Mathematisches
Forschungsinstitut
Oberwolfach

Member of the Leibniz Association

Oberwolfach Preprints

OWP 2020 - 05

DANIELE BARTOLI, HERIVELTO BORGES AND
LUCIANE QUOOS

Rational Functions with Small Value Set

Mathematisches Forschungsinstitut Oberwolfach gGmbH
Oberwolfach Preprints (OWP) ISSN 1864-7596

Oberwolfach Preprints (OWP)

The MFO publishes a preprint series **Oberwolfach Preprints (OWP)**, ISSN 1864-7596, which mainly contains research results related to a longer stay in Oberwolfach, as a documentation of the research work done at the MFO. In particular, this concerns the Research in Pairs-Programme (RiP) and the Oberwolfach-Leibniz-Fellows (OWLF), but this can also include an Oberwolfach Lecture, for example.

A preprint can have a size from 1 - 200 pages, and the MFO will publish it on its website as well as by hard copy. Every RiP group or Oberwolfach-Leibniz-Fellow may receive on request 30 free hard copies (DIN A4, black and white copy) by surface mail.

The full copyright is left to the authors. With the submission of a manuscript, the authors warrant that they are the creators of the work, including all graphics. The authors grant the MFO a perpetual, non-exclusive right to publish it on the MFO's institutional repository.

In case of interest, please send a **pdf file** of your preprint by email to *rip@mfo.de* or *owlf@mfo.de*, respectively. The file should be sent to the MFO within 12 months after your stay as RiP or OWLF at the MFO.

There are no requirements for the format of the preprint, except that the introduction should contain a short appreciation and that the paper size (respectively format) should be DIN A4, "letter" or "article".

On the front page of the hard copies, which contains the logo of the MFO, title and authors, we shall add a running number (20XX – XX). Additionally, each preprint will get a Digital Object Identifier (DOI).

We cordially invite the researchers within the RiP or OWLF programme to make use of this offer and would like to thank you in advance for your cooperation.

Imprint:

Mathematisches Forschungsinstitut Oberwolfach gGmbH (MFO)
Schwarzwaldstrasse 9-11
77709 Oberwolfach-Walke
Germany

Tel +49 7834 979 50
Fax +49 7834 979 55
Email admin@mfo.de
URL www.mfo.de

The Oberwolfach Preprints (OWP, ISSN 1864-7596) are published by the MFO.

DOI 10.14760/OWP-2020-05

Rational functions with Small Value Set

Daniele Bartoli*[1], Herivelto Borges †[2], and Luciane Quoos ‡[3]

[1]Dipartimento di Matematica e Informatica, Università degli Studi di Perugia, Via Vanvitelli, 1, 06123 Perugia, Italy
[2]Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, Avenida Trabalhador São-carlense, 400, CEP 13566-590, São Carlos SP, Brazil
[3]Instituto de Matemática, Universidade Federal do Rio de Janeiro, Rio de Janeiro, CEP 21.941-909 - Brazil

Abstract

In connection with Galois Theory and Algebraic Curves, this paper investigates rational functions $h(x) = f(x)/g(x) \in \mathbb{F}_q(x)$ for which the value set $V_h = \{h(\alpha) \mid \alpha \in \mathbb{F}_q \cup \{\infty\}\}$ is relatively small. In particular, under certain circumstances, it proves that $h(x)$ having a small value set is equivalent to the field extension $\mathbb{F}_q(x)/\mathbb{F}_q(h(x))$ being Galois.

1 Introduction

Let q be a power of a prime p, and let $\mathbb{F}_q$ be the finite field with q elements. For any rational function $h(x) \in \mathbb{F}_q(x)$, its value set is defined as

$$V_h = \{h(\alpha) \mid \alpha \in \mathbb{P}^1\} \subset \mathbb{P}^1 = \mathbb{F}_q \cup \{\infty\}.$$

If $h(x) = \frac{f(x)}{g(x)} \in \mathbb{F}_q(x)$ is a rational function of degree d, that is, $f(x), g(x) \in \mathbb{F}_q[x]$ are such that $\gcd(f(x), g(x)) = 1$ and $d = \max\{\deg f, \deg g\}$, then one has the trivial bound

$$\left\lceil \frac{q+1}{d} \right\rceil \leq \#V_h \leq q+1. \tag{1}$$

Hereafter, a rational function for which the lower bound in (1) is achieved will be called *minimal value set rational function*, abbreviated as *m.v.s.r.f.*.

*daniele.bartoli@unipg.it
†hborges@icmc.usp.br
‡luciane@im.ufrj.br

The previous definition is analogous to the well-known notion of minimal value set polynomials, that is, polynomials $f \in \mathbb{F}_q[x]$ of degree $d \geq 1$ for which the value set $V_f = \{f(\alpha) \mid \alpha \in \mathbb{F}_q\}$ has the smallest possible size $\lceil \frac{q}{d} \rceil$. Note, however, that minimal value set polynomials $f(x) \in \mathbb{F}_q[x]$, seen as rational functions for which $f(\infty) = \infty$, may not give rise to *m.v.s.r.f.*. In fact, if a such polynomial f is considered as a rational function in $\mathbb{F}_q(x)$, then one can easily check that $V_f = \{f(\alpha) \mid \alpha \in \mathbb{P}^1\}$ satisfies

$$\#V_f = \begin{cases} \lceil \frac{q+1}{d} \rceil & \text{if } d \text{ divides } q, \\ \lceil \frac{q+1}{d} \rceil + 1 & \text{otherwise,} \end{cases} \tag{2}$$

where $d = \deg f$. This immediately raises a few questions:

i) Do *m.v.s.r.f.* of degree d, where $d \nmid q$, exist? Can they be characterized?

ii) What about the ones where $d \mid q$? Do they all arise from minimal value set polynomials?

iii) More generally, can one characterize all rational functions $h \in \mathbb{F}_q(x)$ for which $\#V_h = \lceil \frac{q+1}{d} \rceil$ or $\#V_h = \lceil \frac{q+1}{d} \rceil + 1$?

Motivated by these natural questions, this paper investigates rational functions $h \in \mathbb{F}_q(x)$ with somewhat small value set. It addresses many instances of the questions above. In particular, the following main results are proved.

Theorem 1.1. *If the rational function $h(x) \in \mathbb{F}_q(x)$ is such that $\mathbb{F}_q(x)/\mathbb{F}_q(h(x))$ is a Galois extension, then either $\#V_h = \lceil \frac{q+1}{d} \rceil$ or $\#V_h = \lceil \frac{q+1}{d} \rceil + 1$. Moreover, an explicit description of each case can be provided.*

Theorem 1.2. *Let $h(x) = f(x)/g(x)$ be a rational function, where $f(x)$ and $g(x)$ are coprime polynomials over $\mathbb{F}_q$, $\deg(g) = d$ and $\deg(f) = d - s$, $0 < s \leq d$. If $\delta := \sqrt{q} - (d-s)(d-s+1)$ is positive, and*

$$\#V_h < \left\lceil \frac{q+1}{d} \right\rceil + \frac{\delta^2 + 1}{(d-1)d^2} - 1.$$

then $\mathbb{F}_q(x) \mid \mathbb{F}_q(h(x))$ is a Galois extension.

The paper is organized as follows. In Section 2, some notation are presented, and a connection between rational functions $h(x) \in \mathbb{F}_q(x)$ and certain plane algebraic curves $\mathcal{C}_h$ is established. Section 3 proves Theorem 1.1. Section 4 discusses rational functions of degree 3 as a prototype for the following sections. Section 5, in connection with Galois Theory, proves the main facts regarding the components of the plane curve associated to the rational function $h(x)$. Section 6 proves a general result which implies Theorem 1.2.

Remark 1.3. *As the paper is still under revision, the proofs of some assertions are omitted. The complete proofs will appear in a preprint.*

2 Value set and algebraic curves

Given a rational function $h(x) = f(x)/g(x)$, let us consider the algebraic curve $\mathcal{C}_h : G(X,Y) = 0$, where

$$G(X,Y) = f(X)g(Y) - f(Y)g(X). \tag{3}$$

Note that if $h(x)$ is not a permutation of $\mathbb{P}^1(\mathbb{F}_q)$, then one can always assume that $g(x)$ has no roots in $\mathbb{F}_q$. In this case, for any given a point $P = (x_0, y_0) \in \mathcal{C}_h \cap AG(2,q)$, we have

$$f(x_0)/g(x_0) = f(y_0)/g(y_0).$$

This gives a close relationship between $V_h \cap \mathbb{F}_q = \{\alpha_1, \ldots, \alpha_r\}$ and the affine $\mathbb{F}_q$-points on curve $\mathcal{C}_h$. Note that for $n_i := \#h^{-1}(\alpha_i)$, we clearly have $\sum_{i=1}^r n_i = q$.

Since $h(x) = h(y)$ for each $x, y \in h^{-1}(\alpha_i)$, there are exactly $\sum_{i=1}^r n_i^2$ points in $\mathcal{C}_h \cap AG(2,q)$. Also, such a number strictly depends on the number of absolutely irreducible components defined over $\mathbb{F}_q$ of $\mathcal{C}_h$. Roughly speaking, if the degree of h (and then the degree of $\mathcal{C}_h$) is small with respect to q, the smaller the value set the larger the number of absolutely irreducible components defined over $\mathbb{F}_q$ of $\mathcal{C}_h$. This idea will be better detailed in Theorems 6.1 and 6.2. Actually, the type and the number of components of $\mathcal{C}_h$ gives even more information.

Example 2.1. *Let us consider the following example. Let* $h(x) = \frac{f(x)}{g(x)} = \frac{2x^5-5x^4+5x^2-2x}{x^6-15x^4+20x^3-6x+1}$, *where* $6 \mid (q+1)$. *It can be proved that* $h(x)$ *is a m.v.s.r.f.. The polynomial* $G(X,Y) = f(X)g(Y) - f(Y)g(X)$ *factorizes as*

$$(X-Y)(XY-Y+1)(XY-2X+Y+1)(XY-X+1)(XY+X-2Y+1)(2XY-X-Y+2).$$

The components of $\mathcal{C}_h$ *consist of the line* $X = Y$ *and the five conics*

$$Y = c_1(X) = \frac{1}{1-X}, \quad Y = c_2(X) = \frac{2X-1}{X+1}, \quad Y = c_3(X) = \frac{X-1}{X},$$
$$Y = c_4(X) = \frac{X+1}{2-X}, \quad Y = c_5(X) = \frac{X-2}{2X-1}.$$

Consider for instance the component $Y = \frac{2X-1}{X+1}$. *For each* $x_0 \neq -1 \in \mathbb{F}_q$, *we have that* $h(x_0) = h(c_2(x_0)) = h\left(\frac{2x_0-1}{x_0+1}\right)$. *On the other hand*

$$h(x_0) = h(c_2(x_0)) = h(c_2(c_2(x_0))) = \cdots = h(c_2(c_2(\cdots c_2(x_0)))).$$

This shows that all the components of $\mathcal{C}_h$ *can be "composed" in the following way: from* $Y = c_i(X)$ *and* $Y = c_j(X)$ *one gets* $Y = c_i(c_j(X))$. *Each of the above conics can be represented by a* 2×2 *matrix with entries in* $\mathbb{F}_q$ *in the following way*

$$Y = \frac{\alpha X + \beta}{\gamma X + \delta} \mapsto \sigma = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}. \tag{4}$$

Table 1: Rational functions $h(x)$ arising from particular subgroups $\mathcal{H}$ of $\mathcal{G}$

C_3	$\frac{x^3-3x-1}{x^2+x}$
C_4	$\frac{x^4-6x^2+1}{x^3-x}$, $(p>2)$
C_5	$\frac{2x^5-20x^3+(10i-10)x^2+(5i-5)x-2}{x^4-(i-1)x^3-(i-1)x^2+x}$, where $i^2=5$
C_6	$\frac{x^6-15x^4+20x^3-6x+1}{2x^5-5x^4+5x^2-2x}$ $(p>3)$
S_3	$\frac{x^6+3x^5-5x^3+3x+1}{x^4+2x^3+x^2}$
D_8	$\frac{x^8+14x^4+1}{x^6-2x^4+x^2}$
D_{12}	$\frac{4x^{10}-20x^9+25x^8+20x^7-58x^6+20x^5+25x^4-20x^3+4x^2}{4x^{12}-24x^{11}+220x^9-165x^8-924x^7+1782x^6-924x^5-165x^4+220x^3-24x+4}$
$PGL(2,q)$	$\frac{(x^{q^2}-x)^{q+1}}{(x^q-x)^{q^2+1}}$

Clearly, the matrix (as the conic itself) is defined up to a scalar multiple, and its determinant does not vanish and therefore we can suppose it is 1*. Also,* σ *can be seen as an element of* $PGL(2,q)$*. In the example considered above the six matrices associated with the line* $X=Y$ *and the five conics form a group isomorphic to the cyclic group* C_6 *of order* 6*. Actually, we will show that this is not an isolated case. Indeed, to each rational function* h *can be attached a group which correspond to lines and conics which are components of* $\mathcal{C}_h$*; see Theorem 5.7.*

3 Galois extensions and the smallest value sets

The aim of this section is to prove Theorem 1.1. We are going to construct rational functions with "small" value set from certain Galois extensions. We begin with some preliminary facts.

Let $\mathcal{G}=PGL(2,q)$ be the automorphism group of the rational function field $F=\mathbb{F}_q(x)$. For any subgroup $\mathcal{H}=\{id=\sigma^0,\sigma,\ldots,\sigma^{d-1}\}$ of $\mathcal{G}$ of order d, consider its fixed field $F^{\mathcal{H}}$ and the Galois extension $F \mid F^{\mathcal{H}}$ of degree d. The minimum polynomial of x over $F^{\mathcal{H}}$ is

$$p_{\mathcal{H}}(t)=a_0+a_1t+\cdots+a_{d-1}t^{d-1}+t^d, \tag{5}$$

where $a_k=(-1)^{d-k}\sum_{0\le i_1<\cdots<i_{d-k}\le d-1}\sigma^{i_1}(x)\cdots\sigma^{i_k}(x)\in F^{\mathcal{H}}, k=0,\ldots,d-1$.

Lemma 3.1. *Following the notation above, for any* $k=1,\ldots,d$ *such that* a_k *is not a constant we have* $F^{\mathcal{H}}=\mathbb{F}_q(a_k(x))$.

In Table 1, we list some examples of rational functions $h(x)$ arising from particular subgroups $\mathcal{H}$ of $\mathcal{G}$ such that $F^{\mathcal{H}}=\mathbb{F}_q(h(x))$. Actually, in these examples $h(x)$ is always a_0 in (5).

Next proposition provides a link between the Galois group and the ramification structure of $\mathbb{F}_q(x)|\mathbb{F}_q(h(x))$.

Proposition 3.2. *Consider a rational function $h(x)$ over $\mathbb{F}_q$ of degree $d \geq 2$ such that the extension field $\mathbb{F}_q(x) \mid \mathbb{F}_q(h(x))$ is Galois of degree d. For any divisor α of d denote by n_α the number of places in $\overline{\mathbb{F}_q}(h(x))$ that decomposes in α places in $\overline{\mathbb{F}_q}(x)$. Then one of the following holds.*

i) $n_1 = 2$ *and* $n_\alpha = 0$ *for each* $\alpha > 1$,

ii) $d = 24$, $n_6 = n_8 = n_{12} = 1$, *or*

iii) $d = 60$, $n_{12} = n_{20} = n_{30} = 1$.

In Table 2 we list for each subgroup G of $PGL(2, q)$ all the possible configurations of short orbits according to [1]. Here Δ is the difference between the lower bound $\left\lceil \frac{q+1}{|G|} \right\rceil$ and the value set of η where $\mathbb{F}_q(x) \mid \mathbb{F}_q(\eta)$ has G as Galois group.

Theorem 3.3. *Let $h(x) \in \mathbb{F}_q(x)$ be a rational function for which $\mathbb{F}_q(x)/\mathbb{F}_q(h(x))$ is a Galois extension, and let $G \leq PGL(2, q)$ be such that $Gal(\mathbb{F}_q(x)/\mathbb{F}_q(h(x))) \cong G$. Then*

$$\Delta := \#V_h - \left\lceil \frac{q+1}{d} \right\rceil \in \{0, 1\}$$

is given according to Table 2.

Table 2: Oberwolfach table

Group G	Conditions	Short $\mathbb{F}_q$-orbits	Value set size	Lower bound	Δ
C_2	$q \equiv 1 \pmod 4$	$2\mathcal{O}_1$	$\frac{q-1}{2} + 2$	$\frac{q+1}{2}$	1
	$q \equiv 1 \pmod 4$	$--$	$\frac{q+1}{2}$	$\frac{q+1}{2}$	0
	$q \equiv -1 \pmod 4$	$2\mathcal{O}_1$	$\frac{q-1}{2} + 2$	$\frac{q+1}{2}$	1
	$q \equiv -1 \pmod 4$	$--$	$\frac{q+1}{2}$	$\frac{q+1}{2}$	0
C_d, $d > 2$	$d \mid q+1$, $q \equiv 1 \pmod 4$	$--$	$\frac{q+1}{d}$	$\frac{q+1}{d}$	0
	$d \mid q-1$, $q \equiv 1 \pmod 4$	$2\mathcal{O}_1$	$\frac{q-1}{d} + 2$	$\frac{q-1}{d} + 1$	1
	$d \mid q+1$, $q \equiv -1 \pmod 4$	$--$	$\frac{q+1}{d}$	$\frac{q+1}{d}$	0
	$d \mid q-1$, $q \equiv -1 \pmod 4$	$2\mathcal{O}_1$	$\frac{q-1}{d} + 2$	$\frac{q-1}{d} + 1$	1
D_4	$q \equiv 1 \pmod 4$	$3\mathcal{O}_2$	$\frac{q+1-6}{4} + 3$	$\frac{q-1}{4} + 1$	1
	$q \equiv 1 \pmod 4$	$1\mathcal{O}_2$	$\frac{q-1}{4} + 1$	$\frac{q-1}{4} + 1$	0
	$q \equiv -1 \pmod 4$	$2\mathcal{O}_2$	$\frac{q+1-4}{4} + 2$	$\frac{q+1}{4}$	1
	$q \equiv -1 \pmod 4$	$--$	$\frac{q+1}{4}$	$\frac{q+1}{4}$	0

Group	Conditions	Short $\mathbb{F}_q$-orbits	Value set	Lower bound	Δ
D_{2d}, $d>2$	$d \mid \frac{q+1}{2}$, $q \equiv 1 \pmod 4$	$2\mathcal{O}_d$	$\frac{q+1-2d}{2d}+2$	$\frac{q+1}{2d}+1$	1
	$d \mid \frac{q+1}{2}$, $q \equiv 1 \pmod 4$	$--$	$\frac{q+1}{2d}$	$\frac{q+1}{2d}$	0
	$d \mid (q+1)$ $d \nmid \frac{q+1}{2}$ $q \equiv 1 \pmod 4$	$1\mathcal{O}_d$	$\frac{q+1-d}{2d}+1$	$\frac{q+1-d}{2d}+1$	0
	$d \mid \frac{q-1}{2}$, $q \equiv 1 \pmod 4$	$1\mathcal{O}_2$, $2\mathcal{O}_d$	$\frac{q-1-2d}{2d}+3$	$\frac{q-1}{2d}+1$	1
	$d \mid \frac{q-1}{2}$, $q \equiv 1 \pmod 4$	$1\mathcal{O}_2$	$\frac{q-1}{2d}+1$	$\frac{q-1}{2d}+1$	0
	$d \mid (q-1)$ $d \nmid \frac{q-1}{2}$ $q \equiv 1 \pmod 4$	$1\mathcal{O}_2$, $1\mathcal{O}_d$	$\frac{q-1-d}{2d}+2$	$\frac{q-1-d}{2d}+1$	1
	$d \mid \frac{q-1}{2}$, $q \equiv -1 \pmod 4$	$1\mathcal{O}_2$	$\frac{q-1}{2d}+1$	$\frac{q-1}{2d}+1$	0
	$d \mid \frac{q-1}{2}$, $q \equiv -1 \pmod 4$	$1\mathcal{O}_2$, $2\mathcal{O}_d$	$\frac{q-1-2d}{2d}+3$	$\frac{q-1}{2d}+1$	1
	$d \mid (q-1)$, $d \nmid \frac{q-1}{2}$ $q \equiv -1 \pmod 4$	$1\mathcal{O}_2$, $1\mathcal{O}_d$	$\frac{q-1-d}{2d}+2$	$\frac{q-1-d}{2d}+1$	1
	$d \mid \frac{q+1}{2}$, $q \equiv -1 \pmod 4$	$--$	$\frac{q+1}{2d}$	$\frac{q+1}{2d}$	0
	$d \mid \frac{q+1}{2}$, $q \equiv -1 \pmod 4$	$2\mathcal{O}_d$	$\frac{q+1-2d}{2d}+2$	$\frac{q+1}{2d}$	1
	$d \mid (q+1)$, $d \nmid \frac{q+1}{2}$, $q \equiv -1 \pmod 4$	$1\mathcal{O}_d$	$\frac{q+1-d}{2d}+1$	$\frac{q+1-d}{2d}+1$	0
A_4	$q \equiv 1 \pmod{12}$	$1\mathcal{O}_6$, $2\mathcal{O}_4$	$\frac{q+1-6-8}{12}+3$	$\frac{q-1}{12}+1$	1
	$q \equiv 5 \pmod{12}$	$1\mathcal{O}_6$	$\frac{q+1-6}{12}+1$	$\frac{q-5}{12}+1$	0
	$q \equiv 9 \pmod{12}$	$1\mathcal{O}_6$, $1\mathcal{O}_4$	$\frac{q+1-4-6}{12}+2$	$\frac{q-9}{12}+1$	1
	$q \equiv 7 \pmod{12}$	$2\mathcal{O}_4$	$\frac{q+1-8}{12}+2$	$\frac{q-7}{12}+1$	1
	$q \equiv 11 \pmod{12}$	$--$	$\frac{q+1}{12}$	$\frac{q+1}{12}$	0
	$q \equiv 3 \pmod{12}$	$1\mathcal{O}_4$	$\frac{q+1-4}{12}+1$	$\frac{q-3}{12}+1$	0
S_4	$q \equiv 1 \pmod{24}$	$1\mathcal{O}_6$, $1\mathcal{O}_8$, $1\mathcal{O}_{12}$	$\frac{q+1-6-8-12}{24}+3$	$\frac{q-1}{24}+1$	1
	$q \equiv 3 \pmod{24}$	$1\mathcal{O}_4$,	$\frac{q+1-4}{24}+1$	$\frac{q-3}{24}+1$	0
	$q \equiv 5 \pmod{24}$	$1\mathcal{O}_6$,	$\frac{q+1-6}{24}+1$	$\frac{q-5}{24}+1$	0
	$q \equiv 7 \pmod{24}$	$1\mathcal{O}_8$,	$\frac{q+1-8}{24}+1$	$\frac{q-7}{24}+1$	0
	$q \equiv 9 \pmod{24}$	$1\mathcal{O}_4$, $1\mathcal{O}_6$	$\frac{q+1-10}{24}+2$	$\frac{q-9}{24}+1$	1
	$q \equiv 11 \pmod{24}$	$1\mathcal{O}_{12}$	$\frac{q+1-12}{24}+1$	$\frac{q-11}{24}+1$	0
	$q \equiv 13 \pmod{24}$	$1\mathcal{O}_6$, $1\mathcal{O}_8$	$\frac{q+1-6-8}{24}+2$	$\frac{q-13}{24}+1$	1
	$q \equiv 17 \pmod{24}$	$1\mathcal{O}_6$, $1\mathcal{O}_{12}$	$\frac{q+1-6-12}{24}+2$	$\frac{q-17}{24}+1$	1
	$q \equiv 19 \pmod{24}$	$1\mathcal{O}_8$, $1\mathcal{O}_{12}$	$\frac{q+1-8-12}{24}+2$	$\frac{q-19}{24}+1$	1
	$q \equiv 23 \pmod{24}$	$--$	$\frac{q+1}{24}$	$\frac{q+1}{24}$	0
S_5	$q \equiv 1 \pmod{60}$	$1\mathcal{O}_{12}$, $1\mathcal{O}_{20}$, $1\mathcal{O}_{30}$	$\frac{q+1-12-20-30}{60}+3$	$\frac{q-1}{60}+1$	1

Group	Conditions	Short $\mathbb{F}_q$-orbits	Value set	Lower bound	Δ
	$q \equiv 9 \pmod{60}$	$1\mathcal{O}_{10}$	$\frac{q+1-10}{60}+1$	$\frac{q-9}{60}+1$	0
	$q \equiv 11 \pmod{60}$	$1\mathcal{O}_{12}$	$\frac{q+1-12}{60}+1$	$\frac{q-11}{60}+1$	0
	$q \equiv 19 \pmod{60}$	$1\mathcal{O}_{20}$	$\frac{q+1-20}{60}+1$	$\frac{q-19}{60}+1$	0
	$q \equiv 21 \pmod{60}$	$1\mathcal{O}_{10}$, $1\mathcal{O}_{12}$	$\frac{q+1-10-12}{60}+2$	$\frac{q-21}{60}+1$	1
	$q \equiv 29 \pmod{60}$	$1\mathcal{O}_{30}$	$\frac{q+1-30}{60}+1$	$\frac{q-29}{60}+1$	0
	$q \equiv 31 \pmod{60}$	$1\mathcal{O}_{12}$, $1\mathcal{O}_{20}$	$\frac{q+1-12-20}{60}+2$	$\frac{q-31}{60}+1$	1
	$q \equiv 41 \pmod{60}$	$1\mathcal{O}_{12}$, $1\mathcal{O}_{30}$	$\frac{q+1-12-30}{60}+2$	$\frac{q-41}{60}+1$	1
	$q \equiv 49 \pmod{60}$	$1\mathcal{O}_{20}$, $1\mathcal{O}_{30}$	$\frac{q+1-20-30}{60}+2$	$\frac{q-49}{60}+1$	1
	$q \equiv 59 \pmod{60}$	$--$	$\frac{q+1}{60}$	$\frac{q+1}{60}$	0
$\mathbb{Z}_p^m$	$p^m \leq q = p^h$	$1\mathcal{O}_1$	$\frac{q+1-1}{p^m}+1$	$\frac{q}{p^m}+1$	0
$\mathbb{Z}_p^m \rtimes C_d$	$d \mid (q-1)$, $d \mid (p^m-1)$	$1\mathcal{O}_1$, $1\mathcal{O}_{dp^m}$	$\frac{q+1-1-p^m}{dp^m}+2$	$\frac{q-p^m}{dp^m}+1$	1
$PSL(2,p^m)$	$h = 2km$	$1\mathcal{O}_{p^m+1}$, $1\mathcal{O}_{p^m(p^m-1)}$	$\frac{q+1-1-p^m-p^m(p^m-1)}{p^m(p^{2m}-1)/2}+2$	$\frac{q-p^{2m}}{p^m(p^{2m}-1)/2}+1$	1
	$h = (2k+1)m$	$1\mathcal{O}_{p^m+1}$	$\frac{q+1-1-p^m}{p^m(p^{2m}-1)/2}+1$	$\frac{q-p^m}{p^m(p^{2m}-1)/2}+1$	0
$PGL(2,p^m)$	$h = 2km$	$1\mathcal{O}_{p^m+1}$, $1\mathcal{O}_{p^m(p^m-1)}$	$\frac{q+1-1-p^m-p^m(p^m-1)}{p^m(p^{2m}-1)}+2$	$\frac{q-p^{2m}}{p^m(p^{2m}-1)}+1$	1
	$h = (2k+1)m$	$1\mathcal{O}_{p^m+1}$	$\frac{q+1-1-p^m}{p^m(p^{2m}-1)}+1$	$\frac{q-p^m}{p^m(p^{2m}-1)}+1$	0

Remark 3.4. *The examples listed in Table 2 provide m.v.s.r.f., depending on the characteristic of the field and the size of the subgroup.*

4 Degree three rational functions

In this section, we provide a more specific description of the spectrum of possible sizes of the value set of a degree-three rational function $h(x)$. The results here, which are interesting on their own, will serve as prototype for what will be proved in the next sections. Assume $char(k) \neq 2, 3$, and suppose $d \neq 0$. Without loss of generality, up to Möebius transformations, we can consider $h(x) = \frac{x^2+d}{x^3+ax^2+bx+c} \in \mathbb{F}_q(x)$. The curve $\mathcal{C}_h$ has equation $(X-Y)F(X,Y) = 0$, where

$$F(X,Y) := X^2Y^2 + dX^2 + (d-b)XY + (ad-c)X + dY^2 + (ad-c)Y + bd.$$

We start investigating the main features of the curve $F(X,Y) = 0$. We will need these technical results later on.

Proposition 4.1. *If $\mathcal{D}$ is the projective closure of $F(X,Y) = 0$, then the following holds.*

i) $(1:0:0)$ *and* $(0:1:0)$ *are two ordinary singularities of* $\mathcal{D}$.

ii) The remaining singular points of $\mathcal{D}$, if any, lie on the pair of lines

$$(X-Y)\left(X+Y+\frac{ad-c}{2d}\right)=0.$$

iii) The curve $\mathcal{D}$ has a singular point on the line $X+Y+\frac{ad-c}{2d}=0$ if and only if

$$\begin{cases} b=\left(\frac{ad-c}{2d}\right)^2 \\ and \\ \Big(ad-c\Big)\Big((ad-c)^2+4d^3\Big)=0. \end{cases}$$

In this case, the singular point is $P=(\frac{ad-c}{2d}:0:1)$.

iv) The curve $\mathcal{D}$ has a singular point on the line $X-Y=0$ if and only if

$$27(ad-c)^2=b(b-9d)^2.$$

That is, $a=\dfrac{3c+(b-9d)\sqrt{\frac{b}{3}}}{3d}$. In this case, the singular point is $P=(\sqrt{\frac{b}{3}}:\sqrt{\frac{b}{3}}:1)$. [1]

v) The curve $\mathcal{D}$ is reducible if and only if $c=ad$ and $b=9d$. In this case, we have

$$F(X,Y)=\Big(XY-\sqrt{-d}Y+\sqrt{-d}X-3d\Big)\Big(XY+\sqrt{-d}Y-\sqrt{-d}X-3d\Big)$$

In particular, $F(X,Y)$ is reducible over $\mathbb{F}_q$ if, and only if, $-d\in\mathbb{F}_q$ is a square.

Moreover, if $\mathcal{D}$ is irreducible then $\mathcal{D}$ has genus $g(\mathcal{D})=0$ in cases (3) and (4), and genus $g(\mathcal{D})=1$ otherwise.

Recall that we are interested in the number of points in $\mathcal{C}_h\cap AG(2,q)$. By [2, Theorem 9.57] the number R_q of points in $\mathcal{D}\cap PG(2,q)$ satisfies

$$q+1-2g\sqrt{q}-3+g\leq R_q\leq q+1+2g\sqrt{q}+3-g.$$

Denote by ℓ the line $X-Y=0$. Concerning the curve $\mathcal{C}_h$, we have the following possibilities.

i) $\mathcal{D}$ is irreducible. So $\mathcal{C}_h$ factorizes as

$$(X-Y)F(X,Y)$$

[1] Where the choice of $\sqrt{\frac{b}{3}}$ in $P=(\sqrt{\frac{b}{3}}:\sqrt{\frac{b}{3}}:1)$ follows the same choice of $\sqrt{\frac{b}{3}}$ made in the definition of a.

and the number of points in $\mathcal{C}_h \cap AG(2,q)$ is

$$2q - 2\sqrt{q} - 7 \leq \underbrace{q}_{\ell \cap AG(2,q)} + \underbrace{q + 1 - 2g\sqrt{q} - 3 + g}_{\mathcal{D} \cap PG(2,q)} - 6 \leq R_q \leq$$
$$\leq \underbrace{q}_{\ell \cap AG(2,q)} + \underbrace{q + 1 + 2g\sqrt{q} + 3 - g}_{\mathcal{D} \cap PG(2,q)} - 2 \leq 2q + 2\sqrt{q} + 1,$$

where we deleted the ideal points of $X - Y = 0$ and of $\mathcal{D}$ and the (possible) intersection points in $\ell \cap \mathcal{D}$.

ii) $\mathcal{D}$ is reducible and it is the union of two conics not defined over $\mathbb{F}_q$. It is easily seen that the two conics intersect at ℓ and at the ideal line. So, the size of $\mathcal{C}_h \cap AG(2,q)$ is q.

iii) $\mathcal{D}$ is reducible and it is the union of two conics defined over $\mathbb{F}_q$. As above the two conics intersect at ℓ and at the ideal line and the size of $\mathcal{C}_h \cap AG(2,q)$ is either $3q-2$ or $3q-6$, depending on $3d$ being or not a square in $\mathbb{F}_q$.

Now, suppose that $h(x)$ is a permutation of $\mathbb{P}^1$. Then, the size of $\mathcal{C}_h \cap AG(2,q)$ is between $q-1$ and q (depending on $h(\infty) = \infty$ or not). This clearly corresponds to case (ii).

On the other hand, suppose $h(x)$ is a m.v.s.r.f., or, more in general, its value set has size $q/3 + \epsilon$, with $\epsilon < (q - 2\sqrt{q} - 1)/6$. Let n_i be the number of elements $\alpha \in \mathbb{F}_q$ for which $\#h^{-1}(\alpha) = i, i = 0, \ldots, 3$. Then

$$\begin{cases} n_1 + n_2 + n_3 = q/3 + \epsilon, \\ n_1 + 2n_2 + 3n_3 = q. \end{cases}$$

We conclude that n_3 satisfies

$$3n_3 + 2(q/3 + \epsilon - n_3) \geq q \Longrightarrow n_3 \geq q/3 - 2\epsilon.$$

This means that the number of points in $\mathcal{C}_h \cap AG(2,q)$ is at least

$$n_1 + 4n_2 + 9n_3 = (n_1 + 2n_2 + 3n_3) + 2(n_2 + 2n_3) + 2n_3 \geq q + 2(2q/3 - \epsilon) + 2q/3 - 4\epsilon = 3q - 6\epsilon.$$

Since $\epsilon < (q - 2\sqrt{q} - 1)/6$, this case corresponds to case (3). This concept will be generalized and clarified in Theorem 6.2.

5 Components of the curve $\mathcal{C}_h$ associated to a rational function $h(x)$

As we have seen in (4), there is a natural correspondence between elements of $PGL(2,q)$ and degree one rational functions arising from the factorization of $f(X)g(Y) - f(Y)g(X)$. Also, in the previous section we saw that for degree three rational functions $h(x) = \frac{x^2+d}{x^3+ax^2+bx+c} \in \mathbb{F}_q(x)$ the curve $\mathcal{C}_h$ splits into three components, which form a cyclic subgroup of order three in $PGL(2,q)$. The aim of this section is to collect several results that will establish such a relationship for a more general rational function.

Proposition 5.1. *Let K be any field and $H = \{\sigma_i(t) = \frac{a_i t+b_i}{c_i t+d_i} : i = 1, \ldots, n\}$ a finite subgroup of $\mathrm{Aut}(K(t)) \cong PGL(2, K)$. Then the polynomial*

$$G(X,Y) = \prod_{i=1}^{n} \Big((c_i Y + d_i)X - (a_i Y + b_i) \Big)$$

has the following properties.

i) $G(X,Y) = (X-Y)H(X,Y)$, where $H(X,Y)$ is symmetric. In particular, $G(X,Y) = -G(Y,X)$.

ii) There exists a degree-n polynomial $f(t) \in K[t]$, coprime with $g(t) := \prod_{i=1}^{n}(c_i t + d_i)$, such that

$$G(X,Y) := f(X)g(Y) - f(Y)g(X). \tag{6}$$

Moreover, the number of linear factors of $G(X,Y)$ is a divisor of $\deg g(t)$. In particular, if $G(X,Y)$ has a nonlinear factor then $\frac{n}{2} \leq \deg g(t) \leq n-1$, and the number of linear factors is upper bounded by $\frac{n}{2}$.

Lemma 5.2. *Let K be any field. Let $\frac{u(t)}{v(t)}$ and $\frac{f(t)}{g(t)}$ be rational functions in $K(t)$, with $\gcd(u(t), v(t)) = \gcd(f(t), g(t)) = 1$. Then $\frac{u(t)}{v(t)} \in K\left(\frac{f(t)}{g(t)}\right)$ if and only if there exist homogeneous polynomials $T_1, T_2 \in K[X,Y]$ of the same degree such that*

$$u(t) = T_1(f(t), g(t)) \text{ and } v(t) = T_2(f(t), g(t)).$$

Lemma 5.3. *Let K be any field. If $T_1, T_2 \in K[X,Y]$ are homogeneous polynomials of the same degree, then*

$$\frac{T_1(X,Y)T_2(Z,W) - T_1(Z,W)T_2(X,Y)}{XW - YZ}$$

is a homogeneous polynomial in $K[X,Y,Z,W]$.

Proposition 5.4. *Let K be any field. For any subgroup $H \leq \mathrm{Aut}(K(t))$, let $f(t)$ and $g(t)$ be the polynomials given by Proposition 5.1. Then*

i) $\mathrm{Gal}\left(K(t)/K\left(\frac{f(t)}{g(t)}\right)\right) = H$, and

ii) A rational function $\frac{u(t)}{v(t)} \in K(t)$ is H-invariant if and only if

$$u(X)v(Y) - u(Y)v(X) = \Big(f(X)g(Y) - f(Y)g(X)\Big)h(X,Y)$$

for some $h(X,Y) \in K[X,Y]$, homogeneous in the variables $f(X), g(Y), f(Y)$ and $g(X)$.

Lemma 5.5. *Let H be a subgroup of $\mathrm{Aut}(\mathbb{F}_q(t))$ of order n such that the polynomial $g(t)$ in Proposition 5.1 is constant. That is, all elements in the group H are linear. Then H is isomorphic to semidirect product of an elementary abelian p-group of order $p^m, m \geq 0$, with a cyclic group of order N, with $N|(q-1)$. Moreover, for $N > 2$, if $H = \{a_i t + b_i : i = 1, \ldots, n = Np^m\}$ and $F(X) = \prod_{i=1}^{n}(a_i X + b_i)$, then up to a linear change of variables, there exists a p-linearized polynomial $f(X) \in \mathbb{F}_q[X]$ of degree p^m, and an integer N, divisor of $p^m - 1$, such that $F(X) = f(X)^N$.*

Corollary 5.6. *Let H be as in Lemma 5.5. If a rational function $\frac{u(t)}{v(t)} \in \mathbb{F}_q(t)$ is H-invariant, then up to a linear change of variables, we have*

$$u(X)v(Y) - u(Y)v(X) = \Big(f(X)^N - f(Y)^N\Big)h(f(X)^N, f(Y)^N)$$

for some $h(X,Y) \in K[X,Y]$.

Using the previous results, we arrive at the following theorem, which gives the general setting in which Example 2.1 falls.

Theorem 5.7. *Let $G(X,Y) = f(Y)g(X) - f(X)g(Y)$. The factors of degree $d \leq 2$ of type $g_i(X,Y) = a_iXY + b_iX + c_iY + d_i$, where $a_id_i - b_ic_i \neq 0$, (removing repetition, if any) are associated to the elements $\sigma_i(t) := \frac{-b_it-d_i}{a_it+c_i} \in \mathrm{Aut}(\mathbb{F}_q(x)) \cong PGL(2,q)$ and have the induced group structure.*

Corollary 5.8. *Let $G(X,Y) = f(Y)g(X) - f(X)g(Y)$. If the group of factors of degree $d \leq 2$ of $G(X,Y)$ has order N, then there exists polynomials f_1 and f_2 such that*

i) $G(X,Y) = f(Y)g(X) - f(X)g(Y) = \Big(f_1(Y)g_1(X) - f_1(X)g_1(Y)\Big)\prod f_i(X,Y)$,

ii) $\max\{\deg f_1, \deg f_2\} = N$.

In particular, if the group is cyclic of order $N \neq 0 \mod p$, ($N > 2$), then a linear change of variables gives $f_1(Y)g_1(X) - f_1(X)g_1(Y) = X^N - Y^N$.

6 Minimal and almost minimal value set rational functions

Finally, we present our main result on minimal values set rational functions. Also, Theorem 6.2 partially extends these results to rational functions having values sets of size "close" to the minimum.

Theorem 6.1. *Let $h(x) = f(x)/g(x)$ be a non constante rational function, where $f(x)$ and $g(x)$ are coprime polynomials over $\mathbb{F}_q$. Without loss of generality we can suppose that $\deg(g) = d$ and $\deg(f) = d - s$, $0 < s \leq d$. Consider the curve $\mathcal{C}_h$ defined by $G(X,Y) = 0$ as in (3). Then*

i) If a line ℓ is a component of $\mathcal{C}_h$, then $\ell : X - \alpha Y - \beta = 0$, with $\alpha^s = 1$.

ii) No curves of equation $Y = \alpha_r X^r + \alpha_{r-1}X^{r-1} + \cdots + \alpha_0$ or $X = \alpha_r Y^r + \alpha_{r-1}Y^{r-1} + \cdots + \alpha_0$, $r > 1$, $\alpha_r \neq 0$, are components of $\mathcal{C}_h$.

iii) If s is comprime with p all the lines which are components of $\mathcal{C}_h$ are

$$\ell_i \ : \ X = \alpha^i Y + \beta(\alpha^i - 1)/(\alpha - 1), \quad i = 1, \ldots, N, \tag{7}$$

for some $\alpha, \beta \in \mathbb{F}_q, \alpha^s = 1$ of order $N \mid s$.

iv) If N is the number of lines contained in $\mathcal{C}_h$, then $\mathcal{C}_h$ is equivalent to

$$(X^N - Y^N) \prod f_i(X, Y) = 0$$

with $\deg(f_i) > 1$.

v) Suppose that there exist N linear components of $\mathcal{C}_h$ of type (7). Then any other component of $\mathcal{C}_h$ with ideal part different from $X^i Y^j$ has degree at least N.

vi) $\mathcal{C}_h$ can contain at most d components.

vii) If $\mathcal{C}_h$ contains d components, then they are s lines and $d - s$ conics.

Finally, we analyze the case in which the rational function is close to be a m.v.s.r.f..

Theorem 6.2. *Let $h(x) = f(x)/g(x)$ be a rational function, where $f(x)$ and $g(x)$ are coprime polynomials over $\mathbb{F}_q$, $\deg(g) = d$ and $\deg(f) = d - s$, $0 < s \leq d$. If $\delta := \sqrt{q} - (d - s)(d - s + 1)$ is positive, and*

$$\#V_h < \left\lceil \frac{q+1}{d} \right\rceil + \frac{\delta^2 + 1}{(d-1)d^2} - 1.$$

then

i) $\mathcal{C}_h$ contains d absolutely irreducible $\mathbb{F}_q$-rational components.

ii) $\mathcal{C}_h$ contains s lines of type $X = \alpha_i Y + \beta_i$ and $d - s$ conics of type $XY + \gamma_i X + \delta_i Y + \epsilon_i = 0$.

iii) The extension $\mathbb{F}_q(x) \mid \mathbb{F}_q(h(x))$ is Galois of degree d.

Corollary 6.3. *Suppose $\delta := \sqrt{q} - (d - s)(d - s + 1) > 0$. Then there exists no rational function $h(x)$ of degree d over $\mathbb{F}_q$ for which*

$$\left\lceil \frac{q+1}{d} \right\rceil + 2 \leq \#V_h < \left\lceil \frac{q+1}{d} \right\rceil + \frac{\delta^2 + 1}{(d-1)d^2} - 1.$$

Proof. By Theorem 6.2, the extension $\mathbb{F}_q(x) \mid \mathbb{F}_q(h(x))$ is Galois of degree d. Now, Table 2 shows that in all these cases the difference between $\#V_h$ and $\left\lceil \frac{q+1}{d} \right\rceil$ is at most 1. □

7 Acknowledgement

This research was supported through the programme "Research in Pairs" by the Mathematisches Forschungsinstitut Oberwolfach in 2019.

References

[1] P.J. Cameron, G.R.Omid, B. Tayfeh-Rezaie. 3-Designs form $PGL(2, q)$. Electronic Journal of Combinatorics **13**, (2006) #R50.

[2] J.W.P. Hirschfeld, G. Korchmáros, F. Torres. Algebraic curves over a finite field. Princeton Series in Applied Mathematics (2008).