Designs, Codes and Cryptography (2022) 90:2223–2247
https://doi.org/10.1007/s10623-022-01060-0

# The extended coset leader weight enumerator of a twisted cubic code

**Aart Blokhuis**[1] · **Ruud Pellikaan**[1] · **Tamás Szőnyi**[2]

Received: 10 April 2021 / Revised: 17 April 2022 / Accepted: 13 May 2022 /
Published online: 20 June 2022


**Abstract**
The extended coset leader weight enumerator of the generalized Reed–Solomon $[q+1, q-3, 5]_q$ code is computed. In this computation methods in finite geometry, combinatorics and algebraic geometry are used. For this we need the classification of the points, lines and planes in the projective three space under projectivities that leave the twisted cubic invariant. A line in three space determines a rational function of degree at most three and vice versa. Furthermore, the double point scheme of a rational function is studied. The pencil of a true passant of the twisted cubic, not in an osculation plane gives a curve of genus one as double point scheme. With the Hasse–Weil bound on $\mathbb{F}_q$-rational points we show that there is a 3-plane containing the passant.

**Keywords** Extended coset leader weight enumerator · Generalized Reed–Solomon code · Twisted cubic · Classification of lines in three space over finite fields

**Mathematics Subject Classification** 94B50 · 14G15 · 51A05

## 1 Introduction

In general the computation of the weight enumerator of a code is hard and even harder so for the coset leader weight enumerator. Generalized Reed–Solomon codes are MDS, so their

This is one of several papers published in *Designs, Codes and Cryptography* comprising the "Special Issue: The Art of Combinatorics – A Volume in Honour of Aart Blokhuis".

✉ Ruud Pellikaan
g.r.pellikaan@tue.nl

Aart Blokhuis
a.blokhuis@TUE.nl

Tamás Szőnyi
tamas.szonyi@ttk.elte.hu

[1] Department of Mathematics and Computer Science, Eindhoven University of Technology, Eindhoven, The Netherlands

[2] Department Computer Science, Eötvös Loránd University, Budapest, Hungary

weight enumerators are known and its formulas depend only on the size of the finite field, the length and the dimension of the code. The coset leader weight enumerator of an MDS code depends on the geometry of the associated projective system of the dual code. The coset leader weight enumerator of the $\mathbb{F}_q$-ary generalized Reed–Solomon codes of length $q+1$ of codimension four is considered, so its associated projective systems are normal rational curves. Moreover the coset leader weight enumerators of the extensions of these codes over $\mathbb{F}_{q^m}$ are determined. In case of the $[q+1, q-2, 4]_q$ code where the associated projective system consists of the $q+1$ points of an irreducible plane conic, the answer [17] depends on whether the characteristic is odd or even. If the associated projective system of the $[q+1, q-3, 5]_q$ code consists of the $q+1$ points of a twisted cubic, the answer is the main result of this paper and depends on $q$ modulo 6.

Our result depends on the classifications of the points, lines and planes in $\mathbb{P}^3$ under projectivities that leave the twisted cubic invariant. The classification of points and planes was done in [3, 13] and they gave a partition of lines in classes which is not a complete classification. The knowledge of the point-plane incidence matrix is applied to multiple covering codes by [1]. But for our purpose we need to know whether a given line is contained in a 3-plane.

The main result of this paper is a refined partition and the plane-line incidence. Recent papers [4, 5, 10] compute the number of times a line of a given class is contained in a plane of a given class, except for the class $\mathcal{O}_6$ (true passants not in an osculation plane). In [10] a conjecture is given about the number of classes of lines in a complete classification.

We showed that the class $\mathcal{O}_6$ is subdivided further in classes that depend on a modulus, a continuous invariant that is the cross-ratio of an associated 4-tuple of points. It is left as a conjecture whether this gives a complete classification of the classes in $\mathcal{O}_6$.

In our approach, we use the relation between rational functions and codimension two subspaces. Furthermore, the double point scheme $\mathcal{E}_\varphi$ of a rational function $\varphi$ is studied in general. If the rational function $\varphi$ is a separable simple morphism of degree $d$, then $\mathcal{E}_\varphi$ is an absolutely irreducible curve of genus $(d-1)^2$. In particular the pencil of planes containing a given line, that is a true passant, not in an osculating plane defines a rational function and its double point scheme is a curve of genus 1. With the Hasse–Weil bound it is shown that there is a 3-plane containing a given true passant in case $q \geq 23$.

## 2 The coset leader weight enumerator

The extended coset leader weight enumerator of a code is considered and it is just our aim to determine this enumerator of the code associated to the twisted cubic. Let $C$ be an $\mathbb{F}_q$-linear code of length $n$. Let $\mathbf{r} \in \mathbb{F}_q^n$. The *weight of the coset* $\mathbf{r}+C$ is defined by $\mathrm{wt}(\mathbf{r}+C) = \min\{\mathrm{wt}(\mathbf{r}+\mathbf{c}) : \mathbf{c} \in C\}$. A *coset leader* is a choice of an element $\mathbf{r} \in \mathbb{F}_q^n$ of minimal weight in its coset, that is $\mathrm{wt}(\mathbf{r}) = \mathrm{wt}(\mathbf{r}+C)$. Let $\alpha_i$ be the number of cosets of $C$ of weight $i$. The *coset leader weight enumerator* is the polynomial with coefficients $\alpha_i$.

A *coset leader* decoder gives as output $\mathbf{r}-\mathbf{e}$, where $\mathbf{r}$ is the received word and $\mathbf{e}$ is a chosen coset leader of the coset of $\mathbf{r}$. So $\mathbf{r}-\mathbf{e}$ is a nearest codeword to $\mathbf{r}$, but sometimes it is not the only one. The probability of decoding correctly by the coset leader decoder on a $q$-ary symmetric channel with cross-over probability $p$ is computed by means of the coset leader weight enumerator, see [19, Prop. 1.4.32].

Let $C$ be an $\mathbb{F}_q$-linear code with *parameters* $[n, k, d]$, that is of *length* $n$, *dimension* $k$ and *minimum distance* $d$. Then $C \otimes \mathbb{F}_{q^m}$ is the $\mathbb{F}_{q^m}$-linear code generated by $C$ and it is

called the *extension code* of $C$ over $\mathbb{F}_{q^m}$. The weight enumerator of such an extension code has coefficients that are polynomials in $q^m$, see [16, 18]. Similarly the *extended coset leader weight enumerator* of $C$ has coefficients $\alpha_i(T)$ that are polynomials in $T$ such that $\alpha_i(q^m)$ is the number of cosets of $C \otimes \mathbb{F}_{q^m}$ that are of weight $i$, see [12, 17]. Now $\alpha_i(q^m)$ is divisible by $q^m - 1$ for all $m, i \geq 1$, since the coset weight of $\mathbf{r} + C$ and of $\lambda\mathbf{r} + C \otimes \mathbb{F}_{q^m}$ with respect to $C \otimes \mathbb{F}_{q^m}$ have the same size for all nonzero $\lambda \in \mathbb{F}_{q^m}$. So also $\alpha_i(T)$ is divisible by $T - 1$ for all $i \geq 1$. Define

$$a_i(T) := \frac{\alpha_i(T)}{T-1}.$$

Then $a_i(T) = \binom{n}{i}(T-1)^{i-1}$ for all $1 \leq i \leq (d-1)/2$ and $\sum_{i=0}^{n-k} \alpha_i(T) = T^{n-k}$. So $\sum_{i=1}^{n-k} a_i(T) = \sum_{i=0}^{n-k-1} T^i$.

### 2.1 Codes versus projective systems

Let $\mathbb{F}_q$ be the field with $q$ elements, where $q = p^h$ for some prime $p$. The *projective space* of dimension $r$ is denoted by $\mathbb{P}^r$. Let $\mathbb{F}$ be a field. An $\mathbb{F}$-*rational point* of $\mathbb{P}^r$ is an equivalence class of $\mathbb{F}^{r+1} \setminus \{0\}$ under the equivalence relation $\mathbf{x} \equiv \mathbf{y}$ if and only if $\mathbf{x} = \lambda\mathbf{y}$ for some nonzero $\lambda \in \mathbb{F}$. The equivalence class of $\mathbf{x} = (x_0, x_1, \ldots, x_r)$ is denoted by $(x_0 : x_1 : \ldots : x_r)$. Dually a *hyperplane* in $\mathbb{P}^r$ given by the equation $a_0X_1 + a_1X_1 + \cdots + a_rX_r = 0$ is denoted by $[a_0 : a_1 : \ldots : a_r]$. Let $\mathcal{X}$ be a subvariety of $\mathbb{P}^r$. Then the set of $\mathbb{F}$-rational points of $\mathcal{X}$ is denoted by $\mathcal{X}(\mathbb{F})$ and by $\mathcal{X}(q)$ in case $\mathbb{F} = \mathbb{F}_q$.

A subspace of $\mathbb{P}^r(q^m)$ is an intersection of hyperplanes, and it will be called $\mathbb{F}_q$-rational if it extends a corresponding subspace in $\mathbb{P}^r(q)$.

Let $H$ be a *parity check* matrix of $C$, that is an $(n-k) \times n$ matrix such that $\mathbf{c} \in C$ if and only if $H\mathbf{c}^T = 0$. Hence, a codeword of weight $w$ corresponds one-to-one to a linear combination of $w$ columns of a given parity check matrix adding up to zero. The *syndrome* $\mathbf{s}$ (with respect to H) of a received word $\mathbf{r} \in \mathbb{F}_q^n$ is the column vector of length $n-k$ defined by $\mathbf{s} = H\mathbf{r}^T$. This gives a one-to-one correspondence between cosets and syndromes. The coset of a word of minimal weight corresponds one-to-one to a minimal way to write the syndrome of that word as a linear combination of the columns of a given parity check matrix.

From now on we assume that the minimum distance of the code is at least 3, so $H$ has no zero column and no two columns are dependent. So its columns can be viewed as homogeneous coordinates of $n$ distinct points in projective space of dimension $n-k-1$.

More generally, let $H$ be a $l \times n$ matrix of rank $l$ with elements from $\mathbb{F}_q$. We view the columns of $H$ as a *projective system* [19, §8.3.2], that is a set $\mathcal{P}$ of $n$ points in projective space $\mathbb{P}^r(q)$, with $r = l-1$ that do not lie in a hyperplane, in particular we assume that the columns are non-zero, and no pair is dependent. We now want to determine $\alpha_i = \alpha_i(q)$ which is the number of vectors in $\mathbb{F}_q^l$ that are a linear combination of some set of $i$ columns of $H$, but not less. More generally, we want to determine $\alpha_i(q^m)$ which is the number of vectors in $\mathbb{F}_{q^m}^l$ with the same property over $\mathbb{F}_{q^m}$ for $i = 0, \ldots, l$. We think projectively, so for $i = 1, \ldots, r+1$ we want to determine $a_i(q^m)$ the number of points in $\mathbb{P}^r(\mathbb{F}_{q^m})$ that lie in a projective subspace of dimension $i-1$ that intersects $\mathcal{P}$ in exactly $i$ points, and not for smaller $i$.

## 3 The normal rational curve

The *normal rational curve* of degree $r$ is the curve $\mathcal{C}_r$ in $\mathbb{P}^r$ with parametric representation $\{(x^r : x^{r-1}y : \ldots : xy^{r-1} : y^r) \mid (x : y) \in \mathbb{P}^1\}$, see [13, §21.1]. This map gives an

isomorphism of $\mathbb{P}^1$ with $\mathcal{C}_r$ and the point $(x : 1)$ (and $(1 : 0)$) on $\mathbb{P}^1$ is identified with $(x^3 : x^2 : x : 1)$ (and $(1 : 0 : 0 : 0)$) on $\mathcal{C}_r$ and both are denoted by $P(x)$ (and $P(\infty)$) where the context makes it clear what is meant.

Combinatorially, the most important property of $\mathcal{C}_r$ is that no $r + 1$ points are in a hyperplane. In the following, we will take $r = 3$ so we have the curve $\mathcal{C}_3$ in $\mathbb{P}^3$. This curve is also called the *twisted cubic*. In this dimension, the set $\mathcal{C}_r(q)$ is maximal with respect to the property that no 4 points are coplanar (for $q > 3$).

### 3.1 The twisted cubic $\mathcal{C}_3$

The definitions of this section can be found [13].

The *conjugate* of $x \in \bar{\mathbb{F}}_q$ is defined by $\bar{x} = x^q$.

A *chord* is the line joining two points of $\mathcal{C}_3$. We distinguish *real chords*, joining two different points of $\mathcal{C}_3$, *tangents*, where the two points coincide, and *imaginary chords*, where the two points are conjugate points of the extension of $\mathcal{C}_3$ to $\mathbb{P}^3(q^2)$.

An *osculating plane* is a plane that intersects the twisted cubic in one point with multiplicity three. An *axis* is the line of intersection of two osculating planes. A *real axis* is the intersection of two different osculating planes, an *imaginary axis* is the intersection of two osculating planes at conjugate points of $\mathcal{C}_3$ in $\mathbb{P}^3(q^2)$. If $p = 3$, then there is exactly one axis, the intersection of all osculating planes and it is called the axis of $\mathbf{0}_3$.

The *tangent* at the point $P(x) = (x^3 : x^2 : x : 1)$ is the line $\langle (x^3, x^2, x, 1), (3x^2, 2x, 1, 0)\rangle$, and at the point $P(\infty) = (1 : 0 : 0 : 0)$ we have $\langle (1, 0, 0, 0), (0, 0, 1, 0)\rangle$.

A *passant* or *external line* is a line disjoint from $\mathcal{C}_3(q)$, it is called *true* if it is *not* an imaginary chord.

A *unisecant* is a line intersecting $\mathcal{C}_3(q)$ in 1 point, it is called *true* if it is *not* a tangent.

A *bisecant* or simply *secant* is a line intersecting $\mathcal{C}_3(q)$ in 2 points (this is the same as a real chord).

An *i-plane*, $i = 0, 1, 2, 3$, is a plane containing $i$ points of $\mathcal{C}_3(q)$.

A subspace of $\mathbb{P}^3(q^m)$ (so a point, line or plane) will be called *rational* if it extends a corresponding subspace in $\mathbb{P}^3(q)$.

A *regulus* in $\mathbb{P}^3(q)$ is the collection of rational lines that are *transversals* of three given *skew* lines, that is the collection of lines that intersect three given lines that are mutually disjoint. The regulus of three skew lines consists of $q + 1$ skew lines. The *complementary regulus* of the regulus of three skew lines $l_1, l_2, l_3$, is the regulus of any three lines $l'_1, l'_2, l'_3$ in the regulus of $l_1, l_2, l_3$.

### 3.2 The problem

We consider the coset leader weight enumerator for the extended Reed–Solomon $[q + 1, q - 3, 5]$ code with $4 \times (q + 1)$ parity check matrix $H$ whose columns are the vectors $(1, t, t^2, t^3)$ together with $(0, 0, 0, 1)$. The projective system of $H$ is the twisted cubic, that is normal rational curve of degree 3 in $\mathbb{P}^3(q)$.

So, what we want is an answer to the following questions, first for $\mathbb{P}^3(q)$ itself, but also for $\mathbb{P}^3(q^m)$:

$a_1$: How many points belong to the curve $\mathcal{C}_3(q)$?

$a_2$: How many points, not already counted under $a_1$, are on a line containing two points of $\mathcal{C}_3(q)$?

$a_3$: Now the interesting part starts, how many points are there on a 3-plane, that is a plane containing three points of $\mathcal{C}_3(q)$, not already counted under $a_1$ or $a_2$?

The first two questions turn out to be trivial and for the third we introduce the following definition.

**Definition 3.1** Let $\mu_q$ be the number of rational lines of $\mathbb{P}^3(q)$ that lie in one or more 3-planes and are not real chords.

**Theorem 3.2** *The extended coset leader weight enumerator of the extended Reed–Solomon* $[q+1, q-3, 5]$ *code is given by*

$$a_1(T) = q+1 \text{ and } a_2(T) = \tbinom{q+1}{2}(T-1),$$

*and* $a_3(T)$ *is equal to*

$$\tfrac{1}{2}q(q+1)^2 + \tbinom{q+1}{3}\left[T^2+T+1-(q^2+q+1)(T-q+1)\right] + \mu_q \cdot (T-q),$$

*and*

$$a_4(T) = T^3+T^2+T+1-a_1(T)-a_2(T)-a_3(T).$$

***Proof*** The number of points of the curve $\mathcal{C}_3(q)$ is $q+1$. So $a_1 = q+1$ and also $a_1(q^m) = q+1$, since in our problem $\mathcal{C}_3(q)$ is restricted to $\mathbb{P}^3(q)$. Hence $a_1(T) = q+1$.

There are $\binom{q+1}{2}$ secants, each one of them contributes $q-1$ points (for $m$: $q^m-1$), since two secants don't intersect in a point outside $\mathcal{C}_3(q)$, for that would imply four coplanar points on $\mathcal{C}_3(q)$. So $a_2(q^m) = \binom{q+1}{2}(q^m-1)$ for all $m$. Hence $a_2(T) = \binom{q+1}{2}(T-1)$.

These two cases also follow from the general result that $a_i(T) = \binom{n}{i}(T-1)^{i-1}$ for all $1 \le i \le (d-1)/2$ for an $[n,k,d]$ code, since in this case $n = q+1$ and $d = 5$.

Now we consider the computation of $a_3$. In $\mathbb{P}^3(q)$ the answer is easy: the rest, so $\frac{1}{2}q(q+1)^2$. Indeed a point that does not lie on the curve or on a secant or on a 3-plane can be used to extend the arc, but it is well known that the arc is maximal (for $q > 3$).

Outside $\mathbb{P}^3(q)$ we argue as follows: If a point is on more than one 3-plane, then it must be on a line of $\mathbb{P}^3(q)$, so forgetting about these points for the moment, this means that each of the $\binom{q+1}{3}$ different 3-planes contributes $q^{2m}+q^m+1-(q^2+q+1)-(q^2+q+1)(q^m-q)$ points that are certainly in this 3-plane only.

The remaining points are outside $\mathbb{P}^3(q)$ on a line of $\mathbb{P}^3(q)$, which is not a real chord and that is contained in a 3-plane.

We give the formula for $a_3(q^m)$ in terms of the parameter $\mu_q$.

$$\tfrac{1}{2}q(q+1)^2 + \tbinom{q+1}{3}\left[q^{2m}+q^m+1-(q^2+q+1)(q^m-q+1)\right] + \mu_q(q^m-q).$$

Hence, $a_3(T)$ is equal to

$$\tfrac{1}{2}q(q+1)^2 + \tbinom{q+1}{3}\left[T^2+T+1-(q^2+q+1)(T-q+1)\right] + \mu_q(T-q).$$

The first term counts the points $P$ in $\mathbb{P}^3(q)$, not on $\mathcal{C}_3(q)$ that are either on a tangent of a rational point of $\mathcal{C}_3(q)$ or on an imaginary chord of $\mathcal{C}_3(q)$.

The second term is the number of points outside $\mathbb{P}^3(q)$, in a rational plane, but not on a rational line.

The third term is the number of points outside $\mathbb{P}^3(q)$, on a rational line that is contained in a 3-plane and is not a real chord.

Finally $a_1(T)+a_2(T)+a_3(T)+a_4(T) = T^3+T^2+T+1$. Hence, $a_4(T)$ can be expressed in the known terms $a_1(T)$, $a_2(T)$ and $a_3(T)$:

$$a_4(T) = T^3+T^2+T+1-a_1(T)-a_2(T)-a_3(T) \qquad \square$$

The rest of this article is devoted to the determination of the value of $\mu_q$, that turns out to depend on the value of $q$ mod 6 and will be given in Sect. 8.2. In order to do that we will give the relation between rational functions and codimension two subpaces of the projective space in Proposition 6.5. Furthermore, we classify several types of lines in Theorem 8.1.

## 4 The classification of planes and points in $\mathbb{P}^3$

Almost everything in this section can be found in [3] and [13, Chap. 21].

The group $G_q = PGL(2,q)$ of nonsingular $2 \times 2$ matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with $ad - bc \neq 0$, modulo nonzero multiples of the identity. So $G_q$ has order $(q^2-1)(q^2-q)/(q-1) = q(q^2-1)$.

The group $G_q$ acts via $\varphi(x : y) = (ax + by : cx + dy)$ on $\mathbb{P}^1$, also denoted by $\varphi(x) = (ax+b)/(cx+d)$ and it acts sharply 3-transitively on $\mathbb{F}_q \cup \{\infty\}$. If $\varphi \in G_{q^2}$, that is with coefficients in $\mathbb{F}_{q^2}$ we define the *conjugate* of $\varphi$ by $\bar{\varphi}(x) = (\bar{a}x + \bar{b})/(\bar{c}x + \bar{d})$. Furthermore, $G_q$ acts on $\mathcal{C}_3(q)$ and this gives the following map on column vectors:

$$(x^3, x^2, x, 1) \mapsto ((ax+b)^3, (ax+b)^2(cx+d), (ax+b)(cx+d)^2, (cx+d)^3).$$

This mapping has matrix

$$\begin{pmatrix} a^3 & 3a^2b & 3ab^2 & b^3 \\ a^2c & a^2d+2abc & b^2c+2abd & b^2d \\ ac^2 & bc^2+2acd & ad^2+2bcd & bd^2 \\ c^3 & 3c^2d & 3cd^2 & d^3 \end{pmatrix},$$

hence its action extends to a *linear collineation* of $\mathbb{P}^3(q)$. For $q \geq 5$, $G_q$ is the full group of *projectivities* in $\mathbb{P}^3(q)$ fixing $\mathcal{C}_3(q)$ by [13, Lemma 21.1.3]. In [13, p. 233] the action is on row vectors on the left, whereas in this paper the action is on column vectors on the right, since we consider the projective system of the code with the column vectors of the parity check matrix as its points.

**Proposition 4.1** *Under $G_q$ there are five orbits $\mathcal{N}_i$ of planes with $n_i = |\mathcal{N}_i|$ :*
*$\mathcal{N}_1$ : Osculating planes of $\mathbf{0}_3(q)$, $n_1 = q+1$.*
*$\mathcal{N}_2$ : Planes with exactly two points of $\mathcal{C}_3(q)$, $n_2 = q(q+1)$.*
*$\mathcal{N}_3$ : Planes with three points of $\mathcal{C}_3(q)$, $n_3 = \frac{1}{6}q(q^2-1)$.*
*$\mathcal{N}_4$ : Planes with exactly one point of $\mathcal{C}_3(q)$, not osculating, $n_4 = \frac{1}{2}q(q^2-1)$.*
*$\mathcal{N}_5$ : Planes with no points of $\mathcal{C}_3(q)$, $n_5 = \frac{1}{3}q(q^2-1)$.*

***Proof*** See Corollary 4 of Chapter 21 in [13]. □

***Remark 4.2*** There is another way to look at this which is the approach in [10]: For the plane $[1 : c : b : a]$ consider the cubic $f(x) = x^3 + cx^2 + bx + a = (x-\alpha)(x-\beta)(x-\gamma)$.

$\mathcal{N}_1$: If $\alpha = \beta = \gamma$ we have an osculating plane, where $\alpha = \infty$ corresponds to the plane $[0:0:0:1]$, or $X_3 = 0$.

$\mathcal{N}_2$: If $\alpha = \beta \neq \gamma$, we have a plane with two points. The case $\alpha = \beta = \infty$, $\gamma = 0$ corresponds to the plane $[0:0:1:0]$ or $X_2 = 0$.

$\mathcal{N}_3$. If $\alpha, \beta, \gamma$ are different elements from $\mathbb{F}_q$ we get a plane with three points, for $\alpha = \infty$, $\beta = 0$, $\gamma = 1$ we get $[0:1:-1:0]$, or $X_1 = X_2$.

$\mathcal{N}_4$. If $\alpha \in \mathbb{F}_q$, $\beta = \bar{\gamma} \notin \mathbb{F}_q$. If $\alpha = \infty$ then we have the plane $[0 : 1 : -t : n]$ for some irreducible polynomial $X^2 - tX + n = 0$, with $t = \beta + \bar{\beta}$ and $n = \beta\bar{\beta}$.

$\mathcal{N}_5$. Finally if $f$ is irreducible we have a plane without points of $\mathcal{C}_3(q)$.

At each point $P(x) = (x^3 : x^2 : x : 1)$ of $\mathcal{C}_3$ we have an *osculating plane* $\pi(x) = [1 : -3x : 3x^2 : -x^3]$ and $\pi(\infty) = [0 : 0 : 0 : 1]$ parameterizing the *osculating developable* $\mathbf{0}_3$.

If $q \neq 0 \bmod 3$, so if $p \neq 3$ then there is an associated *null-polarity*

$$(a_0 : a_1 : a_2 : a_3) \leftrightarrow [-a_3 : 3a_2 : -3a_1 : a_0]$$

interchanging $\mathcal{C}_3$ and $\mathbf{0}_3$, and their corresponding chords and axes.

**Proposition 4.3** *Under $G_q$ there are five orbits $\mathcal{M}_i$ of points with $m_i = |\mathcal{M}_i|$ :*

*(i) If $p \neq 3$, then*
$\mathcal{M}_1$ : *Points on $\mathcal{C}_3(q)$, $m_1 = q + 1$.*
$\mathcal{M}_2$ : *Points off $\mathcal{C}_3(q)$, on a tangent, $m_2 = q(q + 1)$.*
$\mathcal{M}_3$ : *Points on three osculating planes, $m_3 = \frac{1}{6}q(q^2 - 1)$.*
$\mathcal{M}_4$ : *Points off $\mathcal{C}_3(q)$, on exactly one osculating plane, $m_4 = \frac{1}{2}q(q^2 - 1)$.*
$\mathcal{M}_5$ : *Points on no osculating plane, $m_5 = \frac{1}{3}q(q^2 - 1)$.*
*(ii) If $p = 3$, then*
$\mathcal{M}_1$ : *Points on $\mathcal{C}_3(q)$, $m_1 = q + 1$.*
$\mathcal{M}_2$ : *Points on all osculating planes, $m_2 = q + 1$.*
$\mathcal{M}_3$ : *Points off $\mathcal{C}_3(q)$, on a tangent, on one osculating plane, $m_3 = q^2 - 1$.*
$\mathcal{M}_4$ : *Points off $\mathcal{C}_3(q)$, on a real chord, $m_4 = \frac{1}{2}q(q^2 - 1)$.*
$\mathcal{M}_5$ : *Points on an imaginary chord, $m_5 = \frac{1}{2}q(q^2 - 1)$.*

***Proof*** See Corollary 5 of Chapter 21 in [13]. □

***Remark 4.4*** If $p \neq 3$, then $\mathcal{M}_2$ is also the set of points on exactly two osculating planes, and $\mathcal{M}_3 \cup \mathcal{M}_5$ is the set of points not in $\mathcal{C}_3(q)$ on a real (or imaginary) chord, and $\mathcal{M}_4$ is the set of points not in $\mathcal{C}_3(q)$ on an imaginary (or real) chord if $q \equiv 1 \mod 3$ (or $q \equiv -1 \mod 3$ respectively) by the corollary of [13, Lemma 21.1.11].

If $p = 3$, then $\mathcal{M}_2 \cup \mathcal{M}_3$ is the set of points not in $\mathcal{C}_3(q)$ on a tangent.

Hence, for all $q$ we have that every point not in $\mathcal{C}_3(q)$ is on a unique line that is a tangent, a real chord or an imaginary chord.

***Remark 4.5*** We will give a partition of the lines in $\mathbb{P}^3$ in Sect. 8.

## 5 Algebraic curves

For the theory of algebraic curves we will refer to the textbooks [11, 14, 21]. By an (algebraic) curve we mean an algebraic variety over a field $\mathbb{F}$ of dimension one, so it is absolutely irreducible. Most of the time we assume that the curve is nonsingular, unless stated otherwise. The *genus* of the curve $\mathcal{X}$ is denoted by $g(\mathcal{X})$.

### 5.1 Divisors on a curve

Let $\mathcal{X}$ be a curve over $\mathbb{F}_q$. A *place* of a curve $\mathcal{X}$ over the finite field $\mathbb{F}_q$ is an orbit under the Frobenius of the points of $\mathcal{X}(\mathbb{F}_{q^m})$ of some finite extension $\mathbb{F}_{q^m}$ of $\mathbb{F}_q$. The *degree* of the

place $P$ is the number of points in its orbit and is denoted by $\deg(P)$. Alternatively a place can be defined as a *discrete valuation* of the *function field* $\mathbb{F}_q(\mathcal{X})$.

The number of points of the projective line that are defined over $\mathbb{F}_q$ is equal to $q+1$, and a place of degree $d$ corresponds one-to-one to a monic irreducible polynomial in $\mathbb{F}_q[X]$ of degree $d$. In particular $\frac{1}{2}(q^2-q)$ is the number of places of degree 2.

A *divisor* on a curve $\mathcal{X}$ is a formal sum of places $P$ with integer coefficients such that only finitely many coefficients are nonzero. The degree of the divisor $D = \sum_P m_P P$ is defined by $\deg(D) = \sum_P m_P \deg(P)$. A divisor is called *effective* in case all its coefficients are nonnegative. A divisor $\sum_P m_P$ is called *simple* if $m_P = 0$ or $m_P = 1$ for all places $P$.

### 5.2 Ramified covers

For the following we refer to [11, 14, 21].

**Definition 5.1** Consider a morphism $\varphi : \mathcal{X} \to \mathcal{Y}$ of the nonsingular absolutely irreducible curves $\mathcal{X}$ and $\mathcal{Y}$ over the field $\mathbb{F}$. Then $\mathbb{F}(\mathcal{X})$, the function field of $\mathcal{X}$ is a finite field extension of $\mathbb{F}(\mathcal{Y})$, the function field of $\mathcal{Y}$, via $\varphi$. The degree of this extension is also called the *degree* of $\varphi$ and will be denoted by $\deg(\varphi)$.

The set of rational functions of $\mathbb{F}(\mathcal{X})$ that are defined at a place $P$ is denoted by $\mathcal{O}_P$ and is *local ring*, that is a ring with a unique maximal ideal $\mathcal{M}_P$. Moreover this maximal ideal is a principal ideal and a generator of $\mathcal{M}_P$ is called a *local parameter* at the place $P$. Let $x$ be a local parameter at the place $P$ of $\mathcal{X}$. Then $x$ is a generator of $\mathcal{M}_P$. Let $y$ be a local parameter at the place $Q = \varphi(P)$ of $\mathcal{Y}$. Then the local ring of $\mathcal{Y}$ at $Q$ is via $\varphi$ a subring of $\mathcal{O}_P$. In this way we consider $y$ as an element of $\mathcal{O}_P$ and $y = cx^e$ where $c$ is an invertible element of $\mathcal{O}_P$ and $e$ is a non-negative integer that is called the *ramification index* of $\varphi$ at the place $P$ and is denoted by $e_P(\varphi)$ or by $e_P$. The morphism $\varphi$ is said to *ramify* at $P$ and $P$ a ramification place of $\varphi$ if $e_P > 1$.

***Remark 5.2*** A geometric way to consider ramification is by considering $\Gamma_\varphi = \{(P, \varphi(P)) | P \in \mathcal{X}\}$ in $\mathcal{X} \times \mathcal{Y}$, the *graph* of $\varphi : \mathcal{X} \to \mathcal{Y}$. Now $\Gamma_\varphi$ is a curve on the surface $\mathcal{X} \times \mathcal{Y}$. The ramification index of $\varphi$ at the place $P$ is equal to the intersection multiplicity of $\Gamma_\varphi$ with the 'horizontal' line $\{(P', \varphi(P)) | P' \in \mathcal{X}\}$ at $(P, \varphi(P))$.

**Proposition 5.3** *If $P$ is a place of $\mathcal{X}$ and $\varphi(P) = Q$, then $Q$ is a place of $\mathcal{Y}$ and* $\deg(Q)$ *divides* $\deg(P)$ *and* $\deg(P)/\deg(Q)$ *is called the* relative degree *and denoted by* $\deg(P, Q)$. *If $Q$ is a place of $\mathcal{Y}$, then*

$$\deg(\varphi) = \sum_{\varphi(P)=Q} e_P \deg(P, Q).$$

*In particular, the fibre $\varphi^{-1}(Q)$ consist of at most* $\deg(\varphi)$ *places.*

***Proof*** See [21, Theorem III.1.11]. □

***Remark 5.4*** If $\deg(\varphi) \leq 3$, then $\varphi$ is injective on the set of ramification places by Proposition 5.3.

**Definition 5.5** Let $\varphi : \mathcal{X} \to \mathcal{Y}$ be a *separable* morphism between two curves. The ramification at $P$ is called *tame* if the characteristic does not divide $e_P$, otherwise it is called *wild*. The morphism ramifies at finitely many places. The *ramification divisor* of $\varphi$ is defined by

$$R_\varphi = \sum_P (e_P - 1)P.$$

**Definition 5.6** Consider a morphism $\varphi : \mathcal{X} \to \mathcal{Y}$. Let $x$ be a *local parameter* at the place $P$ of $\mathcal{X}$. Let $y$ be a local parameter at the place $Q = \varphi(P)$ of $\mathcal{Y}$. Then $y = cx^e$ where $c$ is an invertible element of $\mathcal{O}_P$ and $e$ is the ramification index of $\varphi$ at the place $P$. Let $y'$ be the derivative of $y$ with respect to the derivation of $x$. The *different exponent* of $\varphi$ at the place $P$ is the smallest $d$ such that $y' \in \mathcal{M}_P^d$ and is denoted by $d_P(\varphi)$ or by $d_P$. The *different divisor* of $\varphi$ is defined by

$$D_\varphi = \sum_P d_P \deg(P).$$

***Remark 5.7*** By the Leibniz rule we have

$$y' = c'x^e + ecx^{e-1}.$$

Hence, $d_P \geq e_P - 1$, and $d_P = e_P - 1$ if and only if the ramification at $P$ is tame, that is if characteristic of $\mathbb{F}$ does not divide $e_P$. If the ramification is wild then $d_P + 1$ is not divisible by the characteristic.

**Theorem 5.8** (Riemann–Hurwitz genus formula) *Let $\varphi : \mathcal{X} \to \mathcal{Y}$ be a separable morphism between curves that is not constant. Then*

$$2g(\mathcal{X}) - 2 = \deg(\varphi)(2g(\mathcal{Y}) - 2) + \deg(D_\varphi).$$

***Proof*** See [11, Corollary 2.4], [14, Theorem 7.27] and [21, Theorem III.4.12]. □

If the degree of the morphism $\varphi$ is 1, then the morphism is an isomorphism and there is no ramification.

## 6 Rational functions on the projective line

In this section we show that there is a one-to-one correspondence between $L$-equivalence classes of non-constant rational functions on $\mathbb{P}^1$ over $\mathbb{F}$ of degree $d$ and codimension 2 subspaces of $\mathbb{P}^d(\mathbb{F})$. Propositions on the possible ramification behaviour and the Riemann–Hurwitz genus formula give us the $RL$-classification of rational functions of degree 2.

### 6.1 Equivalence of rational functions

**Definition 6.1** A *rational function* $\varphi : \mathbb{P}^1 \dashrightarrow \mathbb{P}^1$ over $\mathbb{F}_q$ of degree $d$. is given by $\varphi(x : y) = (f(x, y) : g(x, y))$ where $f(x, y)$ and $g(x, y)$ are homogeneous polynomials of degree $d$. Let $h(x, y) = \gcd((f(x, y), g(x, y))$. The divisor defined by $h(x, y) = 0$ is called the base divisor $\varphi$ and is denoted by $B_\varphi$. More precisely, let $h(x, y) = \prod_i \pi_i^{m_i}$ where the $\pi_i$ are mutually distinct irreducible polynomials and the $m_i$ are positive integers. Let $P_i$ be the place of $\mathbb{P}^1$ that corresponds to $\pi_i$. The divisor $\sum_i m_i P_i$ is called the *base divisor* of $\varphi$ and is denoted by $B_\varphi$.

**Definition 6.2** Let $\varphi, \psi : \mathbb{P}^1 \to \mathbb{P}^1$ be two rational functions defined over $\mathbb{F}$. They are called *right* (R) *equivalent* if there is an automorphism $\alpha \in PGL(2, \mathbb{F})$ such that $\psi = \varphi \circ \alpha$, and *left* (L) *equivalent* if there is an automorphism $\beta \in PGL(2, \mathbb{F})$ such that $\psi = \beta \circ \varphi$.

Furthermore, $\varphi$ and $\psi$ are called *right-left* (RL) *equivalent* if there automorphisms $\alpha \in PGL(2, \mathbb{F})$ and $\beta \in PGL(2, \mathbb{F})$ such that $\psi = \beta \circ \varphi \circ \alpha$. If moreover $\beta = \alpha^{-1}$, then $\varphi, \psi$ are called *conjugate*.

***Remark 6.3*** Let $\varphi : \mathbb{P}^1 \dashrightarrow \mathbb{P}^1$ be given by $\varphi(x : y) = (f(x, y) : g(x, y))$.

(1) Let $h(x, y) = \gcd((f(x, y), g(x, y))$. Then $\varphi$ is a well-defined map outside the zero zet of $h(x, y)$. Let $\tilde{f}(x, y) = f(x, y)/h(x, y)$, $\tilde{g}(x, y) = g(x, y)/h(x, y)$ and $\tilde{\varphi}(x : y) = (\tilde{f}(x, y) : \tilde{g}(x, y))$. Then $\tilde{\varphi}$ is a well-defined function on $\mathbb{P}^1$, and $\varphi$ and $\tilde{\varphi}$ define the same function outside the zero zet of $h(x, y)$. We call $\tilde{\varphi}$ is the *associated morphism* of $\varphi$.
We will a make distinction between the notions of a *rational function* $\mathbb{P}^1 \dashrightarrow \mathbb{P}^1$ and a *morphism* $\mathbb{P}^1 \to \mathbb{P}^1$.
(2) Let $f(x, y) = \sum_{j=0}^{d} f_j x^{d-j} y^j$ and $g(x, y) = \sum_{j=0}^{d} g_j x^{d-j} y^j$. The $2 \times (d+1)$ matrix with first row $(f_0, f_1, \ldots, f_d)$ and second row $(g_0, g_1, \ldots, g_d)$ has rank $s \leq 2$, then $s \leq d$ and the image of $\varphi$ is contained in a subspace of $\mathbb{P}^1$ of dimension $s - 1$, that is either $\mathbb{P}^1$ or a point when $\varphi$ is constant. Therefore, we assume from now on that the image of $\varphi$ is not constant. Hence, $d \geq 2$.
(3) Under the L-equivalence of the action of $PGL(2, \mathbb{F})$, the projectivities of $\mathbb{P}^1$, we may assume that the $2 \times (d+1)$ matrix is in row reduced echelon form. (4) The corresponding rational function on the affine line is also denoted by $\varphi$ and is given by $\varphi(x) = f(x)/g(x)$, where $f(x)$ and $g(x)$ are univariate polynomials $d = \max\{\deg(f(x)), \deg(g(x))\}$. By (3) we may assume that $d = \deg(f(x)) > \deg(g(x))$, and $f(x)$ and $g(x)$ are monic, and $f_{0e} = 0$ where $e = \deg(g(x))$.

***Remark 6.4*** Let $\varphi : \mathbb{P}^1 \to \mathbb{P}^1$ be a separable morphism. Then $\deg(D_\varphi) = 2d - 2$ by the Riemann–Hurwitz genus formula 5.8.

(1) If $d = \deg(f(x)) > \deg(g(x))$, then $\varphi(P_\infty) = P_\infty$ and the ramification exponent of $P_\infty = (1 : 0)$ is equal to $d - \deg(g(x))$.
(2) Let $P = (x_0 : 1)$ with $x_0$ in some extension of $\mathbb{F}_q$ and $\varphi(x_0) = 0$. Then $\varphi(x) = (x - x_0)^{e_P} \psi(x)$ for some rational function $\psi(x)$ such that $\psi(x_0) \neq 0$. So $\varphi'(x) = e_P (x - x_0)^{e_P - 1} \psi(x) + (x - x_0)^{e_P} \psi'(x)$. Hence, $\varphi$ ramifies at $P$, that is $e_P > 1$ if and only if $\varphi'(x_0) = 0$.

### 6.2 Rational functions versus codimension two subspaces

**Proposition 6.5** *Let $\mathbb{F}$ be a field with algebraic closure $\bar{\mathbb{F}}$. Then there is a one-to-one correspondence between L-equivalence classes of non-constant rational functions on $\mathbb{P}^1$ over $\mathbb{F}$ of degree $d$ and codimension 2 subspaces of $\mathbb{P}^d(\mathbb{F})$. Furthermore,, the rational function is a morphism if and only if the codimension subspace does not intersect $\mathcal{C}_d(\bar{\mathbb{F}})$.*

***Proof*** The proof for morphisms and $\mathbb{F} = \mathbb{C}$ is given in [7, p. 106] and generalizes for arbitrary fields as follows.

Let $\varphi(x : y) = (f(x, y) : g(x, y))$ be a non-constant rational function on $\mathbb{P}^1$ over $\mathbb{F}$ of degree $d$ with $f(x, y) = \sum_{j=0}^{d} f_j x^{d-j} y^j$ and $g(x, y) = \sum_{j=0}^{d} g_j x^{d-j} y^j$ with $f_j, g_j \in \mathbb{F}$ for all $j$. Let $\mathcal{L}_\varphi$ be the subspace of $\mathbb{P}^d(\mathbb{F})$ defined by the homogeneous linear equations $\sum_{j=0}^{d} f_j X_j = 0$ and $\sum_{j=0}^{d} g_j X_j = 0$. The rational map $\varphi$ is not constant. So $f(x, y)$ and $g(x, y)$ are not a constant multiple of each other. Hence, $\mathcal{L}_\varphi$ is a codimension 2 subspace of $\mathbb{P}^d(\mathbb{F})$.

If $f(x, y)$ and $g(x, y)$ have a non-constant factor $h(x, y)$ in common, then $\mathcal{L}_\varphi$ intersects $\mathcal{C}_d(\bar{\mathbb{F}})$ at the zero set of $h(x, y)$.

Conversely, let $\mathcal{L}$ be a codimension 2 subspace of $\mathbb{P}^d(\mathbb{F})$ by the equations $\sum_{j=0}^{d} f_j X_j = 0$ and $\sum_{j=0}^{d} g_j X_j = 0$. Define $f(x, y) = \sum_{j=0}^{d} f_j x^j y^{d-j}$ and $g(x, y) = \sum_{j=0}^{d} g_j x^j y^{d-j}$. Then $f(x, y)$ and $g(x, y)$are not a constant multiple of each other, since $\mathcal{L}$ has codimension

2. So $\varphi_{\mathcal{L}}$ defined by $\varphi_{\mathcal{L}}(x : y) = (f(x, y) : g(x, y))$ is a non-constant rational functions on $\mathbb{P}^1$ over $\mathbb{F}$ of degree $d$.

If $\mathcal{L}$ intersects $\mathcal{C}_d(\bar{\mathbb{F}})$ at $P(x_0 : y_0)$, then $f(x_0, y_0) = 0$ and $g(x_0, y_0) = 0$. Hence, $f(x, y) = (x_0y - y_0x)c(x, y)$ and $g(x, y) = (x_0y - y_0x)d(x, y)$ for some homogeneous polynomials $c(x, y)$ and $d(x, y)$ of degree $d-1$. Therefore, $f(x, y)$ and $g(x, y)$ have a factor in common.

If $\psi$ is $L$-equivalent with $\varphi$, then there are $a, b, c, d \in \mathbb{F}$ such that $ad - bc \neq 0$ and $\psi(x, y) = (af(x, y) + bg(x, y))/(cf(x, y) + dg(x, y))$. Hence, $\mathcal{L}_\psi = \mathcal{L}_\varphi$.

Conversely, another pair of homogeneous linear equations defining $\mathcal{L}$ will give $\psi$, a rational function on $\mathbb{P}^1$ over $\mathbb{F}$ of degree $d$ that is $L$-equivalent with $\varphi$. □

***Remark 6.6*** The number of intersection points of $\mathcal{L}_\varphi$ with $\mathcal{C}_d(\bar{\mathbb{F}})$, counted with multiplicities, that is the degree of the base divisor of $\varphi$ is equal to $\deg(\varphi) - \deg(\tilde{\varphi})$, where $\tilde{\varphi}$ is the associated morphism of $\varphi$.

***Remark 6.7*** Let $\varphi(x) = f(x)/g(x))$ be a non-constant rational function of degree $d$ with $f(x) = \sum_{j=0}^{d} f_j x^{d-j}$ and $g(x) = \sum_{j=0}^{d} g_j x^{d-j}$ and $f_j, g_j \in \mathbb{F}$ for all $j$. Then $x \in \varphi^{-1}(u)$ if and only if $P(x)$ is in the hypersurface $H_{\varphi,u}$ with equation $\sum_{j=0}^{d}(f_j - ug_j)x_j = 0$. More precisely the ramification exponent $e_x(\varphi)$ is equal to the intersection multiplicity of that hypersurface with $\mathcal{C}_r$.

In particular places in the support of $R_\varphi$ correspond one-to-one to those places where $H_{\varphi,u}$ is tangent to $\mathcal{C}_r$ for some $u$. The hypersurfaces $H_{\varphi,u}$ contain $\mathcal{L}_\varphi$ for all $u$ and they form the so called *pencil* of hyperplanes of $\mathcal{L}_\varphi$.

***Remark 6.8*** Every morphism $\varphi : \mathbb{P}^1 \to \mathbb{P}^1$ of degree $d$ has a different divisor $D_\varphi$ that is an effective divisor of degree $2d - 2$. Let $C_d = \frac{1}{d}\binom{2d-2}{d-1}$ be the $d$-th Catalan number. If $\mathbb{F}$ is an algebraically closed field and $D$ an effective divisor of $2d - 2$ mutually distinct points, then there are $C_d$ morphisms on $\mathbb{P}^1$ of degree $d$ with the given $D$ as different divisor [9]. In particular, there are 2 morphisms on $\mathbb{P}^1$ of degree 3 with the given effective divisor $D$ of degree 4 as different divisor.

### 6.3 A partition of morphisms on $\mathbb{P}^1$ of degree 2

**Proposition 6.9** *Let $\varphi : \mathbb{P}^1 \to \mathbb{P}^1$ be a morphism of degree 2 over $\mathbb{F}_q$.*
*Then one of the following cases hold:*
(1) *$q$ is odd and $\varphi$ is separable and tame and $D_\varphi = R_\varphi$ and*
(1.*a*) *there are two $\mathbb{F}_q$-rational points $P_1$ and $P_2$ such that $R_\varphi = P_1 + P_2$,*
(1.*b*) *there is a place $Q$ of degree 2 such that $R_\varphi = Q$,*
(2) *$q$ is even and*
(2.*a*) *$\varphi$ is purely inseparable,*
(2.*b*) *$\varphi$ is separable and $R_\varphi = P$ and $D_\varphi = 2P$ for a $\mathbb{F}_q$-rational point $P$.*

***Proof*** If the morphism is not separable, then the characteristic divides the degree of $\varphi$. Hence, the characteristic is 2 and the map is purely inseparable. If the morphism is separable, then $deg(D_\varphi) = 2$ by Remark 6.4. Furthermore, the ramification index is 2 at every place where $\varphi$ ramifies by Proposition 5.3.

(1) If the characteristic is odd, then the ramification index is 2 at the ramification places, which is not divisible by the characteristic. Hence, $D_\varphi = R_\varphi$ and has degree 2. So either

(1.*a*) there are two $\mathbb{F}_q$-rational points $P_1$ and $P_2$ such that $R_\varphi = P_1 + P_2$, or

(1.*b*) there is a place $Q$ of degree 2 such that $R_\varphi = Q$.

(2) If the characteristic is even, then either

(2.*a*) $\varphi$ is purely inseparable,

(2.*b*) or $\varphi$ is separable and ramifies at a place $P$. Then $e_P = 2$ by Proposition 5.3 and the ramification is wild and $2 = e_P \leq d_P \leq \deg D_\varphi = 2$. So $P$ is an $\mathbb{F}_q$-rational point and $R_\varphi = P$ and $D_\varphi = 2P$ □

***Remark 6.10*** Without proof we mention that all the cases given in Proposition 6.9 do appear and are $RL$-equivalent to one of the following normal forms:

(1.*a*) $\varphi(x) = x^2$ and $R_\varphi = P(0) + P(\infty)$ with $P(0) = \varphi(P(0))$ and $PP(\infty) = \varphi(P(\infty))$.

(1.*b*) $\varphi(x) = (x^2 + d)/x$ where $d$ a chosen non-square in $\mathbb{F}_q$ and $R_\varphi = Q$ with $Q$ the place of degree 2 corresponding to the irreducible polynomial $X^2 - d$.

(2.*a*) $\varphi(x) = x^2$ where $\varphi$ is purely inseparable.

(2.*b*) $\varphi(x) = x^2/(x + 1)$ where $\varphi$ is separable and $R_\varphi = P(0)$ and $D_\varphi = 2P(0)$.

**Definition 6.11** Let $\varphi : \mathbb{P}^1 \to \mathbb{P}^1$ be a morphism. Denote by $p_{i,j,k}$ the number of places $Q$ of $\mathbb{P}^1$ of degree $i$ that have $j$ places of degree $k$ in $\varphi^{-1}(Q)$.

***Remark 6.12*** If $p_{i,j,k}$ is not zero, then $i$ divides $k$ and $j \leq \deg(\varphi)$ by Proposition 5.3.

**Proposition 6.13** *Let $\varphi : \mathbb{P}^1 \to \mathbb{P}^1$ be a separable morphism of degree 2 over $\mathbb{F}_q$. Then corresponding to those given in Proposition 6.9 the following holds:*

(1.*a*) $p_{1,1,1} = 2$, $p_{1,2,1} = p_{1,1,2} = \frac{1}{2}(q - 1)$.

(1.*b*) $p_{1,1,1} = 0$, $p_{1,2,1} = p_{1,1,2} = \frac{1}{2}(q + 1)$.

(2.*a*) $p_{1,1,1} = q + 1$, $p_{2,1,2} = \frac{1}{2}(q^2 - q)$.

(2.*b*) $p_{1,1,1} = 1$, $p_{1,2,1} = p_{1,1,2} = \frac{1}{2}q$.

***Proof*** The cases correspond to those given in Proposition 6.9.

(1.*a*). We have that $R_\varphi = P_1 + P_2$. So $p_{1,1,1} = 2$. Every rational point $P$ of $\mathbb{P}^1$ is mapped to a rational point of $\mathbb{P}^1$, and $\varphi^{-1}(Q)$ has at most 2 rational points for every rational point $Q$ of $\mathcal{Y}$, since $\deg(\varphi) = 2$. So $p_{1,1,1} + 2p_{1,2,1} = q + 1$. For every rational point $Q$ of $\mathcal{Y}$ we have that $\varphi^{-1}(Q)$ consists either of one ramification point or two rational points or one place of degree 2. Hence, $2 + p_{1,2,1} + p_{1,1,2} = q + 1$. Combining these two equations gives the result.

The other cases are treated similarly. □

## 7 The double point scheme of a morphism

In this section we consider the double point scheme of a morphism. This scheme is an absolutely irreducible nonsingular curve of genus $(d - 2)^2$ if the morphism is a simple separable rational function of degree $d$. In particular the curve has genus 1 if the rational function has degree 3. So we can apply the Hasse–Weil bound on the number of rational points. This allows us to conclude that there is a triple $(x, y, z)$ of mutually distinct $\mathbb{F}_q$-rational points of $\mathbb{P}^1$ such that $\varphi(x) = \varphi(y) = \varphi(z)$ for the rational function $\varphi$ if $q \geq 23$. That again will show in Proposition 8.4 that there is a rational plane that intersects the twisted cubic in three mutually distinct $\mathbb{F}_q$-rational points if the plane contains a line of class $\mathcal{O}_6$ (a true passant not in an osculating plane).

Let $\varphi : \mathbb{P}^1 \dashrightarrow \mathbb{P}^1$ be a non-constant rational function of degree $d$ with $\varphi(x) = f(x)/g(x)$. Suppose there exist $x, y \in \mathbb{F}$ such that $x \neq y$ and $\varphi(x) = \varphi(y)$. Then $\frac{\varphi(x)-\varphi(y)}{x-y} = 0$. So $(f(x)g(y) - f(y)g(x))/(x - y) = 0$.

**Definition 7.1** Let $\varphi : \mathbb{P}^1 \dashrightarrow \mathbb{P}^1$ be a rational function of degree $d$ with $\varphi(x) = f(x)/g(x)$. The *double point polynomial* $\Delta_\varphi$ of $\varphi$ is defined by

$$\Delta_\varphi(x, y) = \frac{f(x)g(y) - f(y)g(x)}{x - y}.$$

***Remark 7.2*** Let $h(x) = \gcd(f(x), g(x))$ and $\tilde{f}(x) = f(x)/h(x)$ and $\tilde{g}(x) = g(x)/h(x)$. Then $\tilde{\varphi}(x) = \tilde{f}(x)/\tilde{g}(x)$ is a morphism, that is $\tilde{f}(x)$ and $\tilde{g}(x))$ are relatively prime. Furthermore, $\Delta_\varphi(x, y) = h(x)h(y)\Delta\tilde{\varphi}(x, y)$.

***Remark 7.3*** The double point polynomial of $\varphi$ is a symmetric bivariate polynomial of bidegree at most $(d - 1, d - 1)$. The bihomogenization of the double point polynomial of $\varphi$ is defined by

$$\Delta_\varphi(x_0, x_1, y_0, y_1) = \sum_{0 \leq i, j \leq d-1} a_{ij} x_0^{d-1-i} x_1^i y_0^{d-1-j} y_1^j,$$

where $\Delta\varphi(x, y) = \sum_{0 \leq i, j \leq d-1} a_{ij} x^i y^j$.

Then $\Delta_\varphi(x_0, x_1, y_0, y_1)$ is a symmetric bivariate, bihomogeneous polynomial of bidegree $(d - 1, d - 1)$.

**Definition 7.4** Let $\mathcal{E}_\varphi$ be the subscheme of $\mathbb{P}^1 \times \mathbb{P}^1$ defined by the ideal generated by $\varphi(x_0, x_1, y_0, y_1)$. It is called the *double point scheme* of $\varphi$. See [6, Definition V-41].

***Remark 7.5*** A *permutation rational function* is a rational morphism $\varphi : \mathbb{P}^1 \to \mathbb{P}^1$ defined over $\mathbb{F}_q$ such that the map on the $\mathbb{F}_q$-rational points is a permutation. Clearly $\varphi$ is a permutation rational function if and only if $\mathcal{E}_\varphi$ has no points $\mathbb{F}_q$-rational points outside the diagonal. Similarly, a polynomial $f(x) \in \mathbb{F}_q[x]$ is called *permutation polynomial* if $f$ induces a permutation on $\mathbb{F}_q$. In [15] the polynomial $F(x, y) = [f(x + y)g(x) - f(x)g(x + y)]/y$ is defined for a rational function $\varphi(x) = f(x)/g(y)$. Now $\Delta_\varphi(x, y) = F(x, y - x)$.

**Lemma 7.6** *Let $\varphi(x) = f(x)/g(x)$ be a rational function. Then*

*(1)* $\Delta_\varphi(x, x) = f'(x)g(x) - f(x)g'(x)$,
*(2)* $(x, x) \in \mathcal{E}_\varphi(\bar{\mathbb{F}})$ *if and only if $\varphi$ ramifies at $x$.*

***Proof*** (1) Proved similarly as in Calculus.

(2) $\Delta_\varphi(x, x) = f'(x)g(x) - f(x)g'(x)$ is the numerator of the derivative $\varphi'(x)$. Therefore, $(x, x) \in \mathcal{E}_\varphi(\bar{\mathbb{F}})$ if and only if $\Delta_\varphi(x, x) = 0$ if and only if $\varphi'(x) = 0$ if and only if $\varphi$ ramifies at $x$.

□

**Definition 7.7** The ramification at $P$ is called *simple* if $e_P = 2$. The morphism $\varphi$ is called simple if all its ramification places are simple and if $\varphi$ ramifies at distinct places $P_1$ and $P_2$, then $\varphi(P_1)$ and $\varphi(P_2)$ are distinct.

**Definition 7.8** Let $\pi_1 : \mathcal{E}_\varphi \to \mathbb{P}^1$ be the projection on the first factor and $\pi_2 : \mathcal{E}_\varphi \to \mathbb{P}^1$ the projection on the second factor.

**Proposition 7.9** *Let $\varphi : \mathbb{P}^1 \to \mathbb{P}^1$ be a separable simple morphism. Then $\mathcal{E}_\varphi$ is reduced and nonsingular.*

***Proof*** $\mathcal{E}_\varphi$ is contained in $\mathbb{P}^1 \times \mathbb{P}^1$ and is defined by one equation. So it has no embedded components. Hence, if it nonsingular, then it is reduced. Therefore, it is sufficient to show that $\mathcal{E}_\varphi$ is nonsingular. Let $P = (a, b) \in \mathcal{E}_\varphi(\bar{\mathbb{F}})$.

Let $\mathcal{L} = \pi_1^{-1}(a)$ and $\mathcal{M} = \pi_2^{-1}(b)$. If one of the intersection multiplicities $I(P; \mathcal{L}, \mathcal{E}_\varphi)$ or $I(P; \mathcal{M}, \mathcal{E}_\varphi)$ is 1, then $\mathcal{E}_\varphi$ is nonsingular at $P$. Furthermore, $e_P(\pi_1) = I(P; \mathcal{L}, \mathcal{E}_\varphi)$ and $e_P(\pi_2) = I(P; \mathcal{M}, \mathcal{E}_\varphi)$ holds for the ramification exponents as in 6.7.

(1) If $a = b$, then $\varphi$ ramifies at $a$ by Proposition 7.6 with exponent 2, since $\varphi$ is simple. So $\varphi(x) = (x - a)^2 f(x)/g(x)$ and $f(0) \neq 0 \neq g(0)$. Hence, $\Delta_\varphi(a, y) = -(y - a)^2 f(y)g(0)/(a - y) = (y - a) f(y)g(a)$ and its multiplicity at $y = a$ is 1, since $f(a) \neq 0 \neq g(a)$. Therefore, $I((a, a); \mathcal{L}, \mathcal{E}_\varphi) = e_{(a,a)}(\pi_1) = 1$ and $\mathcal{E}_\varphi$ is nonsingular at $(a, a)$.

(2) If $a \neq b$ and $\varphi$ does not ramify at $a$ and also not at $b$, then $\varphi(x) = (x-a)(x-b) f(x)/g(x)$ and $f(a) \neq 0 \neq g(a)$ and $f(b) \neq 0 \neq g(b)$. Hence, $\Delta_\varphi(a, y) = -(y - a)(y - b) f(y)g(a)/(a - y) = (y - b) f(y)g(a)$ and its multiplicity at $y = b$ is 1, since $f(b) \neq 0 \neq g(a)$. Therefore, $I((a, b); \mathcal{L}, \mathcal{E}_\varphi) = e_P(\pi_1) = 1$ and $\mathcal{E}_\varphi$ is nonsingular at $(a, b)$.

(3) If $a \neq b$ and $\varphi$ ramifies at $a$ or $b$, then not at both, since $\varphi$ is simple. We may assume by symmetry of $\Delta_\varphi(x, y)$ in $x$ and $y$ that $\varphi$ ramifies at $a$ and not at $b$. So $\varphi(x) = (x - a)^2(x - b) f(x)/g(x)$ and $f(a) \neq 0 \neq g(a)$ and $f(b) \neq 0 \neq g(b)$. Hence, $\Delta_\varphi(a, y) = -(y - a)^2(y - b) f(y)g(a)/(a - y) = (y - a)(y - b) f(y)g(a)$ and its multiplicity at $y = b$ is 1, since $a \neq b$ and $f(b) \neq 0 \neq g(a)$. Therefore, $I((a, b); \mathcal{L}, \mathcal{E}_\varphi) = e_P(\pi_1) = 1$ and $\mathcal{E}_\varphi$ is nonsingular at $(a, b)$.

Therefore, $\mathcal{E}_\varphi$ is nonsingular. □

**Proposition 7.10** *Let $\varphi : \mathbb{P}^1 \to \mathbb{P}^1$ be a separable simple morphism of degree $d \geq 2$. Then $\mathcal{E}_\varphi$ is an absolutely irreducible nonsingular curve of genus $(d - 2)^2$.*

***Proof*** Let $\varphi : \mathbb{P}^1 \to \mathbb{P}^1$ be a separable map of degree $d \geq 2$ with simple ramification. Then $\mathcal{E}_\varphi$ is reduced and nonsingular by Proposition 7.9 and of bidegree $(d - 1, d - 1)$.

Suppose $\mathcal{E}_\varphi$ is reducible over the algebraic closure. Then it is the union of $\mathcal{X}$ and $\mathcal{Y}$, say of bidegrees $(a_1, a_2)$ and $(d - 1 - a_1, d - 1 - a_2)$, respectively such that $(a_1, a_2) \neq (0, 0)$ and $(a_1, a_2) \neq (d - 1, d - 1)$. Without loss of generality we may assume that $\mathcal{X}$ and $\mathcal{Y}$ have no component in common. So $\deg(\mathcal{X} \cdot \mathcal{Y}) = a_1(d - 1 - a_2) + a_2(d - 1 - a_1) > 0$ according to the Theorem of Bézout for the product of projective spaces [20, Chapter IV, §2.1] as mentioned in Sect. 5.1. Hence, $\mathcal{X}$ and $\mathcal{Y}$ have a point in common over the algebraic closure. So $\mathcal{E}_\varphi$ is singular at that point, which is a contradiction. Therefore, $\mathcal{E}_\varphi$ absolutely irreducible, that is irreducible over the algebraic closure.

A non-singular curve in $\mathbb{P}^1 \times \mathbb{P}^1$ of bidegree $(m, n)$ has genus $(m - 1)(n - 1)$. This is shown by the adjunction formula for a curve on a surface, see [11, Chapter V, Example 1.5.2]. Hence, $\mathcal{E}_\varphi$ has genus $(d - 2)^2$. □

**Corollary 7.11** *Let $\varphi : \mathbb{P}^1 \to \mathbb{P}^1$ be a separable simple morphism of degree* 3. *Then $\mathcal{E}_\varphi$ is an absolutely irreducible nonsingular curve of genus* 1.

***Proof*** This is a special case of Proposition 7.10. See also [2]. □

***Remark 7.12*** Let $\varphi : \mathbb{P}^1 \to \mathbb{P}^1$ be a separable simple morphism of degree 3. Then $\mathcal{E}_\varphi$ is an absolutely irreducible nonsingular curve of genus 1. Any $\mathbb{F}_q$-rational point of $\mathcal{E}_\varphi$ outside the diagonal gives a pair $(x, y)$ such that $x \neq y$ and $\varphi(x) = \varphi(y)$ and $(x, x)$ and $(y, y)$ not in $\mathcal{E}_\varphi$. Hence, there is a third point $z$, distinct from $x$ and $y$ such that $(x, z) \in \mathcal{E}_\varphi$. $\varphi(x) = \varphi(y) = \varphi(z)$. The number of $\mathbb{F}_q$-rational points of $\mathcal{E}_\varphi$ on the diagonal is at most $\deg(D_\varphi) = 4$ by by Lemma 7.6. For every $(x, x) \in \mathcal{E}_\varphi$ there exists a $y$ such that $(x, y), (y, x) \in \mathcal{E}_\varphi$. So we have to exclude for every at most 12 points from $\mathcal{E}_\varphi(\mathbb{F}_q)$. The Hasse–Weil bound [21, §5.2] gives $|\mathcal{E}_\varphi| \geq q + 1 - 2\sqrt{q}$. Therefor, if $q \geq 23$, then $|\mathcal{E}_\varphi| > 12$ and there is a triple $(x, y, z)$ of mutually distinct $\mathbb{F}_q$-rational points of $\mathbb{P}^1$ such that $\varphi(x) = \varphi(y) = \varphi(z)$.

## 8 Lines in $\mathbb{P}^3$

We start by repeating the observation of Remark 4.4.

Two chords do not intersect in a point outside $\mathcal{C}_3(q)$, as a consequence, every point (not in $\mathcal{C}_3(q)$) is contained in a unique chord.

If $p \neq 3$ then we also have the dual statement: Two axes can only be coplanar in an osculating plane, every non-osculating plane contains exactly one axis.

Let us determine the chord through $(x^3 : x^2 : x : 1)$ and $(y^3 : y^2 : y : 1)$. There are three cases: $x = y \in \mathbb{F}_q \cup \{\infty\}$ and we have a tangent, or $x \neq y$ in $\mathbb{F}_q$ and we have a real chord, or $y = \bar{x} \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ and we have an imaginary chord.

Let $n = xy$ and $t = x + y$ ('Norm' and 'Trace' in the imaginary case). An easy computation shows that the chord is

$$\begin{aligned} c(x, y) &= \langle (-nt, -n, 0, 1), (t^2 - n, t, 1, 0)) \rangle \quad \text{if} \quad x, y \neq \infty \\ c(\infty, y) &= \langle (1, 0, 0, 0), (0, y^2, y, 1) \rangle \quad \text{if} \quad y \neq \infty \\ c(\infty, \infty) &= \langle (1, 0, 0, 0), (0, 1, 0, 0) \rangle \end{aligned}$$

The chord $c(x, y)$ is a tangent, a real chord, or an imaginary chord if the polynomial $X^2 - tX + n$ is a square, reducible but not a square, or irreducible, respectively. In other words, if $t^2 - 4n$ is 0, a square, or a non-square, respectively if $q$ is odd; and $t = 0$, $\mathrm{tr}_2(n/t^2) = 0$, or $\mathrm{tr}_2(n/t^2) = 1$, respectively if $q$ is even.

We know that every point not in $\mathcal{C}_3(q)$ is on a unique chord. In particular:

$(1 : 0 : 0 : 0)$ belongs to $\mathcal{C}_3(q)$;

$(w : 1 : 0 : 0)$ belongs to $c(\infty, \infty)$;

$(w : v : 1 : 0)$ belongs to $c(x, y)$, where $x + y = v$ and $xy = v^2 - w$;

$(w : v : u : 1)$ belongs to $c(x, y)$, where $x + y = (uv - w)/(u^2 - v)$ and $xy = (uw - v^2)/(v - u^2)$ if $v \neq u^2$; and belongs to $c(\infty, u)$ if $v = u^2$.

Next, we determine the axis that is the intersection of the osculating planes $[1 : -3x : 3x^2 : -x^3]$ and $[1 : -3y : 3y^2 : -y^3]$. Again there are three cases: $x = y$ and we have a tangent, or $x \neq y \in \mathbb{F}_q$ and we have a real axis, or $y = \bar{x} \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ and we have an imaginary axis. Similarly to the previous computation, it is easy to check that

$$
\begin{aligned}
a(x, y) &= \langle(-3nt, n - t^2, 0, 3), (3n, t, 1, 0)\rangle \quad \text{if} \quad x, y \neq \infty \\
a(\infty, y) &= \langle(-3y^2, 0, 1, 0), (3y, 1, 0, 0)\rangle \quad \text{if} \quad y \neq \infty \\
a(\infty, \infty) &= \langle(1, 0, 0, 0), (0, 1, 0, 0)\rangle
\end{aligned}
$$

## 8.1 A partition of lines in $\mathbb{P}^3$

From [13] we follow the description of the different kinds of lines and refine the classification. The terminology is slightly different, it is explained in the beginning of the proof.

**Theorem 8.1** *Let $P_a = (a : 1)$ for $a \in \mathbb{F}_q$ and $P_\infty = (1 : 0)$. Let $Q_d$ be the place of degree 2 given by the irreducible polynomial $x^2 - d$, where $d \in \mathbb{F}_q^*$ is a non-square. Choose a fixed irreducible polynomial $x^2 + x + n$, that is with discriminant $1 - 4n$ being a non-square in case $q$ is odd, and $tr(n) = 1$ if $q$ is even. Let $Q$ be the place of degree 2 given by the irreducible polynomial $x^2 + x + n$.*

*The set of lines of $\mathbb{P}^3(q)$ are partitioned in the table below. The parameters $u$, $v$ and $d$ in the table are fixed and chosen such that $u$, $3v$ and $d$ are non-squares. Some classes only occur for characteristic 2 or 3 and are indicated by $\mathcal{O}_i(2)$ and $\mathcal{O}_i(3)$, respectively, and $\mathcal{O}_i'$ is not defined in characteristic 3. All classes except $\mathcal{O}_6$ form orbits under the action of $G_q$.*

*For every orbit a representative line $\mathcal{L}$, the corresponding rational function $\varphi = f(x)/g(x)$, the base divisor $B_\varphi$ of $\varphi$, and the ramification divisor $R_{\tilde{\varphi}}$ and different divisor $D_{\tilde{\varphi}}$ of the associated morphism $\tilde{\varphi}$ are given. The two vectors generating the line $\mathcal{L}$ are given in the first and second row of the corresponding class. The $f(x)$ and $R_{\tilde{\varphi}}$ are given in the first row, and $g(x)$ and $D_{\tilde{\varphi}}$ in the second row.*

*The unisecant, osculating and plane are abbreviated by unisec., oscul. and pl., respectively.*

| *Class* | *Name* | *Size* | $\mathcal{L}$ | $\varphi(x) = f(x)/g(x)$ | $B_\varphi$ | $R_{\tilde{\varphi}}$; $D_{\tilde{\varphi}}$ |
|---|---|---|---|---|---|---|
| $\mathcal{O}_1$ | *Real chords* | $\frac{1}{2}q^2 + \frac{1}{2}q$ | $(1,0,0,0)$<br>$(0,0,0,1)$ | $x^2$<br>$x$ | $P_0 + P_\infty$ | $0$<br>$0$ |
| $\mathcal{O}_1'$ | *Real axes* | $\frac{1}{2}q^2 + \frac{1}{2}q$ | $(0,1,0,0)$<br>$(0,0,1,0)$ | $x^3$<br>$1$ | $0$ | $2P_0 + 2P_\infty$<br>$2P_0 + 2P_\infty$ |
| $\mathcal{O}_2$ | *Tangents* | $q + 1$ | $(0,0,1,0)$<br>$(0,0,0,1)$ | $x^3$<br>$x^2$ | $2P_0$ | $0$<br>$0$ |
| $\mathcal{O}_3$ | *Imaginary chords* | $\frac{1}{2}q^2 - \frac{1}{2}q$ | $(n,-n,0,1)$<br>$(1-n,-1,1,0)$ | $x^3 + (n-1)x - nx$<br>$x^2 + x + n$ | $Q$ | $0$<br>$0$ |
| $\mathcal{O}_3'$ | *Imaginary axes* | $\frac{1}{2}q^2 - \frac{1}{2}q$ | $(3n,n-1,0,3)$<br>$(3n,-1,1,0)$ | $x^3 - 3nx - n$<br>$x^2 + x + \frac{1}{3}(1-n)$ | $0$ | $2Q$<br>$2Q$ |
| $\mathcal{O}_4$ | *True unisec. in oscul. pl.* | $q^2 + q$ | $(0,1,0,0)$<br>$(0,0,0,1)$ | $x^3$<br>$x$ | $P_0$ | $P_0 + P_\infty$<br>$P_0 + P_\infty$ |
| $\mathcal{O}_4^-(2)$ | *True unisec. in oscul. pl.* | $q + 1$ | $(0,1,0,0)$<br>$(0,0,0,1)$ | $x^3$<br>$x$ | $P_0$ | *Purely inseparable* |
| $\mathcal{O}_4^+(2)$ | *True unisec. in oscul. pl.* | $q^2 - 1$ | $(0,1,1,0)$<br>$(0,0,0,1)$ | $x^3$<br>$x^2 + x$ | $P_0$ | $P_0$<br>$2P_0$ |

| *Class* | *Name* | *Size* | $\mathcal{L}$ | $\varphi(x) = f(x)/g(x)$ | $B_\varphi$ | $R_{\tilde{\varphi}}$; $D_{\tilde{\varphi}}$ |
|---|---|---|---|---|---|---|
| $\mathcal{O}_5^-$ | *Unisec. not in oscul. pl.* | $\frac{1}{2}q^3 - \frac{1}{2}q$ | $(-d, 0, 1, 0)$<br>$(0, 0, 0, 1)$ | $x^3 + dx$<br>$x^2$ | $P_0$ | $Q_d$<br>$Q_d$ |
| $\mathcal{O}_5^+$ | *Unisec. not in oscul. pl.* | $\frac{1}{2}q^3 - \frac{1}{2}q$ | $(-1, 0, 1, 0)$<br>$(0, 0, 0, 1)$ | $x^3 + x$<br>$x^2$ | $P_0$ | $P_1 + P_{-1}$<br>$P_1 + P_{-1}$ |
| $\mathcal{O}_5(2)$ | *Unisec. not in oscul. pl.* | $q^3 - q$ | $(1, 0, 1, 0)$<br>$(0, 0, 0, 1)$ | $x^3 + x$<br>$x^2$ | $P_0$ | $P_1$<br>$2P_1$ |
| $\mathcal{O}_5'^-$ | *Passants in oscul. pl.* | $\frac{1}{2}q^3 - \frac{1}{2}q$ | $(0, 0, 1, 0)$<br>$(0, v, 0, 1)$ | $x^3$<br>$x^2 - v$ | 0 | $Q_{3v} + 2P_0$<br>$Q_{3v} + 2P_0$ |
| $\mathcal{O}_5'^+$ | *Passants in oscul. pl.* | $\frac{1}{2}q^3 - \frac{1}{2}q$ | $(0, 0, 1, 0)$<br>$(0, \frac{1}{3}, 0, 1)$ | $x^3$<br>$x^2 - \frac{1}{3}$ | 0 | $P_1 + P_{-1} + 2P_0$<br>$P_1 + P_{-1} + 2P_0$ |
| $\mathcal{O}_5'(2)$ | *Passants in oscul. pl.* | $q^3 - q$ | $(0, 0, 1, 0)$<br>$(0, 1, 0, 1)$ | $x^3$<br>$x^2 + 1$ | 0 | $P_1 + 2P_0$<br>$2P_1 + 2P_0$ |
| $\mathcal{O}_6$ | *Passants not in oscul. pl.* | $q^4 - q^3$<br>$-q^2 + q$ | | | 0 | *Simple* |
| $\mathcal{O}_7(3)$ | *Axis of* $\mathbf{0}_3$ | 1 | $(0, 1, 0, 0)$<br>$(0, 0, 1, 0)$ | $x^3$<br>1 | 0 | *Purely inseparable* |
| $\mathcal{O}_{8.1}^-(3)$ | *Passants meeting axis* | $\frac{1}{2}q^2 - \frac{1}{2}$ | $(0, 1, 0, 0)$<br>$(u, 0, 1, 0)$ | $x^3 - ux$<br>1 | 0 | $2P_\infty$<br>$4P_\infty$ |
| $\mathcal{O}_{8.1}^+(3)$ | *Passants meeting axis* | $\frac{1}{2}q^2 - \frac{1}{2}$ | $(0, 1, 0, 0)$<br>$(1, 0, 1, 0)$ | $x^3 - x$<br>1 | 0 | $2P_\infty$<br>$4P_\infty$ |
| $\mathcal{O}_{8.2}(3)$ | *Passants meeting axis* | $q^3 - q$ | $(1, 1, 0, 0)$<br>$(0, 0, 1, 0)$ | $x^3 - x^2$<br>1 | 0 | $P_0 + 2P_\infty$<br>$P_0 + 3P_\infty$ |

***Proof*** Everything is shown in Lemma 21.1.4 of [13], except the subdivisions of $\mathcal{O}_4$, $\mathcal{O}_5$, $\mathcal{O}_5'$ and $\mathcal{O}_8$, and the statements about the rational functions. We use the term true unisecant for non-tangent lines that intersect $\mathcal{C}_3(q)$ in exactly one point. Similarly, for external lines we also use the term passant, and such a line is called a true passant if it is not a chord.

Every representative line $\mathcal{L}$ of an orbit is given by two vectors, that is by a $2 \times 4$ matrix $L$ of rank 2. Let $H$ be the $2 \times 4$ matrix in row reduced echelon form such that $LH^T = 0$. Then the rows of $H$ give the coefficients of equations of the line $\mathcal{L}$, and the rational function $\varphi_{\mathcal{L}}$ by Proposition 6.5.

$\mathcal{O}_1$: real chords form a single orbit. A representative of a line in this orbit is given by $\mathcal{L} = c(0, \infty) = \langle (1, 0, 0, 0), (0, 0, 0, 1) \rangle$. So $H$ has rows $(0, 1, 0, 0), (0, 0, 1, 0)$. Hence, $\varphi(x) = x^2/x$, $\tilde{\varphi}(x) = x$, and $\varphi$ has base divisor $P(0) + P_\infty$, and $R_{\tilde{\varphi}} = D_{\tilde{\varphi}} = 0$.

$\mathcal{O}_1'$: real axes form a single orbit ($p \neq 3$). So it suffices to consider a particular line $\mathcal{L} = a(0, \infty) = \langle (0, 1, 0, 0), (0, 0, 1, 0) \rangle$. So $H$ has rows $(1, 0, 0, 0), (0, 0, 0, 1)$. Hence, $\varphi(x) = \tilde{\varphi}(x) = x^3$, and $R_\varphi = D_\varphi = 2P(0) + 2P_\infty$.

$\mathcal{O}_3$: imaginary chords form a single orbit with representative $\mathcal{L} = c(\xi, \bar{\xi}) = \langle (n, -n, 0, 1), (1 - n, -1, 1, 0) \rangle$, where $\xi, \bar{\xi}$ are the zeros of $X^2 + X + n$. So $H$ has rows $(1, 0, n - 1, -n), (0, 1, 1, n)$. Hence, $\varphi(x) = (x^3 + (n - 1)x - nx)/(x^2 + x + n)$ and $\tilde{\varphi}(x) = x - 1$, and $\varphi$ has base divisor $Q$, and $R_{\tilde{\varphi}} = D_{\tilde{\varphi}} = 0$.

$\mathcal{O}_3'$: imaginary axes form a single orbit ($p \neq 3$) with representative $\mathcal{L} = a(\xi, \bar{\xi}) = \langle (3n, n-1, 0, 3), (3n, -1, 1, 0) \rangle$. So $H$ has rows $(1, 0, -3n, -n), (0, 1, 1, \frac{1}{3}(1-n))$. Hence, $\varphi(x) = \tilde{\varphi}(x) = (x^3 - 3nx - n)/(x^2 + x + \frac{1}{3}(1 - n))$ and $R_\varphi = D_\varphi = 2Q$.

$\mathcal{O}_2$, $\mathcal{O}_4$ and $\mathcal{O}_5$: unisecants.

It is sufficient to look at the unisecants through $P(0) = (0 : 0 : 0 : 1)$ So, we may apply elements from the stabilizer of $P = P(0)$ in $G_q$, that is $G_{q,P}$. This subgroup consists of the matrices

$$M_{a,c} = \begin{pmatrix} a^3 & 0 & 0 & 0 \\ a^2c & a^2 & 0 & 0 \\ ac^2 & 2ac & a & 0 \\ c^3 & 3c^2 & 3c & 1 \end{pmatrix}.$$

There are three cases: $\mathcal{O}_2$ unisecants that are tangent, $\mathcal{O}_4$ unisecants in an osculating plane, and $\mathcal{O}_5$ unisecants not in an osculating plane. This is the partition in [13, Lemma 21.1.4], we are going to refine this.

The first case is that the line $\langle(0, 0, 0, 1), (0, 0, 1, 0)\rangle$ is mapped to itself. This gives:

$\mathcal{O}_2$: tangents with representative $\mathcal{L} = \langle(0, 0, 0, 1), (0, 0, 1, 0)\rangle$. These lines form a single orbit (of size $q+1$). So $H$ has rows $(1, 0, 0, 0)$, $(0, 1, 0, 0)$. Hence, $\varphi(x) = x^3/x^2$, $\tilde{\varphi}(x) = x$, and $\varphi$ has base divisor $2P(0)$, and $R_{\tilde{\varphi}} = D_{\tilde{\varphi}} = 0$.

A second type of line is $\mathcal{L} = \langle(0, 0, 0, 1), (0, 1, u, 0)\rangle$, $u \neq \infty$. This line in the osculating plane $[1 : 0 : 0 : 0]$, is mapped to $\langle(0, 0, 0, 1), (0, 1, (u + 2c)/a, 1)$ by using $M_{a,c}$.

Consider first the case that $q$ is odd. Choosing $c = -u/2$ gives:

$\mathcal{O}_4$: true unisecants in an osculating plane with $\mathcal{L} = \langle(0, 0, 0, 1), (0, 1, 0, 0)\rangle$ and this also shows that they form a single orbit of size $q(q + 1)$. So $H$ has rows $(1, 0, 0, 0)$, $(0, 0, 1, 0)$. Hence, $\varphi(x) = x^3/x$, $\tilde{\varphi}(x) = x^2$, and $\varphi$ has base divisor $P(0)$, and $R_\varphi = D_\varphi = P(0) + P_\infty$.

We continue with the case that $q$ is even. Now $\langle(0, 0, 0, 1), (0, 1, u/a, 0)\rangle$ is the image of $\mathcal{L}$ under the map $M_{a,c}$. If $u = 0$ we find the same as in the case $q$ odd. If $u \neq 0$ we get $\mathcal{L} = \langle(0, 0, 0, 1), (0, 1, 1, 0)\rangle$. This gives two orbits:

$\mathcal{O}_4^-(2)$: with representative $\mathcal{L} = \langle(0, 0, 0, 1), (0, 1, 0, 0)\rangle$. This orbit has size $q + 1$. So $H$ has rows $(1, 0, 0, 0)$, $(0, 0, 1, 0)$. Hence, $\varphi(x) = x^3/x$ has base divisor $P(0)$, and $\tilde{\varphi}(x) = x^2$ is purely inseparable.

$\mathcal{O}_4^+(2)$: with representative $\mathcal{L} = \langle(0, 0, 0, 1), (0, 1, 1, 0)\rangle$; of size $q^2 - 1$. So $H$ has rows $(1, 0, 0, 0)$, $(0, 1, 1, 0)$. Hence, $\varphi(x) = x^3/(x^2 + x)$, $\tilde{\varphi}(x) = x^2/(x + 1)$, and $\varphi$ has base divisor $P(0)$, and $R_{\tilde{\varphi}} = P(0)$, $D_{\tilde{\varphi}} = 2P(0)$.

The third type of line is $\langle(0, 0, 0, 1), (1, u, v, 0)\rangle$, corresponding essentially to:

$\mathcal{O}_5$: unisecants not in an osculating plane.

This line is mapped by $M_{a,c}$ to $\langle(0, 0, 0, 1), (1, (u + c)/a, (c^2 + 2cu + v)/a^2, 0)\rangle$ (by making the last coordinate 0) and we now take $c = -u$ and obtain $\langle(0, 0, 0, 1), (1, 0, (v - u^2)/a^2, 0)\rangle$. This gives the following two cases:

If $v = u^2$, then $\mathcal{L}$ is the secant through $P(0)$ and $P(\infty)$, so we have already seen these lines.

If $v \neq u^2$, let $w = (u^2 - v)/a^2 \neq 0$ and $d = w^{-1}$. Choosing different $a$'s does not change the quadratic character of $d$, hence we get $\mathcal{L} = \langle(0, 0, 0, 1), (-d, 0, 1, 0)\rangle$ with $d \neq 0$ being a square or a non-square if $q$ is odd, and one case if $q$ is even. Consider the two cases if $q$ is odd:

$\mathcal{O}_5^-$: $d$ is a non-square, with representative $\mathcal{L} = \langle(0, 0, 0, 1), (-d, 0, 1, 0)\rangle$. This orbit has size $\frac{1}{2}q(q^2 - 1)$. So $H$ has rows $(1, 0, d, 0)$, $(0, 1, 0, 0)$. Hence, $\varphi(x) = (x^3 + dx)/x^2$, $\tilde{\varphi}(x) = (x^2 + d)/x$, and $\varphi$ has base divisor $P(0)$, and $R_{\tilde{\varphi}} = D_{\tilde{\varphi}} = Q_d$.

$\mathcal{O}_5^+$: $d$ is a non-zero square, we can take $d = 1$ with representative $\mathcal{L} = \langle(0, 0, 0, 1), (-1, 0, 1, 0)\rangle$. This orbit has size $\frac{1}{2}q(q^2 - 1)$, too. So $\varphi(x) = (x^3 + x)/x^2$, $\tilde{\varphi}(x) = (x^2 + 1)/x$, and $\varphi$ has base divisor $P(0)$, and $R_{\tilde{\varphi}} = D_{\tilde{\varphi}} = P(1) + P(-1)$.

$\mathcal{O}_5(2)$: if $q$ is even every non-zero element is a square and we take $d = 1$ with representative $\mathcal{L} = \langle(0, 0, 0, 1), (1, 0, 1, 0)\rangle$. This orbit has size $q(q^2 - 1)$. So $\varphi(x) = (x^3 + x)/x^2$, $\tilde{\varphi}(x) = (x^2 + 1)/x$, and $\varphi$ has base divisor $P(0)$, and $R_{\tilde{\varphi}} = P(1)$ and $D_{\tilde{\varphi}} = 2P(1)$.

$\mathcal{O}_5'$: passants in an osculating plane, $p \neq 3$.

We take our favourite osculating plane $\pi = [1 : 0 : 0 : 0]$ at the point $P = (0 : 0 : 0 : 1)$. The stabilizer group $G_{q,P}$ of $P$ under $G_q$ is as before and has size $q(q - 1)$. In this plane we take our favourite external line: $\mathcal{L}_v = \langle(0, 0, 1, 0), (0, v, 0, 1)\rangle \subseteq \pi$. It is easy to check that the stabilizer of $\mathcal{L}_v$ under $G_{q,P}$ is generated by $diag(1, -1, 1, -1)$, and $\mathcal{L}_v$ and $\mathcal{L}_{a^2v}$ are in the same orbit. So the orbit of $\mathcal{L}_v$ under $G_{q,P}$ has size $q(q - 1)$ if $q$ is even and $\frac{1}{2}q(q - 1)$ if $q$ is odd. Now $H$ has rows $(1, 0, 0, 0)$, $(0, 1, 0, -v)$. Hence, $\varphi(x) = \tilde{\varphi}(x) = x^3/(x^2 - v)$, and $\varphi'(x) = x^2(x^2 - 3v)/(x^2 - v)^2$. If $q$ is odd, then $\mathcal{L}_u$ and $\mathcal{L}_v$ such that $3u$ is a non-zero square and $3v$ is a non-square are in two different orbits and together they are all external lines in $\pi$.

$\mathcal{O}_5'^-$: with $3v$ a non-square with representative $\mathcal{L} = \langle(0, 0, 1, 0), (0, v, 0, 1), \rangle$. This orbit has size $\frac{1}{2}q(q^2 - 1)$, and $R_\varphi = D_\varphi = 2P(0) + Q_{3v}$.

$\mathcal{O}_5'^+$: with $3v$ a non-zero square, we take $v = \frac{1}{3}$ with representative $\mathcal{L} = \langle(0, \frac{1}{3}, 0, 1), (0, 0, 1, 0)\rangle$. This orbit has size $\frac{1}{2}q(q^2 - 1)$, and $\varphi(x) = \tilde{\varphi}(x) = x^3/(x^2 - \frac{1}{3})$ and $R_\varphi = D_\varphi = 2P(0) + P(1) + P(-1)$.

$\mathcal{O}_5'(2)$: if $q$ is even every non-zero element is a square and we take $v = 1$ with representative $\mathcal{L} = \langle(0, 1, 0, 1), (0, 0, 1, 0)\rangle$. This orbit has size $q(q^2-1)$, and $\varphi(x) = \tilde{\varphi}(x) = x^3/(x+1)^2$, and $R_{\tilde{\varphi}} = 2P(0) + P(1)$ and $D_{\tilde{\varphi}} = 2P(0) + 2P(1)$.

$\mathcal{O}_6 = \mathcal{O}_6'$: true passants not in an osculating plane.

Let $\varphi$ be a rational function in this class. Then $\varphi$ is a morphism, since the corresponding line is a passant so it does not intersect $\mathcal{C}_3$. The ramification exponents $e_P(\varphi)$ for all places $P$ are at most 2, since the passant is not in an osculating plane by Remark 6.7. Hence, $R_\varphi$ is simple. Moreover $\varphi$ does not ramify at two distinct points in a fibre $\varphi^{-1}(Q)$ for all places $Q$ by Proposition 5.3. Hence, $\varphi$ is a simple morphism.

The morphism $\varphi : \mathbb{P}^1 \to \mathbb{P}^1$ of degree 3 gives an extension $L$ of degree 3 of $K = \mathbb{F}_q(x)$, the field of rational functions in one variable, and there exists a unique intermediate field $S$, $K \subseteq S \subseteq L$, such that $S/K$ is separable and $L/S$ is purely inseparable, see [21, Appendix 8]. If the extension degrees of $K \subseteq S \subseteq L$ are $s$ and $l$, respectively then $sl = 3$ the degree of the extension $L/K$. So either $S = L$ and $\varphi$ is separable, or $K = S$ and $L/K$ is purely inseparable and $p = 3$, so $\varphi(x) = x^3$ after a $RL$-transformation which is case $\mathcal{O}_7(3)$. Therefore, $\varphi$ is a separable simple morphism.

$\mathcal{O}_7(3)$: the axis of $\mathbf{0}_3$, $p = 3$ with $\mathcal{L} = \langle(0, 1, 0, 0), (0, 0, 1, 0)\rangle$. So $H$ has rows $(1, 0, 0, 0)$, $(0, 0, 0, 1)$. Hence, $\varphi(x) = \tilde{\varphi}(x) = x^3$ and $\varphi$ is purely inseparable.

$\mathcal{O}_8(3)$: passants meeting the axis, $p = 3$.

Every plane containing the axis is an osculating plane. So every line meeting the axis is in an osculating plane. We may take as osculating plane $\pi(\infty) = [0 : 0 : 0 : 1]$, that is given by $X_3 = 0$. Let $\mathcal{L}$ be a passant contained in $\pi(\infty)$ meeting the axis given by $X_0 = X_3 = 0$

at the point $P = (0 : u : v : 0)$. All $\varphi$ in $G_q$ leave the axis invariant. If $\varphi \in G_q$ leaves $\pi(\infty)$ invariant, then it fixes also $P(\infty)$. So $\varphi(x) = ax + b$, that is with $c = 0$ and $d = 1$, and $\varphi$ leaves $c(\infty, \infty)$, that is the tangent line of $\pi(\infty)$ given by $X_2 = X_3 = 0$ invariant. Hence, $\varphi$ leaves the intersection of the axis and $c(\infty, \infty)$ invariant. So it leaves $P_1 = (0 : 1 : 0 : 0)$ invariant. Indeed $\varphi(0 : u : v : 0) = (0 : au - bv : v : 0)$. So $\varphi(P_1) = P_1$, and for all $v \neq 0$ there exists a $\varphi$ with $a = 1$ and $b = u/v$ such that $\varphi(0 : u : v : 0) = P_2 = (0 : 0 : 1 : 0)$. Therefore, we may assume that the passant meets the axis in $P_1$ or $P_2$. This gives two cases:

Passants in $\pi(\infty)$ through $P_1$ are given by $\mathcal{L}_{1,u} = \langle((0, 1, 0, 0), (u, 0, 1, 0), \rangle$ with $u \neq 0$. The transformation $\varphi(x) = ax$ with $a = 1/u$ maps $\mathcal{L}_{1,u}$ to $\mathcal{L}_{1,a^2u}$ which gives two orbits, since $q$ is odd:

$\mathcal{O}_{8.1}(3)^-$: $u$ a non-square with representative $\mathcal{L} = \langle(0, 1, 0, 0), (u, 0, 1, 0), \rangle$. This orbit has size $\frac{1}{2}(q + 1)(q - 1)$. So $H$ has rows $(1, 0, -u, 0), (0, 0, 0, 1)$. Hence, $\varphi(x) = \tilde{\varphi}(x) = x^3 - ux$ and $R_\varphi = 2P(\infty)$, $D_\varphi = 4P(\infty)$.

$\mathcal{O}_{8.1}(3)^+$: $u$ a non-zero square, we can take $u = 1$ with representative $\mathcal{L} = \langle(0, 1, 0, 0), (1, 0, 1, 0), \rangle$. This orbit has size $\frac{1}{2}(q + 1)(q - 1)$.

Passants in $\pi(\infty)$ through $P_2$ are given by $\mathcal{L}_{2,v}\langle(0, 0, 1, 0), (v, 1, 0, 0)\rangle$ with $v \neq 0$. The transformation $\varphi(x) = ax$ maps $\mathcal{L}_{2,v}$ to $\mathcal{L}_{2,av}$ which gives one orbit:

$\mathcal{O}_{8.2}(3)$: with representative $\mathcal{L} = \langle(0, 0, 1, 0), (1, 1, 0, 0)\rangle$. This orbit has size $(q+1)(q^2-q)$. So $H$ has rows $(1, -1, -0, 0), (0, 0, 0, 1)$. Hence, $\varphi(x) = \tilde{\varphi}(x) = x^3 - x^2$ and $R_\varphi = P(0) + 2P(\infty)$, $D_\varphi = P(0) + 3P(\infty)$. □

***Remark 8.2*** $|\mathcal{O}_6| = q(q - 1)(q^2 - 1)$ and $|G_q| = q(q - 1)(q + 1)$. Hence, $\mathcal{O}_6$ is subdivided in at least $q - 1$ orbits. Without proof we state that if $p \neq 2$ and $p \neq 3$, then $\mathcal{O}_6$ is subdivided in 5 subclasses with different divisors $P_1 + P_2 + P_3 + P_4$, $P_1 + P_2 + Q$, $Q_1 + Q_2$, $P + R$ and $S$, where the $P_i$ and $P$ are places of degree 1, the $Q_i$ and $Q$ are places of degree 2, and $R$ and $S$ are places of degree 3 and 4, respectively. Moreover we conjecture that the cross-ratio of the 4 points over $\bar{\mathbb{F}}_q$ of the different divisor determines the orbit.

***Remark 8.3*** The partition of classes in Theorem 8.1 is a refinement of the one given in [3, 13]. In characteristic 2 the classs $\mathcal{O}_4$ is subdivided in $\mathcal{O}_4(2)^+$ and $\mathcal{O}_4(2)^-$, in odd characteristic $\mathcal{O}_5$ is subdivided in $\mathcal{O}_5^+$ and $\mathcal{O}_5^-$, and $\mathcal{O}_5'$ is subdivided in $\mathcal{O}_5'^+$ and $\mathcal{O}_5'^-$, and in characteristic 3 the class $\mathcal{O}_8$ is subdivided in $\mathcal{O}_{8.1}(3)^+$, $\mathcal{O}_{8.1}(3)^-$ and $\mathcal{O}_{8.2}(3)$.

All classes of Theorem 8.1, except $\mathcal{O}_6$ form orbits under the action of $G_q$, and they are also obtained in [5, Theorem 3.1] and cited also in [4, Theorem 2.3]. Our classification is in agreement with the results of [5].

### 8.2 The determination of $\mu_q$

In the table of the following proposition ($q \geq 23$) rows indicate the classes of lines and column headers indicate $q$ mod 6.

**Proposition 8.4** *Let $q \geq 23$. Then the entries in the following table indicate whether a case contributes to $\mu_q$ by a plus sign, and by a minus sign otherwise.*

| *Class* | *Size* | 1(6) | 2(6) | 3(6) | 4(6) | 5(6) |
|---|---|---|---|---|---|---|
| $\mathcal{O}_1$ | $\frac{1}{2}q^2+\frac{1}{2}q$ | − | − | − | − | − |
| $\mathcal{O}_1'$ | $\frac{1}{2}q^2+\frac{1}{2}q$ | + | − | | + | − |
| $\mathcal{O}_2$ | $q+1$ | − | − | − | − | − |
| $\mathcal{O}_3$ | $\frac{1}{2}q^2-\frac{1}{2}q$ | − | − | − | − | − |
| $\mathcal{O}_3'$ | $\frac{1}{2}q^2-\frac{1}{2}q$ | − | + | | − | + |
| $\mathcal{O}_4$ | $q^2+q$ | + | | + | | + |
| $\mathcal{O}_4^-(2)$ | $q+1$ | | − | | − | |
| $\mathcal{O}_4^+(2)$ | $q^2-1$ | | + | | + | |
| $\mathcal{O}_5$ | $q^3-q$ | + | + | + | + | + |
| $\mathcal{O}_5'$ | $q^3-q$ | + | + | | + | + |
| $\mathcal{O}_6$ | $q^4-q^3-q^2+q$ | + | + | + | + | + |
| $\mathcal{O}_7(3)$ | 1 | | | − | | |
| $\mathcal{O}_{8.1}^-(3)$ | $\frac{1}{2}q^2-\frac{1}{2}$ | | | − | | |
| $\mathcal{O}_{8.1}^+(3)$ | $\frac{1}{2}q^2-\frac{1}{2}$ | | | + | | |
| $\mathcal{O}_{8.2}(3)$ | $q^3-q$ | | | + | | |

***Proof*** The partition of Proposition 8.1 is used. Here the different cases are considered by increasing degree of $\tilde{\varphi}$.

(1) If $\deg(\tilde{\varphi})=1$, then the base divisor has degree 2 and $\mathcal{L}$ is a chord or a tangent: $\mathcal{O}_1$, $\mathcal{O}_2$ or $\mathcal{O}_3$.

$\mathcal{O}_1$: Real chords are in 3-planes, but do not contribute to $\mu_q$, since the points on these lines contribute already to $a_1(T)$ or $a_2(T)$.

$\mathcal{O}_2=\mathcal{O}_2'$: A plane that contains a tangent line at $P$ of $\mathcal{C}_3(q)$, intersects $\mathcal{C}_3$ in the divisor $2P+P'$ where $P'$ is another point of $\mathcal{C}_3(q)$. Hence, tangent lines are not contained in a 3-plane.

$\mathcal{O}_3$: A plane that contains an imaginary chord at $Q$, intersects $\mathcal{C}_3$ in the divisor $Q+P$ where $P$ is a point of $\mathcal{C}_3(q)$ and $Q$ a place of degree 2. Hence, imaginary chords are not contained in a 3-plane.

(2) If $\deg(\tilde{\varphi})=2$, then the base divisor is a place $P_1$ of degree 1 and $\mathcal{L}$ is a unisecant: $\mathcal{O}_4$ or $\mathcal{O}_5$.

$\mathcal{O}_4^-(2)$: In this case $\tilde{\varphi}$ is purely separable and $\tilde{\varphi}^{-1}(x)$ consists of one point, for all $x$. Hence, there are *no* 3-planes containing $\mathcal{L}$.

In all other subcases of $\mathcal{O}_4$ or $\mathcal{O}_5$ the morphism $\tilde{\varphi}$ is separable by Propositions 8.1 and 6.9. Hence, there is an $\mathbb{F}_q$-rational point $x$ on $\mathbb{P}^1$ such that $\tilde{\varphi}^{-1}(x)$ consists of two $\mathbb{F}_q$-rational points $P_2(x)$ and $P_3(x)$ which are distinct from $P_1$ by Proposition 6.13. So apart from $P_1$, that is in all planes containing $\mathcal{L}$, there is a 3-plane that contains $P_1$, $P_2(x)$ and $P_3(x)$.

(3) If $\deg(\tilde{\varphi})=3$, then $\varphi=\tilde{\varphi})$ has no base points and $\mathcal{L}$ is an axis or a passant. These are the remaining cases of Proposition 8.1.

$\mathcal{O}_1'$: real axes with representative rational function $\varphi(x)=x^3$ and corresponding line $\mathcal{L}$. So $\Delta_\varphi(x,y)=x^2+xy+y^2$

If $q=1 \bmod 3$, then the double point scheme $\mathcal{E}_\varphi$ contains $(x,\omega x)$ and $(x,\omega^2 x)$ with $\omega^3=1$ and $\omega\neq 1$. Hence, there is a 3-plane containing $\mathcal{L}$ and the three points $P(x)$, $P(\omega x)$ and $P(\bar{\omega}x)$ if $x\neq 0$ and $x\neq\infty$. So we get a contribution to $\mu_q$. Furthermore, $\mathcal{E}_\varphi$ is reducible over $\mathbb{F}_q$ containing two components of bidegree $(1,1)$ that intersect in $(0,0)$ and $(\infty,\infty)$. If $q=-1 \bmod 3$, then $\mathcal{E}_\varphi$ has no $\mathbb{F}_q$-rational points except $(0,0)$ and $(\infty,\infty)$ and there is no contribution to $\mu_q$. $\mathcal{E}_\mathcal{L}$ is irreducible over $\mathbb{F}_q$, but reducible over $\mathbb{F}_{q^2}$ with two components that are conjugate and intersect in $(0,0)$ and $(\infty,\infty)$.

$\mathcal{O}_3'$: Imaginary axes, $p \neq 3$, with representative rational function $\varphi(x) = (x^3 - 3nx - n)/(x^2 + x + \frac{1}{3}(1-n))$ and corresponding line $\mathcal{L}$. where $x^2 + x + n$ is irreducible, that is the discriminant $1 - 4n$ is a non-square if $q$ is odd, and $tr(n) = 1$ if $q$ is even. Then

$$\Delta_\varphi(x, y) = x^2y^2 + xy(x + y) + \tfrac{1}{3}(1 - n)(x^2 + xy + y^2) + 3xy + n(x + y) + n^2.$$

Let $\xi$ and $\bar{\xi}$ be the roots of $x^2 + x + n$. Consider the line $\mathcal{L}$ and the point $P(x)$ on $\mathcal{C}_3(q)$. Under the null-polarity $\mathcal{L}$ and $P(x)$ are mapped to $\mathcal{L}'$ and $P'(x)$, respectively, where $\mathcal{L}'$ is an imaginary chord of $\mathbf{0}_3$. So $\mathcal{L}'$ intersects $\mathbf{0}_3$ in the conjugate points $P'(\xi)$ and $P'(\bar{\xi})$. There exists a fractional transformation $\varphi \in G_{q^2}$, that is with coefficients in $\mathbb{F}_{q^2}$ such that $\varphi(\xi) = \xi$, $\varphi(\bar{\xi}) = \bar{\xi}$ and $\varphi(x) = 0$. Then $\bar{\varphi}(x) = 0$, $\bar{\varphi}(\bar{\xi})$ is the conjugate of $\varphi(\xi)$ which is $\bar{\xi}$, and similarly $\bar{\varphi}(\xi) = \xi$. So $\bar{\varphi} = \varphi$, since $G_{q^2}$ acts sharply 3-transitive on $\mathbb{P}^1(q^2)$. Hence, $\varphi \in G_q$ and we assume without loss of generality that $x = 0$.

Now $\Delta_\varphi(0, y) = \frac{1}{3}(1 - n)y^2 + ny + n^2$. This quadratic polynomial has discriminant $-3(1 - 4n)n^2/9$. If $q$ is odd there are two distinct solutions if $-3$ is a non-square, since $1 - 4n$ is a non-square. So there is 3-plane containing $\mathcal{L}$ if $q \equiv 2 \mod 3$, and there is no such 3-plane if $q \equiv 1 \mod 3$. If $q$ is even, the quadratic equation becomes $y^2+y+n+1 = 0$, and we find a 3-plane for some $y$ if the trace of $ac/b^2$ is 0, where $a = 1, b = 1$ and $c = n+1$. So $tr(n + 1) = 0$. Hence, $tr(1) = 1$, since $tr(n) = 1$. This again is the case if and only if $q \equiv 2 \mod 3$.

$\mathcal{O}_5'$: Passants in an osculating plane, $p \neq 3$, with representative rational function $= x^3/(x^2 - v)$ and corresponding line $\mathcal{L}$. Then

$$\Delta_\varphi(x, y) = x^2y^2 - v(x^2 + xy + y^2).$$

We first consider the case that $q$ is odd. The discriminant of $\Delta_\varphi(x, y)$ as polynomial in $y$ is $vx^2(4x^2 - 3v)$. This discriminant is a square if and only if $4vx^2 - 3v^2 - u^2 = 0$ has a $\mathbb{F}_q$-rational solution $(x, u)$. The projective curve with equation $4vx^2 - 3v^2z^2 - u^2 = 0$ in the variables $x, u$ and $z$ with parameter $v$ defines a nonsingular conic with $q + 1$ $\mathbb{F}_q$-rational points, with at most 2 points where $z = 0$, at most 2 points for which $u = 0$, at most 2 points leading to a solution $x = y$. So for $q > 6$ there is an $x \in \mathbb{F}_q$ such that the discriminant is a non-zero square giving two solutions of $\Delta_\varphi(x, y) = 0$ in $y$ which are distinct from $x$. So there is a 3-plane that contain the line $\mathcal{L}$.

$\mathcal{O}_5'(2)$: is the subclass of $\mathcal{O}_5'$ with $q$ even. In this case $v$ is a square and we can take $v = 1$. We want $\mathrm{tr}(ac/b^2) = 0$ with $a = x^2 + 1$, $b = x$ and $c = x^2$, so $\mathrm{tr}(x^2 + 1) = 0$. Now the map $x \mapsto x^2 + 1$ is a bijection, so it has trace 0 for $\frac{1}{2}q$ values of $x$. So we get a contribution to $\mu_q$ and the number of 3-planes containing $\mathcal{L}_1$ is $1 + \frac{1}{2}q$.

Hence, in all subcases of $\mathcal{O}_5'$ we get a contribution to $\mu_q$.

$\mathcal{O}_6 = \mathcal{O}_6'$: true passants not in an osculating plane. Let $\mathcal{L}$ be a line in this class. The corresponding rational function $\varphi$ is separable and simple by Proposition 8.1. Hence, $\mathcal{E}_\varphi$ is a curve of genus 1 by Corollary 7.11. Furthermore, for $q \geq 23$ there exist three mutually distinct elements $x, y, z$ in $\mathbb{P}^1(q)$ such that $\varphi(x) = \varphi(y) = \varphi(z)$ by Remark 7.12. Hence, $P(x)$, $P(y)$ and $P(z)$ determine a 3-plane containing $\mathcal{L}$.

$\mathcal{O}_7(3)$: The axis of $\mathbf{0}_3$, $p = 3$. The pencil of planes containing the axis consists of all osculating planes. Hence, the axis does not lie on a 3-plane.

$\mathcal{O}_8(3)$: Passants meeting the axis, $p = 3$. This class has three orbits:

$\mathcal{O}_{8.1}(3)$: The representative rational function is $\varphi(x) = x^3 - ux$ with corresponding line $\mathcal{L}$. Then $\Delta_\varphi(x, y) = x^2 + xy + y^2 - u$ and $\Delta_\varphi(x, y) = 3x^2 - u = -u \neq 0$, since $p = 3$. The discriminant of $\Delta_\varphi(x, y)$ as polynomial in $y$ is $x^2 - 4(x^2 - u) = u$.

$\mathcal{O}_{8.1}(3)^-$: This is the subcase with $u$ a non-square. Hence, $\Delta_\varphi(x, y) = 0$ has no solutions in $y$ for all $x$. The point $x = \infty$ corresponds with a plane tangent to $\mathcal{C}_3$ at $P(\infty)$, which is not a 3-plane. Hence, there are no 3-planes containing $\mathcal{L}$.

$\mathcal{O}_{8.1}(3)^+$: This is the subcase with $u = 1$ a non-zero square. Then the discriminant is 1. Hence, there are two solutions $y = x \pm 1$ which are distinct from $x$. Therefore, there are 3-planes containing $\mathcal{L}$.

$\mathcal{O}_{8.2}(3)$: The representative rational function is $\varphi(x) = x^3 - x^2$ with corresponding line $\mathcal{L}$. Then $\Delta_\varphi(x, y) = x^2 + xy + y^2 - x - y$ and $\Delta_\varphi(x, x) = 3x^2 - 2x = x$, since $p = 3$. So, if $\Delta_\varphi(x, x) = 0$, then $x = 0$. The discriminant of $\Delta_\mathcal{L}(x, y)$ as polynomial in $y$ is $(x - 1)^2 - 4(x^2 - x) = 1 - x$ must be a non-zero-square. If $q > 3$, then there is a $x \in \mathbb{F}_q \setminus \{0, 1\}$ such that $1 - x$ is a non-zero square, and $\Delta_\varphi(x, y) = 0$ has two solutions in $y$ not equal to $x$. Hence, there is a 3-plane containing $\mathcal{L}$. □

***Remark 8.5*** Theorem 8.4 was enough to solve our problem, that is to know wether a line of a given class is contained in a 3-plane or not. In [4, Theorem 3.3] a more detailed result is given:

(a) For all classes of lines, including $\mathcal{O}_6$, the exact number is computed of lines of a given class that are contained in a plane of a given class.
(b) For all classes of lines, apart from $\mathcal{O}_6$, the exact number is computed of planes of a given class through a line of a given class.
(c) For the lines of $\mathcal{O}_6$, the average number is computed of planes of a given class through a line of $\mathcal{O}_6$.

So in fact for all cases, apart from $\mathcal{O}_6$ we could have referred to [4, Theorem 3.3] instead.

***Remark 8.6*** The permutation rational functions of degree 3 are classified in [8]. There are 6 of them and they confirm the findings in the table of Proposition 8.4: $\mathcal{O}_3'$ for $q \equiv 1 \mod 6$, $\mathcal{O}_1'$ for $q \equiv 2 \mod 6$, $\mathcal{O}_7(3)$ and $\mathcal{O}_{8.1}(3)^-$ for $q \equiv 3 \mod 6$, $\mathcal{O}_3'$ for $q \equiv 4 \mod 6$, and $\mathcal{O}_1'$ for $q \equiv 5 \mod 6$.

We summarize our findings in the following.

**Theorem 8.7** *If $q \geq 23$, then*

$$\mu_q = \begin{cases} q^4 + q^3 + \frac{1}{2}q^2 + \frac{1}{2}q & \text{if } q = 1 \mod 6 \\ q^4 + q^3 + \frac{1}{2}q^2 - \frac{3}{2}q - 1 & \text{if } q = 2 \mod 6 \\ q^4 + q^3 + \frac{1}{2}q^2 - \frac{1}{2} & \text{if } q = 3 \mod 6 \\ q^4 + q^3 + \frac{1}{2}q^2 - \frac{1}{2}q - 1 & \text{if } q = 4 \mod 6 \\ q^4 + q^3 + \frac{1}{2}q^2 - \frac{1}{2}q & \text{if } q = 5 \mod 6 \end{cases}$$

***Proof*** This follows from Proposition 8.4 by adding up the sizes of the corresponding entries in the second column if there is a plus sign in the corresponding row and column of $i \mod 6$. □

## 9 Conclusion

The extended coset leader weight enumerator of the generalized Reed–Solomon $[q + 1, q - 3, 5]_q$ code is computed for $q \geq 23$. For this we need to refine the known classification [3, 13] of the points, lines and planes in the projective three space under the action of projectivities

that leave the twisted cubic invariant. The given classification is complete except for the class $\mathcal{O}_6$ of true passants not in an osculating plane. The refined classification and the line-plane incidence, apart from $\mathcal{O}_6$ are also obtained in [4, 5, 10].

The relation between codimension 2 subspaces of $\mathbb{P}^r$ and rational functions of degree at most $r$ is given.

Furthermore, the double point scheme $\mathcal{E}_\varphi$ of a rational function $\varphi$ is studied in general. If the rational function $\varphi$ is a separable simple morphism of degree $d$, then $\mathcal{E}_\varphi$ is an absolutely irreducible curve of genus $(d-1)^2$. In particular, the pencil of a true passant of the twisted cubic, not in an osculating plane gives a curve of genus 1 as double point scheme.

In order to compute the (extended) list weight enumerator [17] of this code is beyond the scope of this article, since one needed to know the distribution of the numbers of $\mathbb{F}_q$-rational points of the double point schemes of all the passants not in an osculating plane.

**Acknowledgements** We found out that the main result of the classification of Theorem 8.1 on lines in three space over finite fields and Proposition 8.4 on the line-plane incidence, with the exception $\mathcal{O}_6$ was also obtained in recent papers by [4, 5] that were submitted one week earlier on arXiv than this paper. We thank the authors for showing us their work. The third author was partly supported by Grant K 124950 of the Hungarian National Research, Development and Innovation Fund. In his case, also the "Application Domain Specific Highly Reliable IT Solutions" project has been implemented with the support provided from the National Research, Development and Innovation Fund of Hungary, financed under the Thematic Excellence Programme TKP2020-NKA-06 (National Challenges Subprogramme) funding scheme.



## References

1. Bartoli D., Davydov A.A., Marcugini S., Pambianco F.: On planes through points off the twisted cubic in PG(3, $q$) and multiple covering codes. Finite Fields Appl. **67**, 101710 (2020).
2. Bos H.J.M., Kers C., Oort F., Raven D.W.: Poncelet's closure theorem. Expo. Math. **5**(4), 289–364 (1987).
3. Bruen A.A., Hirschfeld J.W.P.: Applications of line geometry over finite fields. I. The twisted cubic. Geom. Dedicata **6**(4), 495–509 (1977).
4. Davydov A.A., Marcugini S., Pambianco F.: Twisted cubic and plane-line incidence matrix in PG(3, q). Des. Codes Cryptogr. **89**(10), 2211–2233 (2021).
5. Davydov A.A., Marcugini S., Pambianco F.: Twisted cubic and orbits of lines in PG(3, q). arXiv:2103.12655 (2021).
6. Eisenbud D., Harris J.: The Geometry of Schemes, vol. 197. Graduate Texts in Mathematics. Springer, New York (2000).
7. Eremenko A., Gabrielov A.: Rational functions with real critical points and the B. and M. Shapiro conjecture in real enumerative geometry. Ann. Math. (2) **155**(1), 105–129 (2002).
8. Ferraguti A., Micheli G.: Full classification of permutation rational functions and complete rational functions of degree three over finite fields. Des. Codes Cryptogr. **88**(5), 867–886 (2020).
9. Goldberg L.R.: Catalan numbers and branched coverings by the Riemann sphere. Adv. Math. **85**(2), 129–144 (1991).
10. Gülizar G., Lavrauw M.: On pencils of cubics on the projective line over finite fields of characteristic $\mathbb{F}_{q^3}$. Finite Fields Appl. **78** 101960, 28 (2022).
11. Hartshorne R.: Algebraic Geometry. Graduate Texts in Mathematics, vol. 52. Springer, New York (1977).
12. Helleseth T.: The weight distribution of the coset leaders for some classes of codes with related parity-check matrices. Discret. Math. **28**(2), 161–171 (1979).

13. Hirschfeld J.W.P.: Finite Projective Spaces of Three Dimensions. Oxford Mathematical Monographs. The Clarendon Press, Oxford University Press, Oxford Science Publications, New York (1985).
14. Hirschfeld J.W.P., Korchmáros G., Torres F.: Algebraic Curves over a Finite Field. Princeton Series in Applied Mathematics. Princeton University Press, Princeton (2008).
15. Hou X.-D., Sze C.: On a type of permutation rational functions over finite fields. Finite Fields Appl. **68**, 101758, 9 (2020).
16. Jurrius R., Pellikaan R.: Codes, arrangements and matroids. In: Algebraic Geometry Modeling in Information Theory, volume 8 of Ser. Coding Theory Cryptol., pp. 219–325. World Sci. Publ., Hackensack (2013).
17. Jurrius R., Pellikaan R.: The coset leader and list weight enumerator. In: Topics in Finite Fields, volume 632 of Contemp. Math., pp. 229–251. Amer. Math. Soc., Providence, RI (2015).
18. Jurrius R.P.M.J.: Codes, arrangements, matroids, and their polynomial links. PhD thesis, Technical University Eindhoven (2012).
19. Pellikaan R., Wu X.-W., Bulygin S., Jurrius R.: Codes, Cryptology and Curves with Computer Algebra. Cambridge University Press, Cambridge (2018).
20. Shafarevich I.R.: Basic Algebraic Geometry. Springer, New York (1974). Translated from the Russian by K. A. Hirsch, Die Grundlehren der mathematischen Wissenschaften, Band 213.
21. Stichtenoth H.: Algebraic Function Fields and Codes. Universitext. Springer, Berlin (1993).