Published in Journal of Algebra and Its Applications (2024)
https://doi.org/10.1142/S0219498825503190

CUBIC RATIONAL EXPRESSIONS OVER A FINITE FIELD

SANDRO MATTAREI AND MARCO PIZZATO

Abstract. We study and partially classify cubic rational expressions over a finite field $\mathbb{F}_q$, up to equivalence given by composition with independent Möbius transformations on each side. When q is even we obtain a full classification. When q is odd we restrict our classification to expressions with at most three ramification points. However, we prove a general upper bound of $4q$ for the total number of equivalence classes.

1. Introduction

The initial motivation for this study arose from an enumeration problem for irreducible polynomials over a finite field satisfying certain symmetries. Gauss gave a formula for the number of all irreducible monic polynomials of a given degree over the field $\mathbb{F}_q$ of q elements. A similar formula counting the self-reciprocal irreducible monic polynomials of degree $2n$ was found by Carlitz in [Car67]. Here a polynomial $F(x)$ over a field is *self-reciprocal* if $x^{\deg F} \cdot F(1/x) = F(x)$. It is easy to see that any irreducible self-reciprocal polynomial of degree greater than one has even degree $2n$, and that it can actually be written in the form $F(x) = x^n \cdot f(x + 1/x)$, for some polynomial $f(x)$ of degree n. This led Ahmadi, in [Ahm11], to study polynomials obtained from such $f(x)$ through a more general *quadratic transformation,* namely, polynomials of the form $F(x) = h(x)^n \cdot f\big(g(x)/h(x)\big)$, where $g(x)$ and $h(x)$ are coprime polynomials with $\max(\deg g, \deg h) = 2$, and $n = \deg f$. Over the field $\mathbb{F}_q$ with q odd, the enumeration formula found in [Ahm11, Theorem 2] for the number of monic irreducible polynomials among those, of degree $2n > 2$ and for a given quadratic rational expression $g(x)/h(x)$, equals Carlitz's count for the special case where $g(x)/h(x) = (x^2 + 1)/x = x + x^{-1}$.

The fact that Carlitz's formula extends unchanged to arbitrary quadratic transformations was given a simple explanation in [MP17]. It depends on the fact that such enumeration remains essentially unaffected when the quadratic rational expression $g(x)/h(x)$ is composed with Möbius transformations on either side. In this context, *Möbius transformations* are rational expressions of degree 1 over an arbitrary field, rather than just $\mathbb{C}$ as in the more traditional meaning. In this paper we call *equivalent* two rational expressions, of any degree, if one can be obtained from the other by composing it with Möbius transformations on each side. In particular, one finds that all quadratic rational expressions

2000 *Mathematics Subject Classification.* Primary 12E05.
Key words and phrases. Cubic rational function.

$g(x)/h(x)$ over an algebraically closed field of odd characteristic are equivalent (see Section 3). Over a finite field $\mathbb{F}_q$ with q odd, quadratic rational expressions split into two equivalence classes. However, expressions in both classes happen to give the same enumeration formula for the irreducible polynomials $F(x)$ arising through them.

A natural extension is a study of irreducible polynomials $F(x)$ arising through a transformation of higher degree, that is, obtained as described above but with $g(x)/h(x)$ a rational expression (also commonly called *rational function*) of arbitrary degree r. The special case where $g(x) = 1$ is of practical relevance because of a direct connection with *transformation shift registers,* which have numerous applications including in the design of stream ciphers, see [CHPW15, Section 3]. Polynomials arising through a more general cubic transformation were addressed in [MP22], where various enumeration formulas were found. From a wider perspective, a great interest on the existence, and on enumeration when possible, of irreducible polynomials over finite fields satisfying special properties, can be seen from a glance at [MP13, Chapter 5].

For such investigations it is desirable to have a classification up to equivalence, or at least a partial classification, of cubic rational expressions (or *cubic expressions* for short) over a finite field. That is the main goal of this paper. We should mention that the study of rational expressions up to equivalence may be interpreted in terms of certain extensions of function fields. At the end of Section 2 we review some literature on cubic extensions of function fields. We discuss its connections with our work, and point out how the available literature falls short of providing the explicit results that we need here in view of applications such as those in [MP22]. In the present paper we take a more direct approach and bypass the interpretation in terms of function fields.

As a preliminary step to understanding cubic expressions over a finite field, in Section 4 we describe a classification of cubic expressions over an algebraically closed field K. This is not a hard task, but we could not locate the desired result in the literature. Because equivalence classes are the orbits of a certain action of the group $\mathrm{PGL}_2(K) \times \mathrm{PGL}_2(K)$ on the 7-dimensional variety of all cubic expressions, dimension reasons show that the set of equivalence classes must involve at least one parametric family. In fact, according to Theorem 5, every cubic expression over an algebraically closed field of characteristic different from two or three is either equivalent to x^3, or belongs to a certain 1-parameter family. The elements of the latter are not pairwise inequivalent, but one can explicitly tell which values of the parameter give rise to equivalent expressions, in terms of a cross-ratio formed from the (up to four distinct) ramification points of each expression. We supplement that classification with corresponding classifications in the small characteristics three and two.

Passing from an algebraically closed ground field to a classification of cubic expressions over a finite field $\mathbb{F}_q$, which we address in Section 5, requires understanding how the stabilizer in $\mathrm{PGL}_2(\mathbb{F}_q) \times \mathrm{PGL}_2(\mathbb{F}_q)$ of a cubic expression may permute its ramification points (in $\overline{\mathbb{F}}_q \cup \{\infty\}$). While descending from the

algebraic closure $\overline{\mathbb{F}}_q$ to $\mathbb{F}_q$ could be framed in terms of a certain Galois cohomology group, that description would provide no saving in calculations over the direct approach adopted here. Theorem 11 classifies the cubic expressions, over any finite field of characteristic at least five, that have at most three (distinct) ramification points. Theorem 12 does the same in characteristic three.

In Section 7 we obtain a corresponding result in characteristic two, which is Theorem 15. Although that statement is more complicated than those in the odd characteristics, it classifies the totality of cubic expressions over a finite field of characteristic two, because such expressions cannot have more than two ramification points. In particular, over a finite field $\mathbb{F}_q$ of characteristic two there are a total of $2q + 2$ equivalence classes if q is a square, and $2q$ otherwise. We also compute the cardinalities of each of those equivalence classes (that is, the orbit lengths in the group action described above), in Theorem 17.

Because of our restriction to cubic rational expressions with at most three ramification points, we are unable to compute the exact number of equivalence classes over $\mathbb{F}_q$ in odd characteristic. However, in Section 6 we produce an upper bound of $4q$ for the number of classes over a finite field $\mathbb{F}_q$ of odd characteristic. This requires an analysis of certain stabilizers in the action of $\mathrm{PGL}_2(\mathbb{F}_q) \times \mathrm{PGL}_2(\mathbb{F}_q)$.

After setting up terminology and preliminary results in Section 2, we devote Section 3 to a treatment of quadratic rational expressions over a finite field, which differs from the more direct one given in [MP17]. The present version emphasizes the use of ramification and branch points, and the action of $\mathrm{PGL}_2(\mathbb{F}_q) \times \mathrm{PGL}_2(\mathbb{F}_q)$, anticipating in a simpler setting their later use for the case of cubic rational expressions. In particular, it includes computing the cardinalities of the two equivalence classes of quadratic rational expressions over a finite field.

The research leading to this paper began when the second author was a PhD student at the University of Trento, Italy, under the supervision of the first author. Some of the results in this paper have appeared among other results in [Piz13]: our Theorem 11 is [Piz13, Proposition 3.2.7], our Theorem 12 is [Piz13, Proposition 3.2.8], and our Theorem 15 is essentially [Piz13, Proposition 3.2.9].

We are grateful to a referee for a number of comments and requests for clarification that prompted us to produce an improved exposition.

2. Preliminaries on rational expressions

Let K be an arbitrary field in the first four paragraphs of this section. Consider a rational expression $R(x) = g(x)/h(x) \in K(x)$, where $g(x)$ are $h(x)$ coprime polynomials in $K[x]$. Its *degree* $\deg R$ is the integer $\max(\deg g, \deg h)$; the expression will be called *linear, quadratic, cubic,* etc., when its degree equals $1, 2, 3$, etc. It is easy to see that the degree of the composite of two rational expressions equals the product of their degrees.

In particular, the linear rational expressions, also known as *linear fractional transformations,* form a group isomorphic to the projective general linear group $\mathrm{PGL}_2(K)$, in a way that we briefly recall. Since the projective line $\mathbb{P}^1(K)$ is the set of one-dimensional subspaces of the linear space K^2, we may use homogeneous

coordinates $[x : y]$ on $\mathbb{P}^1(K)$. Each element of $\mathrm{PGL}_2(K)$ may be viewed as the map induced on $\mathbb{P}^1(K)$ by some nonsingular linear map $\left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right) \mapsto \left(\begin{smallmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{smallmatrix}\right)\left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right)$ of K^2. Because the linear maps that induce the identity on $\mathbb{P}^1(K)$ are precisely the (central) homotheties of K^2, the matrix $(a_{ij}) \in \mathrm{GL}_2(K)$ is unique up to multiplication by a scalar factor. Now conveniently identify $\mathbb{P}^1(K)$ with $K \cup \{\infty\}$ via the affine chart $K \to \mathbb{P}^1(K)$ given by $x \mapsto [x : 1]$, supplemented by setting $\infty \mapsto [1 : 0]$. In terms of this extended affine coordinate x, the element of $\mathbb{P}^1(K)$ under consideration reads now as the map $K \cup \{\infty\} \to K \cup \{\infty\}$ given by evaluating the linear expression $A(x) = (a_{11}x+a_{12})/(a_{21}x+a_{22})$. Consequently, if $B(x) = (b_{11}x+b_{12})/(b_{21}x+b_{22})$ is another linear rational expression in $K(x)$, then the matrix product $(b_{ij}) \cdot (a_{ij})$ is a matrix for the composite linear expression $(B \circ A)(x) = B(A(x))$. The group of linear rational expressions in $K(x)$ is usually called *the Möbius group* over K, and for simplicity we will identify it with $\mathrm{PGL}_2(K)$ as described.

The Möbius group $\mathrm{PGL}_2(K)$ acts sharply 3-transitively on $\mathbb{P}^1(K)$, meaning that any ordered triple of distinct points of $\mathbb{P}^1(K)$ is taken to any other such triple by precisely one element of $\mathrm{PGL}_2(K)$. In an explicit form that may be useful for calculations, the unique Möbius transformation that sends $\infty, 0, 1$ to three distinct elements a, b, c of K, respectively, is

$$\frac{a(b-c)x + b(c-a)}{(b-c)x + (c-a)}.$$

This naturally extends to cases where one of a, b, c equals ∞: it should be read as $(c-b)x+b$ when $a = \infty$, as $(ax+(c-a))/x$ when $b = \infty$, and as $(ax-b)/(x-1)$ when $c = \infty$.

The Möbius group is also the full group of automorphisms of the field extension $K(x)/K$, with automorphisms realized as substitutions in the indeterminate. However, in this paper we are interested in an action where a rational expression can be composed with independent linear rational expressions on both sides. Thus, if $R(x) \in K(x)$ is a rational expression of degree n, we let a pair $(B(x), A(x)) \in \mathrm{PGL}_2(K) \times \mathrm{PGL}_2(K)$ act on $R(x)$ (from the left) by setting $(B(x), A(x)) \cdot R(x) = B(R(A^{-1}(x)))$. This defines an action of the group $G(K) = \mathrm{PGL}(2, K) \times \mathrm{PGL}(2, K)$ on $K(x)$, and we call two rational expressions *equivalent* (over K) if they belong to the same orbit. This is the same equivalence that we described more informally in the Introduction. As we mentioned there, besides being the right equivalence relation to consider in view of our application in [MP22], this is a natural one that might be of more general interest.

The main goal of this paper is finding the equivalence classes, or $G(K)$-orbits, of cubic rational expressions when K is a finite field $\mathbb{F}_q$. We will fully achieve this only in characteristic two, and only find representatives for some of the equivalence classes in other characteristics. This is due to a likely unavoidable restriction on ramification points, and we will discuss extensively the difficulties involved at the end of Section 5.

The following result shows that the total number of cubic rational expressions over $\mathbb{F}_q$ equals $q^5(q^2-1)$.

Lemma 1. *The number of rational expressions of degree r over $\mathbb{F}_q$, with $r \geq 1$, equals $q^{2r-1}(q^2-1)$.*

Since we are unable to locate this fact in the literature, we provide a proof that relies on a known result on the probability that two random polynomials in $\mathbb{F}_q[x]$ of given degrees are coprime. When $r = 1$ we obviously recover the order $q(q^2-1)$ of the group $\mathrm{PGL}_2(\mathbb{F}_q)$.

Proof. A rational expression over K can be written uniquely as $\big(a\, g(x)\big)/h(x)$, with $g(x)$ and $h(x)$ monic and coprime in $K[x]$, and $a \in K^*$. Consequently, the desired number equals $q-1$ times the number of (ordered) pairs of coprime monic polynomials $g(x)$ and $h(x)$ in $\mathbb{F}_q[x]$ with $\max(\deg g, \deg h) = r$. Hence our goal is showing that those coprime pairs are in number of $q^{2r-1}(q+1)$.

According to [BB07, Theorem 3], the probability that a random pair of monic polynomials in $\mathbb{F}_q[x]$, of given positive degrees r and s, are coprime equals $1-1/q$. This statement assumes the uniform probability distribution on the set of q^{r+s} arbitrary pairs of monic polynomials of degrees r and s, hence it amounts to saying that the number of such pairs that are coprime equals $q^{r+s-1}(q-1)$. Note that this expression needs to be adjusted to cover the excluded cases where r or s equals zero: pairs of monic polynomials of degrees r and zero (hence with the second polynomial equal to 1) are automatically coprime, and their number equals q^r.

Consequently, the number of pairs of coprime monic polynomials in $\mathbb{F}_q[x]$, with the former having degree r and the latter having degree strictly inferior to r, equals

$$q^r + \sum_{0<s<r} q^{r+s-1}(q-1) = q^{2r-1}.$$

Splitting the set of pairs of coprime monic polynomials that we are counting according to whether $\deg g = \deg h = r$, or $\deg g < \deg h = r$, or $\deg g = r > \deg h$, we find altogether $q^{2r-1}(q-1) + q^{2r-1} + q^{2r-1} = q^{2r-1}(q+1)$ pairs, as desired. □

Before studying the $G(K)$-orbits on $K(x)$ with K a finite field it will be necessary to determine them when K is an algebraically closed field. Characteristic two and three will require special treatment, due to possible inseparability but not only that. A nonconstant rational expression $R(x) \in K(x)$ is called *separable* if the field extension $K(x)/K(R(x))$ is separable, and *inseparable* otherwise. We will use standard terminology such as *ramification points* and the corresponding *ramification indices,* which can be found in any textbook on algebraic geometry or function fields. We will need the following very special case of Hurwitz's Theorem (or the Riemann-Hurwitz formula), which can be conveniently extracted from the more general statements in [Sti09, Corollary 3.5.6] or [Ros02, Theorem 7.16].

Theorem 2 (A special case of Hurwitz's Theorem)**.** *Let K be an algebraically closed field, and let $R(x) \in K(x)$ be a nonconstant separable rational expression.*

Then

$$2\deg(R) - 2 \geq \sum_{P \in \mathbb{P}^1(K)} (e_R(P) - 1),$$

where $e_R(P)$ is the ramification index of $R(x)$ at P. Equality holds if and only if either the characteristic of K is zero or it does not divide $e_R(P)$ for any $P \in \mathbb{P}^1(K)$.

In particular, according to Theorem 2 a separable cubic rational expression can have at most four ramification points, as the left-hand side of the inequality equals four in this case. Of course this consequence is a much more basic fact than Theorem 2, and follows also from the finite ramification points of $R(x) = g(x)/h(x)$ being the zeroes of its derivative $R'(x) = \big(g'(x)h(x) - g(x)h'(x)\big)/h(x)^2$, whose numerator has degree at most four (and some further considerations in case ∞ is a ramification point).

A classification of the $G(K)$-orbits on cubic rational expressions when K is algebraically closed, which we present in Section 4, will require using the action of $G(K)$ to suitably rearrange the ramification points of an expression and their images, which are by definition the corresponding *branch points*. Note that distinct ramification points of a cubic expression necessarily map to distinct branch points. A classification over a finite field $\mathbb{F}_q$, which we begin in Section 5, will require studying the ramification points in its algebraic closure $\overline{\mathbb{F}}_q$ first.

We conclude this section by mentioning a natural field-theoretic interpretation of our results, and how that relates to existing literature. Classifying cubic rational expressions over a field K, up to the equivalence considered in this paper, amounts to classifying the subfields F of the field $K(x)$ of rational expressions, with $K \subseteq F$ and $|K(x)/F| = 3$, up to the action of $\mathrm{Gal}\big(K(x)/K\big)$. This is because according to Lüroth's theorem each such subfield has the form $F = K(z)$ for some cubic rational expression $z = R(x)$ in $K(x)$. Also, z is transcendental over K, and all elements of each of $\mathrm{Gal}\big(K(x)/K\big)$ and $\mathrm{Gal}\big(K(z)/K\big)$ are given by Möbius transformations.

If we switch focus to the subfield $K(z)$, a rational function field, then here we are interested in certain cubic field extensions of that. Cubic extensions L/F of an arbitrary field F of characteristic $p \geq 0$ were described in [MW19], extending classical results based on applications of Kummer theory and Artin-Schreier theory. Any such extension has a generating polynomial of one of the forms $y^3 - a$, $y^3 - 3y - a$ if $p \neq 3$, $y^3 + ay + a^2$ if $p = 3$, for some $a \in F$. Procedures were given in [MW19] to decide when two such cubic field extensions are isomorphic. The cases where F is either a number field or a function field are of special interest, and such field extensions have been extensively studied and tabulated over the years.

In particular, construction and tabulation of (geometric) dihedral extension of odd prime degree ℓ of a rational function field $F = K(z)$ was the primary goal of [WSH13, Wei13], where K is a perfect field of characteristic not dividing 2ℓ. When $\ell = 3$ a different approach was adopted in [KMS21], which focused on

classifying such extensions with a given set of ramified places, and including the case of characteristic two (but not three).

Besides a classification up to isomorphism of field extensions L/F, where $F = K(z)$ is a rational function field, a classification up to *bi-isomorphism* was also obtained in [KMS21], which means allowing also automorphisms of $K(z)$ (hence Möbius transformations over K). When L is also a rational function field, bi-isomorphism of function field extensions L/F as defined in [KMS21] is thus closely related to equivalence of rational expressions as considered in this paper. Consequently, some of our classification results, such as Theorem 11, match some of those obtained in [KMS21, Section 5]. However, in [KMS21] those extensions were discussed in terms of a generating polynomial, of the general form $y^3 - a$ or $y^3 - 3y - a$ for certain $a \in F = K(z)$, while our focus on cubic rational expressions $R(x)$ is rather different and justifies a separate treatment. Furthermore, our treatment includes the case of characteristic three, and a complete analysis of the case of characteristic two, in Section 7. Finally, and differently from [KMS21], our approach naturally leads to and includes counting results, both on the number of equivalence classes in Section 6, and on the cardinalities of each equivalence class in Section 5.

We are indebted to a referee of an early version of this paper for calling our attention to some of the above references.

3. Classification of quadratic expressions, revisited

Before we proceed towards a classification of cubic expressions over an algebraically closed field in the next section, we review the much easier case of quadratic expressions. Their equivalence classes can be determined by direct methods over an arbitrary field K, as in [MP17, Theorem 2] and the discussion that follows it, but here we show how the case of K algebraically closed can be resolved in a few lines using geometric ideas such as ramification points and Hurwitz's Theorem.

Thus, let $R(x)$ be an arbitrary quadratic expression over an algebraically closed field K, which we first assume not to have characteristic two. Then according to Hurwitz's Theorem $R(x)$ has exactly two ramification points, each with index two. By composing on both sides with suitable Möbius transformations we may assume the ramification points to be ∞ and 0, and also that they coincide with the corresponding branch points. In particular, $R(x)$ is equivalent to a quadratic polynomial (a quadratic rational map without poles) and, actually, a scalar multiple of the map x^2 because it has 0 as a ramification point. We conclude that over an algebraically closed field of characteristic different from two every quadratic expression is equivalent to x^2.

Now assume the algebraically closed field K has characteristic two. Here it is possible for the quadratic expression $R(x)$ to be inseparable. This occurs precisely when $R(x)$ is a square in $K(x)$, and clearly all such expressions $R(x)$ are equivalent to x^2. If $R(x)$ is separable then according to Hurwitz's Theorem it has precisely one ramification point. Assuming both that and the corresponding branch point to be ∞, as we may, $R(x)$ becomes a polynomial that is not a

square, which can then be easily seen to be equivalent to $x^2 + x$. Thus, over an algebraically closed field of characteristic two every quadratic expression is equivalent either to x^2 or to x^2+x. Instead of x^2+x one may take the equivalent expression $(1/x) \circ (x^2 + x) \circ \big(x/(x + 1)\big) = x + 1/x$, which has 1 as ramification point and 0 as the corresponding branch point.

In the rest of this section we compute the lengths of the orbits of $G(\mathbb{F}_q)$ on the set of quadratic expressions over $\mathbb{F}_q$. We start with the case of odd characteristic.

Theorem 3. *Let the finite field $\mathbb{F}_q$ have odd characteristic, and fix a nonsquare σ in $\mathbb{F}_q^*$. Of all the $q^3(q^2 - 1)$ distinct quadratic rational expressions over $\mathbb{F}_q$, precisely*

(i) *$q^2(q^2 - 1)(q + 1)/2$ are equivalent to x^2;*
(ii) *$q^2(q^2 - 1)(q - 1)/2$ are equivalent to $(x^2 + \sigma)/(2x)$.*

The expression $(x^2 + \sigma)/(2x)$ of case (ii) of Theorem 3 is clearly equivalent to $(x^2 + \sigma)/x = x + \sigma/x$, but the former matches a more general result that we will prove later, namely, Theorem 9.

Proof. According to the above discussion of the algebraically closed field case, any quadratic expression $R(x)$ over $\mathbb{F}_q$ is equivalent to x^2 over $\overline{\mathbb{F}}_q$. If the ramification points of $R(x)$ belong to $\mathbb{F}_q$, and hence the corresponding branch points as well, then the same argument outlined above for the algebraically closed case shows that $R(x)$ is actually equivalent to x^2 over $\mathbb{F}_q$.

Let τ be a square root of σ in $\mathbb{F}_{q^2}$, and consider

$$\tau\frac{x + \sigma}{x - \sigma} \circ x^2 \circ \tau\frac{x + \tau}{x - \tau} = \frac{x^2 + \sigma}{2x}.$$

This quadratic expression is equivalent to x^2 over $\overline{\mathbb{F}}_q$, and actually already over $\mathbb{F}_{q^2}$, but certainly not over $\mathbb{F}_q$ as its ramification points τ and $-\tau$ do not belong to $\mathbb{F}_q$, with τ and $-\tau$ as corresponding branch points.

Now if the ramification points of $R(x)$ do not belong to $\mathbb{F}_q$, then the qth power Galois automorphism interchanges them, and so it does to the corresponding branch points. Suitable Möbius transformations over $\mathbb{F}_{q^2}$ take those ramification points to τ and $-\tau$, and similarly for the branch points. We refer the reader to the proof of Theorem 9, which deals with a more general situation, for an argument showing that those Möbius transformations can be taken to be defined over $\mathbb{F}_q$, implying that $R(x)$ is equivalent to $(x^2+\sigma)/(2x)$ as desired. In the present proof we bypass that fact by relying on the orbit length count below.

(i) Each element of the stabilizer of x^2, that is, a pair $(B(x), A(x)) \in G(\mathbb{F}_q)$ such that $B(x) \circ x^2 \circ A^{-1}(x) = x^2$, must either fix or interchange the two ramification points of x^2, and similarly for the branch points. This fact and a simple calculation show that the stabilizer consists of the pairs $(B(x), A(x)) = (a^2x, ax)$ and $(a^2/x, a/x)$, with $a \in \mathbb{F}_q^*$. Consequently, the stabilizer has order $2(q-1)$, whence the orbit of x^2 has length $|G(\mathbb{F}_q)|/\big(2(q-1)\big) = q^2(q^2-1)(q+1)/2$.

(ii) Consider now the quadratic expression $x \mapsto (x^2 + \sigma)/(2x)$. As in case (i) each element $(B(x), A(x)) \in G(\mathbb{F}_q)$ of the stabilizer must either fix or

interchange the two ramification points τ and $-\tau$, and also the branch points. The Möbius transformations that fix both τ and $-\tau$ are $(ax+b\sigma)/(bx+a)$, and those who interchange them are $(ax-b\sigma)/(bx-a)$, for $a, b \in \mathbb{F}_q$, not both zero. One then easily finds that the stabilizer consists of all pairs

$$(B(x), A(x)) = \left(\frac{(a^2+\sigma b^2)x + 2\sigma ab}{2abx + (a^2+\sigma b^2)}, \frac{ax+\sigma b}{bx+a} \right)$$

and of all pairs

$$(B(x), A(x)) = \left(\frac{(a^2+\sigma b^2)x - 2\sigma ab}{2abx - (a^2+\sigma b^2)}, \frac{ax-\sigma b}{bx-a} \right)$$

for $a, b \in \mathbb{F}_q$, not both zero. Because proportional pairs a, b yield the same stabilizer element, the stabilizer has order $2(q^2-1)/(q-1) = 2(q+1)$. Hence the orbit has length $|G(\mathbb{F}_q)|/\big(2(q+1)\big) = q^2(q^2-1)(q-1)/2$.

Because the lengths of the two orbits that we have described add up to $q^3(q^2-1)$ we conclude that there are no further orbits. □

According to [MP17, Theorem 2] and the discussion that follows it, every quadratic expression over an arbitrary field K of characteristic different from two is equivalent to $x + \sigma/x$, with $\sigma \in K^*$ uniquely determined up to squares.

Now we consider the case of finite fields of characteristic two.

Theorem 4. *Let $\mathbb{F}_q$ be a finite field of characteristic two. Of all the $q^3(q^2-1)$ distinct quadratic rational expressions over $\mathbb{F}_q$, precisely*

(i) *$q(q^2-1)$ are equivalent to x^2;*
(ii) *$q(q^2-1)^2$ are equivalent to $(x^2+1)/x$.*

Proof. We know from the algebraically closed field case that any quadratic expression $R(x)$ over $\mathbb{F}_q$ is equivalent to x^2 or $x+1/x$ over $\overline{\mathbb{F}}_q$, according to whether it is inseparable or separable. One could now argue directly why this equivalence actually holds over $\mathbb{F}_q$ in either case (as in the proof of Theorem 9), but we can dispense with that as the desired conclusion will follow from a calculation of the orbit lengths under $G(\mathbb{F}_q)$.

(i) In this case the stabilizer of the quadratic expression x^2 is larger than in the odd characteristic case, and is easily found to consist of all pairs

$$(B(x), A(x)) = \left(\frac{a^2x + b^2}{c^2x + d^2}, \frac{ax+b}{cx+d} \right),$$

with $a, b, c, d \in \mathbb{F}_q$ and $ad - bc \neq 0$. Hence this stabilizer is isomorphic with $\mathrm{PGL}_2(\mathbb{F}_q)$, and so it has order $q(q^2-1)$, and the orbit has length $|G(\mathbb{F}_q)|/\big(q(q^2-1)\big) = q(q^2-1)$.

(ii) Instead of working with the quadratic expression $(x^2+1)/x$ it is convenient to consider the equivalent expression $x^2 + x$. For every element $(B(x), A(x)) \in G(\mathbb{F}_q)$ in the stabilizer of the latter, A must fix the only ramification point ∞, and B must fix the only branch point ∞. Consequently, each of A and B is a degree one binomial, and then a simple calculation shows that the stabilizer of x^2+x consists of all pairs $(A(x), B(x)) = (x+b+b^2, x+b)$. with $b \in \mathbb{F}_q$.

Therefore, the stabilizer of $x^2 + x$ is isomorphic with the additive group of $\mathbb{F}_q$. Because the stabilizer has order q, the orbit has length $|G(\mathbb{F}_q)|/q = q(q^2-1)^2$.

As the lengths of the two orbits above add up to $q^3(q^2-1)$ we conclude that there are no further orbits. □

Note that, differently from the case of odd q, only a minority of the quadratic rational expressions over a large finite field $\mathbb{F}_q$ of characteristic two are equivalent to x^2. Thus, a 'random' quadratic rational expressions over a large finite field $\mathbb{F}_q$ of characteristic two is very likely to be equivalent to $x + 1/x$, while that occurs with a probability approaching $1/2$ in the odd q case.

According to [MP17, Theorem 2] and the discussion that follows it, every quadratic expression over an arbitrary field K of characteristic two is equivalent either to x^2, or to $x + \sigma/x$, with $\sigma \in K^*$ uniquely determined up to squares.

4. Cubic expressions over an algebraically closed field

In this section we find representatives for the equivalence classes, or $G(K)$-orbits, of cubic rational expressions $R(x)$ over an algebraically closed field K. Because a cubic expression has up to four ramification points, the description will involve the configurations of quadruple of points of the projective line $\mathbb{P}^1(K)$, which are characterized by their cross-ratio.

Associated to an ordered quadruple of points of $\mathbb{P}^1(K)$ is their cross-ratio

$$\lambda = (x_1, x_2; x_3, x_4) := \frac{(x_1 - x_3)(x_2 - x_4)}{(x_2 - x_3)(x_1 - x_4)},$$

which is computed with respect to any affine coordinate x on $\mathbb{P}^1(K)$. The cross-ratio is an invariant of *ordered* quadruples of the projective line, in the sense that it is left unchanged by all automorphisms of $\mathbb{P}^1(K)$, that is, by all Möbius transformations. The cross-ratio is also unaffected by simultaneously interchanging its entries in disjoint pairs. More generally, when the four points are permuted, their cross-ratio changes within its orbit under the action of the group S of order six generated by the involutions $\lambda \mapsto 1/\lambda$ and $\lambda \mapsto 1 - \lambda$. The remaining elements of S, besides the identity, are the involution $\lambda \mapsto \lambda/(\lambda - 1)$, the substitution $\lambda \mapsto 1/(1 - \lambda)$ of order three, and its inverse $\lambda \mapsto (\lambda - 1)/\lambda$. Thus, as an invariant of *unordered* quadruples of the projective line, the cross-ratio takes its values in the set of S-orbits on $K \cup \{\infty\}$.

Note that the orbits of S on $K \cup \{\infty\}$ have length six, with the only exceptions of the orbits $\{\infty, 0, 1\}$ and $\{1/2, 2, -1\}$ (which coincide if K has characteristic two, and where the latter orbit has just one element if K has characteristic three), and possibly one further orbit consisting of the two roots of $\lambda^2 - \lambda + 1$ in K.

For K of characteristic different from two and three we will also encounter the involution $\lambda \mapsto (\lambda - 2)/(2\lambda - 1)$. Because that commutes with $\lambda \mapsto 1/\lambda$ and with $\lambda \mapsto 1 - \lambda$, it commutes with each element of S. In fact, together with the identity it forms the centralizer of S in the Möbius group. Consequently, the involution $\lambda \mapsto (\lambda - 2)/(2\lambda - 1)$ permutes the S-orbits on $K \cup \{\infty\}$. One

can verify that the only S-orbits fixed by it are the set of roots of $\lambda^2 - \lambda + 1$ (if contained in K), and the set of roots of $(\lambda^2 - 4\lambda + 1)(\lambda^2 + 2\lambda - 2)(2\lambda^2 - 2\lambda - 1)$ (if contained in K).

We are now ready to state and prove a classification of cubic rational maps up to equivalence over an algebraically closed field, postponing the cases of characteristic three and two for later consideration.

Theorem 5. *Let K be an algebraically closed field of characteristic different from two and three. Every cubic rational expression $R(x)$ over K is equivalent either to x^3, or to*

$$R_c(x) := \frac{x^3 + (c-2)x^2}{(2c-1)x - c},$$

for some $c \in K \setminus \{0, 1\}$.

The cubic expressions $R_c(x)$ and $R_{c'}(x)$, for $c, c' \in K \setminus \{0, 1\}$, are equivalent if and only if c and c' belong to the same S-orbit.

The cubic expression $R_c(x)$ has ramification points ∞, 0, 1, λ, with corresponding branch points ∞, 0, 1, μ, where $\lambda = c(2-c)/(2c-1)$ and $\mu = c(2-c)^3/(2c-1)^3$. The four ramification points are distinct, and so are the four branch points, except when $c \in \{1/2, 2, -1\}$. Those three exceptional cases give expressions equivalent to $R_{1/2}(x) = -2x^3 + 3x^2$, whose ramification points are $\infty, 0, 1$, with ∞ of index three.

Proof. According to Hurwitz's formula quoted in Theorem 2, the cubic expression $R(x)$ has at most four ramification points P_i, with ramification indices $(3, 3)$, $(3, 2, 2)$, or $(2, 2, 2, 2)$, and corresponding distinct branch points $R(P_i)$.

If $R(x)$ has only two ramification points, say P_1 and P_2, then after pre- and post-composition with suitable automorphisms of $\mathbb{P}^1(K)$ we may assume those to be 0 and ∞, and the corresponding branch points to be 0 and ∞. More precisely, if $A(x)$ is any Möbius transformation over $\overline{\mathbb{F}}_q$ that maps 0 to P_1, and ∞ to P_2, then $(R \circ A)(x)$ has ramification points 0 and ∞. Similarly, if $B(x)$ is any Möbius transformation over $\overline{\mathbb{F}}_q$ that maps the corresponding branch points $R(P_1)$ and $R(P_2)$ to 0 and ∞, respectively, then $(B \circ R \circ A)(x)$ has ramification points 0 and ∞, each with index three, and with corresponding branch points 0 and ∞. Clearly $(B \circ R \circ A)(x)$ is then a scalar multiple of x^3, and so it is equivalent to x^3.

Now suppose that $R(x)$ has at least three ramification points. Assuming, as we may, that the ramification points include ∞ and 0, with corresponding branch points ∞ and 0 (hence it has ∞ as at least a double pole and 0 as at least a double zero), $R(x)$ will have the form $R(x) = (x^3 + ax^2)/(bx - c)$, for some $a, b, c \in K$. Further imposing, as we may, that $R(x)$ has 1 as a ramification point with corresponding branch point 1, amounts to $R(x-1) - 1$ having a double zero at 0. A short calculation then leads to

$$R(x) = R_c(x) := \frac{x^3 + (c-2)x^2}{(2c-1)x - c},$$

with $c \neq 0, 1$ (otherwise $R_c(x)$ would be quadratic rather than cubic). Because the ramification points besides ∞ are the zeroes of the derivative $R'(x)$, one computes that the fourth ramification point (which may coincide with one of $\infty, 0, 1$) is $\lambda = c(2-c)/(2c-1)$, with corresponding branch point $\mu = c(2-c)^3/(2c-1)^3$. A similar discussion of an equivalent family is given in [Oss06, Example 8.2].

Now we examine when $R(x)$ has precisely three ramification points. We see that $\lambda = \infty, 0, 1$ when $c = 1/2, 2, -1$, respectively. Because μ equals λ for each of those values of c, those three choices of c yield equivalent rational expressions $R_c(X)$, as one can change from one another by suitably permuting the three ramification points, and the branch points correspondingly.

It remains to determine when $R_c(x)$ and $R_{c'}(x)$ are equivalent for $c, c' \in K \setminus \{0, 1, 1/2, 2, -1\}$. A necessary condition is that the corresponding cross-ratios λ and λ' belong to the same S-orbit, but we will see that this alone is not sufficient. Because the substitutions $c \mapsto 1/c$ and $c \mapsto 1-c$ induce $\lambda \mapsto 1/\lambda$ and $\lambda \mapsto 1-\lambda$, respectively, any substitution on c in the group S induces the analogous substitution on the corresponding cross-ratio λ. In other words, the quadratic map sending c to $\lambda = c(2-c)/(2c-1)$ is S-equivariant. In particular, it maps S-orbits of c to S-orbits of λ. Each value of $\lambda \in K \setminus \{0, 1\}$ originates from exactly two choices of $c \in K \setminus \{0, 1, 1/2, 2, -1\}$, except when $c^2 - c + 1 = 0$, which is equivalent to $\lambda^2 - \lambda + 1 = 0$. The involution $c \mapsto (c-2)/(2c-1)$ that we introduced before Theorem 5 interchanges those two choices of c for a given λ. However, those two choices give inequivalent expressions $R_c(x)$ because they yield different values of $\mu = \lambda^3/c^2$. (Here we are not allowed to permute the branch points for computing their cross-ratio μ, having already chosen an ordering for the respective ramification points to compute λ.) We conclude that $R_c(x)$ and $R_{c'}(x)$ are equivalent precisely when c and c' belong to the same S-orbit. □

Remark 6. A variant of the parametric family $R_c(x)$ of Theorem 5 is

$$(-4x+2) \circ R_c(x) \circ \frac{x+1}{2} = \frac{x^3 - bx^2 - 3x - b}{bx+1},$$

where $b = 1 - 2c$. This has ramification points ∞, -1, 1, $(b^2-3)/2b$, with corresponding branch points ∞, 2, -2, $-(b^4 + 18b^2 - 27)/4b^3$. When $c = 1/2$ this expression reads $x^3 - 3x$, which will be a more natural choice than $R_{1/2}(x) = -2x^3 + 3x^2$ when passing to a finite ground field in Theorem 11.

We now consider the cases of characteristics three and two. Besides the possibility that $R(x)$ is inseparable, we must take into account that Hurwitz's Theorem gives a strict inequality, rather than an equality, in case some ramification index is a multiple of the characteristic.

Theorem 7. *Let K be an algebraically closed field of characteristic three. Every cubic rational expression $R(x)$ over K is equivalent to either x^3, or $x^3 + x^2$, or*

$x^3 + x$, *or*

$$R_c(x) := \frac{x^3 + (c+1)x^2}{-(c+1)x - c},$$

for some $c \in K \setminus \mathbb{F}_3$.

The cubic expressions $R_c(x)$ *and* $R_{c'}(x)$, *for* $c, c' \in K \setminus \mathbb{F}_3$, *are equivalent if and only if* c *and* c' *belong to the same* S*-orbit. The cubic expression* $R_c(x)$ *has four distinct ramification points* ∞, 0, 1, c, *with corresponding branch points* ∞, 0, 1, c.

Note that the parametric expression for $R_c(x)$ equals that of Theorem 5 viewed modulo three. Also, for the excluded value $c = -1$ (which also equals $1/2$ and 2 here), the formula for $R_c(x)$ returns the inseparable cubic expression $R_{-1}(x) = x^3$, which is ramified everywhere. The lists of ramification indices for the remaining cubic expressions given in Theorem 7 are $(3, 2)$, (3), and $(2, 2, 2, 2)$ for the parametric family. They exhaust all the possibilities allowed by Hurwitz's Theorem in characteristic three.

Proof. We resort to direct calculation to cover the cases where Hurwitz's formula does not provide an equality. Thus, suppose that $R(x)$ has a ramification point with index 3, which we can assume to be ∞, with image ∞. Hence $R(x)$ is a cubic polynomial, which is then equivalent to a monic one without constant term. In turn, $R(x)$ is easily seen to be equivalent to either the inseparable polynomial x^3, or $x^3 + x^2 + bx$, or $x^3 + bx$, for some $b \in K$. In the second case $R(x)$ is equivalent to

$$(x - b^3 - 2b^2) \circ (x^3 + x^2 + bx) \circ (x - b/2) = x^3 + x^2,$$

which has 0 as a further ramification point, with index 2. In the third case $R(x)$ is equivalent to

$$(x/\sqrt{b}^{\,3}) \circ (x^3 + bx) \circ (\sqrt{b}\, x) = x^3 + x$$

(with $\sqrt{b}$ denoting a fixed square roots of b in K), whose only ramification point is ∞.

Now we may assume that all ramification points of $R(x)$ have indices less than 3, whence equality holds in Hurwitz's formula. Consequently, $R(x)$ has four ramification points, each with index 2. The corresponding part of the proof of Theorem 5 applies and yields the desired conclusions, including the statement on equivalence in terms of c. □

We conclude this section by considering the case where the algebraically closed field K has characteristic two. Then Theorem 2 implies that $R(x) = g(x)/h(x)$ can only have at most two ramification points. An elementary way of confirming this fact is noting that, because the second derivative of every rational expression in characteristic two vanishes, the derivative $R'(x) = \big(g'(x)h(x) - g(x)h'(x)\big)/h(x)^2$ must be a rational expression in x^2, and hence its numerator, which is a polynomial of degree at most four, can only have at most two distinct zeroes.

Theorem 8. *Let K be an algebraically closed field of characteristic two. Every cubic rational expression $R(x)$ over K is equivalent to either x^3, or x^3+x^2, or $(x^3+1)/x$, or $(x^3+c)/(x+c)$ for some $c \in K \setminus \mathbb{F}_2$.*

Different values of c in the parametric family $(x^3+c)/(x+c)$ yield inequivalent expressions. The ramification points of $(x^3+c)/(x+c)$ are ∞ and 1, each of index 2, and they are also the corresponding branch points. The further preimages of those branch points are c and 0.

The lists of ramification indices for the cubic expressions given in Theorem 8 are $(3,3)$, $(3,2)$, (2), and $(2,2)$ for the parametric family. They exhaust all the possibilities allowed by Hurwitz's Theorem in characteristic two.

Proof. The expression $R(x)$ must have at least one ramification point, so we may assume that ∞ is a ramification point, and that ∞ is also the corresponding branch point.

If ∞ has ramification index 3 then $R(x)$ is a polynomial, which we may assume monic, say $R(x) = x^3 + ax^2 + bx + c$. Because the remaining ramification points are the roots of its derivative $x^2 + b$, there is precisely one further ramification point, namely $\sqrt{b}$. We may now assume that this ramification point is 0, and also that 0 is the corresponding branch point. Then $R(x) = x^3 + ax^2$, and when $a \neq 0$ this is equivalent to $x^3 + x^2$.

Now we may suppose that ∞ has ramification index 2. We may also assume that the other preimage of ∞ is 0. Further multiplying $R(x)$ by a scalar we find that it is equivalent to $(x^3 + ax^2 + bx + c)/x$, for some $a, b, c \in K$ with $c \neq 0$.

If $R(x)$ has no ramification point other than ∞, then the expression

$$\frac{d}{dx}\frac{x^3 + ax^2 + bx + c}{x} = \frac{ax^2 + c}{x^2}$$

has no zeroes in K, forcing $a = 0$ (and of course $c \neq 0$). Now $(x^3 + bx + c)/x$ is clearly equivalent to $(x^3 + c)/x$ by adding a constant, and finally to $(x^3 + 1)/x$ as desired.

Finally, suppose $R(x)$ has a further ramification point besides ∞. We may assume that to be 1, whence $a = c \neq 0$, and the corresponding branch point to be 0, whence $b = 1$. Hence $R(x)$ is equivalent to $(x^2 + 1)(x + a)/x$. When $a = 1$ we get $(x + 1)^3/x$, which is ramified at 1 with index 3, and hence is equivalent to $x^3 + x^2$. Otherwise we get a parametric family with $a \in K \setminus \mathbb{F}_2$, having ramification indices $(2, 2)$.

Different values of the parameter a yield inequivalent expressions of the parametric family. In fact, the parameter $a = (\infty, 0; 1, a)$ is determined as the cross-ratio of the quadruple consisting of the preimages of the two branch points, of which two are the ramification points. Note that the value of the cross-ratio is independent of which of the two ramification points was initially chosen to be ∞, as interchanging the first two entries and simultaneously the last two entries of a cross-ratio leaves it unchanged.

The variant of this parametric family given in Theorem 8, which is better suited to the purpose of passing to a finite ground field in Section 7, is obtained

as

$$\left(\frac{x}{a^2+1}+1\right)\circ\frac{(x^2+1)(x+a)}{x}\circ\big((a+1)x+a\big)=\frac{x^3+c}{x+c},$$

where $c=a/(a+1)\in K\setminus\mathbb{F}_2$. □

5. Cubic expressions over a finite field

In this section we find representatives for the equivalence classes of cubic rational expressions $R(x)$ over a finite field, restricting to those of expressions with at most three distinct ramification points. The idea is to view $R(x)$ over the algebraic closure $\overline{\mathbb{F}}_q$ of $\mathbb{F}_q$ and then apply the corresponding classification result from the previous section. Here we view $\mathbb{P}^1(\mathbb{F}_q)$ as a subset of $\mathbb{P}^1(\overline{\mathbb{F}}_q)$, but in our context we may also identify them with $\mathbb{F}_q\cup\{\infty\}$ and $\overline{\mathbb{F}}_q\cup\{\infty\}$, respectively. The Galois group of $\overline{\mathbb{F}}_q/\mathbb{F}_q$, which is topologically generated by $\alpha\mapsto\alpha^q$, acts on the latter, with the former as the set of fixed points. The Galois group permutes the ramification points of $R(x)$ over $\overline{\mathbb{F}}_q$, and the corresponding branch points in a matching way, preserving the ramification indices.

We start with cubic rational expressions having only two ramification points in $\overline{\mathbb{F}}_q\cup\{\infty\}$, hence equivalent to x^3 over $\overline{\mathbb{F}}_q$ according to Theorem 5. In this case it is not any harder to deal with expressions of arbitrary degree r having precisely two ramification points in $\overline{\mathbb{F}}_q$.

Theorem 9. *Let r be a positive integer, let $\mathbb{F}_q$ be a finite field of odd characteristic not dividing r, and let $\sigma\in\mathbb{F}_q$ be a nonsquare. Let $R(x)$ be a rational expression over $\mathbb{F}_q$, of degree r and with only two ramification points in $\overline{\mathbb{F}}_q$. Then $R(x)$ is equivalent over $\mathbb{F}_q$ to either x^r, or*

$$\left(\sum_h\binom{r}{2h}x^{r-2h}\sigma^h\right)\Big/\left(\sum_h\binom{r}{2h+1}x^{r-2h-1}\sigma^h\right).$$

The two special forms for $R(x)$ given in Theorem 9 are inequivalent, as the ramification points of the latter are not all in $\mathbb{P}^1(\mathbb{F}_q)$. Note that the latter form reads $(x^2+\sigma)/(2x)$ when $r=2$, as in Theorem 3, and $(x^3+3\sigma x)/(3x^2+\sigma)$ when $r=3$, which will appear in Theorem 11.

Proof. View $R(x)$ over the algebraic closure $\overline{\mathbb{F}}_q$ of $\mathbb{F}_q$, and let τ be a square root of σ in $\mathbb{F}_{q^2}$. Because the ramification indices satisfy $e_R(P)\le\deg(R)=r$, according to Hurwitz's formula each of the two ramification points has index r.

If the two ramification points of $R(x)$ belong to $\mathbb{P}^1(\mathbb{F}_q)$ then $R(x)$ is equivalent to x^r over $\mathbb{F}_q$. This can be shown exactly as for the corresponding case in the proof of Theorem 5 (for $r=3$ and over $\overline{\mathbb{F}}_q$), just noting that the Möbius transformations $A(x)$ and $B(x)$ used there can be taken to be defined over $\mathbb{F}_q$.

Before dealing with the remaining case note that

$$\tau\frac{x+\tau^r}{x-\tau^r}\circ x^r\circ\tau\frac{x+\tau}{x-\tau}=\frac{\sum_{k\text{ even}}\binom{r}{k}x^{r-k}\tau^k}{\sum_{k\text{ odd}}\binom{r}{k}x^{r-k}\tau^{k-1}}=\frac{\sum_h\binom{r}{2h}x^{r-2h}\sigma^h}{\sum_h\binom{r}{2h+1}x^{r-2h-1}\sigma^h}$$

is equivalent to x^r over $\overline{\mathbb{F}}_q$, but has τ and $-\tau$ as ramification points, with τ and $-\tau$ as corresponding branch points.

Now suppose that two ramification points of $R(x)$ do not belong to $\mathbb{P}^1(\mathbb{F}_q)$. Then they must be Galois-conjugated over $\mathbb{F}_q$, say $\rho, \rho^q \in \overline{\mathbb{F}}_q \setminus \mathbb{F}_q$. There is a unique Möbius transformation $A(x)$ over $\overline{\mathbb{F}}_q$ that maps τ to ρ, $-\tau$ to ρ^q, and fixes some other point of $\mathbb{P}^1(\mathbb{F}_q)$, say 0. But $A(x)$ is actually defined over $\mathbb{F}_q$, because the associated map $\mathbb{P}^1(\overline{\mathbb{F}}_q) \to \mathbb{P}^1(\overline{\mathbb{F}}_q)$ commutes with the Galois automorphism $\alpha \mapsto \alpha^q$ of $\overline{\mathbb{F}}_q$. Now $(R \circ A)(x)$ has ramification points τ and $-\tau$. Similarly, there is a unique Möbius transformation $B(x)$ over $\overline{\mathbb{F}}_q$ that maps the branch points $R(\rho)$ and $R(-\rho)$ of $R(x)$ (or of $(R \circ A)(x)$, for that matter) to τ and $-\tau$, respectively, and maps $R(0)$ to 0, and similarly $B(x)$ must also be defined over $\mathbb{F}_q$. Now $(B \circ R \circ A)(x)$ has ramification points τ and $-\tau$, both with index r, and with corresponding branch points τ and $-\tau$, and maps 0 to 0. But then $(B \circ R \circ A)(x)$ equals the expression given in Theorem 9, because such conditions uniquely characterize the latter among rational expressions of degree r over $\overline{\mathbb{F}}_q$, a fact that can be seen at once on its equivalent expression x^r. □

Remark 10. According to [MP17, Lemma 11], a polynomial $F(x)$ of degree $3n$ over a field satisfies $(x-1)^{3n} \cdot F\big(1/(1-x)\big) = F(x)$ precisely if it has the form $F(x) = (x^2-x)^n \cdot f\big((x^3-3x+1)/(x^2-x)\big)$ for some polynomial $f(x)$ of degree n. This can be thought of a cubic version of the interpretation of self-reciprocal polynomials as arising through a quadratic transformation recalled in the Introduction. However, such polynomial $F(x)$ is very far from the general case of a polynomial arising through an arbitrary cubic transformation, as $(x^3-3x+1)/(x^2-x)$ has precisely two ramification points (in characteristic not three, each with ramification index three), namely, the roots of x^2-x+1. In particular, according to Theorem 9, over a field $\mathbb{F}_q$ with $q-1$ a multiple of three, that cubic expression is equivalent to x^3.

Now we are ready to classify cubic expressions over $\mathbb{F}_q$ having at most three ramification points.

Theorem 11. *Let $\mathbb{F}_q$ be a finite field of characteristic at least five, and let $\sigma \in \mathbb{F}_q$ be a nonsquare. Every cubic rational expression $R(x)$ over $\mathbb{F}_q$ with at most three ramification points (over $\overline{\mathbb{F}}_q$) is equivalent to either x^3, or $(x^3+3\sigma x)/(3x^2+\sigma)$, or x^3-3x, or $x^3-3\sigma x$.*

Proof. View $R(x)$ over the algebraic closure $\overline{\mathbb{F}}_q$ of $\mathbb{F}_q$, and let τ be a square root of σ in $\mathbb{F}_{q^2}$. If $R(x)$ has only two ramification points in $\mathbb{P}^1(\overline{\mathbb{F}}_q)$, then Theorem 9 applies. Hence $R(x)$ is equivalent to either x^3 or to $(x^3+3\sigma x)/(3x^2+\sigma)$ over $\mathbb{F}_q$, depending on whether its ramification points belong to $\mathbb{P}^1(\mathbb{F}_q)$ or not.

Now suppose that $R(x)$ has three ramification points in $\mathbb{P}^1(\overline{\mathbb{F}}_q)$. Then according to Theorem 5 and Remark 6 it is equivalent to x^3-3x over $\overline{\mathbb{F}}_q$. The latter has ramification points ∞ with index 3, and ± 1 with index 2, and corresponding branch points ∞ and ∓ 2. The polynomial $x^3-3\sigma x$ has ∞ as a ramification point with index 3, and τ and $-\tau$ as ramification points with index 2. The

corresponding branch points are ∞, $-2\tau^3$ and $2\tau^3$, respectively. Hence $x^3-3\sigma x$ is also equivalent to x^3-3x over $\overline{\mathbb{F}}_q$ (or even over $\mathbb{F}_{q^2}$), but not over $\mathbb{F}_q$. We now show that $R(x)$ is equivalent to either x^3-3x or $x^3-3\sigma x$ over $\mathbb{F}_q$.

The unique ramification point of $R(x)$ with index 3 must be fixed by the Galois automorphism $\alpha \mapsto \alpha^q$, hence it belongs to $\mathbb{P}^1(\mathbb{F}_q)$, and so does the corresponding branch point. If the other two ramification points belong to $\mathbb{P}^1(\mathbb{F}_q)$, and so obviously do the corresponding branch points, then $R(x)$ is actually equivalent to x^3-3x over $\mathbb{F}_q$. This can be seen by composing $R(x)$ on both sides with appropriate Möbius transformations so as to turn the ramification points of $R(x)$, and also the corresponding branch points, into ∞, 0, and 1, as in the proof of Theorem 5. In fact, the Möbius transformations $A(x)$ and $B(x)$ employed to achieve that are actually defined over $\mathbb{F}_q$ because each takes some particular triple of distinct points of $\mathbb{P}^1(\mathbb{F}_q)$ to another such triple.

Now suppose that $R(x)$ has three ramification points in $\mathbb{P}^1(\overline{\mathbb{F}}_q)$, but those with index two are not in $\mathbb{P}^1(\mathbb{F}_q)$. Then they will be Galois-conjugated over $\mathbb{F}_q$, say ρ and ρ^q. The argument is very similar to the one that we used in the proof of Theorem 9. Thus, there is a unique Möbius transformation $A(x)$ over $\overline{\mathbb{F}}_q$ that maps τ to ρ, $-\tau$ to ρ^q, and the third ramification point of $R(x)$ to 0. There is also a unique Möbius transformation $B(x)$ over $\overline{\mathbb{F}}_q$ that maps the branch points $R(\rho)$ and $R(-\rho)$ of $R(x)$ to $-2\tau^3$ and $2\tau^3$, respectively, and the third branch point of $R(x)$ to ∞. Both $A(x)$ and $B(x)$ are actually defined over $\mathbb{F}_q$. Then $(B\circ R\circ A)(x)$ equals $x^3-3\sigma x$, as the latter is uniquely characterized among cubic rational expressions by having ramification points ∞, τ, $-\tau$ with corresponding images ∞, $-2\tau^3$, $2\tau^3$, and ∞ having ramification index three. □

Theorem 12. *Let $\mathbb{F}_q$ be a finite field of characteristic three, and let $\sigma \in \mathbb{F}_q$ be a nonsquare. Every cubic rational expression $R(x)$ over $\mathbb{F}_q$ with at most three ramification points is equivalent to either x^3+x^2, or x^3+x, or $x^3+\sigma x$.*

Proof. According to Theorem 7, the cubic expression $R(x)$ is equivalent over $\overline{\mathbb{F}}_q$ to either x^3+x^2 or x^3+x, according to whether it has ramification indices $(3,2)$ or (3). In both cases $R(x)$ has a unique ramification point of index 3, which must therefore belong to $\mathbb{P}^1(\mathbb{F}_q)$. Therefore $R(x)$ can be replaced with an equivalent one that has ∞ as ramification point with index 3, and corresponding branch point ∞. We may now follow the corresponding part of the proof of Theorem 7, where most reductions can be done over $\mathbb{F}_q$, and we point out those that require modification. Thus, $R(x)$ is a cubic polynomial, and being separable by hypothesis one finds that it is equivalent over $\mathbb{F}_q$ to either x^3+x^2+bx, or x^3+bx, for some $b \in \mathbb{F}_q$. The former polynomial is seen to be equivalent to x^3+x^2 as in the proof of Theorem 7. The polynomial x^3+bx, however, is equivalent to $(x/\sqrt{b}^{\,3}) \circ (x^3+bx) \circ (\sqrt{b}\,x) = x^3+x$ only when b is a square in $\mathbb{F}_q$. In the complementary case one can similarly show that $R(x)$ is equivalent to $x^3+\sigma x$. □

Over a finite field $\mathbb{F}_q$ of characteristic three we also have inseparable cubic expressions, which are ramified everywhere. Those are easily seen to be all equivalent to x^3 already over $\mathbb{F}_q$.

As suggested by Theorem 8, the picture over finite fields of characteristic two will differ more drastically than in characteristic three from the generic case of Theorem 11, and we postpone a treatment of that to Section 7.

In order to complete a classification of cubic rational expressions $R(x)$, up to equivalence, over a finite field $\mathbb{F}_q$ of odd characteristic, one would need to deal with the cubic expressions that have four ramification points in $\overline{\mathbb{F}}_q \cup \{\infty\} = \mathbb{P}^1(\overline{\mathbb{F}}_q)$. Because of its complexity we limit ourselves to a generic discussion of the difficulties involved in achieving such a classification. There would be five cases according to how the four ramification points of $R(x)$ in $\overline{\mathbb{F}}_q \cup \{\infty\}$ are permuted by the action of $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$:

(1) all four ramification points are fixed by the Galois action, that is, they belong to $\mathbb{F}_q \cup \{\infty\}$;
(2) two ramification points are fixed and the other two are interchanged, hence the latter are the roots of an irreducible quadratic polynomial over $\mathbb{F}_q$;
(3) only one ramification point is fixed, and the other three are the roots of an irreducible cubic polynomial over $\mathbb{F}_q$;
(4) the ramification points form two Galois orbits of length two, and hence they are the roots of two irreducible quadratic polynomials over $\mathbb{F}_q$;
(5) the ramification points form a single Galois orbit, and hence they are the roots of an irreducible quartic polynomial over $\mathbb{F}_q$.

In each of these cases a classification would involve a parametric family of representatives for the equivalence classes of those cubic expressions, related to the family $R_c(x)$ of Theorem 5. For example, in case (1) one can show that $R(x)$ must be equivalent over $\mathbb{F}_q$ to $R_c(x)$ for some $c \in \mathbb{F}_q \setminus \{0, 1, 1/2, 2, -1\}$, and the number of inequivalent ones is then easily found. However, finding representatives seems nontrivial in certain cases, especially cases (3) and (5). Furthermore, in those cases the very number of equivalence classes could not be determined exactly, as it would depend on the number of $\mathbb{F}_q$-rational points of certain curves of positive genus.

In addition to the difficulties illustrated above, we mention that achieving a detailed classification of those cases with four ramification points would be inconsequential to applications such as those developed in [MP22]. That is because an exact count of the irreducible polynomials arising through a given cubic transformation (see our Introduction) where $R(x)$ has four ramification points cannot be achieved, again because it involves counting $\mathbb{F}_q$-rational points of certain curves of genus one (see [MP22, Theorem 14]).

6. Bounding the number of equivalence classes

According to Lemma 1 there are a total of $q^5(q^2-1)$ cubic rational expressions over $\mathbb{F}_q$. They divide into a number of equivalence classes, that is, orbits under the action of $G(\mathbb{F}_q) = \mathrm{PGL}_2(\mathbb{F}_q) \times \mathrm{PGL}_2(\mathbb{F}_q)$ defined in Section 2. In Section 5 we have determined representatives for those orbits consisting of expressions with at most three ramification points. In this section we will produce an upper bound

for the total number of equivalence classes, making use of the orbit-stabilizer theorem to estimate the size of classes where explicit representatives are not available.

The gist of our argument is that a lower bound on the length of an orbit of cubic rational expressions with four distinct ramification points follows from an upper bound on the order of the stabilizer in $G(\mathbb{F}_q)$ of any expression $R(x)$ in the orbit. The stabilizer of $R(x)$ permutes the four ramification points of $R(x)$ in $\overline{\mathbb{F}}_q \cup \{\infty\}$, and the four branch points correspondingly. Thus, we may identify the stabilizer of $R(x)$ with a subgroup of the symmetric group S_4 on the four ramification points of $R(x)$. Consequently, the stabilizer has order at most $|S_4| = 24$, and hence the orbit has length at least $q^2(q^2-1)^2/24$. However, it turns out that the stabilizer cannot have order larger than 4, except for at most one orbit with stabilizer of order 12. Proving that requires the following auxiliary result, which might be of independent interest.

Lemma 13. *Let $R(x)$ be a cubic rational expression over an algebraically closed field K, and suppose $R(x)$ has four distinct ramification points. Then the stabilizer of $R(x)$ in the action of $\mathrm{PGL}_2(K) \times \mathrm{PGL}_2(K)$ acts as the Klein Four-Group on the ramification points, except if the cross-ratio of the ramification points is a primitive sixth root of unity. If the latter occurs, then $R(x)$ is equivalent to $3x^2/(2x^3+1)$, whose stabilizer acts as the alternating group A_4 on the ramification points.*

Proof. Because $R(x)$ has four distinct ramification points, K does not have characteristic two. According to Theorems 5 and 7, the cubic expression $R(x)$ is equivalent to

$$R_c(x) = \frac{x^3 + (c-2)x^2}{(2c-1)x - c}$$

for some $c \in K \setminus \{0, 1, 1/2, 2, -1\}$. Now $R_c(x)$ has ramification points ∞, 0, 1, λ, with corresponding branch points ∞, 0, 1, μ, where $\lambda = c(2-c)/(2c-1)$ and $\mu = c(2-c)^3/(2c-1)^3$. Let H be the stabilizer of $R_c(x)$ in the action of $G(K)$. Every element of H induces a permutation of the four ramification points in the domain of $R_c(x)$, and the same permutation of the four branch points in the codomain.

One may check that

$$(\mu/x) \circ R_c(x) \circ (\lambda/x) = R_c(x)$$

and

$$\frac{x-\mu}{x-1} \circ R_c(x) \circ \frac{x-\lambda}{x-1} = R_c(x).$$

Because λ/x induces the permutation $(\infty, 0)(1, \lambda)$ on the ramification points, and $(x-\lambda)/(x-1)$ induces the permutation $(\infty, 1)(0, \lambda)$, we conclude that H always contains the Klein Four-Group.

No element of H can induce the transposition $(\infty, 0)$ on the ramification points, because

$$(1/x) \circ R_c(x) \circ (1/x) = R_{1/c}(x)$$

equals $R_c(x)$ if and only if $c = \pm 1$, which are excluded values. Consequently, H cannot act as the full symmetric group S_4 on the four ramification points.

It also follows that H cannot act as a dihedral group of order eight. In fact, precisely one of the transpositions $(\infty, 0)$, $(\infty, 1)$, $(0, 1)$ belongs to each of the three subgroups of order eight of the symmetric group on the four ramification points ∞, 0, 1, λ of $R_c(x)$. We have already ruled out the first case. If some element of the stabilizer H of $R_c(x)$ induced the transposition $(\infty, 1)$ on the ramification points, then the corresponding (conjugate) element of the stabilizer of

$$\frac{1}{1-x} \circ R_c(x) \circ \frac{x-1}{x} = R_{1/(1-c)}(x)$$

would induce the transposition $(\infty, 0)$ on the ramification points ∞, 0, 1, $1/(1-\lambda)$ of $R_{1/(1-c)}(x)$, but we have shown that to be impossible. The third case is similarly ruled out by considering $R_{(c-1)/c}(x)$.

Thus, either H acts as the Klein Four-Group on the four ramification points of $R_c(x)$, or as the alternating group A_4. The latter occurs if and only if some element of H acts as a 3-cycle fixing the fourth ramification point λ. That is the case precisely when $R_{1/(1-c)}(x)$ equals $R_c(x)$, hence when $c^2 - c + 1 = 0$. Because $c \neq -1$, the characteristic of K is different from three. The condition $c^2 - c + 1 = 0$ is then equivalent to $\lambda^2 - \lambda + 1 = 0$, which means that λ is a primitive sixth root of unity.

To prove the final claim note that the four ramification points of $R(x) = 3x^2/(2x^3 + 1)$ coincide with the corresponding branch points, and they are 0, 1, and the two primitive sixth roots of unity in K. Because their cross-ratio is also a primitive sixth root of unity, $R(x)$ is equivalent to $R_c(x)$ with c a primitive sixth root of unity. □

Because of the orbit-stabilizer theorem, Lemma 13 provides us with a lower bound on the lenght of each $G(\mathbb{F}_q)$-orbit on cubic expressions with four ramification points. Combining that with our classification of cubic expressions with less than four ramification points, which we obtained in Section 5, yields the following upper bound on the total number of $G(\mathbb{F}_q)$-orbits.

Theorem 14. *Over a finite field $\mathbb{F}_q$ of odd characteristic, there are no more than $4q$ equivalence classes of cubic rational expressions.*

Proof. Suppose first that q is not a power of three. According to Theorem 11, under the action of $G(\mathbb{F}_q)$ there are precisely four orbits of cubic rational expressions over $\mathbb{F}_q$ having at most three ramification points. We will use the orbit-stabilizer theorem to compute the length of those orbits, and then by difference to bound the number of orbits of cubic rational expressions with four ramification points.

Similarly to the proof of Theorem 3 one finds that the stabilizer of the cubic expression x^3 has order $2(q-1)$. A calculation shows that the stabilizer of the other cubic expression with only two ramification points, namely $(x^3+3\sigma x)/(3x^2+\sigma)$, where $\sigma \in \mathbb{F}_q$ is a nonsquare, has order $2(q+1)$. Consider now the two expressions $x^3 - 3x$ and $x^3 - 3\sigma x$. Each has two (opposite) ramification points

with index two, and one with index three. Each element of a stabilizer must fix this third ramification point and permute the other two (and the branch points accordingly), hence it is either the identity or the map given by pre- and post-composition with $-x$. Hence in both cases the stabilizer has order 2.

Thus far, we have seen two orbits consisting of $q^2(q^2-1)(q+1)/2$ and $q^2(q^2-1)(q-1)/2$ cubic expressions, and another two orbits consisting of $q^2(q^2-1)^2/2$ expressions each. Adding up these numbers, we find $q^2(q^2-1)(q^2+q-1)$ cubic rational expressions having two or three ramification points. Subtracting this from the total number $q^5(q^2-1)$ of cubic expressions we find that, over a finite field $\mathbb{F}_q$ of characteristic at least five, the cubic expressions with four ramification points are in number of $q^2(q^2-1)^2(q-1)$.

Now suppose $\mathbb{F}_q$ has characteristic three, so Theorem 12 applies. As in case (i) of Theorem 4, the stabilizer of x^3 in $G(\mathbb{F}_q)$ is isomorphic to $\mathrm{PGL}_2(\mathbb{F}_q)$, and hence the orbit of x^3 has length $q(q^2-1)$. Using the two ramification points of the expression x^3+x^2 it follows at once that it has trivial stabilizer, and hence orbit length $q^2(q^2-1)^2$. Finally, one easily finds that each of the expressions x^3+x, or $x^3+\sigma x$ has stabilizer of order $2q$, and hence orbit length $q(q^2-1)^2/2$. We conclude by difference that, over $\mathbb{F}_q$ of characteristic three, the number of cubic expressions with precisely four ramification points is given by $q^2(q^2-1)^2(q-1)$, the same expression that we found for larger characteristic.

Now consider a cubic expression $R(x)$ over $\mathbb{F}_q$ with four distinct ramification points in $\overline{\mathbb{F}}_q \cup \{\infty\}$. Its stabilizer H in $G(\mathbb{F}_q)$ permutes those ramification points, and the four branch points correspondingly. Suppose $|H| > 4$. Because H is a subgroup of the stabilizer of $R(x)$ in $G(\overline{\mathbb{F}}_q)$, Lemma 13 implies that $\mathbb{F}_q$ does not have characteristic three, that $H \cong A_4$, and that $R(x)$ is equivalent to $3x^2/(2x^3+1)$ over $\overline{\mathbb{F}}_q$. We will show that they are actually equivalent over $\mathbb{F}_q$, and that $q \equiv 1 \pmod 3$.

The Galois automorphism $\alpha \mapsto \alpha^q$ of $\overline{\mathbb{F}}_q$ permutes the four ramification points of $R(x)$. However, because H is a subgroup of $G(\mathbb{F}_q)$ the Galois automorphism commutes with the action of H on the ramification points. Since A_4, the permutation group induced by H on the ramification points, has trivial centralizer in the symmetric group S_4, the Galois automorphism must act trivially on the ramification points. It follows that the ramification points are in $\mathbb{F}_q \cup \{\infty\}$, and hence so are the corresponding branch points. Using a Möbius transformation that maps the four ramification points of $R(x)$ to those of $3x^2/(2x^3+1)$, which are 0, 1, and the the primitive sixth roots of unity, and another suitable Möbius transformation for the branch points, we find that $R(x)$ is equivalent to $3x^2/(2x^3+1)$. Furthermore, because the cross-ratio of the ramification points is a primitive sixth root of unity, that belongs to $\mathbb{F}_q$, and hence $q \equiv 1 \pmod 3$.

Summarizing, each orbit of cubic expressions with four ramification points has length at least $q^2(q^2-1)^2/4$, except for precisely one orbit of length $q^2(q^2-1)^2/12$ if $q \equiv 1 \pmod 3$. It follows that the number of orbits consisting of cubic rational expressions with four ramification points does not exceed $4(q-1)$, including in the case where $q \equiv 1 \pmod 3$ (as the one shorter orbit only increases the integer

bound by 1/3). The conclusion follows after including the remaining four orbits in the count. □

7. Cubic expressions in characteristic two

In this section we determine representatives and lengths for all $G(\mathbb{F}_q)$-orbits of cubic expressions in characteristic two. Recall from Theorem 8 that no such expression can have more than two ramification points. Thus, in characteristic two we do not encounter the difficulties of dealing with expressions with four ramification points, which we have outlined at the end of Section 5. We start with finding representatives for those $G(\mathbb{F}_q)$-orbits.

Theorem 15. *Let $\mathbb{F}_q$ be a finite field of characteristic two. Let $\sigma \in \mathbb{F}_q$ be an element of absolute trace 1. If q is a square then let θ be a non-cube in $\mathbb{F}_q$. Then every cubic rational expression $R(x)$ over $\mathbb{F}_q$ is equivalent to precisely one of the following:*

(i) x^3, *with ramification indices* $(3,3)$;
(ii) $\dfrac{x^3+\sigma x+\sigma}{x^2+x+\sigma+1}$, *with ramification indices* $(3,3)$;
(iii) x^3+x^2, *with ramification indices* $(3,2)$;
(iv) $(x^3+1)/x$ *or, only in case q is a square,* $(x^3+\theta)/x$ *or* $(x^3+\theta^2)/x$; *all these have ramification indices* (2);
(v) $(x^3+c)/(x+c)$, *with ramification indices* $(2,2)$, *for some $c \in \mathbb{F}_q \setminus \mathbb{F}_2$, uniquely determined by $R(x)$;*
(vi) $\dfrac{x^3+bx^2+\sigma x+(b+1)\sigma}{x^2+x+b+1+\sigma}$, *with ramification indices* $(2,2)$, *for some $b \in \mathbb{F}_q \setminus \mathbb{F}_2$, uniquely determined by $R(x)$.*

Proof. According to Theorem 8, over the algebraic closure $\overline{\mathbb{F}}_q$ of $\mathbb{F}_q$ the expression $R(x)$ is equivalent to either x^3, or x^3+x^2, or $(x^3+1)/x$, or $(x^3+c)/(x+c)$, with $c \in \overline{\mathbb{F}}_q \setminus \mathbb{F}_2$. Let $\tau \in \mathbb{F}_{q^2}$ satisfy $\tau^2+\tau=\sigma$. Since $\sigma+\sigma^2+\sigma^4+\cdots+\sigma^{q/2}=1$ by our choice of σ, we have

$$\tau^q+\tau=(\tau+\tau^2)+(\tau+\tau^2)^2+\cdots+(\tau+\tau^2)^{q/2}=1$$

and, consequently, $\tau^{q+1}=(\tau+1)\tau=\sigma$.

The simplest case is when $R(x)$ is equivalent to x^3+x^2 over $\overline{\mathbb{F}}_q$, which occurs precisely when it has ramification indices $(3,2)$. Because the ramification indices are different, each of the two ramification points must be fixed by the Galois automorphism $\alpha \mapsto \alpha^q$, hence it belongs to $\mathbb{P}^1(\mathbb{F}_q)$, and so does the corresponding branch point. Consequently, the ramification points can be assumed to be ∞ and 0 and to coincide with the corresponding branch points, yielding that $R(x)$ is equivalent to x^3+x^2 over $\mathbb{F}_q$.

Now suppose that $R(x)$ is equivalent to x^3 over $\overline{\mathbb{F}}_q$, which occurs precisely when it has ramification indices $(3,3)$. In this case the two ramification points could be either fixed or interchanged by the Galois automorphism $\alpha \mapsto \alpha^q$. In

fact, a cubic expression equivalent to x^3 over $\mathbb{F}_{q^2}$ but not over $\mathbb{F}_q$ is

$$\frac{\tau x+\tau^q}{x+1}\circ x^3\circ\frac{x+\tau^q}{x+\tau}=\frac{x^3+\sigma x+\sigma}{x^2+x+\sigma+1},$$

which has τ and $\tau^q=\tau+1$ as ramification points, and also as the corresponding branch points. An argument that we fully spelled out in the proof of Theorem 9 now shows that $R(x)$ is either equivalent to x^3 over $\overline{\mathbb{F}}_q$, or to the other expression found above.

If $R(x)$ is equivalent to $(x^3+1)/x$ over $\overline{\mathbb{F}}_q$ then it has ramification indices (2). Hence its only ramification point is Galois-invariant and can be taken to be ∞, with ∞ as the corresponding branch point. The further preimage of ∞ is also Galois-invariant and hence can be taken to be 0, that is, $R(0)=\infty$. As in the proof of Theorem 8, we find that $R(x)$ is equivalent to $(x^3+c)/x$ for some $c\in\mathbb{F}_q^*$. However, after those stipulations all freedom we have left is passing to $a^2x\circ((x^3+c)/x)\circ x/a=(x^3+a^3c)/x$. If q is not a square then $q\equiv -1 \pmod 3$, and so the cubing map is bijective on $\mathbb{F}_q$ and $R(x)$ is equivalent to $(x^3+1)/x$. If q is a square then c equals a cube in $\mathbb{F}_q^*$ times either 1, θ, or θ^2, and hence $R(x)$ is equivalent to precisely one of the three expressions given.

Finally, suppose that $R(x)$ has ramification indices $(2,2)$. Then according to Theorem 8 it is equivalent to $(x^3+c)/(x+c)$, over $\overline{\mathbb{F}}_q$, for some $c\in\overline{\mathbb{F}}_q\setminus\mathbb{F}_2$. Uniqueness of c implies its Galois-invariance, whence $c\in\mathbb{F}_q\setminus\mathbb{F}_2$. Recall that this cubic expression has ∞ and 1 as ramification points, coinciding with the corresponding branch points, whose further preimages are c and 0.

Now if the ramification points of $R(x)$ belong to $\mathbb{F}_q$ then so do the corresponding branch points and also their further preimages. In this case the proof of Theorem 8 shows that $R(x)$ is actually equivalent to $(x^3+ax^2)/(x+1)$ over $\mathbb{F}_q$, and in turn to $(x^3+c)/(x+c)$.

The other possibility is that the Galois automorphism $\alpha\mapsto\alpha^q$ interchanges the two ramification points of $R(x)$, and consequently the corresponding branch points, and also their further preimages. Setting $c=1/b^2$ we find

$$B(x)\circ\frac{b^2x^3+1}{b^2x+1}\circ A(x)=\frac{x^3+bx^2+\sigma x+(b+1)\sigma}{x^2+x+b+1+\sigma},$$

where

$$A(x)=\frac{x+\tau^q(b+1)+b\tau}{bx+b\tau}\qquad\text{and}\qquad B(x)=\frac{b\tau x+\tau^q(b+1)+b\tau}{bx+1}.$$

This cubic expression is equivalent to $(x^3+c)/(x+c)$ over $\mathbb{F}_{q^2}$ but not over $\mathbb{F}_q$, as it has ramification points τ and $\tau^q=\tau+1$. These coincide with the corresponding branch points, whose further preimages are $\tau+b$ and τ^q+b. A similar argument as that in the proof of Theorem 9 now shows that $R(x)$ is equivalent to this expression over $\mathbb{F}_q$. □

Note that when $q=2$ the cases (v) and (vi) of Theorem 15 are vacuous, hence any cubic expression over $\mathbb{F}_2$ is equivalent to one of the following four possibilities: x^3, $(x^3+x+1)/(x^2+x)$, x^3+x^2, and $(x^2+1)/x$. In general, Theorem 15 yields the following count of equivalence classes.

Corollary 16. *Over a finite field $\mathbb{F}_q$ of characteristic two there are exactly $2q+2$ equivalence classes of cubic rational expressions if q is a square, and $2q$ otherwise.*

In our final result we compute the length of each $G(\mathbb{F}_q)$-orbit of cubic expressions that we have determined in Theorem 15.

Theorem 17. *Assume the hypotheses and notation of Theorem 15. Of all the $q^5(q^2-1)$ distinct cubic rational expressions over $\mathbb{F}_q$, precisely*

(i) *$q^2(q^2-1)(q+1)/2$ are equivalent to x^3;*
(ii) *$q^2(q^2-1)(q-1)/2$ are equivalent to $\dfrac{x^3+\sigma x+\sigma}{x^2+x+\sigma+1}$;*
(iii) *$q^2(q^2-1)^2$ are equivalent to x^3+x^2;*
(iv) *$q^2(q^2-1)^2$ are equivalent to one of $(x^3+1)/x$, $(x^3+\theta)/x$ or $(x^3+\theta^2)/x$, equally split among these in case q is a square;*
(v) *$q^2(q^2-1)^2/2$ are equivalent to $(x^3+c)/(x+c)$, for each given $c \in \mathbb{F}_q \setminus \mathbb{F}_2$;*
(vi) *$q^2(q^2-1)^2/2$ are equivalent to $\dfrac{x^3+bx^2+\sigma x+(b+1)\sigma}{x^2+x+b+1+\sigma}$, for each given $b \in \mathbb{F}_q \setminus \mathbb{F}_2$.*

Adding up these numbers, allowing for b, c to vary as appropriate, gives the expected total of $q^5(q^2-1)$.

Proof. (i) Each element of the stabilizer of x^3, that is, a pair $(B, A) \in G(\mathbb{F}_q)$ such that $B(x) \circ x^3 \circ A^{-1}(x)$, must either fix or interchange the two ramification points of x^3, and similarly for the branch points. This fact and a simple calculation show that the stabilizer consists of the pairs $(B, A) = (a^3x, ax)$ and $(a^3/x, a/x)$, with $a \in \mathbb{F}_q^*$. Consequently, the stabilizer has order $2(q-1)$, whence the orbit of x^3 has length $|G(\mathbb{F}_q)|/\big(2(q-1)\big) = q^2(q^2-1)(q+1)/2$.

(ii) The expression $R(x)$ under consideration is equivalent to x^3 over $\mathbb{F}_{q^2}$, and hence its stabilizer T_R in $G(\mathbb{F}_{q^2})$ is conjugated to the one described in (i), but with a ranging in $\mathbb{F}_{q^2}^*$, call that T_{x^3}. With notation as in the proof of Theorem 15 we have

$$T_R = \left(\frac{\tau x+\tau^q}{x+1}, \frac{\tau x+\tau^q}{x+1}\right) \cdot T_{x^3} \cdot \left(\frac{x+\tau^q}{x+\tau}, \frac{x+\tau^q}{x+\tau}\right),$$

from which one may work out explicit expressions for all elements of T_R and then decide which of them belong to $G(\mathbb{F}_q)$. The second component of the element of T_R conjugated to $(B, A) = (a^3x, ax) \in T_{x^3}$ is

$$\frac{\tau x+\tau^q}{x+1} \circ ax \circ \frac{x+\tau^q}{x+\tau} = \frac{(a\tau+\tau^q)x+(a+1)\tau^{q+1}}{(a+1)x+(a\tau^q+\tau)},$$

and we see that the qth power automorphism maps this to the corresponding conjugate of $a^{-q}x$. An analogous assertion clearly holds for the first component, and a similar calculation would yield the same conclusion when taking $(B, A) = (a^3/x, a/x) \in T_{x^3}$. Consequently, the elements of T_R that are fixed by the qth power automorphism are precisely those conjugated to those in T_{x^3} satisfying $a^{-q} = a$. Therefore $|T_R \cap G_(\mathbb{F}_q)| = 2(q+1)$, and so the orbit of $R(x)$ has length $|G(\mathbb{F}_q)|/\big(2(q+1)\big) = q^2(q^2-1)(q-1)/2$.

(iii) Because the two ramification points ∞ and 0 of x^3+x^2 have different indices, each must be fixed by its stabilizer of $R(x)$, and similarly the branch points. Therefore, any element in the stabilizer has the form $(B, A) = (bx, ax)$ for some $a, b \in \mathbb{F}_q$, and one concludes at once that $a = b = 1$. Hence in this case the stabilizer is trivial, and the orbit has length $|G(\mathbb{F}_q)| = q^2(q^2-1)^2$.

(iv) The expression $(x^3+c)/x$ has the single ramification point ∞, which is also the branch point, whose other preimage is 0. Consequently, if (B, A) is in its stabilizer then A must fix each of ∞ and 0, and B must fix ∞. A quick calculation then shows that the stabilizer consists of the pairs $(ax, x/a)$ with $a^3 = 1$. Hence the orbit has length $|G(\mathbb{F}_q)|/3 = q^2(q^2-1)^2/3$ when 3 divides $q-1$, which occurs precisely when q is a square, and $q^2(q^2-1)^2$ otherwise.

(v) The expression $(x^3+c)/(x+c)$, for some $c \in \mathbb{F}_q \setminus \mathbb{F}_2$, has ∞ and 1 as ramification points of index 2, each coinciding with the corresponding branch point, and that the further preimages of the branch points are c and 0, respectively. Hence any element of its stabilizer in $G(\mathbb{F}_q)$ either fixes all these four points, or interchanges ∞ with 1 and c with 0. Consequently, the stabilizer consists of the identity and the pair $\big((x+c)/(x+1), (x+c)/(x+1)\big)$, and so the orbit has length $|G(\mathbb{F}_q)|/2 = q^2(q^2-1)^2/2$.

(vi) This case is similar to the previous case. The expression under consideration has has τ and $\tau^q = \tau+1$ as ramification points of index 2, each coinciding with the corresponding branch point, and the further preimages of the branch points are $\tau + b$ and $\tau^q + b$, respectively. Arguing as in the previous case one concludes that its stabilizer consists of the identity and the pair $(x+1, x+1)$, and so the orbit has length $|G(\mathbb{F}_q)|/2 = q^2(q^2-1)^2/2$. □

According to Theorems 15 and 17, a 'random' cubic expressions over a finite field $\mathbb{F}_q$ of characteristic two is equally likely to have one of the three ramification types $(3,2)$, (2) or $(2,2)$, with the remaining ramification type $(3,3)$ becoming less and less likely as q grows.

References

[Ahm11] Omran Ahmadi, *Generalization of a theorem of Carlitz*, Finite Fields Appl. **17** (2011), no. 5, 473–480. MR 2831706 (2012f:11231)

[BB07] Arthur T. Benjamin and Curtis D. Bennett, *The probability of relatively prime polynomials*, Math. Mag. **80** (2007), no. 3, 196–202. MR 2322084

[Car67] L. Carlitz, *Some theorems on irreducible reciprocal polynomials over a finite field*, J. Reine Angew. Math. **227** (1967), 212–220. MR 0215815 (35 #6650)

[CHPW15] Stephen D. Cohen, Sartaj Ul Hasan, Daniel Panario, and Qiang Wang, *An asymptotic formula for the number of irreducible transformation shift registers*, Linear Algebra Appl. **484** (2015), 46–62. MR 3385053

[KMS21] Valentijn Karemaker, Sophie Marques, and Jeroen Sijsling, *Cubic function fields with prescribed ramification*, Int. J. Number Theory **17** (2021), no. 9, 2019–2053.

[MP13] Gary L. Mullen and Daniel Panario (eds.), *Handbook of finite fields*, Discrete Math. Appl. (Boca Raton), Boca Raton, FL: CRC Press, 2013 (English).

[MP17] Sandro Mattarei and Marco Pizzato, *Generalizations of self-reciprocal polynomials*, Finite Fields Appl. **48** (2017), 271–288. MR 3705747

[MP22] ———, *Irreducible polynomials from a cubic transformation*, Finite Fields Appl. **84** (2022), 22 (English), Id/No 102111.

[MW19] Sophie Marques and Kenneth Ward, *Cubic fields: a primer*, Eur. J. Math. **5** (2019), no. 2, 551–570.

[Oss06] Brian Osserman, *Rational functions with given ramification in characteristic p*, Compos. Math. **142** (2006), no. 2, 433–450. MR 2218904

[Piz13] Marco Pizzato, *Some problems concerning polynomials over finite fields*, Ph.D. thesis, University of Trento, Italy, December 2013.

[Ros02] Michael Rosen, *Number theory in function fields*, Graduate Texts in Mathematics, vol. 210, Springer-Verlag, New York, 2002. MR 1876657

[Sti09] Henning Stichtenoth, *Algebraic function fields and codes*, 2nd ed. ed., Grad. Texts Math., vol. 254, Berlin: Springer, 2009.

[Wei13] Colin Weir, *Constructing and Tabulating Dihedral Function Fields*, Ph.D. thesis, University of Calgary, 2013.

[WSH13] Colin Weir, Renate Scheidler, and Everett W. Howe, *Constructing and tabulating dihedral function fields*, ANTS X. Proceedings of the tenth algorithmic number theory symposium, San Diego, CA, USA, July 9–13, 2012, Berkeley, CA: Mathematical Sciences Publishers (MSP), 2013, pp. 557–585.

Dipartimento di Matematica e Applicazioni, Università degli Studi di Milano–Bicocca, via Cozzi 55, I-20125 Milano, Italy

Email address: sandro.mattarei@unimib.it

Dipartimento di Matematica, Università degli Studi di Trento, via Sommarive 14, I-38123 Povo (Trento), Italy

Email address: marco.pizzato1@gmail.com