^4v+c^7u^4v+du^4v+a^2du^4v+c^2du^4v+a^4d^2u^4v+c^4d^2u^4v+d^4u^4v+$$
$$ad^4u^4v+cd^4u^4v+au^5v+a^2u^5v+a^3u^5v+a^6u^5v+b^2u^5v+b^4u^5v+cu^5v+a^2cu^5v+$$
$$c^2u^5v+ac^2u^5v+a^4c^2u^5v+c^3u^5v+c^6u^5v+d^2u^5v+d^4u^5v+a^2u^6v+a^3u^6v+a^5u^6v+$$
$$bu^6v+b^2u^6v+au^7v+a^2u^7v+a^4u^7v+a^4cv^2+a^6cv^2+b^4cv^2+a^2b^4cv^2+b^6cv^2+$$
$$a^4c^2v^2+a^4bc^2v^2+b^4c^2v^2+a^4c^3v^2+b^4c^3v^2+ac^4v^2+a^2c^4v^2+a^3c^4v^2+bc^4v^2+$$
$$b^2c^4v^2+b^3c^4v^2+ac^6v^2+bc^6v^2+a^4dv^2+a^4b^2dv^2+b^4dv^2+a^2b^4dv^2+b^4c^2dv^2+$$
$$a^4d^2v^2+a^5d^2v^2+b^4cd^2v^2+ac^4d^2v^2+bc^4d^2v^2+a^4d^3v^2+ad^4v^2+a^2d^4v^2+a^3d^4v^2+$$
$$bd^4v^2+a^2bd^4v^2+ab^2d^4v^2+ac^2d^4v^2+bc^2d^4v^2+ad^6v^2+a^4c^2uv^2+b^4c^2uv^2+$$
$$ab^4c^2uv^2+a^4c^3uv^2+b^4c^3uv^2+ac^4uv^2+a^2c^4uv^2+a^3c^4uv^2+b^2c^4uv^2+a^2c^5uv^2+$$
$$b^2c^5uv^2+ac^6uv^2+a^4d^2uv^2+a^5d^2uv^2+b^4d^2uv^2+a^4cd^2uv^2+ac^4d^2uv^2+ad^4uv^2+$$
$$a^2d^4uv^2+b^2d^4uv^2+a^2cd^4uv^2+ac^2d^4uv^2+a^4b^2cu^2v^2+b^4c^2u^2v^2+bc^4u^2v^2+$$
$$a^2bc^4u^2v^2+b^2c^4u^2v^2+ab^2c^4u^2v^2+bc^6u^2v^2+a^4du^2v^2+a^6du^2v^2+a^4c^2du^2v^2+$$
$$a^4d^2u^2v^2+a^4cd^2u^2v^2+ac^4d^2u^2v^2+a^2d^4u^2v^2+a^5c^2u^3v^2+a^4c^3u^3v^2+ac^4u^3v^2+$$
$$b^2c^4u^3v^2+a^2c^5u^3v^2+ac^6u^3v^2+a^4d^2u^3v^2+cu^4v^2+a^2cu^4v^2+c^2u^4v^2+a^4c^2u^4v^2+$$
$$bc^2u^4v^2+c^3u^4v^2+bc^4u^4v^2+c^6u^4v^2+d^2u^4v^2+ad^2u^4v^2+d^4u^4v^2+c^2u^5v^2+c^3u^5v^2+$$
$$c^5u^5v^2+du^5v^2+d^2u^5v^2+a^4cv^3+a^4b^2cv^3+b^4cv^3+a^2b^4cv^3+a^4c^2v^3+a^5c^2v^3+$$
$$b^4c^2v^3+ab^4c^2v^3+a^4c^3v^3+a^2c^4v^3+a^3c^4v^3+b^2c^4v^3+ab^2c^4v^3+a^2c^5v^3+b^2c^5v^3+$$
$$a^4d^2v^3+a^5d^2v^3+b^4d^2v^3+a^2d^4v^3+a^3d^4v^3+b^2d^4v^3+a^2cd^4v^3+a^4c^2uv^3+b^4c^2uv^3+$$
$$a^2c^4uv^3+b^2c^4uv^3+a^4d^2uv^3+a^2d^4uv^3+a^4cu^2v^3+a^6cu^2v^3+a^5c^2u^2v^3+a^3c^4u^2v^3+$$
$$b^2c^4u^2v^3+a^2c^5u^2v^3+a^4d^2u^2v^3+a^4c^2u^3v^3+a^2c^4u^3v^3+c^2u^4v^3+ac^2u^4v^3+c^3u^4v^3+$$
$$ac^4u^4v^3+c^5u^4v^3+du^4v^3+d^2u^4v^3+cu^5v^3+c^2u^5v^3+c^4u^5v^3+a^2cv^4+a^4cv^4+$$
$$b^2cv^4+a^4b^2cv^4+b^4cv^4+ac^2v^4+a^4c^2v^4+bc^2v^4+ac^4v^4+a^2c^4v^4+bc^4v^4+a^2bc^4v^4+$$
$$b^2c^4v^4+ab^2c^4v^4+a^2dv^4+a^6dv^4+b^2dv^4+b^4dv^4+ad^2v^4+bd^2v^4+ad^4v^4+a^2d^4v^4+$$
$$bd^4v^4+auv^4+a^3uv^4+a^7uv^4+buv^4+a^2buv^4+a^4b^2uv^4+b^4uv^4+ab^4uv^4+cuv^4+$$
$$a^2cuv^4+a^6cuv^4+b^4cuv^4+bc^2uv^4+c^3uv^4+ac^4uv^4+b^2c^4uv^4+a^2c^5uv^4+ac^6uv^4+$$
$$c^7uv^4+duv^4+a^2duv^4+c^2duv^4+ad^2uv^4+c^4d^2uv^4+d^4uv^4+cd^4uv^4+au^2v^4+$$
$$a^2u^2v^4+a^3u^2v^4+a^6u^2v^4+b^2u^2v^4+b^4u^2v^4+b^2cu^2v^4+ac^2u^2v^4+a^2c^4u^2v^4+$$
$$a^2du^2v^4+a^4du^2v^4+a^2u^3v^4+a^3u^3v^4+a^5u^3v^4+bu^3v^4+b^2u^3v^4+a^2cu^3v^4+$$
$$a^4cu^3v^4+au^4v^4+a^2u^4v^4+a^4u^4v^4+cu^4v^4+c^2u^4v^4+c^4u^4v^4+av^5+a^3v^5+a^7v^5+$$
$$bv^5+a^2bv^5+a^4b^2v^5+b^4v^5+ab^4v^5+cv^5+b^2cv^5+ac^2v^5+bc^2v^5+c^3v^5+a^3c^4v^5+$$
$$b^2c^4v^5+a^2c^5v^5+ac^6v^5+c^7v^5+dv^5+a^2dv^5+c^2dv^5+c^4d^2v^5+d^4v^5+ad^4v^5+cd^4v^5+$$
$$auv^5+a^2uv^5+a^3uv^5+a^6uv^5+b^2uv^5+b^4uv^5+cuv^5+a^2cuv^5+c^2uv^5+ac^2uv^5+$$
$$c^3uv^5+a^2c^4uv^5+c^6uv^5+d^2uv^5+d^4uv^5+a^2u^2v^5+a^3u^2v^5+a^5u^2v^5+bu^2v^5+$$
$$b^2u^2v^5+au^3v^5+a^2u^3v^5+a^4u^3v^5+cv^6+a^2cv^6+c^2v^6+bc^2v^6+c^3v^6+a^2c^4v^6+$$
$$bc^4v^6+c^6v^6+d^2v^6+ad^2v^6+d^4v^6+c^2uv^6+c^3uv^6+c^5uv^6+duv^6+d^2uv^6+c^2v^7+$$
$$ac^2v^7+c^3v^7+ac^4v^7+c^5v^7+dv^7+d^2v^7+cuv^7+c^2uv^7+c^4uv^7+cv^8+c^2v^8+c^4v^8).$$

## APPENDIX B:

## LIST OF ALL PRS IN CASE I

### B.1 Case I, $q$ Odd

**Table 1.** All PRs of the form $f(X) = X^3 + aX^2 + bX + (cX + d)/(X^2 - r)$.

| $q$ | $\{a, b, c, d, r\}$ |
|---|---|
| 3 | $\{0,0,2,0,2\}, \{0,1,1,0,2\}, \{0,2,1,0,2\}, \{0,2,2,0,2\}, \{1,0,0,2,2\}, \{1,0,2,2,2\},$ $\{1,1,0,2,2\}, \{1,1,1,2,2\}, \{1,2,1,2,2\}, \{1,2,2,2,2\}, \{2,0,0,1,2\}, \{2,0,2,1,2\},$ $\{2,1,0,1,2\}, \{2,1,1,1,2\}, \{2,2,1,1,2\}, \{2,2,2,1,2\}$ |
| 5 | $\{0,0,3,0,2\}, \{0,0,3,0,3\}, \{0,1,1,0,3\}, \{0,1,3,0,2\}, \{0,1,3,0,3\}, \{0,1,4,0,2\},$ $\{0,2,2,0,3\}, \{0,2,3,0,3\}, \{0,3,2,0,2\}, \{0,3,3,0,2\}, \{0,4,1,0,2\}, \{0,4,3,0,2\},$ $\{0,4,3,0,3\}, \{0,4,4,0,3\}, \{1,0,4,0,2\}, \{1,2,1,0,2\}, \{1,3,2,0,3\}, \{1,3,4,0,3\},$ $\{1,4,1,0,3\}, \{1,4,2,0,2\}, \{2,0,4,0,3\}, \{2,1,1,0,2\}, \{2,1,2,0,3\}, \{2,2,2,0,2\},$ $\{2,2,4,0,2\}, \{2,3,1,0,3\}, \{3,0,4,0,3\}, \{3,1,1,0,2\}, \{3,1,2,0,3\}, \{3,2,2,0,2\},$ $\{3,2,4,0,2\}, \{3,3,1,0,3\}, \{4,0,4,0,2\}, \{4,2,1,0,2\}, \{4,3,2,0,3\}, \{4,3,4,0,3\},$ $\{4,4,1,0,3\}, \{4,4,2,0,2\}$ |
| 7 | $\{0,1,1,0,6\}, \{0,1,6,0,6\}, \{0,2,3,0,5\}, \{0,2,4,0,5\}, \{0,3,4,0,3\}, \{0,3,4,0,6\},$ $\{0,3,5,0,6\}, \{0,3,6,0,3\}, \{0,4,2,0,3\}, \{0,4,5,0,3\}, \{0,5,1,0,3\}, \{0,5,1,0,5\},$ $\{0,5,3,0,3\}, \{0,5,5,0,5\}, \{0,6,2,0,5\}, \{0,6,2,0,6\}, \{0,6,3,0,6\}, \{0,6,6,0,5\},$ $\{1,3,5,0,6\}, \{1,5,1,0,5\}, \{1,6,2,0,5\}, \{2,3,4,0,6\}, \{2,5,3,0,3\}, \{2,6,2,0,6\},$ $\{3,3,4,0,3\}, \{3,5,1,0,3\}, \{3,6,6,0,5\}, \{4,3,4,0,3\}, \{4,5,1,0,3\}, \{4,6,6,0,5\},$ $\{5,3,4,0,6\}, \{5,5,3,0,3\}, \{5,6,2,0,6\}, \{6,3,5,0,6\}, \{6,5,1,0,5\}, \{6,6,2,0,5\}$ |
| $3^2$ | $\{0,0,1+2u,0,u\}, \{0,0,1+2u,0,2u\}, \{0,0,2+u,0,1+u\}, \{0,0,2+u,0,2+2u\},$ $\{0,u,2+u,0,u\}, \{0,2u,2+u,0,2u\}, \{0,1+u,1+2u,0,1+u\},$ $\{0,2+2u,1+2u,0,2+2u\}, \{u,1+2u,2,0,2u\}, \{u,1+2u,2,0,2+2u\},$ $\{u,2+u,2,0,u\}, \{u,2+u,2,0,1+u\}, \{2u,1+2u,2,0,2u\}, \{2u,1+2u,2,0,2+2u\},$ $\{2u,2+u,2,0,u\}, \{2u,2+u,2,0,1+u\}, \{1,1,1,0,u\}, \{1,1,1,0,2+2u\}, \{1,2,1,0,2u\},$ $\{1,2,1,0,1+u\}, \{1+u,1+2u,2,0,2u\}, \{1+u,1+2u,2,0,2+2u\}, \{1+u,2+u,2,0,u\},$ $\{1+u,2+u,2,0,1+u\}, \{1+2u,1,1,0,u\}, \{1+2u,1,1,0,2+2u\}, \{1+2u,2,1,0,2u\},$ $\{1+2u,2,1,0,1+u\}, \{2,1,1,0,u\}, \{2,1,1,0,2+2u\}, \{2,2,1,0,2u\}, \{2,2,1,0,1+u\},$ $\{2+u,1,1,0,u\}, \{2+u,1,1,0,2+2u\}, \{2+u,2,1,0,2u\}, \{2+u,2,1,0,1+u\},$ $\{2+2u,1+2u,2,0,2u\}, \{2+2u,1+2u,2,0,2+2u\}, \{2+2u,2+u,2,0,u\},$ $\{2+2u,2+u,2,0,1+u\}$, where $u^2+u+2=0$. |

Continued on next page

**Table 1 – continued from previous page**

| $q$ | $\{a, b, c, d, r\}$ |
|---|---|
| 11 | $\{0,1,5,0,6\}, \{0,2,2,0,2\}, \{0,2,2,0,7\}, \{0,3,1,0,7\}, \{0,4,3,0,2\}, \{0,5,4,0,8\}, \{0,6,7,0,6\}, \{0,6,7,0,10\}, \{0,7,8,0,7\}, \{0,7,8,0,8\}, \{0,8,10,0,6\}, \{0,8,10,0,8\}, \{0,9,9,0,10\}, \{0,10,6,0,2\}, \{0,10,6,0,10\}$ |
| 13 | $\{0,0,7,0,2\}, \{0,0,7,0,11\}, \{0,0,8,0,5\}, \{0,0,8,0,8\}, \{0,0,11,0,6\}, \{0,0,11,0,7\}, \{0,1,7,0,5\}, \{0,1,7,0,7\}, \{0,3,11,0,2\}, \{0,3,11,0,8\}, \{0,4,8,0,2\}, \{0,4,8,0,7\}, \{0,9,8,0,6\}, \{0,9,8,0,11\}, \{0,10,11,0,5\}, \{0,10,11,0,11\}, \{0,12,7,0,6\}, \{0,12,7,0,8\}$ |

### B.2 Case I, $q$ Even

**Table 2.** All PRs of the form $f(X) = X^3 + aX^2 + bX + (cX + d)/(X^2 + X + t)$.

| $q$ | $\{a, b, c, d, t\}$ |
|---|---|
| 2 | $\{0,0,0,1,1\}, \{0,1,1,0,1\}, \{0,1,1,1,1\}, \{1,0,1,0,1\}, \{1,0,1,1,1\}, \{1,1,0,1,1\}$ |
| $2^2$ | $\{0,0,1,u,1+u\}, \{0,0,1,1,u\}, \{0,0,1,1,1+u\}, \{0,0,1,1+u,u\}, \{0,u,1,0,1+u\}, \{0,u,1,1,1+u\}, \{0,1,1,u,u\}, \{0,1,1,1,u\}, \{0,1,1,1,1+u\}, \{0,1,1,1+u,1+u\}, \{0,1+u,1,0,u\}, \{0,1+u,1,1,u\}, \{u,0,1,u,1+u\}, \{u,0,1,1+u,1+u\}, \{u,u,1,0,1+u\}, \{u,u,1,1,u\}, \{u,u,1,1+u,u\}, \{u,u,1,1+u,1+u\}, \{u,1,1,u,u\}, \{u,1,1,1+u,u\}, \{u,1+u,1,0,u\}, \{u,1+u,1,1,1+u\}, \{u,1+u,1,1+u,u\}, \{u,1+u,1,1+u,1+u\}, \{1,0,1,0,u\}, \{1,0,1,0,1+u\}, \{1,0,1,u,1+u\}, \{1,0,1,1+u,u\}, \{1,u,1,0,u\}, \{1,u,1,1,u\}, \{1,1,1,0,u\}, \{1,1,1,0,1+u\}, \{1,1,1,u,u\}, \{1,1,1,1+u,1+u\}, \{1,1+u,1,0,1+u\}, \{1,1+u,1,1,1+u\}, \{1+u,0,1,u,u\}, \{1+u,0,1,1+u,u\}, \{1+u,u,1,0,1+u\}, \{1+u,u,1,u,u\}, \{1+u,u,1,u,1+u\}, \{1+u,u,1,1,u\}, \{1+u,1,1,u,1+u\}, \{1+u,1,1,1+u,1+u\}, \{1+u,1+u,1,0,u\}, \{1+u,1+u,1,u,u\}, \{1+u,1+u,1,u,1+u\}, \{1+u,1+u,1,1,1+u\}$, where $u^2+u+1=0$. |
| $2^3$ | $\{0,u^2,0,u,1+u+u^2\}, \{0,u,0,u+u^2,1+u^2\}, \{0,u+u^2,0,u^2,1+u\}, \{u^2,0,0,u^2,1\}, \{u^2,u^2,0,u+u^2,1+u+u^2\}, \{u^2,u,0,u,1+u^2\}, \{u^2,u+u^2,0,0,1\}, \{u^2,u+u^2,0,0,1+u^2\}, \{u^2,u+u^2,0,0,1+u\}, \{u^2,u+u^2,0,0,1+u+u^2\}, \{u,0,0,u,1\}, \{u,u^2,0,0,1\}, \{u,u^2,0,0,1+u^2\}, \{u,u^2,0,0,1+u\}, \{u,u^2,0,0,1+u+u^2\}, \{u,u,0,u^2,1+u^2\}, \{u,u+u^2,0,u+u^2,1+u\}, \{u+u^2,0,0,u+u^2,1\}, \{u+u^2,u^2,0,u^2,1+u+u^2\}, \{u+u^2,u,0,0,1\}, \{u+u^2,u,0,0,1+u^2\}, \{u+u^2,u,0,0,1+u\}, \{u+u^2,u,0,0,1+u+u^2\}, \{u+u^2,u+u^2,0,u,1+u\}, \{1,1+u^2,0,u,1+u+u^2\}, \{1,1+u,0,u+u^2,1+u^2\}, \{1,1+u+u^2,0,u^2,1+u\}, \{1+u^2,1,0,u^2,1\}, \{1+u^2,1+u^2,0,u+u^2,1+u+u^2\}, \{1+u^2,1+u,0,u,1+u^2\}, \{1+u^2,1+u+u^2,0,0,1\}, \{1+u^2,1+u+u^2,0,0,1+u^2\}, \{1+u^2,1+u+u^2,0,0,1+u\}, \{1+u^2,1+u+u^2,0,0,1+u+u^2\}, \{1+u,1,0,u,1\}, \{1+u,1+u^2,0,0,1\}, \{1+u,1+u^2,0,0,1+u^2\}, \{1+u,1+u^2,0,0,1+u\}, \{1+u,1+u^2,0,0,1+u+u^2\}, \{1+u,1+u,0,u^2,1+u^2\}, \{1+u,1+u+u^2,0,u+u^2,1+u\}$, |

Continued on next page

**Table 2 – continued from previous page**

| $q$ | $\{a, b, c, d, t\}$ |
|---|---|
| | $\{1+u+u^2, 1, 0, u+u^2, 1\}, \{1+u+u^2, 1+u^2, 0, u^2, 1+u+u^2\}, \{1+u+u^2, 1+u, 0, 0, 1\},$ $\{1+u+u^2, 1+u, 0, 0, 1+u^2\}, \{1+u+u^2, 1+u, 0, 0, 1+u\},$ $\{1+u+u^2, 1+u, 0, 0, 1+u+u^2\}, \{1+u+u^2, 1+u+u^2, 0, u, 1+u\},$ where $u^3+u+1=0$. |

## APPENDIX C:

## THE EQUATION IN (5.79)

$$a^2b^5+ab^6+a^2b^4d+ab^4d^2+a^2bd^4+ab^2d^4+a^2d^5+ad^6+a^3b^4u+a^3d^4u+a^4bu^2+a^4b^2u^2+a^4b^3u^2+ab^4u^2+a^2b^4u^2+ab^6u^2+a^4du^2+a^4b^2du^2+b^4du^2+a^4d^2u^2+a^4bd^2u^2+ab^4d^2u^2+a^4d^3u^2+ad^4u^2+a^2d^4u^2+bd^4u^2+ab^2d^4u^2+ad^6u^2+a^5u^3+a^4b^2u^3+a^5b^2u^3+a^2b^4u^3+a^4d^2u^3+a^5d^2u^3+b^4d^2u^3+ad^4u^3+a^2d^4u^3+b^2d^4u^3+a^2bu^4+a^6bu^4+ab^2u^4+ab^4u^4+a^2b^4u^4+a^2du^4+a^4du^4+a^6du^4+b^2du^4+b^4du^4+ad^2u^4+a^4d^2u^4+bd^2u^4+ad^4u^4+bd^4u^4+a^3u^5+a^7u^5+bu^5+a^4b^2u^5+b^4u^5+du^5+ad^2u^5+d^4u^5+ad^4u^5+au^6+a^2u^6+b^2u^6+ab^2u^6+b^4u^6+a^2du^6+a^4du^6+a^2u^7+bu^7+b^2u^7+au^8+a^2u^8+a^4u^8+a^3b^4v+a^3d^4v+a^5u^2v+a^4b^2u^2v+a^5b^2u^2v+ab^4u^2v+a^2b^4u^2v+a^4d^2u^2v+a^5d^2u^2v+b^4d^2u^2v+a^2d^4u^2v+b^2d^4u^2v+a^4b^2u^3v+a^2b^4u^3v+a^4d^2u^3v+a^2d^4u^3v+a^3u^4v+a^5u^4v+a^7u^4v+bu^4v+ab^2u^4v+a^4b^2u^4v+b^4u^4v+ab^4u^4v+du^4v+d^4u^4v+a^6u^5v+b^2u^5v+b^4u^5v+d^2u^5v+d^4u^5v+a^2u^6v+a^3u^6v+a^5u^6v+bu^6v+b^2u^6v+au^7v+a^2u^7v+a^4u^7v+a^4bv^2+a^4b^2v^2+a^4b^3v^2+ab^4v^2+a^2b^4v^2+ab^6v^2+a^4dv^2+a^4b^2dv^2+b^4dv^2+a^4d^2v^2+a^4bd^2v^2+ab^4d^2v^2+a^4d^3v^2+ad^4v^2+a^2d^4v^2+bd^4v^2+ab^2d^4v^2+ad^6v^2+a^5uv^2+a^4b^2uv^2+a^5b^2uv^2+a^2b^4uv^2+a^4d^2uv^2+a^5d^2uv^2+b^4d^2uv^2+ad^4uv^2+a^2d^4uv^2+b^2d^4uv^2+a^4bu^2v^2+a^4b^2u^2v^2+a^2b^4u^2v^2+a^4du^2v^2+a^4d^2u^2v^2+a^2d^4u^2v^2+a^5u^3v^2+a^4b^2u^3v^2+a^4d^2u^3v^2+au^4v^2+a^2u^4v^2+a^2bu^4v^2+a^4bu^4v^2+d^2u^4v^2+ad^2u^4v^2+d^4u^4v^2+a^2u^5v^2+a^3u^5v^2+a^5u^5v^2+du^5v^2+d^2u^5v^2+a^5v^3+a^4b^2v^3+a^5b^2v^3+ab^4v^3+a^2b^4v^3+a^4d^2v^3+a^5d^2v^3+b^4d^2v^3+a^2d^4v^3+b^2d^4v^3+a^4b^2uv^3+a^2b^4uv^3+a^4d^2uv^3+a^2d^4uv^3+a^5u^2v^3+a^4b^2u^2v^3+a^4d^2u^2v^3+a^2u^4v^3+du^4v^3+d^2u^4v^3+au^5v^3+a^2u^5v^3+a^4u^5v^3+a^2bv^4+a^4bv^4+a^6bv^4+ab^2v^4+a^4b^2v^4+ab^4v^4+a^2dv^4+a^6dv^4+b^2dv^4+b^4dv^4+ad^2v^4+bd^2v^4+ad^4v^4+a^2d^4v^4+bd^4v^4+a^3uv^4+a^5uv^4+a^7uv^4+buv^4+b^4uv^4+duv^4+ad^2uv^4+a^4d^2uv^4+d^4uv^4+ad^4uv^4+au^2v^4+a^2u^2v^4+b^2u^2v^4+ab^2u^2v^4+b^4u^2v^4+a^2du^2v^4+a^4du^2v^4+a^2u^3v^4+bu^3v^4+b^2u^3v^4+a^3v^5+a^7v^5+bv^5+ab^2v^5+b^4v^5+ab^4v^5+dv^5+a^4d^2v^5+d^4v^5+a^6uv^5+b^2uv^5+b^4uv^5+d^2uv^5+d^4uv^5+a^2u^2v^5+a^3u^2v^5+a^5u^2v^5+bu^2v^5+b^2u^2v^5+au^3v^5+a^2u^3v^5+a^4u^3v^5+av^6+a^2v^6+a^2bv^6+a^4bv^6+d^2v^6+ad^2v^6+d^4v^6+a^2uv^6+a^3uv^6+a^5uv^6+duv^6+d^2uv^6+a^2v^7+dv^7+d^2v^7+auv^7+a^2uv^7+a^4uv^7+av^8+a^2v^8+a^4v^8=0.$$