GEOMETRIC AND COMBINATORIAL ASPECTS OF NORMAL RATIONAL CURVES IN $\mathrm{PG}(2,Q)$ AND $\mathrm{PG}(3,Q)$

by
GÜLİZAR GÜNAY

Submitted to the Graduate School of Engineering and Natural Sciences
in partial fulfilment of
the requirements for the degree of Doctor of Philosophy

Sabancı University
July 2021

GEOMETRIC AND COMBINATORIAL ASPECTS OF NORMAL RATIONAL CURVES IN $\mathrm{PG}(2,Q)$ **AND** $\mathrm{PG}(3,Q)$

Approved by:

Prof. Dr. Michel Lavrauw .....
(Dissertation Supervisor)

Prof. Dr. Cem Güneri .....

Prof. Dr. Erkay Savaş .....

Assoc. Prof. Dr. Simeon Ball .....

Asst. Prof. Dr. Morgan Rodgers .....

Date of Approval: July 13, 2021

ABSTRACT

GEOMETRIC AND COMBINATORIAL ASPECTS OF NORMAL RATIONAL CURVES IN PG$(2,Q)$ AND PG$(3,Q)$

GÜLİZAR GÜNAY

MATHEMATICS Ph.D DISSERTATION, JULY 2021

Dissertation Supervisor: Prof. Dr. Michel Lavrauw

Keywords: arc, projective plane, pencil of cubics, twisted cubic, line orbit

In this thesis, firstly, we study the small complete arcs in PG$(2,q)$, for q odd, with at least $(q+1)/2$ points on a conic. We give a short comprehensive proof of the completeness problem left open by Segre in his seminal work (Segre, 1962) using algebraic curves. This also gives an alternative to Pellegrino's long proof published in a series of works in 1980s. As a corollary of our proof, we obtain example of arcs which give counterexamples to the statement in (Hirschfeld, 1993). This concerns the existence of a line satisfying the hypothesis for the main theorem from (Pellegrino, 1993a) in which Pellegrino studied the complete arcs sharing (any) $(q+1)/2$ points with a conic but with an extra assumption.

Secondly, we study combinatorial invariants of the equivalence classes of pencils of cubics on PG$(1,q)$, for q odd and q not divisible by 3. These equivalence classes are considered as orbits of lines in PG$(3,q)$, under the action of the stabiliser group of the twisted cubic $\mathcal{C}_3$. In particular we determine the point orbit distribution and plane orbit distributions of all lines which, are contained in an osculating plane of $\mathcal{C}_3$, have non-empty intersection with $\mathcal{C}_3$, or are imaginary chords, or axes.

ÖZET

PG$(2,Q)$ VE PG$(3,Q)$'DE NORMAL RASYONEL EĞRİLERİN GEOMETRİK VE KOMBİNATÖREL YÖNLERİ

GÜLİZAR GÜNAY

MATEMATIK DOKTORA TEZİ, TEMMUZ 2021

Tez Danışmanı: Prof. Dr. Michel Lavrauw

Anahtar Kelimeler: yay, projektif düzlem, kübik kalemleri, bükülmüş kübik, doğru yörüngesi

Bu tezde, ilk olarak, bir konik üzerinde en az $(q+1)/2$ nokta ile q tek için PG$(2,q)$ içindeki küçük tam yayları inceliyoruz. Segre'nin çığır açan çalışmasında (Segre, 1962) açık bıraktığı tamlık probleminin cebirsel eğrileri kullanarak, kısa ve kapsamlı bir kanıtını veriyoruz. Bu, Pellegrino'nun 1980'ler deki makale serisinde elde edilen uzun kanıtına bir alternatif sunar. Kanıtımızın bir sonucu olarak, (Hirschfeld, 1993)'daki ifadeye karşıt örnekler veren yay örnekleri elde ediyoruz. Bu, Pellegrino'nun konik ile (herhangi) $(q+1)/2$ tane nokta kapsayan, ancak fazladan bir varsayımla tam yayları incelediği (Pellegrino, 1993a) deki ana teoremi için hipotezi karşılayan bir çizginin varlığıyla ilgilidir.

İkinci olarak, PG$(1,q)$ üzerinde, q tek ve 3 ile bölünemez için kübik kalemlerin denklik sınıflarının kombinatoryal değişmezlerini inceliyoruz. Bu denklik sınıfları, bükülmüş kübik $\mathcal{C}_3$'ın dengeleyici grubunun etkisi altında PG$(3,q)$ içindeki doğruların yörüngeleri olarak kabul edilir. Özellikle, $\mathcal{C}_3$ osilasyon düzleminde yer alan, $\mathcal{C}_3$ ile kesişimi, boş olmayan, veya sanal kirişler veya eksenler olan tüm çizgilerin nokta yörünge dağılımını ve düzlem yörünge dağılımlarını belirleriz.

ACKNOWLEDGEMENTS

I would like to thank my supervisor Prof. Dr. Michel Lavrauw for all his guidance, support, and patience throughout my thesis. I appreciate very much for his suggestions, detailed reviews, patience on reading my multiple drafts and valuable advices. It was a great opportunity to study Finite Geometry with his leadership.

I want to thank my friends; Başak Aslı Çankaya and Leyla Akmeşe for being there whenever I needed them and making distances close, Emine Tuğba Yesin and Melike Efe for reminding me I am not alone in the academy and that we have common problems and for being with me the whole process, and many others for their valuable friendship. I would like to thank Tekgül Kalaycı for her friendship and for making me come to Sabancı University because I met my husband here.

Deepest gratitude to my husband Ahmet and to my mother, father, and sister. This thesis dedicated with love to them for their unconditional support and beliefs. It was incredible to meet Ahmet and fall in love with him during my PhD. Throughout my entire PhD, he has always been incredibly understanding towards me and he has always shown his faith in me. I am grateful to him for all he has done.

Finally, I would like to acknowledge Sabancı University and Scientific and Technological Research Council of Turkey (TÜBİTAK) for supporting me with scholarships throughout my studies. This thesis is supported by TÜBİTAK under the contract 118F159.

To my lovely husband Ahmet

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1. INTRODUCTION

In this thesis, we are concerned with the completion of planar arcs in $\mathrm{PG}(2,q)$ containing $(q+1)/2$ points from a conic, for q odd, and classification of lines in $\mathrm{PG}(3,q)$ under the action of a stabiliser of the twisted cubic, for $3 \nmid q$. We combine the results of two papers (Günay & Lavrauw, 2021) and (Günay & Lavrauw, 2021) in this thesis.

Historically, arcs are well-known and they have been studied from the mid-twentieth century. Let K be a k-arc in $\mathrm{PG}(2,q)$. In 1947, Bose showed that if q is odd and $q \geq 3$, then $k \leq q+1$; if q is even, then $k \leq q+2$.

In 1950s Beniamino Segre first proposed important questions about arcs as follows:

1.1 For given n and q, what is the maximum value of k such that k-arc exists in $\mathrm{PG}(n,q)$?

1.2 Are there values of n and q with $q > n+1$ such that every $(q+1)$-arc of $\mathrm{PG}(n,q)$ is a normal rational curve?

1.3 What are the values of k for which a complete k-arc exists in $\mathrm{PG}(n,q)$?

In 1952, Bush showed that an arc in $\mathrm{PG}(n-1,q)$, for q odd and $n \geq q+1$, has size at most $n+1$. An arc attaining this bound is equivalent to a frame of $\mathrm{PG}(n-1,q)$. In 1955, Segre classified $(q+1)$–arcs as conics in $\mathrm{PG}(2,q)$ for q odd. After this classification, Segre's initial studies on arcs naturally led to the following questions:

2.1 What are the possible sizes of complete arcs in $\mathrm{PG}(2,q)$?

2.2 How many points can a conic have in common with a complete arc which is not a conic?

These questions have been extensively studied and many mathematicians have contributed to the large variety of constructions of complete arcs. For a survey of answers to Segre's questions see (Hirschfeld & Storme, 2001), (Hirschfeld, Korchmáros & Torres, 2013)(Chapter 13), (Ball, 2012), and (Ball & De Beule, 2012). There

is a relationship between arcs and certain algebraic curves in $\mathrm{PG}(n,q)$. Therefore, in many arc constructions, a large portion of the points of the arc is chosen among the points of a conic or a cubic curve, following up on ideas from (Segre, 1962) and (Lombardo-Radice, 1956). Many bounds have been found from arcs to algebraic curves and algebraic hypersurfaces; see (Hirschfeld, 1998), (Hirschfeld & Thas, 1991), (Thas, 1968), and Bruen et al. (Bruen, Thas & Blokhuis, 1988).

Let $\mathrm{C} \in \mathbb{F}_q^n$ be a linear $[n,k,d]$ code. A linear code C is called *maximum distance separable* (MDS)-code if C meets the Singleton bound. For $k \geq 3$, it is well known that arcs are equivalent to MDS-codes and there is a vast literature on this subject (see (Hirschfeld, James William Peter & Hirschfeld, 1979), (Hirschfeld, 1998), (Hirschfeld et al., 2013), and (Segre, 1959)).

Now, let us look at our problem. In this thesis, we study small complete arcs in $\mathrm{PG}(2,q)$, for q odd, with at least $(q+1)/2$ points on a conic. One of the first such constructions for q odd, suggested by Segre, gives rise to arcs containing roughly half of the points of a conic. The construction starts from a conic $\mathcal{C}_2$ and one point R outside $\mathcal{C}_2$. Depending on whether R is external (on two tangents) or internal (on no tangents) to $\mathcal{C}_2$ one obtains an arc of size $(q+5)/2$ or $(q+3)/2$ by choosing one point on each of the secants through R (and including the points of tangency in the case that R is external). This clearly gives an arc K, but it remains to be determined whether the arc K is complete or not. If K is not complete, then the ensuing natural problem is to decide which points (how many) can be added to complete K. To prove the completeness of an arc, there are several known methods, relying on known results from group theory, algebraic geometry, or Galois fields. In the next paragraphs, we describe further details concerning the complete arcs obtained from Segre's construction.

Assume that R is an external point to the conic $\mathcal{C}_2$. If $q \equiv 3 \pmod 4$, then the completeness of the arc K of size $(q+5)/2$ obtained from the above mentioned construction, was proved by (Segre, 1967, p. 152). In 1992, Pellegrino (Pellegrino, 1992) proved that if K is a complete arc containing the external point R, for q odd, containing $(q+3)/2$ points from an irreducible conic $\mathcal{C}_2$ of $\mathrm{PG}(2,q)$, then the possible sizes for K are $(q+5)/2$ and $(q+7)/2$ in general, with the additional values $(q+9)/2$ for $q \equiv 3 \pmod 4$. Later, in 2001, using linear collineations, Korchmáros and Sonnino provide an alternative proof to Pellegrino's result that in $\mathrm{PG}(2,q)$, with $(q+1)/2$ an odd prime, every arc sharing $(q+3)/2$ points with a conic contains at most four points outside the conic. This number is reduced to two, when, in addition $q^2 \equiv 1 \pmod{16}$ is assumed (Korchmáros & Sonnino, 2003, Theorem 1.1).

In the case in which R is an internal point to the conic $\mathcal{C}_2$, the completeness of K

was left as an open problem by (Segre, 1967). In this thesis, we give a short proof for the solution to this problem in Chapter 2. Our proof offers an alternative to the proofs contained in a series of papers by Pellegrino from the 1980s (see (Pellegrino, 1981a,8,8,8).) These papers were written in Italian, and some of which were difficult to obtain. In 1981 Pellegrino constructed examples of complete arcs of size $(q+3)/2$ in $\mathrm{PG}(2,q)$ for $q \equiv 3 \pmod 4$ in (Pellegrino, 1981a). One year later, he constructed complete arcs of size $(q+3)/2$ in $\mathrm{PG}(2,q)$ for $q \equiv 1 \pmod 4$ in (Pellegrino, 1982a). The method used in these papers relied on results in finite fields from (Pellegrino, 1982b) and (Pellegrino, 1981b), whereas our proof uses bounds for the number of points on algebraic curves over a finite field.

The classification of the one-dimensional linear systems of cubic forms on $\mathrm{PG}(1,q)$ is a list of the orbits of the one-dimensional subspaces of $\mathrm{PG}(3,q)$ under the induced action of $\mathrm{PGL}(2,q)$ (the projectivity group of $\mathrm{PG}(1,q)$) on $\mathrm{PG}(3,q)$. Therefore, the classification of pencils of cubics on $\mathrm{PG}(1,q)$ is equivalent to the classification of G-orbits of lines in $\mathrm{PG}(3,q)$ where $G \leq \mathrm{PGL}(4,q)$ isomorphic to $\mathrm{PGL}(2,q)$. The twisted cubic $\mathcal{C}_3$ is left invariant under the action of the group G (see e.g. (Harris, 2013, p. 118)).

The classification of points and planes in $\mathrm{PG}(3,q)$ under $\mathrm{PGL}(2,q)$ is well-known (see e.g. (Bruen & Hirschfeld, 1977)). Moreover, there are nine line classes in $\mathrm{PG}(3,q)$. As a second problem, we study the classification of lines of $\mathrm{PG}(3,q)$ under the action of the stabiliser group G of the twisted cubic. Since line classes of $\mathrm{PG}(3,q)$ are known, we try to find which line classes form a unique orbit, which line classes are union of some orbits.

A normal rational curve in $\mathrm{PG}(3,q)$ is called a *twisted cubic*. The twisted cubic in $\mathrm{PG}(3,q)$ has remarkable geometric properties which have led to many interesting applications. The points on a twisted cubic form an arc of size $q+1$ and the related MDS code is known as the Reed-Solomon code.

The classification of cubic curves is an old problem. In 1711, the classification of cubic curves was first considered and performed by Newton. He aimed to classify cubic curves according to their asymptotic behavior. Cubic curves are defined by the general non-degenerate cubic equation in two real variables where

$$AY^3 + BXY^2 + CX^2Y + DX^3 + EY^2 + FXY + GX^2 + HY + KX + L.$$

Newton reduced cubic curves into four types where

$$Y = AX^3 + BX^2 + CX + D$$

$$XY = AX^3 + BX^2 + CX + D$$

$$Y^2 = AX^3 + BX^2 + CX + D$$

$$MXY^2 + NXY = AX^3 + BX^2 + CX + D, M \neq 0.$$

To classify the cubic curves, he used classical algebra which involved passing through an equation with 84 terms. Using a general affine change of coordinates, Newton enlarged the group of transformations beyond the Euclidean group, which suffices to classify the conics. Newton divided cubic curves into 72 species according to their asymptotic behavior (see (Nunemacher, 1991)). In 1717, Stirling added new 4 species of cubic curves to the classification of Newton and he corrected some mistakes of Newton. Two additional species were given by Murdoch or Cramer in 1746. Totally, 78 species of cubic curves were found. Newton's classification scheme was criticized by Euler and other mathematicians because his geometric criteria appeared to lack a unifying theme and resulted in so many different species. Therefore, a new classification was made by Plücker in his *System der Analytishen Geometrie* in 1835. This classification was made according to the nature of the infinite branches, but after his six head divisions, and some subordinate divisions, Plücker establishes the divisions called Groups, which have nothing analogous to Newton's method; there are sixty-one groups, and the total number of species is 219.

Newton asserted that all non-degenerate cubic curves have as a projective image one of the five species of types because he noticed that there is a connection between cubic curves and the Weierstrass p-function. Then Newton proved that any cubic curve can be transformed into

$$Y^2 = 4X^3 - cX - d,$$

with c, d as real constants. Suppose that

$$4X^3 - cX - d = 4(X - x_1)(X - x_2)(X - x_3),$$

where $x_1 \geq |x_3|$ and $x_1 \geq |x_2|$. Newton distinguishes cubic curves into 5 classes under the action of the complex projective linear group. For the discussion of the full classification of cubic curves see (Brieskorn, 1986).

The classification of pencils of binary cubics over an algebraically closed field was given by (Newstead, 1981). These results were extended over the real numbers by (Wall, 1983). There is a one-to-one correspondence between pencils of cubics in $\mathrm{PG}(1, q)$ and lines of $\mathrm{PG}(3, q)$. Hence, the classification of lines of $\mathrm{PG}(3, q)$ is a kind

of classification problem of pencils of cubics in $\mathrm{PG}(1,q)$.

Pencils of cubics can also be seen as vectors in the space of partially symmetric tensors $S^3\mathbb{F}_q^2 \otimes \mathbb{F}_q^2$, where $S^3\mathbb{F}_q^2$ denotes the space of symmetric tensors in $\mathbb{F}_q^2 \otimes \mathbb{F}_q^2 \otimes \mathbb{F}_q^2$. As such, our results fit into the larger research project of classifying tensors over finite fields (Lavrauw, 2020b), and our approach is inspired by the classifications obtained in (Lavrauw & Sheekey, 2015), and (Lavrauw & Popiel, 2020). The combinatorial invariants studied here were motivated by the combinatorial invariants for the orbits of nets of conics studied in (Lavrauw, Popiel & Sheekey, Lavrauw et al.). We publish tensor representation of ten G-orbits of lines in $\mathrm{PG}(3,q)$.

1.1 Thesis Organization

In Chapter 2, an overview is given of required basic concepts and definitions on projective geometry over finite fields and selected known results from group theory. At the end of the chapter, we describe arcs, its related code, algebraic curves, and required properties of $\mathrm{PG}(3,q)$.

Chapter 3 aims to provide a comprehensive proof of the problem left open by (Segre, 1967). As a corollary of our proof, we obtain examples of arcs that give counterexamples to the statement in (Hirschfeld, 1993). This concerns the existence of a line satisfying the hypothesis for the main theorem from (Pellegrino, 1993b) in which Pellegrino studied the completion of arcs sharing (any) $(q+1)/2$ points with a conic but with an extra assumption.

In Chapter 4, we classify all of the G-orbits on lines of $\mathrm{PG}(3,q)$, for $3 \nmid q$ odd, which are contained in an osculating plane of $\mathcal{C}_3$ and the G-orbits on lines which have a non-empty intersection with $\mathcal{C}_3$. We determine the point orbit distributions and plane orbit distributions of all G-orbits of lines contained in an osculating plane of $\mathcal{C}_3$, have a non-empty intersection with $\mathcal{C}_3$, or are imaginary chords or axes. For these line orbits, we find the sizes of line orbits and sizes of their stabilisers under G. We summary all results on the classification of G-orbits on lines in $\mathrm{PG}(3,q)$ except the line class $\mathcal{O}_6$. We mention codes related to twisted cubic.

Chapter 5 summarizes our results and associates them with other topics and (or questions).

2. PRELIMINARIES

In this chapter, we will give some known definitions and basic notations. We introduce some concepts and results which will be needed in the following chapters.

2.1 Projective spaces over finite fields

Let p be a prime and q be a power of a prime p. Assume that $\mathbb{F}_q$ denotes the finite field with q elements. In this thesis, q is always odd. The set of squares of $\mathbb{F}_q$ is denoted by $\square$ and the set of non-squares of $\mathbb{F}_q$ is denoted by $\triangle$.

Definition 1. Let V be the $n+1$-dimensional vector space over the finite field of order q, where $q = p^h$, p prime, $h \geq 1$. The n-dimensional *Desarguesian projective space* over $\mathbb{F}_q$, denoted as $\mathrm{PG}(n,q)$, is the quotient of $V \setminus \{0\}$ by the equivalence relation

$$x \ y \Leftrightarrow x = \lambda y \text{ for some } \lambda \in \mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}.$$

The 0-dimensional subspaces of $\mathrm{PG}(n,q)$ are the one-dimensional subspaces of $V(n+1,q)$, the one-dimensional subspaces of $\mathrm{PG}(n,q)$ are the two-dimensional subspaces of $V(n+1,q)$, ..., etc. The *dimension* of $\mathrm{PG}(n,q)$ is n. The *codimension* of a subspace of dimension $n-k$ of $\mathrm{PG}(n,q)$ is k. A subspace of dimension 0, 1, 2, 3 and $n-1$ is called a *point*, a *line*, a *plane*, a *solid* and a *hyperplane*, respectively.

Theorem 2. *Let θ_n denote the number of points of* $\mathrm{PG}(n,q)$. *Then*

$$\theta_n = \frac{q^{n+1}-1}{q-1} = q^n + q^{n-1} + \ldots + 1.$$

Theorem 3. *The number of $k+1$-dimensional subspaces of $V(n+1,q)$ is*

$$\begin{aligned}\begin{bmatrix} n+1 \\ k+1 \end{bmatrix}_q &= \frac{(q^{n+1}-1)(q^{n+1}-q)...(q^{n+1}-q^k)}{(q^{k+1}-1)(q^{k+1}-q)...(q^{k+1}-q^k)} \\ &= \frac{(q^{n+1}-1)(q^n-1)...(q^{n-k+1}-1)}{(q^{k+1}-1)(q^k-1)...(q-1)}.\end{aligned}$$

Then the number of $k+1$-dimensional subspaces of $V(n+1,q)$ containing a $r+1$-dimensional subspace U is equal to the number of $k-r$-dimensional subspaces in $V(n-r,q)$. Hence, the number is

$$\begin{bmatrix} n-r \\ k-r \end{bmatrix}_q.$$

Consider $\Pi : (\mathcal{P}, \mathcal{L}, \mathcal{I})$ with points $\mathcal{P}$, lines $\mathcal{L}$, and incidence $\mathcal{I}$, and Π is called *projective plane* if it has the following axioms.

3.1 Any two distinct lines are incident with a point.

3.2 Any two distinct points are incident with exactly one line.

3.3 There exits a set of 4 points, no three of which are collinear.

Moreover, Π is called *Desarguesian* projective plane if $\Pi \cong \mathrm{PG}(2,q)$. Then, it contains q^2+q+1 points and q^2+q+1 lines. There are $q+1$ points on a line and $q+1$ lines through a point.

An *affine plane* is an incidence structure that is obtained by deleting a line ℓ and the points incident with ℓ of a projective plane. The line ℓ is called the line at *infinity* of the affine plane.

The projective space $\mathrm{PG}(3,q)$ contains q^3+q^2+q+1 points and planes. There are $(q^2+q+1)(q^2+1)$ lines and q^2+q+1 lines through every point. Every line has $q+1$ points and a line meets every plane. Dually, there are $q+1$ planes through a line. A plane of $\mathrm{PG}(3,q)$ has q^2+q+1 points.

2.2 Group theory

Definition 4. Let $(G,\cdot)$ be a group and Ω be a non-empty set. A *(right) group action* is a map from

$$\begin{array}{ccc}(G,\Omega) & \to & \Omega \\ (g,x) & \mapsto & xg\end{array}$$

satisfying

4.1 $xe = x$ for every $x \in \Omega$.

4.2 $(xg_1)g_2 = x(g_1g_2)$ for every $g_1,\ g_2 \in \Omega$.

Definition 5. (i) The *orbit* of $x \in \Omega$ under G is

$$x^G = \{y \in \Omega \mid \exists g \in G \text{ such that } xg = y\}$$

(ii) The *stabiliser* of an element $x \in \Omega$ is the subgroup

$$G_x = \{g \in G \mid xg = x\}.$$

(iii) For a subgroup $H \leqslant G$ and an element $g \in G$ the *conjugate subgroup*

$$g^{-1}Hg = \{g^{-1}hg \mid h \in H\}.$$

(iv) The group G acts *transitively* on Ω if and only if G has only one orbit on Ω; equivalently, if for each $x,\ y \in \Omega$ there exists a $g \in G$ for which $x^g = y$.

(v) The group G acts *t-transitively* on Ω, if for each two t-tuples $(x_1,...,x_t)$ and $(y_1,..,y_t)$ of elements in Ω, there exists an element $g \in G$ satisfying $x_i^g = y_i$ for each $i = 1,...,t$.

Theorem 6. *Given group action $(G,\Omega) \to \Omega$, we have the followings:*

(i) The orbits of G partition the set Ω. If $H \leqslant G$, then each orbit of G is the union of orbits of H.

(ii) $G_x \leqslant G$ for every $x \in \Omega$.

(iii) $G_{x^g} = (G_x)^g$ for each $x \in \Omega$ and $g \in G$.

(iv) If $y \in x^G$, then $G_x \cong G_y$.

(v) If $|\Omega| > 2$ and $t > 1$, then G acts t-transitively on Ω if and only if G_x acts $(t-1)$-transitively on $\Omega \setminus \{x\}$ for each $x \in \Omega$.

Theorem 7. (Orbit-stabiliser formula) *Let G be a finite group and $(G,\Omega) \to \Omega$ be the given group action. Then*

$$|G| = |x^G||G_x|.$$

Definition 8. A *permutation* of a set Ω is a bijection from Ω to Ω. The *symmetric group of degree n* is denoted by S_n and consists of all permutations of the set $I_n = \{1,2,...,n\}$, with composition as a group operation. The group of all permutations of an arbitrary set Ω is called the *symmetric group* of Ω and is denoted by $Sym(\Omega)$. Any subgroup of a symmetric group is called a *permutation group*.

Definition 9. Let V be a finite dimensional vector space over a field K. The group of all nonsingular linear maps on V is called the *general linear group* and it is denoted by $\mathrm{GL}(V)$. The group of all nonsingular semi-linear maps on V is denoted by $\Gamma\mathrm{L}(V)$.

2.3 Collineations, correlations and polarities

Definition 10. Let $\mathrm{PG}(V)$ and $\mathrm{PG}(W)$, with $n = \dim(\mathrm{V}) = \dim(\mathrm{W}) \geq 3$ be two spaces. A *morphism* is a type-preserving and incidence-preserving map from the subspaces of $\mathrm{PG}(V)$ to the subspaces of $\mathrm{PG}(W)$. A morphism is called an *isomorphism* or a *colineation* if it is a bijection.

A collineation σ induced by φ is denoted by $\sigma = \overline{\varphi}$. If $\varphi = (A,\theta)$ then the action of σ on the points of $\mathrm{PG}(V)$ is defined by

$$\langle P\rangle^\sigma = \langle P_1\rangle, \text{where } P^{T\theta}A = P_1^T,$$

here T denotes the transpose of the matrix A. If the collineation σ is induced by $\varphi = (A,\theta)$, with $\theta = id$, then σ is called a *projectivity*. The group of all collineations induced by $\Gamma\mathrm{L}(V)$ is called *projective semilinear group* of $\mathrm{PG}(V)$ and it is denoted by $\mathrm{P\Gamma L}(n+1,q)$. Its subgroup of all projectivities of $\mathrm{PG}(V)$ is called *projective general linear group* and it is denoted by $\mathrm{PGL}(n+1,q)$. The order of $\mathrm{PGL}(n+1,q)$ is

$$\frac{(q^{n+1}-1)(q^{n+1}-q)...(q^{n+1}-q^n)}{q-1}.$$

Definition 11. If there exists a projectivity which sends the object O to the object O', then O and O' are *projectively equivalent*; otherwise they are *projectively distinct*.

Theorem 12. *(The Fundamental Theorem of Projective Geometry)*

(i) The set of projectivities of $\mathrm{PG}(n,q)$ *and the set of collineations of* $\mathrm{PG}(n,q)$*, form a group with composition as operator.*

(ii) If ϕ *is a collineation of* $\mathrm{PG}(n,q)$*, then* ϕ *is the composition of an automorphic collineation* θ *and a projectivity* A*. We write* $\phi = (A,\theta)$*.*

(iii) If $\{P_1,P_2,...,P_{n+1}\}$ *and* $\{Q_1,Q_2,...,Q_{n+1}\}$*, are sets of points of* $\mathrm{PG}(n,q)$ *such that the subspace spanned by each of these sets is* $\mathrm{PG}(n,q)$*, then there exists a unique projectivity* α *such that* $P_i^{\alpha} = Q_i$*,* $i = 1,2,...,n$*.*

Definition 13. An *anti-isomorphism* or a *correlation* τ between $\mathrm{PG}(V)$ and $\mathrm{PG}(W)$ is a collineation between $\mathrm{PG}(V)$ and the dual space $\mathrm{PG}(W^{\vee})$ of $\mathrm{PG}(V)$. If $V = W$, then a correlation of $\mathrm{PG}(V)$ is often considered as a morphism with domain and image equal to the set of subspaces of $\mathrm{PG}(V)$. A correlation of order two is called a *polarity* of $\mathrm{PG}(V)$.

Definition 14. Let τ be the polarity, with matrix A.

(i) If $A^T = -A$, then τ is called *symplectic* polarity.

(ii) If $A^T = A$ and $\mathrm{char}(K) \neq 2$, then τ is called *orthogonal* polarity.

(iii) If $A^T = A$ and $\mathrm{char}(K) = 2$, then τ is called *pseudo* polarity.

2.4 Arcs

Definition 15. A *k-arc* in $\mathrm{PG}(n,q)$, with $k \geq n+1 \geq 3$, is a set of k points such that no $n+1$ points of the arc are contained in a hyperplane of $\mathrm{PG}(n,q)$. An arc is *complete* if it is not contained in $(k+1)$-arc.

Consider the projective plane $\mathrm{PG}(2,q)$. A set of k points such that no 3 points are collinear is called a *k-arc*. Arcs in $\mathrm{PG}(2,q)$ are also known as *planar arcs* and are the two-dimensional version of arcs in projective spaces of any dimension ≥ 2.

Theorem 16. *(Bose, 1947) Let* K *be a* k*-arc in* $\mathrm{PG}(2,q)$*. If* q *is odd, then* $k \leq q+1$*. If* q *is even, then* $k \leq q+2$*.*

Definition 17. A $(q+1)$-arc is called an *oval*, and a $(q+2)$-arc is called a *hyperoval*.

A line intersecting the arc K in exactly one point is called a *tangent line*. A line intersecting the arc K in two points is called a *secant line*. A line not meeting the arc K is called an *external line*. Given an arc K we say that a point of $\mathrm{PG}(2,q) \setminus K$ is K*-covered* if it lies on a secant of K and K*-free* otherwise. For q even, the $q+1$ tangent lines of an oval are concurrent in $\mathrm{PG}(2,q)$. The intersection point is called a *nucleus* of the oval. A hyperoval of $\mathrm{PG}(2,q)$ is obtained by adding the nucleus to the oval.

Example 18. Let σ be the automorphism of $\mathbb{F}_q$, $q = 2^h$, which takes x to x^{2^e}. The set

$$K = \{(1,t,t^\sigma) \mid t \in \mathbb{F}_q\} \cup \{(0,0,1),(0,1,0)\}$$

is an arc of size $q+2$ points in $\mathrm{PG}(2,q)$, whenever $(e,h) = 1$.

Definition 19. A symmetric bilinear form $b(X,Y)$ on $\mathbb{F}_q^k$ is *degenerate* if $b(X,y) = 0$ for some point y. A quadratic form $f(X)$ is *degenerate* if $f(y) = 0$ and $b(X,y) = 0$ for some point y, where

$$b(X,Y) = f(X+Y) - f(X) - f(Y)$$

is the bilinear form associated to $f(X)$.

Definition 20. A conic $\mathcal{C}_2$ over $\mathbb{F}_q$ is the zero set of a homogenous quadratic equation in three variables over a field $\mathbb{F}_q$. The conic equation can be written as

$$a_{00}X^2 + a_{11}Y^2 + a_{22}Z^2 + a_{01}XY + a_{02}XZ + a_{12}YZ,$$

where $a_{ij} \in \mathbb{F}_q$, $i, j \in \{0,1,2\}$.

Any 5-arc determines a unique conic in $\mathrm{PG}(2,q)$.

Theorem 21. *((Segre, 1954), (Segre, 1955b)) For q odd, every oval is a conic in* $\mathrm{PG}(2,q)$.

If q is odd, then every point P not on a conic $\mathcal{C}_2$ is either on two tangent lines to $\mathcal{C}_2$ or on no tangent line to $\mathcal{C}_2$. If P is on two tangent lines to $\mathcal{C}_2$, then it is called an *external point*, otherwise, it is called an *internal point*. There are $(q(q+1)(q^2+q+1))/2$ external points and $(q(q-1)(q^2+q+1))/2$ internal points for q odd.

2.5 MDS conjecture

A *linear code* C is a subspace of $\mathbb{F}_q^n$. The *Hamming distance* $d(x,y)$ between any two elements $x, y \in \mathbb{F}_q^n$ is the number of coordinates in which they differ. Let $\mathrm{C} \subseteq \mathbb{F}_q^n$ be a code and $\mathrm{C} \neq \{0\}$, its *minimum distance*

$$d(\mathrm{C}) = \min\{d(c,c') \mid c \neq c' \in \mathrm{C}\}.$$

For a vector $x = (x_1, x_2, ..., x_n)$ in $\mathbb{F}_q^n$, the *weight*

$$wt(x) = |\{i \mid x_i \neq 0\}| = d(x,0).$$

Let $\mathrm{C} \subseteq \mathbb{F}_q^n$ be a code, $\mathrm{C} \neq \{0\}$. Then

$$d(\mathrm{C}) = \min\{wt(x) \mid x \in \mathrm{C},\ x \neq 0\}.$$

If the *rank* of the code $\mathrm{C} \subseteq \mathbb{F}_q^n$ is $k = \dim_{\mathbb{F}_q}\mathrm{C}$, then C has size q^k. We denote an $\mathbb{F}_q$-linear code C of length n, dimension k and minimum distance d by $[n,k,d]$.

Let x be a vector in $\mathbb{F}_q^n$ and $t > 0$ be an integer. A *Hamming sphere* of radius t centered at x is

$$B_t(x) = \{y \in \mathbb{F}_q^n \mid d(y,x) \leq t\}.$$

Definition 22. Let $\mathrm{C} \subseteq \mathbb{F}_q^n$ be a code t, $e \geq 0$, then

C is called *t-error detecting* if

$$B_t(\mathrm{c}) \cap \mathrm{C} = \{c\},\ \forall c \in \mathrm{C}.$$

C is called *e-error correcting* if

$$B_e(c) \cap B_e(c') = \varnothing,\ \forall c \neq c' \in \mathrm{C}.$$

Theorem 23. *Let* $\mathrm{C} \subseteq \mathbb{F}_q^n$ *be a code with* $d(\mathrm{C}) = d$, *then*

(i) C *is t-error detecting, for any* $t \leq d-1$.

(ii) C *is e-error correcting, for any* $e \leq \lfloor \frac{d-1}{2} \rfloor$.

Definition 24. The *covering radius* R_0 of $\mathrm{C} \subseteq \mathbb{F}_q^n$ is

$$R_0 = \max\{\min\{d(x,c) : c \in \mathrm{C}\}\ x \in \mathbb{F}_q^n\}.$$

The covering radius of $\mathrm{C} \subseteq \mathbb{F}_q^n$ is the smallest integer R_0 such that the Hamming spheres of radius R_0 centered at the codewords cover the whole space.

Simple example of a code with radius 1 is as follows.

Example 25. Let $\mathrm{C} = \{(0,0,0),(1,1,1)\}$ be a binary $[3,1]$ code with $R_0 = 1$. Then $\mathbb{F}_2^3 = \{(0,0,0),(1,0,0),(0,1,0),(0,0,1),(1,0,1),(0,1,1),(1,1,0),(1,1,1)\}$. For any $x \in \mathbb{F}_2^3$, $\min_{c\in\mathrm{C}}\{d(x,c)\} = 1$. It follows maximum distance of any vector $x \in \mathbb{F}_2^3$ from the codewords is $R_0 = 1$.

Theorem 26. *(Singleton bound) Let* C *be a linear* $[n,k,d]$*-code. Then*

$$|\mathrm{C}| \leq q^{n+1-d}.$$

A linear code C of dimension k is called *maximum distance separable* (MDS) code if $|\mathrm{C}| = q^{n+1-d}$. It implies that an MDS code corrects the maximum number of errors given its size and length.

Example 27. Let C be the k-dimensional space defined as

$$\mathrm{C} = \{(x_1,x_2,...,x_k,x_1+x_2+...+x_k) \mid (x_1,x_2,...,x_k) \in \mathbb{F}_q^k\}.$$

C is a linear MDS code with $n = k+1$, $n-k+1 = 2$.

Definition 28. The *dual* of a linear code C of length n over $\mathbb{F}_q$ is,

$$\mathrm{C}^{\perp} = \{x \in \mathbb{F}_q^n \mid u.x = 0 \text{ for all } u \in \mathrm{C}\}$$

where $u.x$ denotes the standard inner product $u.x = u_1x_1 + u_2x_2 + ... + u_nx_n$. If C has dimension k, then $\mathrm{C}^{\perp}$ has dimension $n-k$.

Given $[n,k]$ code over $\mathbb{F}_q$, $k \geq 1$. The matrix G of rank k is called a *generator matrix* for the code, if

$$\mathrm{C} = \{x\mathrm{G} \mid x \in \mathbb{F}_q^k\}.$$

The matrix H of size $(n-k)\times n$ is called a *parity check matrix* for the code, if

$$\mathrm{C} = \{x \in \mathbb{F}_q^n \mid \mathrm{H}x^T = 0\}.$$

The matrix H can be given by column vectors in $\mathbb{F}_q^{n-k}$,

$$\mathrm{H} = \begin{pmatrix} | & & | \\ c_1 & \cdots & c_n \\ | & & | \end{pmatrix},$$

and $\mathrm{rank}(\mathrm{H}) = (n-k)$. The matrix H is a generator matrix for $\mathrm{C}^{\perp}$.

For a given $[n,k,d]$ code, minimum distance of $\mathrm{C} \subseteq \mathbb{F}_q^n$ is

$$d(\mathrm{C}) = \min\{m \geq 1 : \text{there exist } m \text{ linearly dependent column vectors in H}\}.$$

For an element $x \in \mathbb{F}_q^n$, let $s(x) = \mathrm{H}x^T$, denote the *syndrome* of x. In terms of parity check matrix H, an $[n,k,d]$ code $\mathrm{C} \subseteq \mathbb{F}_q^n$ has the covering radius R_0, if every syndrome $s(x)$ in $\mathbb{F}_q^{n-k}$ is the sum of at most R_0 columns of a parity check matrix of this code and R_0 is the smallest value with such property.

Lemma 29. *Let $x \in \mathbb{F}_q^n$. Then, the number of codewords $c \in \mathrm{C}$ such that $d(x,c) = R_0$ is the number of distinct vectors $v \in \mathbb{F}_q^n$ of weight R_0 such that*

$$s(x) = Hv^T.$$

Proof. Since $Hx^T = Hv^T$, $H(x-v)^T = 0$. $H(x-v)^T = 0$ if and only if $x - v = c \in \mathrm{C}$ with $d(x,c) = wt(v)$. □

Definition 30. An $[n,k,d]R_0$ code $\mathrm{C} \subseteq \mathbb{F}_q^n$ is an (R_0,μ) *multiple covering of the farthest-off points* ((R_0,μ)-MCF code) if for all $x \in \mathbb{F}_q^n$ such that $d(x,C) = R_0$, the number of codewords c such that $d(x,c) = R_0$ is at least μ.

Let $K = \{\langle v_j \rangle \mid j = 1,2,...,n\}$ be the set of one-dimensional subspaces of $V(k,q)$ spanned by the columns of G, in which,

$$G = \begin{pmatrix} | & & | \\ v_1 & \cdots & v_n \\ | & & | \end{pmatrix}.$$

So the elements of K are points of $\mathrm{PG}(k-1,q)$.

Lemma 31. *Let $u = (u_1,u_2,...,u_k)$ be a non-zero vector of $\mathbb{F}_q^k$. The hyperplane*

$$H = \mathcal{Z}(u_1X_1 + u_2X_2 + ... + u_kX_k)$$

contains $n-w$ points of K if and only if the codeword uG has weight w.

Proof. Let $c \in \mathrm{C}$ has weight w. For each zero coordinate of $c = uG$ there is a column of G such that

$$c = u_1 v_i^1 + u_2 v_i^2 + ... + u_k v_i^k = 0$$

where $v_i = (v_i^1, v_i^2, ..., v_i^k)$ a column of G. Then the vector c has $n - w$ zero coordinates. □

Corollary 32. *Linear MDS codes ($d = n - k + 1$) are equivalent with arcs in projective spaces.*

Theorem 33. *The linear code* C *generated by the matrix G, whose columns are the coordinate vectors of the points of an arc is a linear MDS code, and vice versa, the set of columns of a generator matrix of an MDS code considered as a set of points of the projective space, is an arc.*

Lemma 34. *The linear code* C *is MDS if and only if* $\mathrm{C}^\perp$ *is MDS.*

Proof. Suppose that C is an MDS code of length n, dimension k and $\mathrm{C}^\perp$ is not MDS. $\mathrm{C}^\perp$ contains a non-zero vector v of weight less than $n - (n-k) + 1 = k + 1$. Let G be a generator matrix of C. Then $Gv = 0$ since $v \in \mathrm{C}^\perp$. It follows v has at most k non-zero coordinates. The columns of G corresponding to non-zero coordinates of v are linearly dependent. It gives a contradiction, since k columns of G is linearly independent. □

Example 35. (Normal rational curve) For $q \geq k$, let

$$\mathcal{C}_{k-1} = \{(1, t, t^2, ..., t^{k-1}) \mid t \in \mathbb{F}_q\} \cup \{(0, ..., 1)\}.$$

Then $\mathcal{C}_{k-1}$ is a NRC of size $n = q + 1$ in $\mathrm{PG}(k-1, q)$. The corresponding $[q+1, q+1-k, k+1]$ code is known as the (extended) Reed-Solomon code.

For $k - 1 = 3$,

$$\mathcal{C}_3 = \{(1, t, t^2, t^3) \mid t \in \mathbb{F}_q\} \cup \{(0, 0, 0, 1)\}$$

is a twisted cubic of size $q + 1$. For distinct elements $t_i \in \mathbb{F}_q$, the parity check matrix is

$$\mathrm{H} = \begin{pmatrix} 1 & 1 & ... & 1 & 0 \\ t_1 & t_2 & ... & t_q & 0 \\ t_1^2 & t_2^2 & ... & t_q^2 & 0 \\ t_1^3 & t_2^3 & ... & t_q^3 & 1 \end{pmatrix}.$$

Since any 4 points of $\mathcal{C}_3$ generate $\mathrm{PG}(3, q)$, 5 columns of H are linearly dependent. Then, $d = 5$ and $n = q + 1$, $\mathcal{C}_3$ is a $[q+1, q-3, 5]$ code.

If C is a linear MDS code of dimension $k \geq q+1$ and length n, then $n \leq k+1$. The MDS conjecture is related to a case $k \leq q$.

Conjecture 36. *For a linear MDS code of length n and dimension $k \leq q$ over $\mathbb{F}_q$,*

$$n \leq q+1$$

unless $k=3$ or $k=q-1$ and q is even, in which case $n \leq q+2$.

For q odd, NRC is the example of the longest MDS code if the conjecture is true. Many mathematicians have contributed to possible solutions of MDS conjecture and many examples of MDS conjecture have been given so far (see (Ball & Lavrauw, 2019)). Here, we mention some of the results on the MDS conjecture.

If $k=4$, then the truthness of MDS conjecture is proved in (Segre, 1955a) for q odd, and in (Casse, 1969) for q even. Furthermore, MDS conjecture is true for $k=5$ and it is proved in (Segre, 1962) for q odd, and in (Casse, 1969) for q even.

For $k \geq 6$, there are some results on MDS conjecture. The proof of the MDS conjecture for $k=6$, q even is published in (Ball & Lavrauw, 2019). Kaneta and Maruta proved MDS conjecture for $k=7$, $q \geq 16$ even in (Maruta & Kaneta, 1991). Segre-Blokhuis-Bruen-Thas proved MDS conjecture in (Storme & Thas, 1993) for $k < \frac{1}{2}\sqrt{q} + \frac{15}{4}$. In (Voloch, 1991) and (Ball & Lavrauw, 2018), MDS conjecture is published for $k < \frac{1}{4}\sqrt{pq} - \frac{29}{16}p + 4$, q odd non-square. If q is odd square, then $k < \sqrt{q} - \sqrt{q}/p + 2$.

The complete planar arcs of size $q-1$ occur for $q=7$, 9, 11, and 13. There are complete planar arcs of size $q-2$ for $q=8$, 9, 11 (Ball & Lavrauw, 2018). On planar arcs for $k \leq \frac{1}{2}\sqrt{q}$, the truthness of MDS conjecture is published in (Hirschfeld & Korchmáros, 1996) and (Hirschfeld & Korchmáros, 1998).

If q is an odd square and $k \leq \sqrt{q} - \sqrt{q}/p + 2$, then MDS conjecture is proved in (Ball & Lavrauw, 2018).

There have been studies on MDS conjecture for q even. For q even, there are examples of arcs of size $q+2$ which are projectively inequivalent. The list of hyperovals is complete for $q=8$, $q=16$, and $q=64$ (see e.g. (O'Keefe & Penttila, 1991), (Hall, 1975), (Vandendriessche, 2019)). For more examples of hyperovals, see e.g. Cherowitzo's hyperoval page, pointing to examples of Segre, Glynn, Payne, Cherowitzo, Penttila, Pinneri, Royle, and O'Keefe.

For $q=p^h$, p prime, $h>1$, $k \leq 2p-2$ MDS conjecture has been proved by Ball and later extended by Ball and De Beule in (Ball & De Beule, 2012).

MDS conjecture is also true for all $q \leq 27$, for all $k \leq 5$ and $k \geq q-3$ and for $k = 6$, 7, $q-4$, $q-5$, in the paper of (Hirschfeld & Storme, 1998), pointing to results of Segre, Thas, Casse, Glynn, Bruen, Blokhuis, Voloch, Storme, Hirschfeld and Korchmáros.

Definition 37. Let $\mathrm{C} \subseteq \mathbb{F}_q^n$ and $x \in \mathbb{F}_q^n$. The *weight of the coset* $x + \mathrm{C}$ is defined by

$$\mathrm{wt}(x + \mathrm{C}) = \min\{\mathrm{wt}(x + c) \mid c \in \mathrm{C}\}.$$

A *coset leader* is a choice of an element $x \in \mathbb{F}_q^n$ of minimal weight in its coset, that is $\mathrm{wt}(x) = \mathrm{wt}(x + \mathrm{C})$. Let θ_i be the number of cosets of C of weight i. The *coset leader weight enumerator* is the polynomial with coefficients θ_i. A *coset leader* decoder gives as output $x - e$, where x is the received word and e is the chosen coset leader of the coset of x. Hence, $x - e$ is a nearest codeword to x, but sometimes it is not the only one. The probability of decoding correctly by the coset leader decoder can be computed.

There is a one-to-one correspondence between cosets and syndromes. A coset leader corresponds to a minimal way to write its syndrome as a linear combination of the columns of a parity check matrix.

2.6 Algebraic curves

Definition 38. An *algebraic curve* $\mathcal{F}$ in $\mathrm{PG}(2, q)$ is equal to zero locus of a homogeneous polynomial $F \in \mathbb{F}_q[X, Y, Z]$.

Definition 39. The curve $\mathcal{F}$ is *irreducible*, if F is irreducible over $\mathbb{F}_q$; $\mathcal{F}$ is *absolutely irreducible* if F is irreducible over $\overline{\mathbb{F}}_q$, the algebraic closure of $\mathbb{F}_q$.

Definition 40. If $P = \langle U \rangle$ is a point of the irreducible curve $\mathcal{F} = \mathcal{Z}(F)$ of degree d and $\ell = \langle U, V \rangle$ is a line not contained in $\mathcal{F}$, then the *intersection multiplicity* $m_P(\ell, \mathcal{F})$ is the multiplicity of $t = 0$ in $F(U + tV)$.

The *multiplicity* of P on $\mathcal{F}$, denoted $m_P(\mathcal{F})$, is the minimum of $m_P(\ell, \mathcal{F})$ for all lines ℓ through P. Then P is a *singular* point of $\mathcal{F}$ if $m_P(\mathcal{F}) > 1$. A line ℓ is a *tangent line* to $\mathcal{F}$ at P if $m_P(\ell, \mathcal{F}) > m_P(\mathcal{F})$. The point P is called an *ordinary singular point* if $\mathcal{F}$ has $m_P(\mathcal{F})$ distinct tangents at the point P.

Definition 41. The set of $\mathbb{F}_q$*-rational points* of the curve $\mathcal{F}$ is defined as the set of points of $\mathrm{PG}(2, q)$ where F vanishes.

Definition 42. Let P be a point on the algebraic curve $\mathcal{F}$ in $\mathrm{PG}(2,q)$ where $P = (x,y,z)$, then P is a *singular* point if

$$\frac{\partial \mathcal{F}}{\partial X}(P) = \frac{\partial \mathcal{F}}{\partial Y}(P) = \frac{\partial \mathcal{F}}{\partial Z}(P) = 0.$$

Definition 43. An algebraic curve $\mathcal{F}$ in $\mathrm{PG}(2,q)$ is *non-singular* if $\mathcal{F}$ does not have any singular point.

Lemma 44. *(Segre & Bartocci, 1971, Lemma 8) Let $\mathcal{F}$ be a projective plane curve of degree k defined over an arbitrary field E. If there exists a point P of $\mathcal{F}$ and a tangent line ℓ at P, for which*

(i) ℓ counts once among the tangents of $\mathcal{F}$ at P,

(ii) the intersection multiplicity of $\mathcal{F}$ and ℓ at P is equal to k, and

(iii) $\mathcal{F}$ has no linear component through P,

then $\mathcal{F}$ is absolutely irreducible.

The following theorem is well-known.

Theorem 45. *(Weil, 1948) If $\mathcal{F}$ is an absolutely irreducible nonsingular projective curve in $\mathrm{PG}(2,q)$ of degree d, and N denotes the number of $\mathbb{F}_q$-rational points of $\mathcal{F}$, then*

$$|q+1-N| \leq (d-1)(d-2)\sqrt{q}.$$

2.7 The normal rational curve

The Veronese map ν_d from $\mathrm{PG}(1,q)$ to $\mathrm{PG}(d,q)$ is defined by

$$\nu_d : (x_0, x_1) \mapsto (x_0^d, x_0^{d-1}x_1, ..., x_1^d).$$

Definition 46. The *normal rational curve* of degree d is an algebraic curve which is an image of $\nu_d(\mathrm{PG}(1,q))$.

The normal rational curve of degree d has the property that no $d+1$ points of $\mathcal{C}_d$ are in a hyperplane. Therefore, it gives an arc of size $q+1$.

Definition 47. The normal rational curve of degree 3 is called a *twisted cubic*. The set of points of the twisted cubic is maximal with the property that no 4 points are contained in a hyperplane of $\mathrm{PG}(3,q)$.

Let the twisted cubic be denoted by $\mathcal{C}_3$. We represents points $P=(y_0,y_1,y_2,y_3)$ of $\mathrm{PG}(3,q)$ by

$$M=\begin{pmatrix} y_0 & y_1 & y_2 \\ y_1 & y_2 & y_3 \end{pmatrix}.$$

The twisted cubic $\mathcal{C}_3$ in $\mathrm{PG}(3,q)$ is described by the zero locus of 2×2 minors of M. The twisted cubic is the first example of an algebraic variety that is not a hypersurface.

2.8 Cubic curves

A p-function with its derivative is used to parameterize the elliptic functions. Weierstrass' function $u(t)$ has a formula

$$u(t)=\int_t^\infty \frac{dX}{\sqrt{4X^3-cX-d}}$$

where c, d are real constants and u is a function of p. It follows that

$$\frac{du}{dt}=\frac{-1}{\sqrt{4t^3-ct-d}} \text{ or}$$

$$\left(\frac{dt}{du}\right)^2=4t^3-ct-d.$$

As $X=t$ and $Y=\left(\frac{dt}{du}\right)^2$:

$$y^2=4x^3-cx-d.$$

Assume that $y=0$ and the curve has roots x_1, x_2 and x_3. Then

$$4X^3-cX-d=4(X-x_1)(X-x_2)(X-x_3),$$

and by equating the coefficients of equal powers of x on both sides

$$x_1+x_2+x_3=0,$$

$$x_1x_2 + x_1x_3 + x_2x_3 = -\frac{1}{4}c,$$

$$x_1x_2x_3 = \frac{1}{4}d.$$

Suppose that

$$4X^3 - cX - d = 4(X - x_1)(X - x_2)(X - x_3),$$

where $x_1 \geq |x_3|$ and $x_1 \geq |x_2|$. Newton distinguishes cubic curves into 5 classes under the action of the complex projective linear group.

11.1 Parabolic class. $x_1 \in \mathbb{R}$, and x_2, $x_3 \in \mathbb{C}$. The curve consists of a single branch.

11.2 Acnodal class. x_1, $x_2 = x_3 \in \mathbb{R}$. The curve has an isolated double point or acnode.

11.3 Conchoidal class. x_1, x_2, $x_3 \in \mathbb{R}$ and all different. The curve has two separate branches.

11.4 Crunodal (or strophoidal) class. $x_1 = x_2 \in \mathbb{R}$ and $x_2 \in \mathbb{C}$. The curve has a double point, or crunode.

11.5 Cuspidal (or cissoidal) class. $x_1 = x_2 = x_3$. The curve has a cusp.

A quadratic equation and a cubic equation may have distinct or coincident roots. The discriminant of quadratic or cubic equations helps us to understand the roots of the equation. For a quadratic equation

$$f(x) = ax^2 + bx + c,$$

the discriminant is

$$D_f = b^2 - 4ac.$$

If $D_f = 0$, then the equation f has a double root. If D_f is nonzero, then f has two distinct roots.

For a cubic equation

$$f(X) = aX^3 + bX^2 + cX + d = 0,$$

the discriminant is

$$D_f = 18abcd - 4b^3d + b^2c^2 - 4ac^3 - 27a^2d^2.$$

If $D_{a,b,c,d} = 0$, then f has a multiple root, otherwise f has distinct roots. The cubic

equation f can be transformed into equation

$$f(Y) = Y^3 + kY + m$$

by substituting

$$x = y - \frac{b}{3a}.$$

The discriminant $D_{k,m} = -4k^3 - 27m^2$.

Theorem 48. *Let $f(X) = aX^3 + bX^2 + cX + d \in \mathbb{F}_q[X]$, and let $D_f \neq 0$. Then*

$$f(X) = a_1(X - \beta_1)^3 + a_2(X - \beta_2)^3,$$

where $a_1 = \frac{f(\beta_2)}{(\beta_2 - \beta_1)^3}$, $a_2 = \frac{f(\beta_1)}{(\beta_1 - \beta_2)^3}$ and β_1, β_2 are the roots of the Hessian *H of f, where*

$$H(X) = (3ac - b^2)X^2 + (9ad - bc)X + (3bd - c^2).$$

The homogenization of the polynomial f is

$$\mathcal{F}(X_0, X_1) = aX_0^3 + bX_0^2X_1 + cX_0X_1^2 + dX_1^3.$$

The set of rational points of $\mathcal{F}$ is given by

$$\mathcal{F}(\mathbb{F}_q) = \{(x_0, x_1) : x_0, x_1 \in \mathbb{F}_q \text{ and } \mathcal{F}(x_0, x_1) = 0\}.$$

If $\mathcal{F}$ is an absolutely irreducible nonsingular projective curve in $\mathrm{PG}(1, q)$ of degree 3, then the number of $\mathbb{F}_q$-rational points of $\mathcal{F}$ is finite by Hasse-Weil theorem.

Theorem 49. *Let f be a cubic polynomial over $K = \mathbb{F}_q$ with $q = p^h$ and $p \neq 3$, such that $D_f \neq 0$. Let x_1, x_2, x_3 be the roots of f and β_1, β_2 the roots of its Hessian H, also $e = f(\beta_1)/f(\beta_2)$. Then these 5 roots are distinct and related by Table 2.1 where $\mathcal{F}_q'$, $\mathcal{F}_q''$, and $\mathcal{F}_q'''$ are respectively quadratic, cubic and sextic extensions of $\mathbb{F}_q$ and, K, K', K_1, K_2, K_3 are subsets of fields. Assume $q \equiv c \pmod 3$, β_1, $\beta_2 \in K$, $e = s^3$, $s \in K'$ and $x_i \in K_i$ for $i \in \{1, 2, 3\}$.*

2.9 Linear systems

c	K	K'	K_1	K_2	K_3
1	$\mathbb{F}_q$	$\mathbb{F}_q$	$\mathbb{F}_q$	$\mathbb{F}_q$	$\mathbb{F}_q$
1	$\mathbb{F}_q$	$\mathbb{F}''_q \setminus \mathbb{F}_q$	$\mathbb{F}''_q \setminus \mathbb{F}_q$	$\mathbb{F}''_q \setminus \mathbb{F}_q$	$\mathbb{F}''_q \setminus \mathbb{F}_q$
1	$\mathbb{F}'_q \setminus \mathbb{F}_q$	$\mathbb{F}'_q$	$\mathbb{F}_q$	$\mathbb{F}'_q \setminus \mathbb{F}_q$	$\mathbb{F}'_q \setminus \mathbb{F}_q$
-1	$\mathbb{F}_q$	$\mathbb{F}_q$	$\mathbb{F}_q$	$\mathbb{F}'_q \setminus \mathbb{F}_q$	$\mathbb{F}'_q \setminus \mathbb{F}_q$
-1	$\mathbb{F}'_q \setminus \mathbb{F}_q$	$\mathbb{F}'_q$	$\mathbb{F}_q$	$\mathbb{F}_q$	$\mathbb{F}_q$
-1	$\mathbb{F}'_q \setminus \mathbb{F}_q$	$\mathbb{F}'''_q \setminus \mathbb{F}'_q$	$\mathbb{F}''_q \setminus \mathbb{F}_q$	$\mathbb{F}''_q \setminus \mathbb{F}_q$	$\mathbb{F}''_q \setminus \mathbb{F}_q$

Figure 2.1 Table of fields of roots of cubic polynomial

Definition 50. A *form on* $\mathrm{PG}(n,q)$ is a homogeneous polynomial $f \in \mathbb{F}[X_0,...,X_n]$. The space of forms of degree d on $\mathrm{PG}(n,q)$ comprises a vector space W of dimension

$$\dim W = \binom{n+d}{d}.$$

Definition 51. A *hypersurface of degree* d in $\mathrm{PG}(n,q)$ is the zero locus

$$\mathcal{Z}(f) = \{P \in \mathrm{PG}(n,q) \mid f(P) = 0\}$$

of a form f on $\mathrm{PG}(n,q)$ of degree d.

Definition 52. A (k-dimensional) linear system of hypersurfaces of degree d is a (k-dimensional) subspace of $\mathrm{PG}(\binom{n+d}{d}-1,q)$. One-dimensional linear systems are called *pencils*.

Definition 53. A *cubic* $\mathbf{C}$ on $\mathrm{PG}(1,q)$ is the zero locus of a homogenous polynomial $f(X_0,X_1)$ of degree 3 in $\mathbb{F}_q[X_0,X_1]$.

The cubic forms on $\mathrm{PG}(1,q)$ form a four-dimensional vector space W, and subspaces of the projective space $\mathrm{PG}(3,q)$ are called *linear systems of cubics*.

Definition 54. The *pencil defined by two cubics* $\mathbf{C}_1 = \mathcal{Z}(f_1)$ and $\mathbf{C}_2 = \mathcal{Z}(f_2)$ is

$$\mathcal{P}(\mathbf{C}_1,\mathbf{C}_2) = \{\mathcal{Z}(\alpha f_1 + \beta f_2) \mid (\alpha,\beta) \in \mathrm{PG}(1,q)\}.$$

The intersection $\mathbf{C}_1 \cap \mathbf{C}_2$ is called a *base locus* and its points are called the *base points* of the pencil.

Let δ_3 denote the map from a cubic of $\mathrm{PG}(1,q)$ to the plane of $\mathrm{PG}(3,q)$. A cubic $\mathbf{C} = \mathcal{Z}(f)$ with

$$f = y_{30}X_0^3 + y_{21}X_0^2X_1 + y_{12}X_0X_1^2 + y_{03}X_1^3 \in \mathbb{F}_q[X_0,X_1]$$

in $\mathrm{PG}(1,q)$ is mapped by δ_3 to the plane $\delta_3(\mathbf{C}) = H[y_{30}, y_{21}, y_{12}, y_{03}]$ where $H[y_{30}, y_{21}, y_{12}, y_{03}]$ denotes the plane $\mathcal{Z}(y_{30}Y_0 + y_{21}Y_1 + y_{12}Y_2 + y_{03}Y_3)$. Conversely, every cubic in $\mathrm{PG}(1,q)$ is the preimage of a plane in $\mathrm{PG}(3,q)$. We can extend the definition of δ_3 from the set of cubics to the set of pencils of cubics. Given any set of cubics C in $\mathrm{PG}(1,q)$,

$$\delta_3(C) = \bigcap_{\mathbf{C}\in C} \delta_3(\mathbf{C}).$$

2.10 Fractional transformations

Definition 55. A rational morphisms on $\mathrm{PG}(1,q)$ of degree one over a field $\mathbb{F}_q$ is of the form $\alpha(x,y) = (ax+cy, bx+dy)$ where a, b, c, $d \in \mathbb{F}_q$ and $ad-bc \neq 0$. It is called a *Möbius* or *fractional transformation.*

The set of fractional transformations over a field $\mathbb{F}_q$ form a group with binary operation as composition. This group is isomorphic to the group $\mathrm{PGL}(2,q)$ and $\mathrm{PGL}(2,q)$ is a set of 2×2 invertible matrices with entries in $\mathbb{F}_q$ modulo scalar matrices. The group $\mathrm{PGL}(2,q)$ acts 3-transitively on the projective line $\mathrm{PG}(1,q)$ and it has $(q^2-1)(q^2-q)/(q-1) = q(q^2-1)$ elements.

For each $\alpha \in \mathrm{PGL}(2,q)$ there exists an $\tilde{\alpha} \in \mathrm{PGL}(4,q)$ such that $(\nu_3(P))^{\tilde{\alpha}} = \nu_3(P^{\alpha})$ for every $P \in \mathrm{PG}(1,q)$.

It gives a homomorphim:

$$\begin{array}{ccccc} \varphi : \mathrm{PGL}(2,q) & \to & \mathrm{PGL}(4,q) \\ \alpha & \mapsto & \tilde{\alpha} \end{array}$$

with $G = Im(\varphi)$, where the projectivity α induced by $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is mapped to the projectivity $\tilde{\alpha}$ induced by

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

Then $Im(\varphi) = G \cong \mathrm{PGL}(2,q)$. It gives an action of $\mathrm{PGL}(2,q)$ on the twisted cubic

$\mathcal{C}_3$ and this group fixes the twisted cubic $\mathcal{C}_3$. In this thesis, right group action is defined on row vectors.

2.11 Tensor products

In physics, engineering, and other areas, tensors are often defined to be multidimensional arrays. The problem of determining the complexity of matrix multiplication can be considered as the problem of decomposing a particular tensor (the matrix multiplication operator) according to its rank. Tensor decomposition has many application areas.

Definition 56. Let V and W be two vector spaces over the field $\mathbb{F}_q$, with $\text{rank}(V) = n$, $\text{rank}(W) = m$. The *tensor product* of V and W, denoted by $V \bigotimes W$ is the set of all linear combinations of elements of

$$\{v \otimes w \mid v \in V, w \in W\}$$

with coefficients in $\mathbb{F}_q$, where $\otimes$ is a binary operation satisfying

$$(v_1 + v_2) \otimes w = v_1 \otimes w + v_2 \otimes w,$$

$$v \otimes (w_1 + w_2) = v \otimes w_1 + v \otimes w_2,$$

$$(\lambda v) \otimes w = \lambda(v \otimes w),$$

$$v \otimes (\lambda w) = \lambda(v \otimes w),$$

for all v, v_1, $v_2 \in V$, w, w_1, $w_2 \in W$, and $\lambda \in \mathbb{F}_q$.

It follows that $V \bigotimes W$ is a vector space over $\mathbb{F}_q$ of rank mn.

Let $\{v_1, v_2, ..., v_n\}$ be a basis for V and $\{w_1, w_2, ..., w_m\}$ be a basis for W, then the set

$$\{v_i \otimes w_j \mid 1 \leq i \leq n, 1 \leq j \leq m\}$$

is a basis for $V \bigotimes W$.

Definition 57. If a vector $u \in V \bigotimes W$ can be written as $v \otimes w$, with $v \in V$ and $w \in W$, then u is called a *pure tensor* of $V \otimes W$.

Definition 58. Let V_1, V_2, ..., V_k be vector spaces. A function

$$f : V_1 \times V_2 \times ... \times V_k \to W$$

is *multilinear* if it is linear in each factor V_l. The space of such multilinear functions is denoted $V_1^* \otimes V_2^* \otimes ... \otimes V_k^* \otimes W$.

The space $S^k V^*$ is defined as the space of homogenous polynomials of degree k on V. Therefore, $S^3\mathbb{F}_q^2$ denotes the space of homogenous polynomials of degree 3 on $\mathbb{F}_q^2$. $S^3\mathbb{F}_q^2$ is a subspace of $\mathbb{F}_q^2 \otimes \mathbb{F}_q^2 \otimes \mathbb{F}_q^2$.

3. ON PLANAR ARCS OF SIZE $(q+3)/2$

The aim of this chapter to give the proof of the completeness of the arc $K = H \cup \{R\}$ of size $(q+3)/2$ where H is contained in a conic $\mathcal{C}_2$ and consists of one point on each of the secants of $\mathcal{C}_2$ through R.

3.1 Completeness proof

Lemma 59. *If $\mathcal{C}_2 = \mathcal{Z}(f)$ is a conic in $\mathrm{PG}(2,q)$, q odd, and $f(P) \in \square$ (resp. $\triangle$) for an external point P, then a point $Q \notin \mathcal{C}_2$ is external (resp. internal) if $f(Q) \in \square$ and internal (resp. external) if $f(Q) \in \triangle$.*

This lemma gives an algebraic way to distinguish between internal and external points of a conic in $\mathrm{PG}(2,q)$.

In our arc construction, we fix $\mathcal{C}_2$ to be the conic $\mathcal{C}_2 = \mathcal{Z}(XY - Z^2)$, and we define the set $H \subseteq \mathcal{C}_2$ as

$$H = \{(1, s^4, s^2) \mid s \in \mathbb{F}_q\}$$

and $H' = \mathcal{C}_2 \setminus H$. Our aim is to determine the set of H-free points in $\mathrm{PG}(2,q)$.

For the point

$$R(a,b,c) \notin \mathcal{C}_2$$

we define an involution τ_R on the points of $\mathcal{C}_2$ as follows. If $P(1,s^2,s)$ is a point of $\mathcal{C}_2$, then $\tau_R(P) = Q(1,t^2,t)$ is the second intersection of the line PR with $\mathcal{C}_2$. If PR is a tangent line, then we define $\tau_R(P) = P$. The collinearity of the points P, Q and R gives the equation

$$ast + b - c(s+t) = 0.$$

Therefore, $t = \frac{cs-b}{as-c}$. The stabiliser of $\mathcal{C}_2$ inside $\mathrm{PGL}(3,q)$ is isomorphic to $\mathrm{PGL}(2,q)$,

and under a suitable isomorphism this involution corresponds to the projectivity φ_R of $\mathrm{PG}(1,q)$ with matrix

$$M_R = \begin{pmatrix} c & -b \\ a & -c \end{pmatrix}.$$

Notice that $-c^2+ba \neq 0$, since R does not belong to the conic $\mathcal{C}_2$. Parameterising the projective line as the set $\mathbb{F}_q \cup \{\infty\}$, we consider ∞ as a non-square, i.e. $\infty \in \triangle$. We obtain $\varphi_R(s) = \frac{cs-b}{as-c}$ for $as-c \neq 0$, $\varphi_R(\infty) = ca^{-1}$ and $\varphi_R(ca^{-1}) = \infty$. This leads to the following characterisation of H-covered points.

Lemma 60. *The point R is H-covered if and only if there exist some $x \in \square$ for which $\varphi_R(x) \in \square$.*

Proof. Observing that ∞ corresponds to the point $(0,0,1)$ which does not belong to H, the proof follows from the above. □

First we focus on the case $abc \neq 0$.

Lemma 61. *If $q \geq 17$ and the point $R(a,b,c)$, where $abc \neq 0$, does not belong to $\mathcal{C}_2$ then $R(a,b,c)$ is H-covered.*

Proof. To the point $R(a,b,c)$ we associate the affine algebraic curve $\mathcal{F}_{a,b,c} = \mathcal{Z}(f)$ where

$$f(X,Y) = (cX^2-b) - \mu Y^2(aX^2-c) \text{ with } \mu \in \triangle.$$

We will show that the hypothesis that $R(a,b,c)$ is H-free leads to a contradiction with the number of points on the curve $\mathcal{F}_{a,b,c}$ whenever $q \geq 17$. We begin by proving that $\mathcal{F}_{a,b,c}$ satisfies the conditions of the irreducibility criterion given in Lemma 44.

(i) First we prove that $\mathcal{F}_{a,b,c}$ has no affine singular points. The partial derivatives of $f(X,Y)$ is

$$\frac{\partial f}{\partial X} = \frac{\partial(cX^2 - a\mu Y^2X^2)}{\partial X} = 2X(c-\mu aY^2),$$
$$\frac{\partial f}{\partial Y} = \frac{\partial(c\mu Y^2 - \mu aX^2Y^2)}{\partial Y} = 2\mu Y(c-aX^2).$$

Setting the partial derivatives of $f(X,Y)$ evaluated at an affine point (x,y) equal to zero, we have

$$\frac{\partial f}{\partial X}(x,y) = 0 \quad \Rightarrow \quad x = 0 \text{ or } c = \mu a y^2 \Rightarrow y^2 = \mu^{-1}a^{-1}c, \text{ and}$$
$$\frac{\partial f}{\partial Y}(x,y) = 0 \quad \Rightarrow \quad y = 0 \text{ or } c = ax^2 \Rightarrow x^2 = \alpha^{-1}c.$$

If in addition (x,y) lies on $\mathcal{F}_{a,b,c}$ we are left with the following cases.

12.1 If $x = 0$, $y = 0$, then $f(x,y) = -b = 0$, contradicting $b \neq 0$.

12.2 If $x = 0$ and $c = ax^2$, then $c = 0$, contradicting $c \neq 0$.

12.3 If $c = \mu a y^2$ and $y = 0$, then again $c = 0$. But $c \neq 0$.

12.4 If $c = \mu a y^2$ and $c = ax^2$, then $\mu y^2 = x^2$ again a contradiction.

So $f(x,y)$ has no affine singularities.

(ii) Next we show that the ideal points $X_\infty(1,0,0)$ and $Y_\infty(0,1,0)$ of the projective closure $\mathcal{F}$ of $\mathcal{F}_{a,b,c}$ are ordinary singularities of multiplicity 2. The curve $\mathcal{F}$ is equal to the zero locus of F where

$$F(X,Y,Z) = (cX^2Z^2 - bZ^4) - \mu Y^2(aX^2 - cZ^2). \tag{3.1.1}$$

Calculating the partial derivatives of F, we obtain

$$\begin{aligned} \frac{\partial F}{\partial X} &= 2X(cZ^2 - a\mu Y^2), \ \frac{\partial F}{\partial Y} = -2\mu Y(aX^2 - cZ^2), \\ \frac{\partial F}{\partial Z} &= 2Z(cX^2 - 2bZ^2 + \mu c Y^2). \end{aligned}$$

It is straightforward to verify that the points X_∞ and Y_∞ are singular points of $\mathcal{F}$. Also the multiplicity of the point X_∞ on $\mathcal{F}$ is 2, since the multiplicity of $t = 0$ in $F(1,t,0) = -\mu a t^2$ is 2, and similarly for Y_∞. By Bézout's theorem X_∞ and Y_∞ are the only points of $\mathcal{F}$ on the line $Z = 0$.

Now, the tangent lines through X_∞ have an equation $dY - eZ = 0$, and the only line with $d = 0$ is $Z = 0$. Since the points X_∞, $Y_\infty \in \mathcal{F}$, the line with equation $Z = 0$ is not a tangent line of $\mathcal{F}$. So w.l.o.g. we may take $d = 1$. If $f(x,e)$ has no solution for $x \in \overline{\mathbb{F}}_q$, then the line $Y = e$ is a tangent line of $\mathcal{F}$. Substituting the point (x,e) into the equation of the curve, we obtain

$$f(x,e) = (cx^2 - b) - \mu e^2(ax^2 - c) = x^2(c - \mu a e^2) - b + \mu c e^2 = 0.$$

If $c = \mu e^2 a$ and $f(x,e) = 0$, then $f(x,e) = -ba + c^2 = 0$, contradicting the fact that $R(a,b,c)$ does not belong to the conic $\mathcal{C}_2$. If $c \neq \mu e^2 a$, then the above equation has a solution for $x \in \overline{\mathbb{F}}_q$. Hence the tangents of $\mathcal{F}$ at X_∞ are exactly the lines

$$Y = e, \text{ where } e^2 = \mu^{-1}a^{-1}c.$$

To determine whether the polynomial $t(e) = \mu e^2 a - c$ has a multiple root or not, we compute its derivative and obtain $2\mu ea = 0$. Substituting $e = 0$ into the equation $t(e)$ gives $t(e) = -c = 0$. This is a contradiction. So the polynomial $t(e)$ has no multiple roots. This shows that there are 2 distinct tangents at X_∞ and therefore X_∞ is an ordinary singular point with multiplicity 2. Similarly one verifies that also the point Y_∞ is an ordinary singular point with multiplicity 2.

(iii) We show that the intersection multiplicity of $\mathcal{F}$ and a tangent line $\ell : Y = e$ at the point X_∞ is 4. From the definition of intersection multiplicity for $X_\infty(1,0,0)$ and $V(0,e,1)$, where $e^2 = \mu^{-1}a^{-1}c$, we obtain that

$$h(t) \quad = \quad F((1,0,0) + t(0,e,1)) = F(1,et,t) = t^4(-b + \mu ce^2).$$

The multiplictiy of the root $t = 0$, and therefore, the intersection multiplicity of the curve $\mathcal{F}$ and the tangent line $Y = e$, in which, $e^2 = \mu^{-1}a^{-1}c$, is 4.

(iv) Finally we show that $\mathcal{F}$ has no linear component through X_∞. Assume, by way of contradiction, that the curve $\mathcal{F}$ has a linear component $\ell = \mathcal{Z}(h)$ with $h \mid F$ through X_∞. Note that, the linear component ℓ can not be $\mathcal{Z}(h)$ where $h^2 \mid F$, since $\mathcal{F}$ has no affine singular points. Define a polynomial $f_1 \neq 0$ such that $f = hf_1$, so $\deg(f_1) = 3$. Then the linear component ℓ intersects $\mathcal{Z}(f_1)$ in 3 points over $\overline{\mathbb{F}}_q$, and all these points are singular points. This is a contradiction with (i) and (ii).

It follows from Lemma 44 that $\mathcal{F}$ is absolutely irreducible. Hence, we can use the Hasse-Weil theorem

$$|N - q + 1| \leq 2g\sqrt{q} \;\Rightarrow\; q + 1 - 2g\sqrt{q} \leq N \leq q + 1 + 2g\sqrt{q}$$

where g denotes the genus of the curve $\mathcal{F}$. A projective irreducible curve with no affine singularities has genus

$$g = \binom{d-1}{2} - \sum_{P \in Sing(\mathcal{F})} \binom{m_P}{2}$$

where d denotes the degree of the curve and m_p denotes the multiplicity of the singular point P of the projective curve. For the curve $\mathcal{F}$, we have 2 singular points X_∞ and Y_∞ of multiplicities 2. Therefore $g = 1$.

Assume that $R(a,b,c)$ is H-free. Fix $\mu \in \triangle$. For each $x^2 \in \square$, we have

$$\frac{cx^2 - b}{ax^2 - c} = \mu y^2 \text{ for some } y \in \mathbb{F}_q.$$

We will show that this leads to a contradiction unless $q < 17$, by further analysing the curve $\mathcal{F} = \mathcal{Z}(F)$ as defined in 3.1.1.

(i) Clearly X_∞ and Y_∞ are the only two points of the form $(x,y,0)$ on $\mathcal{F} = \mathcal{Z}(F)$, because

$$F(x,y,0) = -\mu y^2(ax^2) = 0 \quad \Rightarrow \quad x = 0 \text{ or } y = 0.$$

(ii) A point of the form $(x,0,1)$, respectively of the form $(0,y,1)$, lies on the curve $\mathcal{F}$ if and only if

$$F(x,0,1) = cx^2 - b = 0 \text{ and } F(0,y,1) = -b + \mu y^2 c = 0.$$

It gives $x^2 = c^{-1}b$, and $y^2 = \mu^{-1}c^{-1}b$. Therefore, the points of these forms can not lie on the curve $\mathcal{F}$ at the same time. It follows that the curve $\mathcal{F}$ has 2 points of the form $(x,0,1)$ or $(0,y,1)$.

(iii) If the point $(x,y,1)$ lies on the curve $\mathcal{F}$, then

$$F(x,y,1) = (cx^2 - b) - \mu y^2(ax^2 - c) = 0$$

Hence $\mu y^2(ax^2 - c) = cx^2 - b$. By the hypothesis, for each $x^2 \notin \{\frac{c}{a}, \frac{b}{c}\}$ we obtain two such points on $\mathcal{F}$. If $x^2 = \frac{c}{a}$, then $c^2 - ba = 0$, contradicting the fact that $R(a,b,c)$ is not on the conic $\mathcal{C}_2 = \mathcal{Z}(XY - Z^2)$. If $x^2 \neq \frac{c}{a}$ but $x^2 = \frac{b}{c}$ then $y = 0$ and this case is already accounted for in (ii) above. So excluding the previous cases (i) and (ii) we obtain at least $2(q-5)$ points on the curve $\mathcal{F}$ of the form $(x,y,1)$ with $x,y \neq 0$.

We conclude that the number of $\mathbb{F}_q$-rational points on the curve $\mathcal{F}$ is at least $2q-6$. The Hasse-Weil bound gives $2q - 6 \leq q + 1 + 2\sqrt{q}$, which implies $q \leq 13$. □

If $abc = 0$, then we have the following cases.

Remark 62. If $c = 0$, then $ab \neq 0$ and φ_R sends x to $y = -(ba^{-1})x^{-1}$. If $ba^{-1} \in \square$, then the point $R(a,b,0)$ is H-free for $q \equiv 3 \pmod 4$. Similarly, if $ba^{-1} \in \triangle$, then the point $R(a,b,0)$ is H-free for $q \equiv 1 \pmod 4$.

Remark 63. If both b and a are 0, then φ_R sends $x \in \square$ to $\varphi_R(x) \in \square$ for $q \equiv 1 \pmod 4$ and it sends $x \in \triangle$ to $\varphi_R(x) \in \square$ for $q \equiv 3 \pmod 4$. Therefore, if $q \equiv 1 \pmod 4$, then $R(0,0,1)$ is H-covered, and if $q \equiv 3 \pmod 4$, then the point $R(0,0,1)$ is H-free.

Remark 64. Next consider the cases $b = 0$, $ac \neq 0$ and $a = 0$, $bc \neq 0$.

Lemma 65. *If $q \geq 17$, then the points $U(0,b,c)$ and $V(a,0,c)$ are H-covered for*

$bc \neq 0$ *and* $ac \neq 0$.

Proof. Assume that the point $U(0,b,c)$ is H-free. Then it can not be on chords of H which consist of the lines

$$\ell_k : Y = \alpha^{2k} Z, \text{ where } k = 1,2,..,(q-1)/2$$

which pass through the points $(1,0,0)$ and $(1,\alpha^{4k},\alpha^{2k})$, and

$$\ell_{ij} : Y = (\alpha^{2i} + \alpha^{2j})Z - (\alpha^{2j})(\alpha^{2i})X, \text{ where } i,j = 1,2,..,(q-1)/2,\ i \neq j$$

which pass through the points $(1,\alpha^{4i},\alpha^{2i})$ and $(1,\alpha^{4j},\alpha^{2j})$, where $\mathbb{F}_q^* = \langle\alpha\rangle$. Therefore, for the point $U(0,b,c)$, this implies

$$b \neq \alpha^{2k} c \text{ and } bc^{-1} \neq \alpha^{2i} + \alpha^{2j} \text{ where } i,j,k = 1,..,(q-1)/2.$$

This contradicts the fact that a non-square element bc^{-1} in $\mathbb{F}_q$ can be written as the sum of two nonzero square elements. We conclude that the point $U(0,b,c)$ is H-covered.

From the above it also follows that the point $V(a,0,c)$ lies on the chord ℓ_{ij} if and only if

$$(\alpha^{2i} + \alpha^{2j})c - (\alpha^{2j})(\alpha^{2i})a = 0, \text{ where } i,j = 1,2,..,(q-1)/2,\ i \neq j.$$

For $\alpha^{2i} = X$, $\alpha^{2j} = Y$ and $a^{-1}c = \mu'$, we obtain the curve $\mathcal{Z}(f')$ with

$$f'(X,Y) = X^2Y^2 - \mu'(X^2 + Y^2) = 0 \text{ with } \mu' \neq 0.$$

Therefore the point $V(a,0,c)$ is H-covered if the curve $\mathcal{Z}(f')$ has points with coordinates in $\mathbb{F}_q$. Taking the partial derivatives evaluated at an affine point (x,y), we obtain

$$\frac{\partial f'}{\partial X} = 2xy^2 - 2\mu' x = 2x(y^2 - \mu'),$$
$$\frac{\partial f'}{\partial Y} = 2yx^2 - 2\mu' y = 2y(x^2 - \mu').$$

Then $2x(y^2 - \mu') = 0$ and $2y(x^2 - \mu') = 0$ imply that for $x = 0$, $y = 0$ or $x^2 = \mu'$, and for $y^2 = \mu'$, $y = 0$ or $x^2 = \mu'$. Since $\mu' \neq 0$, the partial derivatives are zero at the point $(0,0)$. Evaluating $f'(X,Y)$ at $(0,0)$, we find that $(0,0)$ is an affine singular point of the curve $\mathcal{Z}(f'(X,Y))$.

The projective closure of the curve $\mathcal{Z}(f')$ is $\mathcal{F} = \mathcal{Z}(F')$ where

$$F'(X,Y,Z) = X^2Y^2 - \mu' Z^2(X^2+Y^2).$$

One easily verifies that the points $(0,0,1)$, $(0,1,0)$ and $(1,0,0)$ are the singular points of $\mathcal{F}$ and the multiplicity of the point $(1,0,0)$ on $\mathcal{F}$ is 2, since the multiplicity of $t=0$ in $\mathcal{F}(1,t,0) = t^2$ is 2. Moreover, since the curve is symmetric for X and Y coordinates, it follows that the point $(0,1,0)$ has multiplicity 2. Similarly, one verifies that the point $(0,0,1)$ has multiplicity 2 on the curve $\mathcal{F}$.

Now we want to prove that the curve $\mathcal{F}$ is absolutely irreducible. Since the degree of the curve is 4, the degrees of the irreducible factors of the polynomial defining the curve are either 1 and 3 or 2 and 2.

If the degrees of the irreducible factors are 1 and 3, then the curve $\mathcal{F}$ has a linear component. Define a polynomial $f_1 \neq 0$ and $f_2 \neq 0$ such that $\mathcal{F} = f_1 f_2$ with $\deg(f_1) = 1$ and $\deg(f_2) = 3$. Then $\mathcal{Z}(f_1)$ intersects $\mathcal{Z}(f_2)$ in 3 points over $\overline{\mathbb{F}}_q$, and all these points are singular points. Lines through the point $(0,0,1)$ have equation $dX - eY$. Since $\mathcal{Z}(X)$ is not a linear component of the curve $\mathcal{F}$, we may assume that $e = 1$, and consider the lines $\mathcal{Z}(Y - dX)$ intersecting the curve $\mathcal{Z}(f')$. Since

$$f'(x,dx) = d^2x^4 - \mu'(x^2 + d^2x^2) = x^2(d^2x^2 - \mu'(1+d^2))$$

is not zero for all $x \in \mathbb{F}_q$, the curve $\mathcal{F}$ has no linear component of the form $\mathcal{Z}(Y - dX)$. Now, assume that $P = (1,0,0)$, and $\mathcal{Z}(f_1)$ is a line through the point P. The lines passing through the point P have equation $dY - eZ = 0$. Since $\mathcal{Z}(Z)$ is not a linear component of the curve $\mathcal{F}$, we may assume that $d = 1$ and evaluating $f'(X,Y)$ at (x,e) gives

$$f'(x,e) = x^2e^2 - \mu'(x^2+e^2) = x^2(e^2 - \mu') - \mu' e^2.$$

Since $f'(x,e)$ is not zero for all $x \in \mathbb{F}_q$, $\mathcal{F}$ has no linear component of the form $\mathcal{Z}(Y - eZ)$. The curve $\mathcal{F}$ is symmetric with coordinates X and Y. Hence, the curve $\mathcal{F}$ has no component of the form $\mathcal{Z}(X - fZ)$, either. This shows that the curve $\mathcal{F}$ has no linear component.

If we assume that the curve $\mathcal{F}$ has two irreducible factors of degrees 2, then there are 2 polynomials $f_1 \neq 0$ and $f_2 \neq 0$ such that $\mathcal{F} = f_1 f_2$ with $\deg(f_1) = 2$ and $\deg(f_2) = 2$. The conic $\mathcal{Z}(f_1)$ intersects with the conic $\mathcal{Z}(f_2)$ in 3 points, since there are 3 singular points on the curve $\mathcal{F}$. It follows from the classification of pencils of conics in $\mathrm{PG}(3,q)$, q odd, that the pencil $\mathcal{P}(\mathcal{Z}(f_1), \mathcal{Z}(f_2))$ is equivalent to the pencil of

type o_{13}, i.e. $\mathcal{P}(2XY, Y^2 - Z^2)$, corresponding to the second column of Table 5 of (Lavrauw & Popiel, 2020), since this is the only pencil of conics with 3 base points. The points $(1,0,0)$, $(0,1,1)$ and $(0,-1,1)$ are the base points of the pencil $\mathcal{P}(2XY, Y^2 - Z^2)$. After a suitable coordinate transformation, we may therefore assume that $\mathcal{Z}(f_1)$ corresponds to $C_1 = \mathcal{Z}(2XY + Y^2 - Z^2)$ and $\mathcal{Z}(f_2)$ corresponds to $C_2 = \mathcal{Z}(2\gamma XY + Y^2 - Z^2)$ for some $\gamma \in \mathbb{F}_q \setminus \{0,1\}$. The tangent lines of these nondegenerate conics at (x_0, y_0, z_0) are

$$\mathcal{T}_{C_1} : 2y_0X + (2x_0 + 2y_0)Y - 2z_0Z = 0, \text{ and}$$

$$\mathcal{T}_{C_2} : 2\gamma y_0X + (2\gamma x_0 + 2y_0)Y - 2z_0Z = 0.$$

Considering the tangent lines of the conics C_1 and C_2 at the base points, we find that $\mathcal{Z}(Y)$ is a common tangent line of the conics at $(1,0,0)$ and there are 2 different tangent lines at each of the points $(0,1,1)$ and $(0,-1,1)$.

Now we determine the tangent lines of the curve

$$\mathcal{F} : X^2Y^2 - \mu' Z^2(X^2 + Y^2) = 0$$

at the singular points $(0,0,1)$, $(1,0,0)$ and $(0,1,0)$. For the point $(0,0,1)$, we consider the affine curve $\mathcal{Z}(f')$, with

$$f'(X,Y) = X^2Y^2 - \mu'(X^2 + Y^2) = f'_4(X,Y) + f'_2(X,Y)$$

where f'_i is a form in $\mathbb{F}_q[X,Y]$ of degree i. Since $f'_2(X,Y) = -\mu'(X^2 + Y^2) = -\mu'(X + Y)^2$ if and only if $\mathbb{F}_q$ has even characteristic, the curve $\mathcal{F}$ has 2 distinct tangent lines at $(0,0,1)$. Similarly, at the point $(1,0,0)$, we have the affine curve $\mathcal{Z}(h')$, with

$$h'(Y,Z) = Y^2 - \mu'(Z^2 + Y^2Z^2) = -\mu' Y^2Z^2 + Y^2 - \mu' Z^2$$

where $h'_2(Y,Z) = Y^2 - \mu' Z^2$. Since q is odd, the curve $\mathcal{F}$ has 2 distinct tangent lines at $(1,0,0)$. Similarly, the curve $\mathcal{F}$ has 2 distinct tangent lines at the point $(0,1,0)$, since it is symmetric according to variables X and Y. By comparison to the tangent lines at the singular points of the curve $C_1 \cup C_2$ we may conclude that the curve $\mathcal{F}$ has no component of degree 2.

It follows that the curve $\mathcal{F}$ is absolutely irreducible and the genus of $g = \binom{3}{2} - \sum_{P \in Sing(\mathcal{F})} \binom{2}{2} = 0$. The curve $\mathcal{F}$ with $g = 0$ is a rational curve. Since there are $q+1$ points on the curve $\mathcal{F}$, there exist a chord ℓ_{ij} through $V(a,0,c)$. Therefore, the point $V(a,0,c)$ is H-covered. □

As we have seen in case 62, there is always a point with coordinates $(a,b,0)$ which is H-free. To get a complete arc, we now define the point $R_0(a_0,b_0,0)$ where $a_0b_0 \in \square$ for $q \equiv 3 \pmod 4$ and $a_0b_0 \in \triangle$ for $q \equiv 1 \pmod 4$. Consequently, the point R_0 is an internal point to $\mathcal{C}_2$. Let the arc K be defined as $H \cup \{R_0\}$.

Lemma 66. *If $q \geq 17$ then each point $P' \in H' = \mathcal{C}_2 \setminus H$ is K-covered.*

Proof. Each secant line through R_0 intersects the conic $\mathcal{C}_2$ in points $P \in H$ and $P' \in H'$, since the point R_0 is not H-covered. But the arc K contains both H and R_0, so the points $P' \in H'$ are K-covered. □

Lemma 67. *If $q \equiv 1 \pmod 4$, then the point $(0,0,1)$ is H-covered and if $q \equiv 3 \pmod 4$, then the point $(0,0,1)$ is K-covered, if $\frac{b_0}{a_0} \in \{u^4 : u \in \mathbb{F}_q \setminus \{0\}\}$.*

Proof. The proof of the first part of the lemma follows from Lemma 63. For the second part of the lemma, we need to show that there is a chord of K through the point $(0,0,1)$. The line passing through the points $(1,\alpha^{4k},\alpha^{2k})$ and R_0 contains $(0,0,1)$ if and only if $b_0a_0^{-1} = \alpha^{4k}$.

□

Theorem 68. *If $q \geq 17$ and $R_0(a_0,b_0,0)$, with $a_0b_0 \in \triangle$ for $q \equiv 1 \pmod 4$ and $\frac{b_0}{a_0} = u^4$ for some $u \in \mathbb{F}_q \setminus \{0\}$ for $q \equiv 3 \pmod 4$, then the arc $K = H \cup \{R_0\}$ is complete.*

Proof. By Lemma 61 the point $R(a,b,c) \notin \mathcal{C}_2$, where $abc \neq 0$, is H-covered. The points $U(0,b,c)$ and $V(a,0,c)$, where $bc \neq 0$, $ac \neq 0$ are H-covered by Lemma 65. The point $P' \in H'$ is K-covered by Lemma 66. If $q \equiv 1 \pmod 4$, then the point $(0,0,1)$ is H-covered, and if $q \equiv 3 \pmod 4$, then the point $(0,0,1)$ is K-covered by Lemma 67. □

3.2 On Pellegrino's condition

The complete arc $K = H \cup \{R\}$ of size $(q+3)/2$ contains $(q+1)/2$ points from the conic $\mathcal{C}_2$ and the internal H-free points are on the line $Z = 0$. But the line $Z = 0$ is not an external line to the conic $\mathcal{C}_2$. Hence, we have the following corollary.

Corollary 69. *For $q \geq 17$, if $q \equiv 1 \pmod 4$, then the only H-free points are internal points on the line $Z = 0$ and if $q \equiv 3 \pmod 4$, then the H-free points are internal points on the line $Z = 0$ and the point $(0,0,1)$.*

Remark 70. Pellegrino proved that if H is a set of $(q+1)/2$ points on a conic $\mathcal{C}_2$, satisfying the condition that there exists an external line ℓ to $\mathcal{C}_2$ containing two internal H-free points P_1, P_2, then for $q > 13$:

(i) when $q \equiv 3 \pmod 4$, the arc $K = H \cup \{P_1, P_2\}$ is complete;

(ii) when $q \equiv 1 \pmod 4$, the arcs $K = H \cup \{P_1, P_2\}$ and $K' = H \cup \{P\}$ are complete where P is the pole of ℓ with respect to a conic $\mathcal{C}_2$.

However, Corollory 69 shows that Pellegrino's condition from (Pellegrino, 1993b), precisely, that there exists an external line containing two internal H-free points is not always satisfied. This gives a counterexample to the claim in (Hirschfeld, 1993).

3.3 Final comments

Using the same construction, for small values of q computations using the GAP (les courbes algébriques et les variétés qui s'en déduisent, 2018)-package and FinInG (Bamberg, Betten, Cara, De Beule, Lavrauw & Neunhöffer, 2018) show that if $q = 9$, then we should add 3 internal H-free points to the set H to obtain a complete arc K from the set H. Then $|K| = (q+7)/2 = 8$, and it is known that there is a unique such complete arc in $\mathrm{PG}(2,9)$. If $q = 11$ or 13, then we should add 2 internal H-free points to the set H giving the complete arcs of size either 8 or 9. For $q = 9$, 11 and 13, the complete arc examples are given below.

Example 71. If $q = 9 \equiv 1 \pmod 4$, then $\mathbb{F}_9 = \{0, 1, 2, \beta, 1+\beta, 2+\beta, 2\beta, 1+2\beta, 2+2\beta\}$ where β is a root of the irreducible polynomial x^2+1. Let us say $\beta + 1 = \alpha$, then α is a primitive element of $\mathbb{F}_9^*$. Take

$$H = \{(1,0,0), (1,\alpha^8,\alpha^8), (1,\alpha^8,\alpha^4), (1,\alpha^4,\alpha^2), (1,\alpha^4,\alpha^6)\}.$$

As an additional internal H-free point pick $R = (1,\alpha^3,0)$, then

$$K = \{(1,0,0), (1,\alpha^8,\alpha^8), (1,\alpha^8,\alpha^4), (1,\alpha^4,\alpha^2), (1,\alpha^4,\alpha^6), (1,\alpha^3,0), (1,\alpha^3,\alpha^4), (1,0,\alpha^2)\}$$

is a complete arc of size 8.

Example 72. Assume that $q = 11 \equiv 3 \pmod 4$ and $\mathbb{F}_{11}^* = \langle 2 \rangle$. Take

$$H = \{(1,0,0),(1,5,4),(1,3,5),(1,4,9),(1,9,3),(1,1,1)\}.$$

Let us select the point $(1,1,0)$ as the internal H-free point. One can find

$$K = \{(1,0,0),(1,5,4),(1,3,5),(1,4,9),(1,9,3),(1,1,1),(1,1,0),(1,2,5)\}$$

is a complete arc of size 8.

Example 73. Assume that $q = 13 \equiv 1 \pmod 4$ and $\mathbb{F}_{13}^* = \langle 2 \rangle$. Take

$$H = \{(1,0,0),(1,4,2),(1,12,5),(1,10,6),(1,10,7),(1,12,8),(1,4,11)\}.$$

One can select the point $(1,2,0)$ as the internal H-free point. Then the arc

$$K = \{(1,0,0),(1,4,2),(1,12,5),(1,10,6),(1,10,7),(1,12,8),(1,4,11),(1,2,0),(1,2,12)\}$$

is a complete arc of size 9.

In summary, if the point R is an external point of $\mathcal{C}_2$ and roughly half of the points of the non-degenerate conic is taken, then there are complete arcs of sizes at least $(q+5)/2$ and at most $(q+11)/2$, and if the point R is an internal point of $\mathcal{C}_2$, then there are complete arcs of sizes at least $(q+3)/2$ and at most $(q+5)/2$.

4. ON PENCILS OF CUBICS ON THE PROJECTIVE LINE OVER FINITE FIELDS OF CHARACTERISTIC > 3

4.1 Some properties of the twisted cubic $\mathcal{C}$

For $n \geq 1$, the set of $\mathbb{F}_{q^n}$-rational points of $\mathcal{C}_3$ in $\mathrm{PG}(3, q^n)$ is denoted by $\mathcal{C}_3(\mathbb{F}_q^n)$. Let $P(t)$ denote the point with coordinates $(1, t, t^2, t^3)$ of $\mathcal{C}_3(\mathbb{F}_{q^n})$, for $t \in \mathbb{F}_{q^n}$, and $P(\infty)$ the point of $\mathcal{C}_3$ with coordinates $(0, 0, 0, 1)$.

Definition 74. A line ℓ of $\mathrm{PG}(3, q)$ is a *chord* of $\mathcal{C}_3$ if it is a line joining either two distinct points of $\mathcal{C}_3$, two coinciding points, or a pair of conjugate points (P, P^q) of $\mathcal{C}_3(\mathbb{F}_{q^2}) \setminus \mathcal{C}_3(\mathbb{F}_q)$. The line ℓ is, respectively, called a *real chord*, a *tangent* or an *imaginary chord* of $\mathcal{C}_3$. A line ℓ of $\mathrm{PG}(3, q)$ is called a *unisecant* if it is a line meeting $\mathcal{C}_3$ in one point and ℓ is called an *external* if it is line disjoint from $\mathcal{C}_3$.

A *regulus* in $\mathrm{PG}(3, q)$ 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.

The chord $\ell = \langle P(t_1), P(t_2) \rangle$, $t_1, t_2 \notin \{0, \infty\}$, is determined by the equations

$$\begin{cases} t_1 t_2 Y_1 - (t_1 + t_2) Y_2 + Y_3 = 0, \\ -t_1 t_2 Y_0 + (t_1 + t_2) Y_1 - Y_2 = 0. \end{cases}$$

Moreover, the tangent line ℓ of $\mathcal{C}_3$ at the point $P(t)$, $t \notin \{0, \infty\}$, is determined by the equations

$$\begin{cases} t^2 Y_1 - 2t Y_2 + Y_3 = 0, \\ -t^2 Y_0 + 2t Y_1 - Y_2 = 0, \end{cases}$$

while the tangent line of $\mathcal{C}_3$ at the point $P(0)$ is $\mathcal{Z}(Y_2, Y_3)$ and the tangent line of $\mathcal{C}_3$ at $P(\infty)$ is $\mathcal{Z}(Y_0, Y_1)$.

Lemma 75. *If $\mathcal{C}_3$ is a twisted cubic in* $\mathrm{PG}(3,q)$*, then*

(i) no two chords of $\mathcal{C}_3$ meet off $\mathcal{C}_3$;

(ii) every point off $\mathcal{C}_3$ lies on exactly one chord of $\mathcal{C}_3$.

Proof. (i) If two chords of $\mathcal{C}_3$ can meet off $\mathcal{C}_3$, counted with multiplicity, then they would span a plane intersecting $\mathcal{C}_3$ in 4 points. The twisted cubic in $\mathrm{PG}(3,q)$ is an arc and it can not contain 4 points in a plane.

(ii) A real chord contains $(q-1)$, a tangent has q and an imaginary chord has $(q+1)$ points off $\mathcal{C}_3$. There are $\binom{q+1}{2}$ real chords, $(q+1)$ tangents and $\binom{q}{2}$ imaginary chords. Then total number of points is

$$(q-1)\frac{q(q+1)}{2} + q(q+1) + (q+1)\frac{q^2-q}{2} + (q+1) = (q+1)(q^2+1) = |\mathrm{PG}(3,q)|.$$

□

Definition 76. A plane Π intersecting the twisted cubic in three coinciding points P is called the *osculating plane* at P.

The osculating plane at $P(t)$ is denoted by $\Pi(t)$ and has equation

$$\Pi(t) : -t^3Y_0 + 3t^2Y_1 - 3tY_2 + Y_3 = 0.$$

Definition 77. 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 $\mathcal{C}_3(\mathbb{F}_{q^2}) \setminus \mathcal{C}_3(\mathbb{F}_q)$.

4.2 The classification of points and planes in $\mathrm{PG}(3,q)$

Consider a point $P_1(y_0, y_1, y_2, y_3)$ of $\mathrm{PG}(3,q)$.

$$-t^3y_0 + 3t^2y_1 - 3ty_2 + y_3 = 0.$$

Through P_1, there are 3 osculating planes $\Pi(t_1)$, $\Pi(t_2)$ and $\Pi(t_3)$ of $\mathcal{C}$ with

$$[-y_0 : 3y_1 : -3y_2 : y_3] = [1 : -(t_1+t_2+t_3) : (t_1t_2+t_1t_3+t_2t_3) : -t_1t_2t_3].$$

The plane Π' joining the points $P(t_1)$, $P(t_2)$, $P(t_3)$ is

$$\Pi' : y_3Y_0 - 3y_2Y_1 + 3y_1Y_2 - y_0Y_3 = 0.$$

The map σ mapping the point with coordinates (y_0, y_1, y_2, y_3) to the plane with dual coordinates $[-y_3, 3y_2, -3y_1, y_0]$ is a symplectic or null polarity of $\mathrm{PG}(3,q)$, and the plane P^σ is called the *polar plane* of the point P. Note that for a point $P(t)$ of $\mathcal{C}_3$, the polar plane of $P(t)$ is the osculating plane $\Pi(t)$ of $\mathcal{C}_3$ at $P(t)$. The polar plane of a point P not on $\mathcal{C}_3$ is the span of the contact points of the three osculating planes through P.

The osculating planes of $\mathcal{C}_3$ form the *osculating developable* Γ to $\mathcal{C}_3$. The symplectic polarity σ sends the chords of the twisted cubic $\mathcal{C}_3$ to the *axes* of Γ. For $q = 3$, Γ is a *pencil of planes*. For $q = 2$, the tangents form a regulus lying on $\mathcal{Z}(Y_0Y_3 + Y_1Y_2)$; for $q \neq 2$, no four of the tangents lie in a regulus.

A point P lies on a line ℓ in $\mathrm{PG}(3,q)$ if and only if ℓ^σ is contained in the plane P^σ where σ is the polarity in $\mathrm{PG}(3,q)$ defined as above. For a line ℓ, if $\ell^\sigma = \ell$, then ℓ is called *self polar*.

Lemma 78. *The self polar lines which pass through a given point P of $\mathcal{C}_3$ are all the lines through P in the polar plane P^σ of P.*

Proof. Let $\ell = \langle P, Q\rangle$ be a line in P^σ, passing through P. Since $Q \in P^\sigma$, $P \in Q^\sigma$. Then Q^σ contains both P and Q. Hence, $\ell = \ell^\sigma = P^\sigma \cap Q^\sigma$. Conversely, suppose that ℓ is a self polar line through P. Then $\ell = \ell^\sigma = P^\sigma \cap R^\sigma$ where R is a distinct point from P of ℓ. It follows $\ell \subset P^\sigma$. □

For a point $P \in \mathcal{C}_3$, there is a unique tangent line ℓ through P in the osculating plane P^σ. By Lemma 78, the tangent line ℓ is a self polar line through P. Also, a unisecant line in the osculating plane P^σ which passes through the point $P \in \mathcal{C}_3$ is a self polar line. The following lemma describes the polar of the intersection of two osculating planes.

Lemma 79. *If ℓ is a line contained in the intersection of two osculating planes Π_1, Π_2 where Π_1 is an osculating plane at P_1 of $\mathcal{C}_3$ and Π_2 is an osculating plane at P_2 of $\mathcal{C}_3$, then ℓ^σ is a chord through points P_1, P_2 of the twisted cubic $\mathcal{C}_3$.*

Proof. Let $\ell = \langle Q_1, Q_2 \rangle$ be a line contained in the intersection of osculating planes Π_1, Π_2. Since $\ell \subset \Pi_1$ and $\ell \subset \Pi_2$, $\Pi_1^\sigma \in \ell^\sigma$ and $\Pi_2^\sigma \in \ell^\sigma$. That is $P_1 \in \ell^\sigma$ and $P_2 \in \ell^\sigma$. Therefore, $\ell^\sigma = \langle P_1, P_2 \rangle$ is a chord through points P_1, P_2 of the twisted cubic $\mathcal{C}_3$. □

The G-orbits on points and planes of $\mathrm{PG}(3,q)$ are well understood. There are 5 G-orbits of planes in $\mathrm{PG}(3,q)$.

$\mathcal{H}_1$. Osculating planes of $\mathcal{C}_3$, $\mathcal{H}_1$ has size $q+1$.

$\mathcal{H}_2$. Planes with exactly two points of $\mathcal{C}_3$, $\mathcal{H}_2$ has size $q(q+1)$

$\mathcal{H}_3$. Planes with three points of $\mathcal{C}_3$, $\mathcal{H}_3$ has size $q(q^2-1)/6$.

$\mathcal{H}_4$. Planes with exactly one point of $\mathcal{C}_3$, not osculating, $\mathcal{H}_4$ has size $q(q^2-1)/2$.

$\mathcal{H}_5$. Planes with no points of $\mathcal{C}_3$, $\mathcal{H}_5$ has size $q(q^2-1)/3$.

There is a symplectic polarity σ between points and planes of $\mathrm{PG}(3,q)$. There are 5 G-orbits of planes giving 5 G-orbits of points in $\mathrm{PG}(3,q)$.

$\mathcal{P}_1$. Points on $\mathcal{C}_3$ corresponding to osculating planes of $\mathcal{C}_3$ under σ.

$\mathcal{P}_2$. Points on tangent lines of the twisted cubic (not on the twisted cubic) correspond to planes containing exactly 2 points of $\mathcal{C}_3$ under σ.

$\mathcal{P}_3$. Points on three osculating planes correspond to planes through 3 distinct points of $\mathcal{C}_3$ under σ.

$\mathcal{P}_4$. Points not on $\mathcal{C}_3$ which lie on exactly one osculating plane correspond to planes through exactly one point of $\mathcal{C}_3$ under σ.

$\mathcal{P}_5$. Finally, the points which do not lie on any osculating plane correspond to planes containing no point of $\mathcal{C}_3$ under σ.

$\mathcal{P}_2$ is the set of points on exactly two osculating planes, $\mathcal{P}_3 \cup \mathcal{P}_5$ is the set of points not in $\mathcal{C}_3$ on a real (or imaginary) chord, $\mathcal{P}_4$ is the set of points not in $\mathcal{C}_3$ on an imaginary (or real) chord if $q \equiv 1 \bmod 3$ (or $q \equiv -1 \bmod 3$ respectively).

If $q = 3$, then

$\mathcal{P}_1$. Points on $\mathcal{C}_3$. $|\mathcal{P}_1| = q+1$.

$\mathcal{P}_2$. Points on all osculating planes. $|\mathcal{P}_2| = q+1$.

$\mathcal{P}_3$. Points not on $\mathcal{C}_3$, on a tangent, on one osculating plane. $|\mathcal{P}_3| = q^2-1$.

$\mathcal{P}_4$. Points not on $\mathcal{C}_3$ which lie on a real chord. $|\mathcal{P}_4| = q(q^2-1)/2$.

$\mathcal{P}_5$. Points on an imaginary chord. $|\mathcal{P}_5| = q(q^2-1)/2$.

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

4.3 Line classes in PG$(3,q)$

The lines of PG$(3,q)$ can be partitioned into classes which are unions of orbits under G, for $3 \nmid q$ odd. Each of these classes is denoted by $\mathcal{O}_i$, $i \in \{1,...,6\}$, and the set of polar lines of lines in the class $\mathcal{O}_i$ is denoted by $\mathcal{O}_i^\perp$.

(i) The class $\mathcal{O}_1$ contains real chords of the twisted cubic $\mathcal{C}_3$ and has size $q(q+1)/2$. Its dual $\mathcal{O}_1^\perp$ contains the real axes of Γ.

(ii) The class $\mathcal{O}_2 = \mathcal{O}_2^\perp$ contains tangents of the twisted cubic $\mathcal{C}_3$ and has size $q+1$.

(iii) The class $\mathcal{O}_3$ contains imaginary chords and has size $q(q-1)/2$. Its dual $\mathcal{O}_3^\perp$ contains the imaginary axes of Γ.

(iv) The class $\mathcal{O}_4 = \mathcal{O}_4^\perp$ contains non-tangent unisecants in osculating planes and has size $q(q+1)$.

(v) The class $\mathcal{O}_5$ contains unisecants not in osculating planes and has size $q(q^2-1)$. Its dual $\mathcal{O}_5^\perp$ contains external lines in osculating planes.

(vi) The class $\mathcal{O}_6 = \mathcal{O}_6^\perp$ contains external lines, (not chords and not in osculating planes) and has size $q(q-1)(q^2-1)$.

If the characteristic of the finite field is 3, then we have the following line classes.

(i) The class $\mathcal{O}_1$ contains real chords of the twisted cubic $\mathcal{C}_3$ and has size $q(q+1)/2$.

(ii) The class $\mathcal{O}_2$ contains tangents of the twisted cubic $\mathcal{C}_3$ and has size $q+1$.

(iii) The class $\mathcal{O}_3$ contains imaginary chords and has size $q(q-1)/2$.

(iv) The class $\mathcal{O}_4$ contains non-tangent unisecants in osculating planes and has size $q(q+1)$.

(v) The class $\mathcal{O}_5$ contains unisecants not in osculating planes and has size $q(q^2-1)$.

(vi) The class $\mathcal{O}_6$ contains external lines, (not chords and not in osculating planes) and has size $q(q-1)(q^2-1)$.

(vii) The class $\mathcal{O}_7$ contains axis of Γ and has size 1.

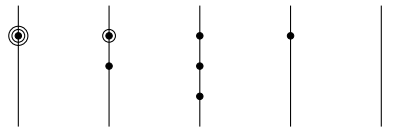
(viii) The class $\mathcal{O}_8$ contains external lines meeting the axis of Γ and it has size $(q+1)(q^2-1)$.

4.4 Combinatorial invariants

Main body of our study to compute the combinatorial invariants for the G-orbits on lines. In this section, we give the description of these G-orbits. Also, since the classification of lines in $\mathrm{PG}(3,q)$ under the action of G is equivalent to the classification of pencils of cubics in $\mathrm{PG}(1,q)$, we include the relation between cubics of $\mathrm{PG}(1,q)$ and planes of $\mathrm{PG}(3,q)$ (under the map δ_3). There are 5 types of cubics in $\mathrm{PG}(1,q)$, giving 5 G-orbits of planes in $\mathrm{PG}(3,q)$.

- The cubics which consist of a triple point are called *type* 1 cubic. The corresponding planes are the osculating planes and they form one G-orbit $\mathcal{H}_1$ of size $q+1$.
- A cubic which has a double point and a single point is called a *type* 2 cubic. The corresponding planes form one G-orbit. There are $q(q+1)$ such planes, and this orbit is denoted by $\mathcal{H}_2$.
- A cubic which has 3 distinct points is called a *type* 3 cubic, and corresponds to a plane meeting the twisted cubic in 3 distinct points. There are $q(q^2-1)/6$ such planes and they form one G-orbit denoted by $\mathcal{H}_3$.
- A cubic which has a 1 single point and 2 imaginary points is called a *type* 4 cubic. These cubics correspond to the $q(q^2-1)/2$ planes through exactly 1 point of the twisted cubic $\mathcal{C}_3$, which are not osculating planes. They form the G-orbit $\mathcal{H}_4$.
- A cubic which has 3 imaginary points is called a *type* 5 cubic. The corresponding G-orbits of planes are denoted by $\mathcal{H}_5$ and consist of $q(q^2-1)/3$ planes.

The five types of cubics on $\mathrm{PG}(1,q)$ (equivalently the five G-orbits $\mathcal{H}_1,\ldots,\mathcal{H}_5$) will be represented using the following diagrams. The vertical line represents $\mathrm{PG}(1,q)$ and on it, the number of $\mathbb{F}_q$-rational points of the cubic are represented. Simple points are represented by bullets, double points by a bullet and a circle, and triple points by a bullet and two circles. The positions of the points on the vertical lines



$\mathcal{H}_1$ $\mathcal{H}_2$ $\mathcal{H}_3$ $\mathcal{H}_4$ $\mathcal{H}_5$

Figure 4.1 The five G-orbits of planes in $\mathrm{PG}(3,q)$.

are meaningless and will be changed at will. For example, the G-orbit $\mathcal{H}_2$ may also be represented by its diagram above with the positions of the simple point and the double point interchanged.

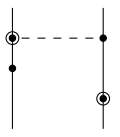
We are now in a position to define the combinatorial invariants in which we are interested.

Definition 80. The *point orbit distribution* of a line ℓ in $\mathrm{PG}(3,q)$, is denoted by $OD_0(\ell)$ is a list $[a_0,b_0,c_0,d_0,\ e_0]$ where the entries a_0, b_0, c_0, d_0 and e_0 are the number of points on ℓ in the point orbits $\mathcal{P}_1$, $\mathcal{P}_2$, $\mathcal{P}_3$, $\mathcal{P}_4$ and $\mathcal{P}_5$ of $\mathrm{PG}(3,q)$.

Definition 81. The *plane orbit distribution* of a line ℓ in $\mathrm{PG}(3,q)$, is denoted by $OD_2(\ell) = [a_2,b_2,c_2,d_2,e_2]$ where the entries a_2, b_2, c_2, d_2 and e_2 are the number of planes through ℓ in the plane orbits $\mathcal{H}_1$, $\mathcal{H}_2$, $\mathcal{H}_3$, $\mathcal{H}_4$ and $\mathcal{H}_5$ of $\mathrm{PG}(3,q)$.

Clearly, we must have $a_2+b_2+c_2+d_2+e_2 = a_0+b_0+c_0+d_0+e_0 = q+1$.

Each of the G-orbits of lines in $\mathrm{PG}(3,q)$ is denoted by $\mathcal{L}_i$ and the G-orbit of ℓ^σ with $\ell \in \mathcal{L}_i$ is denoted by $\mathcal{L}_i^\perp$. For each G-orbit, we will include a diagram representing the corresponding pencils of cubics, say $\mathcal{P}(\mathbf{C}_1,\mathbf{C}_2)$, on $\mathrm{PG}(1,q)$. The diagram consists of two vertical lines, each representing a copy of $\mathrm{PG}(1,q)$ with its cubic $\mathbf{C}_i$, $i=1,2$, as explained above. Horizontal dashed lines are used to indicate that the point on the two copies of $\mathrm{PG}(1,q)$ coincide. For example the pencil $\mathcal{P}(\mathbf{C}_1,\mathbf{C}_2)$ with $\mathbf{C}_1 = \mathcal{Z}(X_0^2X_1)$ and $\mathbf{C}_2 = \mathcal{Z}(X_0(X_0+X_1)^2)$ is represented by the following diagram.



The corresponding G-orbit of lines in $\mathrm{PG}(3,q)$ will be represented by the same diagram. Obviously different diagrams may represent the same G-orbit. As we will see, some diagrams represent a unique G-orbit of lines in $\mathrm{PG}(3,q)$, while others represent several G-orbits.

4.5 Lines contained in osculating planes

We start our classification with the lines which are the intersection of two osculating planes of the twisted cubic. The fact that these lines form one G-orbit is well known. For the sake of completeness, we have included an argument for this fact in the proof of the following lemma. The main contribution of the lemma is the determination of the point and plane orbit distributions of such lines.

Lemma 82. *There is one orbit $\mathcal{L}_1 = \mathcal{O}_1^\perp$ of external lines contained in the intersection of osculating planes of the twisted cubic $\mathcal{C}_3$ in* $\mathrm{PG}(3,q)$. *A line $\ell \in \mathcal{L}_1$ has plane orbit distribution $OD_2(\ell) = [2,0,0,(q-1),0]$ and point orbit distribution $OD_0(\ell) = [0,2,(q-1),0,0]$ for $q \equiv 5 \pmod 6$, and $OD_2(\ell) = [2,0,\frac{(q-1)}{3},0,\frac{2(q-1)}{3}]$ and $OD_0(\ell) = [0,2,(q-1),0,0]$ for $q \equiv 1 \pmod 6$.*

Proof. Consider the pencil $\mathcal{P}(\mathbf{C}_1, \mathbf{C}_2)$ with

$$\mathbf{C}_1 = \mathcal{Z}(X_0^3) \quad \text{and} \quad \mathbf{C}_2 = \mathcal{Z}(X_1^3).$$

The line ℓ is determined by the image of cubics $\mathbf{C}_1$, $\mathbf{C}_2$ under δ_3. Thus, $\ell = \delta_3(\mathbf{C}_1) \cap \delta_3(\mathbf{C}_2) = \mathcal{Z}(Y_0, Y_3)$. In order to determine the point orbit distribution of ℓ, firstly we try to find the points on ℓ contained in the osculating planes of the twisted cubic $\mathcal{C}_3$. Consider

$$\ell \cap \Pi(t) = \mathcal{Z}(-t^3Y_0 + 3t^2Y_1 - 3tY_2 + Y_3, Y_0, Y_3)$$

where $\Pi(t)$ is the osculating plane of $\mathcal{C}_3$ at the point $P(t)$. Then the points of ℓ contained in $\Pi(t)$ are of the form $(0,1,t,0)$ for $t \in \mathbb{F}_q$.
(1) If $t = 0$, then the point $(0,1,0,0)$ is on the tangent line of $\mathcal{C}_3$ at $P(0)$.
(2) If $t \neq 0$, then the point $(0,1,t,0) \in \Pi(t)$, $\Pi(\infty) = \mathcal{Z}(Y_0)$, $\Pi(0) = \mathcal{Z}(Y_3)$. If the point $(0,1,s,0) \in \ell$ is also contained in $\Pi(t)$, then

$$3t^2 - 3ts = (3t)(t-s) = 0.$$

Since t is nonzero, $t = s$. Therefore, each point of the form $(0,1,t,0)$ is contained in three osculating planes.
(3) The remaining point $(0,0,1,0) \in \ell$ is on the tangent line of $\mathcal{C}_3$ at $P(\infty)$.

In total, the line ℓ contains 2 points from the point orbit $\mathcal{P}_2$ and $(q-1)$ points from the point orbit $\mathcal{P}_3$. It follows that the point orbit distribution of ℓ is $OD_0(\ell) = [0,2,(q-1),0,0]$.

To determine the plane orbit distribution of ℓ, consider a plane $\Pi = \langle \ell, P(t) \rangle$. Then Π has equation $\mathcal{Z}(t^3 Y_0 - Y_3)$. If the point $(1, s, s^2, s^3)$ of $\mathcal{C}_3$ is contained in Π, then $t^3 = s^3$. Therefore, defining the map

$$\begin{array}{rccc} \psi: & \mathbb{F}_q^* & \to & \mathbb{F}_q^* \\ & t & \mapsto & t^3 \end{array}$$

the size of the image $|Im(\psi)|$ gives the number of planes of the form $\mathcal{Z}(t^3 Y_0 - Y_3)$.

If $3 \nmid (q-1)$, then ψ is bijective. If $q \equiv 5 \pmod 6$ then ℓ lies on $(q-1)$ distinct planes containing 1 point of the twisted cubic $\mathcal{C}_3$. The planes $\Pi(\infty) = \mathcal{Z}(Y_0)$ and $\Pi(0) = \mathcal{Z}(Y_3)$ are the osculating planes of the twisted cubic $\mathcal{C}_3$ containing ℓ. The plane orbit distribution of ℓ is therefore $OD_2(\ell) = [2, 0, 0, (q-1), 0]$ for $q \equiv 5 \pmod 6$.

If $q \equiv 1 \pmod 6$, then $3 \mid (q-1)$. In this case ℓ lies on $(q-1)/3$ planes containing 3 points of the twisted cubic $\mathcal{C}_3$ and there are $2(q-1)/3$ planes containing no point of the twisted cubic $\mathcal{C}_3$. In total there are 2 planes from the plane orbit $\mathcal{H}_2$, $(q-1)/3$ planes from the plane orbit $\mathcal{H}_3$ and $2(q-1)/3$ planes from the plane orbit $\mathcal{H}_5$ containing the line ℓ. Hence, the plane orbit distribution of ℓ is $OD_2(\ell) = [2, 0, \frac{(q-1)}{3}, 0, \frac{2(q-1)}{3}]$ for $q \equiv 1 \pmod 6$.

The fact that G acts transitively on this set of external lines follows from the fact that the corresponding pencils are completely determined by two points on $\mathrm{PG}(1, q)$. □

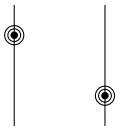


Figure 4.2 A pencil of cubics corresponding to $\mathcal{L}_1$

In the following lemma we consider the tangent lines of the twisted cubic.

Lemma 83. *There is one orbit $\mathcal{L}_2 = \mathcal{O}_2$ of tangent lines to the twisted cubic $\mathcal{C}_3$ in $\mathrm{PG}(3, q)$. A tangent line of the twisted cubic $\mathcal{C}_3$ has plane orbit distribution $OD_2(\ell) = [1, q, 0, 0, 0]$ and point orbit distribution $OD_0(\ell) = [1, q, 0, 0, 0]$.*

Proof. Since G acts transitively on the points of $\mathcal{C}_3$ it follows that G also acts transitively on the tangent lines. Consider the pencil $\mathcal{P}(\mathbf{C}_1, \mathbf{C}_2)$ with $\mathbf{C}_1 = \mathcal{Z}(X_1^3)$ and $\mathbf{C}_2 = \mathcal{Z}(X_1^2 X_0)$. The line ℓ is given by $\ell = \delta_3(\mathbf{C}_1) \cap \delta_3(\mathbf{C}_2) = \mathcal{Z}(Y_2, Y_3)$. The line ℓ is the tangent line of $\mathcal{C}_3$ at the point $(1, 0, 0, 0)$. It implies that the line contains 1 point from the point orbit $\mathcal{P}_1$ and q points from the point orbit $\mathcal{P}_2$. Then ℓ has a point orbit distribution $OD_0(\ell) = [1, q, 0, 0, 0]$. By Lemma 78, the line ℓ of $\mathcal{C}_3$ is self

polar. Therefore, $OD_0(\ell) = OD_2(\ell)$.

The union of the cubics of the pencil $\mathcal{P}(\mathbf{C}_1, \mathbf{C}_2)$ consists of two points of $\mathrm{PG}(1,q)$. Since G acts transitively on two points of $\mathcal{P}(\mathbf{C}_1, \mathbf{C}_2)$, every two such pencils are projectively equivalent. Therefore, there is one orbit of lines in $\mathrm{PG}(3,q)$ with the given plane and point orbit distributions. □

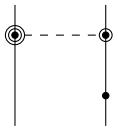


Figure 4.3 A pencil of cubics corresponding to $\mathcal{L}_2$

The following lemma describes the orbits consisting of non-tangent unisecants contained in osculating planes of the twisted cubic. They form one orbit. Since these lines are self polar (see Lemma 78) their point orbit distribution is equal to their plane orbit distribution.

Lemma 84. *There is one orbit $\mathcal{L}_3 = \mathcal{O}_4$ of non-tangent unisecants in osculating planes of the twisted cubic $\mathcal{C}_3$ in $\mathrm{PG}(3,q)$ with the same plane and point orbit distributions $OD_2(\ell) = OD_0(\ell) = [1, 1, \frac{(q-1)}{2}, \frac{(q-1)}{2}, 0]$.*

Proof. Consider the non-tangent unisecant line $\ell = \mathcal{Z}(Y_1, Y_3)$. Then ℓ corresponds to the pencil $\mathcal{P}(\mathbf{C}_1, \mathbf{C}_2)$ with

$$\mathbf{C}_1 = \mathcal{Z}(X_1^3) \quad \text{and} \quad \mathbf{C}_2 = \mathcal{Z}(X_0^2 X_1).$$

We first determine which points on ℓ are contained in osculating planes of the twisted cubic $\mathcal{C}_3$. The intersection of ℓ with an osculating plane is given by

$$\ell \cap \Pi(t) = \mathcal{Z}(-t^3 Y_0 + 3t^2 Y_1 - 3tY_2 + Y_3, Y_1, Y_3)$$

where $\Pi(t)$ is an osculating plane of $\mathcal{C}_3$ at the point $P(t)$. The points of ℓ which are contained in $\Pi(t)$ are of the form $(1, 0, \frac{-t^2}{3}, 0)$ for $t \in \mathbb{F}_q$.

18.1 If $t = 0$, then the point $(1,0,0,0)$ is a point of $\mathcal{C}_3$.

18.2 Assume that $t \neq 0$. If the point $(1,0,s,0) \in \ell$ is contained in $\Pi(t)$, then

$$-t^3 - 3ts = -t(t^2 + 3s) = 0.$$

This implies $t^2 = -3s$. If $-3s \in \square$ for $s \in \mathbb{F}_q \setminus \{0\}$, then the point $(1,0,s,0) \in \ell$ is contained in three osculating planes $\Pi(t_1)$, $\Pi(t_2)$ and $\Pi(0)$, for $t_1 \neq 0$, $t_2 \neq 0$, $t_1^2 = t_2^2 = -3s$. If $-3s \in \triangle$, then the point $(1,0,s,0) \in \ell$ is contained in exactly one osculating plane $\Pi(0)$. This gives $(q-1)/2$ points of ℓ contained in three osculating planes and $(q-1)/2$ points of $\ell \setminus \mathcal{C}_3$ contained in just one osculating plane.

18.3 The point $(0,0,1,0)$ is a point on the tangent line $\mathcal{Z}(Y_0, Y_1)$ at $P(\infty)$.

Summarizing these cases, we may conclude that $OD_0(\ell) = [1, 1, \frac{(q-1)}{2}, \frac{(q-1)}{2}, 0]$. By Lemma 78, the line ℓ of $\mathcal{C}_3$ is self polar. Therefore, $OD_0(\ell) = OD_2(\ell)$.

Since the pencil $\mathcal{P}(\mathbf{C}_1, \mathbf{C}_2)$ is completely determined by just two points of $\mathrm{PG}(1,q)$, each two such pencils are projectively equivalent. Hence, there is one orbit of lines in $\mathrm{PG}(3,q)$ with the given plane and point orbit distributions. □

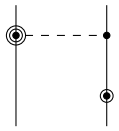


Figure 4.4 A pencil of cubics corresponding to $\mathcal{L}_3$

The next type of lines that we consider is the lines belonging to $\mathcal{O}_5^\perp$, which are lines in osculating planes which do not intersect the twisted cubic and which are not contained in two distinct osculating planes. We will show that $\mathcal{O}_5^\perp$ splits into different G-orbits. The point orbit distributions and plane orbit distributions depend on -3 being a square or not in $\mathbb{F}_q$. Moreover, both orbit distributions serve as complete combinatorial invariants for these orbits.

Lemma 85. *If -3 is a nonsquare in $\mathbb{F}_q$ then there is one orbit $\mathcal{L}_4 \subset \mathcal{O}_5^\perp$ of external lines in osculating planes of the twisted cubic $\mathcal{C}_3$ in $\mathrm{PG}(3,q)$ with orbit distributions*

$$OD_2(\ell) = [1, 2, \frac{(q-5)}{6}, \frac{(q-3)}{2}, \frac{(q+1)}{3}] \text{ and } OD_0(\ell) = [0, 3, \frac{(q-3)}{2}, \frac{(q-1)}{2}, 0].$$

If -3 is a square in $\mathbb{F}_q$ then there is one orbit $\mathcal{L}_4 \subset \mathcal{O}_5^\perp$ with orbit distributions

$$OD_2(\ell) = [1, 2, \frac{(q-7)}{6}, \frac{(q-1)}{2}, \frac{(q-1)}{3}] \text{ and } OD_0(\ell) = [0, 3, \frac{(q-3)}{2}, \frac{(q-1)}{2}, 0].$$

The number of lines in the G-orbit $\mathcal{L}_4$ is $q(q^2-1)$.

Proof. Consider the pencil $\mathcal{P}(\mathbf{C}_1, \mathbf{C}_2)$ with $\mathbf{C}_1 = \mathcal{Z}(X_0^3)$, and $\mathbf{C}_2 = \mathcal{Z}(X_1^2(X_0 - X_1))$, with diagram shown in Fig.4.5. The corresponding line ℓ in $\mathrm{PG}(3,q)$ is given by

$\delta_3(\mathbf{C}_1) \cap \delta_3(\mathbf{C}_2) = \mathcal{Z}(Y_0, Y_2 - Y_3)$. Firstly, we look at osculating planes through points on ℓ. We have

$$\ell \cap \Pi(t) = \mathcal{Z}(-t^3 Y_0 + 3t^2 Y_1 - 3tY_2 + Y_3, Y_0, Y_2 - Y_3)$$

where as before $\Pi(t)$ is the osculating plane of $\mathcal{C}_3$ at the point $P(t)$. The points of ℓ which are contained in $\Pi(t)$ are of the form $(0, 3t-1, 3t^2, 3t^2)$ for $t \in \mathbb{F}_q$.

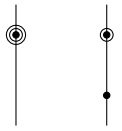


Figure 4.5 A pencil of cubics corresponding to $\mathcal{L}_4$

If $t = 0$, then we get the point $(0,1,0,0)$ which is on the tangent line $\mathcal{Z}(Y_2, Y_3)$ of $\mathcal{C}_3$ at $P(0)$, and for $t = \frac{1}{3}$, we get the point $(0,0,1,1)$ on the tangent line $\mathcal{Z}(Y_0, Y_1)$ of $\mathcal{C}_3$ at $P(\infty)$.

If the point $(0,1,s,s)$ of ℓ is contained in the osculating plane $\Pi(t)$ for $s \neq 0$, then s and t must satisfy

$$3t^2 - 3st + s = 0.$$

This is a quadratic equation in t, with discriminant

$$D_s = 9s^2 - 12s = 3s(3s-4).$$

For $s = \frac{12}{9}$, $D_s = 0$, and the point $(0,1,\frac{12}{9},\frac{12}{9})$ is contained in the osculating planes $\Pi(\frac{2}{3})$, and $\Pi(\infty)$ where $t = \frac{s}{2}$. Therefore, the point $(0,1,\frac{12}{9},\frac{12}{9})$ lies on the tangent line of $\mathcal{C}_3$ at $P(\frac{2}{3})$.

If $D_s = 9s^2 - 12s$ is a nonzero square, then there are three osculating planes $\Pi(t_1)$, $\Pi(t_2)$, and $\Pi(\infty)$ containing the point $(0,1,s,s)$ of ℓ where $t_{1,2} = \frac{3s \pm \sqrt{9s^2-12s}}{6}$. To determine how many values of s, $D_s \in \square$, consider the equation

$$9s^2 - 12s = y^2.$$

Homogenizing gives the quadratic form

$$g(s,y,z) = 9s^2 - 12sz - y^2.$$

The number of points of the form $(s,y,0)$ on the conic $\mathcal{Z}(g)$ is 2 and the number of points of the form $(s,0,1)$ is also 2. Therefore, there are $(q-3)/2$ values of s, for which the equation $9s^2 - 12s$ is a nonzero square in $\mathbb{F}_q$.

If $D_s \in \triangle$, then the point $(0,1,s,s)$ is contained in exactly one osculating plane $\Pi(\infty)$. By the above, there remain

$$q - \frac{q+1}{2} = \frac{q-1}{2}$$

values of s for which $D_s \in \triangle$.

In total, the line ℓ contains 3 points from the point orbit $\mathcal{P}_2$, $(q-3)/2$ points from the point orbit $\mathcal{P}_3$, and $(q-1)/2$ points from the point orbit $\mathcal{P}_4$. Hence, the point orbit distribution is $OD_0(\ell) = [0,3,\frac{(q-3)}{2},\frac{(q-1)}{2},0]$.

Now, to determine the plane orbit distribution of ℓ, consider the plane

$$\Pi = \langle \ell, P(t) \rangle,$$

where $P(t)$ is a point of $\mathcal{C}_3$. Then $\Pi = \langle \ell, P(\infty) \rangle$ is the osculating plane $\mathcal{Z}(Y_0)$, and $\Pi = \mathcal{Z}((t^3-t^2)Y_0 + Y_2 - Y_3)$ for $t \in \mathbb{F}_q$.

If $t^2(t-1) = 0$, then $\mathcal{Z}(Y_2 - Y_3)$ is a plane containing the points $(1,0,0,0)$ and $(1,1,1,1)$ of the twisted cubic $\mathcal{C}_3$. This plane belongs to $\mathcal{H}_2$.

Assume that $t^2(t-1) \neq 0$. If Π contains another point $(1,s,s^2,s^3)$ of $\mathcal{C}_3$, then

$$t^3 - t^2 = s^3 - s^2.$$

Since $s \neq t$, this gives $f(s) = s^2 + s(t-1) + t^2 - t = 0$, which is a quadratic equation in s. Note that $s = t$ is a solution of $f(s) = 0$ if and only if $t = 0$ or $t = \frac{2}{3}$. The discriminant of $f(s)$ is

$$D_t = (t-1)^2 - 4(t^2 - t) = -3t^2 + 2t + 1 = (1-t)(3t+1).$$

If $t^3 - t^2 \neq 0$ and $D_t = 0$, then Π is the plane containing 2 points $(1,t,t^2,t^3)$, and $(1,s_1,s_1^2,s_1^3)$ of the twisted cubic $\mathcal{C}_3$. Since $t^3 - t^2 \neq 0$, $D_t = 0$ for $t = -\frac{1}{3}$. Then Π is the plane containing $(1,-\frac{1}{3},(-\frac{1}{3})^2,(-\frac{1}{3})^3)$ and $(1,\frac{2}{3},(\frac{2}{3})^2,(\frac{2}{3})^3)$, and therefore $\Pi \in \mathcal{H}_2$.

If $t^3 - t^2 \neq 0$ and $D_t = -3t^2 + 2t + 1$ is a nonzero square in $\mathbb{F}_q \setminus \{0,1\}$ then the two solutions of $f(s) = 0$ are

$$s_{1,2} = \frac{(1-t) \pm \sqrt{-3t^2 + 2t + 1}}{2}.$$

In this case the plane Π contains 3 points $(1,s_1,s_1^2,s_1^3)$, $(1,s_2,s_2^2,s_2^3)$, and $(1,t,t^2,t^3)$ of the twisted cubic $\mathcal{C}_3$, i.e. $\Pi \in \mathcal{H}_3$.

Next, we determine for how many of the remaining values of $t \in \mathbb{F}_q$, D_t is a nonzero square. By the condition on D_t, it is convenient to consider the conic $\mathcal{Z}(g)$ in $\mathrm{PG}(2,q)$ defined by

$$g(X,Y,Z) = -3X^2 + 2XZ + Z^2 - Y^2.$$

Then $\mathcal{Z}(g)$ is a non-degenerate conic since it has no singular point. The points on the conic $\mathcal{Z}(g)$ can be parameterized as

$$\{(x,y,1),(x,-y,1) \mid -3x^2+2x+1 \in \square\} \cup \{(1,-\sqrt{-3},0),(1,\sqrt{-3},0)\}$$

where $y = \sqrt{-3x^2+2x+1}$.

19.1 A point of the form $(0,y,1)$ lies on the conic $\mathcal{Z}(g)$ if and only if $y^2 = 1$. Hence, there are 2 points $(0,1,1)$ and $(0,-1,1)$ of the given form. They both correspond to $t = 0$.

19.2 A point of the form $(x,0,1)$ lies on the conic $\mathcal{Z}(g)$ if and only if $-3x^2+2x+1 = (1-x)(3x+1) = 0$. In this case we find the points $(1,0,1)$ and $(-\frac{1}{3},0,1)$ of the given form. Also these points do not contribute to the values of t for which D_t is a nonzero square in $\mathbb{F}_q$.

19.3 A point of the form $(1,y,0)$ lies on the conic $\mathcal{Z}(g)$ if and only if $-3 = y^2$. There exists a point of the given form if and only if -3 is a square in $\mathbb{F}_q$. Therefore, there are either 2 points $(1,\sqrt{-3},0)$ and $(1,-\sqrt{-3},0)$ or no points of the form $(1,y,0)$. Again these points do not contribute to the values of t for which D_t is a nonzero square in $\mathbb{F}_q$.

19.4 A point of the form $(x,y,1)$ with $xy \neq 0$ lies on the conic $\mathcal{Z}(g)$ if and only if $-3x^2+2x+1 = y^2$. From the previous parts we have already either 4 or 6 points on the conic $\mathcal{Z}(g)$. For $x = \frac{2}{3}$, which corresponds to the value $t = \frac{2}{3}$ in part of the proof determining the point orbit distribution, we must have $\sqrt{-3x^2+2x+1} = 1$, and we get 2 points $(\frac{2}{3},1,1)$ and $(\frac{2}{3},-1,1)$. There remain either $(q-5)/2$ or $(q-7)/2$ pairs on the conic $\mathcal{Z}(g)$ of the form $(x,y,1)$ and $(x,-y,1)$.

Consequently, there are either $(q-5)/2$ or $(q-7)/2$ values of t for which D_t is a nonzero square in $\mathbb{F}_q$. For these values of t, there is a plane Π through ℓ containing 3 points $(1,s_1,s_1^2,s_1^3)$, $(1,s_2,s_2^2,s_2^3)$, $(1,t,t^2,t^3)$ of the twisted cubic $\mathcal{C}_3$. Since each such plane is counted three times, there are either $(q-5)/6$ or $(q-7)/6$ such planes.

If $t^3 - t^2 \neq 0$ and $D_t = -3t^2+2t+1$ is a non-square in $\mathbb{F}_q$, then Π is the plane containing 1 point $(1,t,t^2,t^3)$ of the twisted cubic $\mathcal{C}_3$. We know that for $t = 1$ and $t = -\frac{1}{3}$, $D_t = 0$

and for $t = 0$ and $t = \frac{2}{3}$, $D_t = 1$. We have determined that there are either $(q-5)/2$ or $(q-7)/2$ nonzero square values of $D_t \neq 1$, hence the number of non-square values of D_t is either

$$q - \frac{(q+3)}{2} = \frac{(q-3)}{2} \text{ or } q - \frac{(q+1)}{2} = \frac{(q-1)}{2}.$$

Therefore, if -3 is a square in $\mathbb{F}_q$, then there are $(q-1)/2$ planes through ℓ containing 1 point of the twisted cubic $\mathcal{C}_3$, otherwise, there are $(q-3)/2$ such planes.

Summarizing all the results, for the plane orbit distribution we found $[a_2, b_2, c_2, d_2, e_2]$ with $a_2 = 1$, $b_2 = 2$, c_2 is either $(q-5)/6$ or $(q-7)/6$ and d_2 is either $(q-3)/2$ or $(q-1)/2$. Since $e_2 = q+1-(a_2+b_2+c_2+d_2)$, e_2 is $(q+1)/3$, if $-3 \in \triangle$, and e_2 is $(q-1)/3$, if $-3 \in \square$. This determines the plane orbit distribution of the line ℓ.

Clearly, each pencil of cubics in $\mathrm{PG}(1,q)$ which contains a cubic of type 1 and a cubic of type 2 can be mapped to any other such pencil by the unique projectivity of $\mathrm{PG}(1,q)$ mapping the two frames of $\mathrm{PG}(1,q)$ determined by the two pairs of cubics (one of type 1 and one of type 2) onto each other. It follows that, up to equivalence, there is a unique such pencil. Equivalently, there is a unique G-orbit of lines in $\mathrm{PG}(3,q)$ with the given orbit distributions.

Counting triples (ℓ, Π_1, Π_2) with $\ell \in \mathcal{L}_4$, $\Pi_1 \in \mathcal{H}_1$, and $\Pi_2 \in \mathcal{H}_2$, we get

$$|\mathcal{L}_4|\ 2 = (q+1)q(q-1)$$

where the left hand side follows from the fact that a line $\ell \in \mathcal{L}_4$ is contained in a unique plane from $\mathcal{H}_1$ and in two planes from $\mathcal{H}_2$. The right hand side follows from the fact that there are $q+1$ choices for a plane $\Pi_1 \in \mathcal{H}_1$ and $q(q-1)$ choices for a plane $\Pi_2 \in \mathcal{H}_2$ which does not pass through the contact point of Π_1. The number of lines in this G-orbit is, therefore, equal to $q(q^2-1)$. □

Remark 86. Note that the total number of lines in the G-orbit is equal to $q(q^2-1)/2$, since such a line is determined by the choice of a cubic of type 1 and a cubic of type 2 disjoint from it, and for each such pencil there are two choices for the cubic of type 2. It follows that the number of lines in an osculating plane belonging to the G-orbit $\mathcal{L}_4$ is

$$\frac{q(q^2-1)/2}{q+1} = \frac{q(q-1)}{2},$$

which follows from the total number of lines in $\mathcal{L}_4$ and the fact that each line of $\mathcal{L}_4$ is contained in exactly one osculating plane, plus the fact that each osculating plane

must contain the same number of lines from $\mathcal{L}_4$.

Recall that the cross ratio of a 4-tuple of points (P_1, P_2, P_3, P_4) with affine coordinates x_1, x_2, x_3 and x_4 with respect to a frame Λ of $\mathrm{PG}(1,q)$ is given by

$$(P_1, P_2; P_3, P_4) = \frac{(x_3 - x_1)(x_4 - x_2)}{(x_3 - x_2)(x_4 - x_1)}.$$

For any quadruple $T = \{P_1, P_2, P_3, P_4\}$ of distinct points of $\mathrm{PG}(1,q)$, define its J-invariant as

$$J(T) = \sum_{i<j} u_i u_j.$$

where the u_i's are the (in general 6) cross ratios which can be obtained from T. Abusing notation, we also define

$$J(X) = 6 - \frac{(X^2 - X + 1)^3}{X^2(X-1)}.$$

It is well known that $J(T) = J(u_i)$ for each $u \in \{u_1, u_2, u_3, u_4, u_5, u_6\}$. For a pair of cubics $(\mathbf{C}_1, \mathbf{C}_2)$ on $\mathrm{PG}(1,q)$, where $\mathbf{C}_1$ cubic of type 1 and $\mathbf{C}_2$ cubic of type 3, define $J(\mathbf{C}_1, \mathbf{C}_2)$ as $J(T)$ where $T = \{P_1, P_2, P_3, P_4\}$ with P_4 the triple point of $\mathbf{C}_1$, and P_1, P_2, P_3 are the points of $\mathbf{C}_2$.

Lemma 87. *Let $\mathcal{P}(\mathbf{C}_1, \mathbf{C}_2)$ be a pencil with empty base, with $\mathbf{C}_1$ of type 1 and $\mathbf{C}_2$ of type 3. There exists $u \in \mathbb{F}_q$ such that $J(u) = J(\mathbf{C}_1, \mathbf{C}_2)$ satisfying $u^2 - u + 1$ is a non-square in $\mathbb{F}_q$ if and only if $\mathcal{P}(\mathbf{C}_1, \mathbf{C}_2)$ contains no cubic of type 2.*

Proof. Consider a pencil $\mathcal{P}(\mathbf{C}_1, \mathbf{C}_2)$ satisfying the hypotheses. Then without loss of generality we may assume that

$$\mathbf{C}_1 = \mathcal{Z}((X_1 - uX_0)^3) \text{ and } \mathbf{C}_2 = \mathcal{Z}(X_0 X_1 (X_0 - X_1)),$$

where $u^2 - u + 1$ is a non-square in $\mathbb{F}_q$. A cubic $\mathbf{C}_s \in \mathcal{P}(\mathbf{C}_1, \mathbf{C}_2)$ is of the form $\mathbf{C}_s = \mathcal{Z}(f_s)$ for $s \in \mathbb{F}_q \cup \{\infty\}$, where

$$f_s(X_0, X_1) = X_1^3 - 3uX_1^2 X_0 + 3u^2 X_1 X_0^2 - u^3 X_0^3 + s(X_0^2 X_1 - X_0 X_1^2).$$

By way of contradiction, suppose $\mathbf{C}_s$ is of type 2. Then $s \neq 0$ and $f_s(1, X_1)$ must have repeated roots in $\mathbb{F}_q$. The substitution $X_1 \mapsto X_1 - (-3u - s)/3$ gives

$$f_s(1, X_1) = X_1^3 + \left(-2su + s - \frac{s^2}{3}\right) X_1 + \left(\frac{-2s^3 - 18s^2 u + 9s^2 - 27su^2 + 27su}{27}\right)$$

where

$$k = -2su + s - \frac{s^2}{3} \text{ and } m = \frac{-2s^3 - 18s^2u + 9s^2 - 27su^2 + 27su}{27}.$$

Since $f_s(1, X_1)$ has repeated roots, the discriminant $D_{f_s} = 0$, where

$$D_{f_s} = -4k^3 - 27m^2 = s^2(s^2 + (-2(2u-1)(u-2)(u+1))s - 27u^2(u-1)^2).$$

But since the discriminant of the polynomial

$$g_u(s) = s^2 + (-2(2u-1)(u-2)(u+1))s - 27u^2(u-1)^2$$

is equal to

$$D_{g_u} = 16(u^2 - u + 1)^3$$

this contradicts that fact that $u^2 - u + 1$ is a non-square in $\mathbb{F}_q$. □

Lemma 88. *The line $\ell = \delta_3(\mathbf{C}_1) \cap \delta_3(\mathbf{C}_2)$ with $\mathbf{C}_1 = \mathcal{Z}((X_1 - uX_0)^3)$ and $\mathbf{C}_2 = \mathcal{Z}(X_0X_1(X_0 - X_1))$, where $u^2 - u + 1$ is a non-square in $\mathbb{F}_q$, has plane orbit distribution $OD_2(\ell) = [1, 0, \frac{(q-1)}{6}, \frac{(q+1)}{2}, \frac{(q-1)}{3}]$ and point orbit distribution $OD_0(\ell) = [0, 1, \frac{(q-1)}{2}, \frac{(q+1)}{2}, 0]$ for $-3 \in \square$, and $OD_2(\ell) = [1, 0, \frac{(q+1)}{6}, \frac{(q-1)}{2}, \frac{(q+1)}{3}]$, $OD_0(\ell) = [0, 1, \frac{(q-1)}{2}, \frac{(q+1)}{2}, 0]$ for $-3 \in \triangle$.*

Proof. The line $\ell = \delta_3(\mathbf{C}_1) \cap \delta_3(\mathbf{C}_2)$ is given by

$$\ell = \mathcal{Z}(Y_3 - 3uY_2 + 3u^2Y_1 - u^3Y_0, Y_1 - Y_2),$$

and its points can be parameterized as

$$\{(1, s, s, (3u - 3u^2)s + u^3) \mid s \in \mathbb{F}_q\} \cup \{(0, 1, 1, (3u - 3u^2))\}.$$

(OD_0) Firstly, we determine the points on ℓ which are contained in the osculating planes of the twisted cubic $\mathcal{C}_3$. We have

$$\ell \cap \Pi(t) : -t^3 + 3t^2s - 3ts + (3u - 3u^2)s + u^3 = 0$$

where $\Pi(t)$ is an osculating plane of $\mathcal{C}_3$ at the point $P(t)$. In order to solve this cubic equation we make the substitution $t \mapsto t + s$. This gives

$$f(t) = -t^3 + (3s^2 - 3s)t + 2s^3 - 3s^2 - 3su^2 + 3su + u^3$$

where

$$k = 3s^2 - 3s \text{ and } m = 2s^3 - 3s^2 - 3su^2 + 3su + u^3.$$

The discriminant of $f(t)$ is

$$D_s = 27(2su - s - u^2)^2(3s^2 + 2su - 4s - u^2).$$

The roots of the polynomial $f(t)$ are

$$t_1 = u - s,\ t_2 = \frac{-\sqrt{9s^2 + 6s(u-2) - 3u^2} + s - u}{2},\ t_3 = \frac{\sqrt{9s^2 + 6s(u-2) - 3u^2} + s - u}{2}.$$

(1) The discriminant D_s is zero if and only if

$$2su - s - u^2 = 0 \text{ or } 3s^2 + 2su - 4s - u^2 = 0.$$

The equation $2su - s - u^2 = 0$ implies that $s(2u-1) = u^2$. This gives

$$s = \frac{u^2}{2u-1} \text{ for } u \neq \frac{1}{2}.$$

The point $(1, s, s, (3u - 3u^2)s + u^3)$ is contained in the osculating planes $\Pi(t_1)$, $\Pi(t_2)$ where

$$t_1 = u \text{ and } t_2 = -\frac{(2-u)u}{2u-1}, \text{ for } s = \frac{u^2}{2u-1}.$$

Note that for $u = \frac{1}{2}$, $u^2 - u + 1 = \frac{3}{4}$. For $3 \in \triangle$, $\frac{3}{4} \in \triangle$. Therefore, if $3 \in \triangle$ and $u = \frac{1}{2}$, then $D_s = 0$ for no values of s.

The equation

$$3s^2 + s(2u-4) - u^2 = 0$$

has a solution if and only if its discriminant

$$D_u = 16(u^2 - u + 1)$$

is either 0 or a nonzero square in $\mathbb{F}_q$. By the hypothesis, D_u is a non-square in $\mathbb{F}_q$.

(2) The discriminant D_s is a nonzero square if and only if

$$-3(-3s^2 - 2su + 4s + u^2) \in \square.$$

This means that -3 and $(-3s^2 - 2su + 4s + u^2)$ have the same quadratic residue in $\mathbb{F}_q$. In this case there are three osculating planes $\Pi(t_1)$, $\Pi(t_2)$, $\Pi(t_3)$ containing the point $(1, s, s, (3u - 3u^2)s + u^3)$ of ℓ.

Suppose that $-3 \in \square$. We want to determine for how many values of $s \in \mathbb{F}_q$, the

discriminant D_s is a nonzero square. Define

$$g(S,Y,Z) = -3S^2 - (2u-4)SZ + u^2Z^2 - Y^2.$$

Then $\mathcal{Z}(g)$ is a non-degenerate conic if and only if $u^2 - u + 1 \neq 0$, which is satisfied by the hypothesis. We have

$$\mathcal{Z}(g) = \{(s,y,1),(s,-y,1) \mid -3s^2 - (2u-4)s + u^2 \in \square\} \cup \{(1,\sqrt{-3},0),(1,-\sqrt{-3},0)\}.$$

A point of the form $(0,y,1)$ lies on the conic $\mathcal{Z}(g)$ if and only if $u^2 = y^2$. There are 2 points $(0,u,1)$ and $(0,-u,1)$ on the conic. A point of the form $(1,y,0)$ lies on the conic $\mathcal{Z}(g)$ if and only if $-3s^2 = y^2$. Since -3 is a square in $\mathbb{F}_q$, there are 2 such points $(1,\sqrt{-3},0)$ and $(1,-\sqrt{-3},0)$. A point of the form $(s,y,1)$ with $sy \neq 0$ lies on the conic $\mathcal{Z}(g)$ if and only if $-3s^2 - (2u-4)s + u^2 = y^2$. From the previous parts we have already 4 points on the conic $\mathcal{Z}(g)$. There remain $(q-3)/2$ pairs on the conic $\mathcal{Z}(g)$ of the form $(s,y,1)$ and $(s,-y,1)$.

In total, for $-3 \in \square$, the expression $-3s^2 - (2u-4)s + u^2$ is a nonzero square in $\mathbb{F}_q$ for $(q-1)/2$ values of $s \in \mathbb{F}_q$. Therefore, if $-3 \in \square$, then $D_s \in \square$ for $(q-1)/2$ values of s. Note that for $s = \frac{u^2}{2u-1}$ (with $u \neq \frac{1}{2}$) the point $(\frac{u^2}{2u-1},y,1)$ is on the conic $\mathcal{Z}(g)$ if and only if

$$g(\frac{u^2}{2u-1},y,1) = -3u^2(u-1)^2 - y^2(2u-1)^2 = 0.$$

Since $u \neq 0,1$ it follows that if the point $(\frac{u^2}{2u-1},y,1)$ lies on the conic $\mathcal{Z}(g)$ then $-3 \in \square$. Hence, $s = \frac{u^2}{2u-1}$ is one of the values of s for which $D_s \in \square$. We can conclude that there are three osculating planes containing $(1,s,s,(3u-3u^2)s+u^3)$ for $(q-3)/2$ values of s.

(3) If the discriminant D_s is a non-square, then there exists an osculating plane $\Pi(u-s)$ containing the point $(1,s,s,(3u-3u^2)s+u^3)$ of ℓ. The discriminant D_s is a non-square if and only if $-3(-3s^2-2su+4s+u^2) \in \triangle$. From the previous discussions, we can easily say that if $-3 \in \square$, then for $(q+1)/2$ values of s, the expression $-3s^2 - 2su + 4s + u^2$ is a non-square in $\mathbb{F}_q$.

(4) Finally consider the point $(0,1,1,(3u-3u^2)) \in \Pi(\infty)$. It is contained in the osculating plane $\Pi(t)$ of $\mathcal{C}_3$ if and only if

$$3t^2 - 3t + (3u-3u^2) = -3(-t^2+t-u+u^2) = 0.$$

It follows that the point $(0,1,1,(3u-3u^2))$ of ℓ is contained in the osculating planes

$\Pi(\infty)$, $\Pi(u)$, and $\Pi(1-u)$. The number of osculating planes through $(0,1,1,(3u-3u^2))$ is two for $1-u=u=\frac{1}{2}$, and three otherwise.

Collecting the results for $-3 \in \square$ and $u \neq \frac{1}{2}$, it follows that the line ℓ has 1 point from the point orbit $\mathcal{P}_2$, $(q-1)/2$ points from the point orbit $\mathcal{P}_3$ and $(q+1)/2$ points from the point orbit $\mathcal{P}_4$.

Similarly, if $-3 \in \triangle$, then $-3s^2-(2u-4)s+u^2$ is nonzero square in $\mathbb{F}_q$ for $(q+1)/2$ values of $s \in \mathbb{F}_q$. There remain $q-(q+1)/2=(q-1)/2$ values of s for which $-3s^2-(2u-4)s+u^2$ is a non-square in $\mathbb{F}_q$. Therefore, if $-3 \in \triangle$, then D_s is a nonzero square for $(q-1)/2$ values of s.

If $-3 \in \triangle$, then for $(q+1)/2$ values of s, $(-3s^2-2su+4s+u^2) \in \square$. Hence, if $-3 \in \triangle$, then D_s is a non-square for $(q-1)/2$ values of s.

Collecting all the results, we have that if $-3 \in \triangle$ and $u \neq \frac{1}{2}$, then the line ℓ has 1 point from the point orbit $\mathcal{P}_2$, $(q-1)/2$ points from the point orbit $\mathcal{P}_3$ and $(q+1)/2$ points from the point orbit $\mathcal{P}_4$. In addition, if either $-3 \in \square$ or $-3 \in \triangle$ and $u=\frac{1}{2}$, then the line ℓ has 1 point from the point orbit $\mathcal{P}_2$, $(q-1)/2$ points from the point orbit $\mathcal{P}_3$ and $(q+1)/2$ points from the point orbit $\mathcal{P}_4$.

(OD_2) Now, in order to determine the plane orbit distribution of ℓ, consider the plane $\Pi=\langle \ell, P(t)\rangle$ where $P(t)$ is a point of $\mathcal{C}_3$. Then Π has equation

$$(t^2u^3-tu^3)Y_0+(3t^2u-3t^2u^2-t^3+u^3)Y_1+(t^3+3tu^2-3tu-u^3)Y_2+(t-t^2)Y_3=0.$$

If $t=0$, then $Z(u^3(Y_1-Y_2))$ is a plane containing the points $(1,0,0,0)$, $(1,1,1,1)$ and $(0,0,0,1)$ of the twisted cubic $\mathcal{C}_3$. This plane belongs to $\mathcal{H}_3$.

If $t=u$ then Π is the osculating plane containing the point $(1,u,u^2,u^3)$ of the twisted cubic $\mathcal{C}_3$, which belongs to $\mathcal{H}_1$.

For the remaining cases, it therefore suffices to consider $t \in \mathbb{F}_q \setminus \{0,1,u\}$. If Π contains another point $(1,v,v^2,v^3)$ of $\mathcal{C}_3$, $t \neq v$, then

$$(t-v)f(v)=0,$$

where

$$f(v)=(t^2-t)v^2+(3tu+u^3-3tu^2-t^2)v+tu^3-u^3.$$

If the discriminant $D_t = (t-u)^2(t^2+(6u^2-4u^3-4u)t+u^4)$ of $f(v)$ is equal to zero then

$$t^2+(6u^2-4u^3-4u)t+u^4=0,$$

since $t \neq u$. So $D_t = 0$ occurs only for values of $t \in \{t_1, t_2\}$, where

$$t_1 = 2u^3-3u^2-2u(u-1)\sqrt{u^2-u+1}+2u,\ t_2 = 2u^3-3u^2+2u(u-1)\sqrt{u^2-u+1}+2u.$$

Since u^2-u+1 is a non-square in $\mathbb{F}_q$, this implies that the discriminant $D_t \neq 0$.

To determine the values of t for which the discriminant D_t is a nonzero square in $\mathbb{F}_q$, define

$$g(T,Y,Z) = T^2+(6u^2-4u^3-4u)TZ+u^4Z^2-Y^2.$$

Then $\mathcal{Z}(g)$ is a non-degenerate conic since u^2-u+1 is a non-square in $\mathbb{F}_q$. The points on the conic $\mathcal{Z}(g)$ are of the following type. A point of the form $(t,y,0)$ lies on the conic $\mathcal{Z}(g)$ if and only if $t^2-y^2=0$ giving 2 points $(t,y,0)$ and $(t,-y,0)$. Furthermore, $\mathcal{Z}(g)$ contains no points on the line $Y=0$, since u^2-u+1 is a non-square. A point of the form $(0,y,1)$ lies on the conic $\mathcal{Z}(g)$ if and only if $u^4=y^2$, which gives another two points $(0,u^2,1)$ and $(0,-u^2,1)$.

For $t=u$, the point $(u,y,1)$ is on the conic $\mathcal{Z}(g)$ if and only if

$$g(u,y,1) = u^2+(6u^2-4u^3-4u)u+u^4-y^2=0.$$

Since this implies $y^2=-3u^2(u-1)^2$, there two such points for $-3 \in \square$, and no such points otherwise.

For $t=1$, we obtain the points $(1,(u-1)^2,1)$ and $(1,-(u-1)^2,1)$ on the conic $\mathcal{Z}(g)$.

So the number of points of on the conic $\mathcal{Z}(g)$ which we need to exclude in our count of the values of $t \in \mathbb{F}_q \setminus \{0,1,u\}$ for which D_t is a nonzero square in $\mathbb{F}_q$, equals 8 points if $-3 \in \square$ and 6. The remaining points on $\mathcal{Z}(g)$ of the form $(t,y,1)$ with $t \in \mathbb{F}_q \setminus \{0,1,u\}$ and $y \neq 0$, come in pairs $(t,y,1)$ and $(t,-y,1)$, where each such pair counts towards one value of t for which D_t is a nonzero square.

A point of the form $(t,y,1)$ with $ty \neq 0$ lies on the conic $\mathcal{Z}(g)$ if and only if

$$t^2+(6u^2-4u^3-4u)t+u^4=y^2.$$

We may conclude that the discriminant D_t is a nonzero square in $\mathbb{F}_q$ for $(q-7)/2$ or $(q-5)/2$ values of $t \in \mathbb{F}_q \setminus \{0,1,u\}$, depending on whether -3 is a square in $\mathbb{F}_q$ or not.

For these values of $t \in \mathbb{F}_q$, the plane Π contains 3 points of the twisted cubic $\mathcal{C}_3$. Taking into account the plane $\langle \ell, P(0) \rangle$ which also meets the twisted cubic in three points, and the fact that each such plane is counted three times, we obtain $(q-1)/6$ planes through ℓ containing 3 points of the twisted cubic $\mathcal{C}_3$ if $-3 \in \square$, and $(q+1)/6$ such planes through ℓ for $-3 \in \triangle$.

If $D_t \in \triangle$ and $t \in \mathbb{F}_q \setminus \{0,1,u\}$, then Π is the plane containing 1 point $(1,t,t^2,t^3)$ of the twisted cubic $\mathcal{C}_3$. By the above the number of values of t for which Π meets $\mathcal{C}_3$ in exactly one point is therefore

$$q-3-\frac{(q-7)}{2} = \frac{(q+1)}{2} \text{ for } -3 \in \square, \text{ and } q-3-\frac{(q-5)}{2} = \frac{(q-1)}{2} \text{ for } -3 \in \triangle.$$

This proves that the line ℓ has the plane orbit distribution $OD_2(\ell)$ as claimed. $\square$

Lemma 89. *The stabiliser in G of the line $\ell = \mathcal{Z}(Y_3 - 3uY_2 + 3u^2Y_1 - u^3Y_0, Y_1 - Y_2)$, with $u^2 - u + 1$ a non-square in $\mathbb{F}_q$, has order two.*

Proof. In order to simplify the computation, we map the line ℓ to the line ℓ' contained in the osculating plane $\Pi(0)$ by an element of G. Using the element $\varphi(\beta)$ of G, where β is the element of $\mathrm{PGL}(2,q)$ induced by the matrix

$$\begin{pmatrix} 1 & -u \\ 0 & 1 \end{pmatrix}.$$

we obtain $\ell' = \mathcal{Z}(Y_2 - (1-2u)Y_1 - u(1-u)Y_0, Y_3)$. Since ℓ (and hence ℓ') is contained in a unique osculating plane, the stabiliser of ℓ' is contained in the stabiliser of $\Pi(0)$, which has order $q(q-1)$ and consists of elements $\varphi_{c,d} \in G$, induced by the matrices of the form

$$\begin{pmatrix} 1 & 0 \\ c & d \end{pmatrix}$$

where $c, d \in \mathbb{F}_q$ and $d \neq 0$.

First suppose that $u \neq 1/2$. The condition that the image under an element $\varphi_{c,d} \in G_{\Pi(0)}$ of the point $(2u-1, u(1-u), 0, 0) \in \ell'$ belongs to ℓ' gives

$$c = \frac{(1-d)(1-2u)}{3u(1-u)}. \tag{4.5.1}$$

After substituting this value for c in $\varphi_{c,d}$, the condition that the image of the point

$(0,1,1-2u,0)$ under $\varphi_{c,d}$ belongs to ℓ' gives

$$\frac{(d^2-1)(2u-1)}{u(u-1)} = 0.$$

Since $u \neq 1/2$ this implies $d^2 = 1$. Hence, the stabiliser in G of ℓ' has order two.

If $u = 1/2$ then the line ℓ' is spanned by the points $(0,1,0,0)$ and $(1,u,u(1-u),0)$. In this case, the condition that the image of $(0,1,0,0)$ under $\varphi_{c,d}$ lies on ℓ' gives $c = 0$. Computing the image under $\varphi_{0,d}$ of $(1,u,u(1-u),0)$ then gives $(1,0,d^2u(1-u),0)$ which belongs to ℓ' if and only if $d^2 = 1$. Again the stabiliser in G of ℓ' has order two. □

It follows from Lemma 89 that there are $q(q-1)/2$ lines in the unique osculating plane through ℓ which belong to the G-orbit of ℓ.

Lemma 90. *The set of lines in osculating planes which are not contained in the union of the G-orbits $\mathcal{L}_1 \cup \mathcal{L}_2 \cup \mathcal{L}_3 \cup \mathcal{L}_4$ form one G-orbit, which we denote by $\mathcal{L}_5$.*

Proof. Consider an osculating plane $\Pi(t)$ at the point $P(t)$ of $\mathcal{C}_3$. The number of lines of the G-orbit $\mathcal{L}_1$ in $\Pi(t)$ is q, since each such line is the intersection of $\Pi(t)$ with exactly one other osculating plane $\Pi(s)$ with $s \neq t$. Furthermore, there is a unique tangent line in $\Pi(t)$, and there are q lines in $\Pi(t)$ which belong to the G-orbit $\mathcal{L}_3$ (non-tangent unisecants). By Remark 86, this leaves $q(q-1)/2$ lines in $\Pi(t)$ which not are contained in the union of the G-orbits $\mathcal{L}_1 \cup \mathcal{L}_2 \cup \mathcal{L}_3 \cup \mathcal{L}_4$. By Lemma 89 these lines form one G-orbit, since the stabiliser in G of an osculating plane has size $q(q-1)$. □

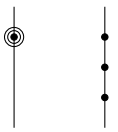


Figure 4.6 Diagram of the orbit $\mathcal{L}_5$

Corollary 91. *There is no line with plane orbit distribution $OD_2(\ell) = [1,0,0,d_2,e_2]$ where $d_2 \geq 1$.*

Proof. This simply follows by counting the lines in the orbits $\mathcal{L}_i$, $i \in \{1,\ldots,5\}$, which are contained in a fixed osculating plane. □

4.6 Lines meeting the twisted cubic

Since the polar of a line meeting the twisted cubic is a line contained in an osculating plane of the twisted cubic, the orbit distributions determined in the previous sections imply the orbit distributions of all lines meeting the twisted cubic. In this section, we collect the results for the G-orbits which consist of lines meeting the twisted cubic, but not contained in an osculating plane.

The polar of a line belonging to the G-orbit $\mathcal{L}_1$ is a chord of the twisted cubic $\mathcal{C}_3$, and so the orbit distributions follow from the orbit distributions of $\mathcal{L}_1$.

Lemma 92. *There is one orbit $\mathcal{L}_6 = \mathcal{L}_1^{\perp} = \mathcal{O}_1$ of real chords of the twisted cubic $\mathcal{C}_3$ in* $\mathrm{PG}(3,q)$. *A real chord ℓ of the twisted cubic $\mathcal{C}_3$ has plane orbit distribution $OD_2(\ell) = [0,2,(q-1),0,0]$ and point orbit distribution $OD_0(\ell) = [2,0,0,(q-1),0]$ for $q \equiv 5$ (mod 6). If $q \equiv 1$ (mod 6) then the orbit distributions are $OD_2(\ell) = [0,2,(q-1),0,0]$ and $OD_0(\ell) = [2,0,\frac{(q-1)}{3},0,\frac{2(q-1)}{3}]$.*

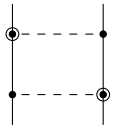


Figure 4.7 Diagram of the pencil of cubics corresponding to $\mathcal{L}_6$

Now, let ℓ be an external line contained in the osculating plane Π at the point P of $\mathcal{C}_3$. Since self polar lines through P are all lines through P which are contained in Π, the line ℓ^{σ} is a unisecant through P which is not contained in Π. Since we already determined the point orbit distribution and the line orbit distribution of the external lines in osculating planes of $\mathcal{C}_3$ (the G-orbits $\mathcal{L}_4$ and $\mathcal{L}_5$) we immediately have the following lemma's.

Lemma 93. *There is one orbit $\mathcal{L}_7 = \mathcal{L}_4^{\perp} \subset \mathcal{O}_5$ of unisecants not in osculating planes of the twisted cubic $\mathcal{C}_3$ in* $\mathrm{PG}(3,q)$ *with plane orbit distribution $OD_2(\ell) = [0,3,\frac{(q-3)}{2},\frac{(q-1)}{2},0]$ and point orbit distribution $OD_0(\ell) = [1,2,\frac{(q-5)}{6},\frac{(q-3)}{2},\frac{(q+1)}{3}]$ for $-3 \in \triangle$ and $OD_2(\ell) = [0,3,\frac{(q-3)}{2},\frac{(q-1)}{2},0]$, $OD_0(\ell) = [1,2,\frac{(q-7)}{6},\frac{(q-1)}{2},\frac{(q-1)}{3}]$ for $-3 \in \square$.*

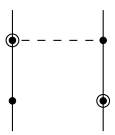


Figure 4.8 Diagram of the pencil of cubics corresponding to $\mathcal{L}_7$

Lemma 94. *There is one orbit $\mathcal{L}_8 = \mathcal{L}_5^{\perp} \subset \mathcal{O}_5$ of unisecants not in osculating planes of the twisted cubic $\mathcal{C}_3$ in* $\mathrm{PG}(3,q)$ *with plane orbit distribution $OD_2(\ell) =$*

$[0,1,\frac{(q-1)}{2},\frac{(q+1)}{2},0]$ *and point orbit distribution* $OD_0(\ell)=[1,0,\frac{(q+1)}{6},\frac{(q-1)}{2},\frac{(q+1)}{3}]$ *for* $-3\in\triangle$, $OD_2(\ell)=[0,1,\frac{(q-1)}{2},\frac{(q+1)}{2},0]$ *and* $OD_0(\ell)=[1,0,\frac{(q-1)}{6},\frac{(q+1)}{2},\frac{(q-1)}{3}]$ *for* $-3\in\square$.

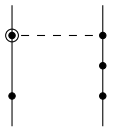


Figure 4.9 Diagram of the pencil of cubics corresponding to $\mathcal{L}_8$

Lemma 95. *If a pencil of cubics on* $\mathrm{PG}(1,q)$ *has a base point, then it belongs to one of the orbits* $\mathcal{L}_2$, $\mathcal{L}_3$, $\mathcal{L}_6$, $\mathcal{L}_7$ *or* $\mathcal{L}_8$.

Proof. The line corresponding to a pencil of cubics on $\mathrm{PG}(1,q)$ with a base point P corresponds to a line of $\mathrm{PG}(3,q)$ meeting the twisted cubic $\mathcal{C}_3$ in the point $\nu_3(P)$, and these lines are contained in the union of the orbits $\mathcal{L}_2$, $\mathcal{L}_3$, $\mathcal{L}_6$, $\mathcal{L}_7$, and $\mathcal{L}_8$. □

4.7 Orbits of imaginary chords and imaginary axes

We start with the imaginary chords.

Lemma 96. *There is one orbit* $\mathcal{L}_9=\mathcal{O}_3$ *of imaginary chords of the twisted cubic* $\mathcal{C}_3$ *in* $\mathrm{PG}(3,q)$ *with plane orbit distribution* $[0,0,0,q+1,0]$. *The point orbit distribution of an imaginary chords* ℓ *is*

$$OD_0(\ell)=[0,0,\frac{(q+1)}{3},0,\frac{2(q+1)}{3}].$$

if -3 *is a non-square in* $\mathbb{F}_q$ *and*

$$OD_0(\ell)=[0,0,0,q+1,0],$$

if -3 *is a square in* $\mathbb{F}_q$.

Proof. Consider an imaginary chord ℓ. Let P, P^τ denote the two points of $\ell(q^2)\cap\mathcal{C}_3(q^2)$ (here τ denotes the Frobenius collineation of $\mathrm{PG}(3,q^2)$). Since a plane $\Pi=\langle\ell,P(t)\rangle$ with $P(t)\in\mathcal{C}_3$ has the property that $\Pi(q^2)$ meets $\mathcal{C}_3(q^2)$ in the three points P, P^τ, and $P(t)$, the plane Π belongs to $\mathcal{H}_4$. This proves that $OD_2(\ell)=[0,0,0,q+1,0]$, as claimed.

Consider two imaginary chords ℓ and ℓ'. Then $\ell(q^2)$ and $\ell'(q^2)$ belong to the same orbit under the extension $G(q^2) \cong \mathrm{PGL}(2,q^2)$ of G. Let $\alpha \in G(q^2)$ be such that $\ell(q^2)^\alpha = \ell'(q^2)$. Consider three distinct planes Π_1, Π_2, and Π_3 through ℓ in $\mathrm{PG}(3,q)$. By the above each of these planes meets $\mathcal{C}_3$ in a points. Let P_1, P_2, and P_3 denote these points of $\mathcal{C}_3$. Then $\Gamma(P, P^\tau, P_1, P_2, P_3)$ is a frame of $\mathrm{PG}(3,q^2)$, since Γ consists of five points on the twisted cubic $\mathcal{C}_3(q^2)$. But then $\alpha\tau\alpha^{-1}\tau = id$, since it fixes frame Γ. Therefore $\alpha\tau = \tau\alpha$, which implies $\alpha \in \mathrm{PGL}(4,q)$. Hence ℓ and ℓ' belong to the same G-orbit.

To determine the point orbit distribution, consider the imaginary chord

$$\ell = \mathcal{Z}(Y_0 + bY_2, Y_1 + bY_3),$$

whose points can be parameterized as

$$\{(-b, -bs, 1, s) \mid s \in \mathbb{F}_q\} \cup \{(0, -b, 0, 1)\},$$

where $-b$ a non-square in $\mathbb{F}_q$.

First note that the point $(0,-b,0,1) \in \ell$ lies on the osculating plane $\Pi(\infty)$ and lies on the osculating plane $\Pi(t)$ if and only if $-3t^2b + 1 = 0$. This means that if -3 is a non-square in $\mathbb{F}_q$ then $(0,-b,0,1)$ is on three osculating planes, otherwise, it is only on one osculating plane.

A point $(-b,-bs,1,s) \in \ell$ lies in the osculating plane $\Pi(t)$ of the twisted cubic $\mathcal{C}_3$ if

$$bt^3 - 3t^2bs - 3t + s = 0.$$

In order to solve this cubic equation we make the substitution $t \mapsto t + s$. This gives

$$f(t) = t^3 + (\frac{-3}{b})(bs^2+1)t + (\frac{-2s}{b})(bs^2+1).$$

whose discriminant is

$$D_f = 108\frac{(bs^2+1)^2}{b^3},$$

which is not zero because $-b$ is a non-square in $\mathbb{F}_q$. This implies that $OD_0(\ell) = [0,0,a_3,a_4,a_5]$.

Also D_f is a non-square if and only if -3 is a nonzero square in $\mathbb{F}_q$. In this case every point of ℓ lies on exactly one osculating plane defined over $\mathbb{F}_q$ (and two conjugate osculating planes of $\mathcal{C}(q^2)$). This gives $OD_0(\ell) = [0,0,0,q+1,0]$.

If -3 is a non-square in $\mathbb{F}_q$, then D_f is a square in $\mathbb{F}_q \setminus \{0\}$. In this case $OD_0(\ell) = [0,0,a_3,0,a_5]$, and each point of ℓ either lies on three distinct osculating planes of $\mathcal{C}_3$ or on zero osculating planes of $\mathcal{C}_3$. Since there are $q+1$ osculating planes, each of them intersecting ℓ, we obtain

$$OD_0(\ell) = [0,0,\frac{(q+1)}{3},0,\frac{2(q+1)}{3}].$$

This concludes the proof. □

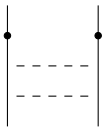


Figure 4.10 Diagram of the pencil of cubics corresponding to $\mathcal{L}_9$

Since the polar line of an imaginary line is an imaginary axes of $\mathcal{C}_3$, we have the following lemma.

Lemma 97. *There is one orbit $\mathcal{L}_{10} = \mathcal{L}_9^{\perp} = \mathcal{O}_3^{\perp}$ of imaginary axes of $\mathcal{C}_3$ in* $\mathrm{PG}(3,q)$ *with plane orbit distribution $OD_2(\ell) = OD_0(\ell^{\perp})$ and $OD_0(\ell) = OD_2(\ell^{\perp})$, for $\ell \in \mathcal{L}_{10}$.*

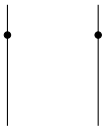


Figure 4.11 Diagram of the pencil of cubics corresponding to $\mathcal{L}_{10}$

We determine the point orbit distributions and plane orbit distributions of ten orbits of lines in $\mathrm{PG}(3,q)$ with respect to the twisted cubic over the finite field of characteristic $q > 3$. We find the group description of the stabilisers of G-orbits of lines. We determine the sizes of stabilisers and line orbits. These results are given in Table 4.1, Table 4.2 and Table 4.3.

We classified all lines in $\mathrm{PG}(3,q)$ except the external lines that are not contained in the osculating planes of the twisted cubic. We conclude that most of the line classes form a unique orbit. The unisecant lines that are not contained in the osculating planes of the twisted cubic form two line orbits. Dually, external lines in the osculating planes of the twisted cubic form two line orbits (see Table 4.4).

A line in any line orbit is generated by two points and points of $\mathrm{PG}(3,q)$ can be represented by 2×3 matrices. Therefore, each line orbit can be represented by 2×3 matrices (see Table 4.7).

The classification of lines of $\mathrm{PG}(3,q)$ under the stabiliser group of the twisted cubic simultaneously is studied by different two groups. The results are published on arXiv

Table 4.1 The point orbit distribution of ten line orbits over the finite field with characteristic > 3.

Orbit	Point-orbit distribution	Condition
$\mathcal{L}_1$	$[0,2,(q-1),0,0]$	
$\mathcal{L}_2$	$[1,q,0,0,0]$	
$\mathcal{L}_3$	$[1,1,(q-1)/2,(q-1)/2,0]$	
$\mathcal{L}_4$	$[0,3,(q-3)/2,(q-1)/2,0]$	
$\mathcal{L}_5$	$[0,1,(q-1)/2,(q+1)/2,0]$	
$\mathcal{L}_6 = \mathcal{L}_1^\perp$	$[2,0,(q-1),0,0]$ $[2,0,(q-1)/3,0,2(q-1)/3]$	$-3 \in \triangle$ $-3 \in \square$
$\mathcal{L}_7 = \mathcal{L}_4^\perp$	$[1,2,(q-5)/6,(q-3)/2,(q+1)/3]$ $[1,2,(q-7)/6,(q-1)/2,(q-1)/3]$	$-3 \in \triangle$ $-3 \in \square$
$\mathcal{L}_8 = \mathcal{L}_5^\perp$	$[1,0,(q\pm1)/6,(q\pm1)/2,(q\pm1)/3]$	$q \equiv \pm 2 (\mathrm{mod} 3)$
$\mathcal{L}_9$	$[0,0,(q+1)/3,0,2(q+1)/3]$ $[0,0,0,(q+1),0]$	$-3 \in \triangle$ $-3 \in \square$
$\mathcal{L}_{10} = \mathcal{L}_9^\perp$	$[0,0,0,(q+1),0]$	

one week apart (see (Davydov, Marcugini & Pambianco, 2021), (Blokhuis, Pellikaan & Szőnyi, 2021) and (Günay & Lavrauw, 2021)). We need to emphasize that our results are mentioned in the seminars (Lavrauw, 2020a) and (Lavrauw, 2020b) in 2020 by my advisor Lavrauw. The classification of lines of $\mathrm{PG}(3,q)$ under $\mathrm{PGL}(2,q)$ over the finite field of characteristic 2, 3, and > 3 is described in (Davydov et al., 2021) and (Blokhuis et al., 2021). In these two papers, different approaches are followed and the results are summarized in Table 4.5 and Table 4.6. In (Davydov et al., 2021), group-theoretic results are applied and in (Blokhuis et al., 2021), the relation between rational functions and codimension two subspaces is used. The classification of lines in the line classes $\mathcal{O}_6$ which contains external lines (not chords and not in the osculating planes) is still an open problem.

4.8 Orbits of tensors in $S^3\mathbb{F}_q^2 \otimes \mathbb{F}_q^2$

Here $S^3\mathbb{F}_q^2$ denotes the space of homogenous polynomials of degree 3 on $\mathbb{F}_q^2$. $S^3\mathbb{F}_q^2$ is a subspace of $\mathbb{F}_q^2 \otimes \mathbb{F}_q^2 \otimes \mathbb{F}_q^2$. The orbits on the partially symmetric tensors in $S^3\mathbb{F}_q^2 \otimes \mathbb{F}_q^2$ (i.e G-orbits of lines in $S^3\mathbb{F}_q^2$) are given in terms of a basis $\{e_1, e_2\}$ of $\mathbb{F}_q^2$ in the

Table 4.2 The plane orbit distribution of ten line orbits over the finite field with characteristic > 3.

Orbit	Plane-orbit distribution	Condition	Base
$\mathcal{L}_1$	$[2,0,0,(q-1),0]$	$-3 \in \triangle$	$\varnothing$
	$[2,0,(q-1)/3,0,2(q-1)/3]$	$-3 \in \square$	$\varnothing$
$\mathcal{L}_2$	$[1,q,0,0,0]$		$\mathcal{Z}(X_1^2)$
$\mathcal{L}_3$	$[1,1,(q-1)/2,(q-1)/2,0]$		$\mathcal{Z}(X_1)$
$\mathcal{L}_4$	$[1,2,(q-5)/6,(q-3)/2,(q+1)/3]$	$-3 \in \triangle$	$\varnothing$
	$[1,2,(q-7)/6,(q-1)/2,(q-1)/3]$	$-3 \in \square$	$\varnothing$
$\mathcal{L}_5$	$[1,0,(q\pm1)/6,(q\mp1)/2,(q\pm1)/3]$	$q \equiv \pm 2 (\mathrm{mod} 3)$	$\varnothing$
$\mathcal{L}_6 = \mathcal{L}_1^\perp$	$[0,2,(q-1),0,0]$		$\mathcal{Z}(X_0, X_1)$
$\mathcal{L}_7 = \mathcal{L}_4^\perp$	$[0,3,(q-3)/2,(q-1)/2,0]$		$\mathcal{Z}(X_1)$
$\mathcal{L}_8 = \mathcal{L}_5^\perp$	$[0,1,(q-1)/2,(q+1)/2,0]$		$\mathcal{Z}(X_1)$
$\mathcal{L}_9$	$[0,0,0,(q+1),0]$		$\mathcal{Z}(X_0^2 + bX_1^2)$
$\mathcal{L}_{10} = \mathcal{L}_9^\perp$	$[0,0,(q+1)/3,0,2(q+1)/3]$	$-3 \in \triangle$	$\varnothing$
	$[0,0,0,(q+1),0]$	$-3 \in \square$	$\varnothing$

Table 4.8

For each such G-orbit we determine the plane orbit distribution and the point orbit distribution. In Figure 4.8, we give the tensor representation of these 10 G-orbits.

4.9 Codes related with the twisted cubic

Let $\mathrm{C} \subseteq F_q^n$ be an $[n,k,d]$ code with $d \geq 3$ and H a parity check matrix for C. Since $d \geq 3$, the columns of H represent pairwise linearly independent vectors of $\mathbb{F}_q^k$.

Define a set $\mathcal{S} = \{P_1, P_1, .., P_n\}$ of n points in $\mathrm{PG}(n-k-1,q)$ where point P_i corresponds to the column vector c_i of the parity check matrix H.

The covering radius of C is R_0 corresponds the following property of $\mathcal{S}$:*every point x in* $\mathrm{PG}(n-k-1,q)$ *is linearly dependent with R_0 points from $\mathcal{S}$, and there exists a point in* $\mathrm{PG}(n-k-1,q)$ *which is linearly independent with any set of R_0-1 points from $\mathcal{S}$.*

Fix $x \in \mathbb{F}_q^n$. There are 2 cases according to the syndrome of x.

Table 4.3 Stabiliser group description and sizes of ten line orbits over the finite field with characteristic > 3.

Orbit	Stabilisers of line orbits in $\mathrm{PG}(3,q)$ under $G = \mathrm{PGL}(2,q)$	$\lvert G_\ell \rvert$	$\lvert \mathcal{L}_i \rvert$
$\mathcal{L}_1 = \mathcal{O}_1^\perp$	$D_{2(q-1)}$	$2(q-1)$	$q(q+1)/2$
$\mathcal{L}_2 = \mathcal{O}_2$	$(C_q : C_{q-1})$	$q(q-1)$	$(q+1)$
$\mathcal{L}_3 = \mathcal{O}_4$	C_{q-1}	$(q-1)$	$q(q+1)$
$\mathcal{L}_4 \subset \mathcal{O}_5^\perp$	C_2	2	$q(q-1)(q+1)/2$
$\mathcal{L}_5 \subset \mathcal{O}_5^\perp$	C_2	2	$q(q-1)(q+1)/2$
$\mathcal{L}_6 = \mathcal{L}_1^\perp = \mathcal{O}_1$	$D_{2(q-1)}$	$2(q-1)$	$q(q+1)/2$
$\mathcal{L}_7 = \mathcal{L}_4^\perp \subset \mathcal{O}_5$	C_2	2	$q(q-1)(q+1)/2$
$\mathcal{L}_8 = \mathcal{L}_5^\perp \subset \mathcal{O}_5$	C_2	2	$q(q-1)(q+1)/2$
$\mathcal{L}_9 = \mathcal{O}_3$	$D_{2(q+1)}$	$2(q+1)$	$q(q-1)/2$
$\mathcal{L}_{10} = \mathcal{L}_9^\perp = \mathcal{O}_3^\perp$	$D_{2(q+1)}$	$2(q+1)$	$(q-1)(q+1)/2$

20.1 $s(x)$ is a linear combination of $R_0 - 1$ columns of H.
Since $d(x,C) < R_0$, $s(x) = 0$ or a point in some space of dimension $t \le R_0 - 2$.

20.2 $s(x)$ is not a linear combination of $R_0 - 1$ columns of H.
Let P be the point of $\mathrm{PG}(n-k-1,q)$ corresponding to $s(x)$. Then P does not belong to any space of dimension $t \le R_0 - 2$ generated by the points of $\mathcal{S}$. As the covering radius of $\mathcal{S}$ is R_0, the point belongs to at least one subspace of dimension $R_0 - 1$ generated by the points of $\mathcal{S}$.

21.1 Let $\{T_1, T_2, .., T_h\}$ be the distinct subspaces containing P of dimension $R_0 - 1$ generated by some points in $\mathcal{S}$.

21.2 Let $V_i = T_i \cap \mathcal{S}$. Then V_i contains at least R_0 independent points of $\mathcal{S}$.

21.3 Let u_i be the number of distinct sets of R_0 independent points of $\mathcal{S}$ in T_i. There are u_i ways of expressing $s(x)$ as a linear combination of R_0 columns of H. In order for x to satisfy the condition of (R_0, μ)-MCF code, $u_1 + .. + u_h$ is at least μ.

Definition 98. Let $\mathcal{S} = \{P_1, P_2, .., P_n\}$ be an n-subset of points of $\mathrm{PG}(N,q)$. Then $\mathcal{S}$ is said to be (ρ,μ)-*saturating* if:

22.1 $\mathcal{S}$ generates $\mathrm{PG}(N,q)$;

22.2 there exists a point $Q \in \mathrm{PG}(N,q)$ which does not belong to any subspace of dimension $\rho - 1$ generated by the points of $\mathcal{S}$;

Table 4.4 The description of G-orbits of lines over the finite field with characteristic >3

Line classes	Description	G-orbits
$\mathcal{O}_1^\perp$	real axes of Γ	$\mathcal{L}_1$
$\mathcal{O}_1$	real chords of $\mathcal{C}_3$	$\mathcal{L}_6 = \mathcal{L}_1^\perp$
$\mathcal{O}_2$	tangent lines of $\mathcal{C}_3$	$\mathcal{L}_2$
$\mathcal{O}_3$	imaginary chords of $\mathcal{C}_3$	$\mathcal{L}_9$
$\mathcal{O}_3^\perp$	imaginary axes of Γ	$\mathcal{L}_{10} = \mathcal{L}_9^\perp$
$\mathcal{O}_4$	unisecants contained in osc. pl.	$\mathcal{L}_3$
$\mathcal{O}_5$	unisecants not contained in osc. pl.	$\mathcal{L}_4^\perp \cup \mathcal{L}_5^\perp$
$\mathcal{O}_5^\perp$	external lines in osc. pl.	$\mathcal{L}_4 \cup \mathcal{L}_5$

Table 4.5 The description of G-orbits of lines over the finite field with characteristic 2

Line classes	Description	G-orbits	Sizes
$\mathcal{O}_1^\perp$	real axes of Γ	$\mathcal{L}_1(2)$	$q(q+1)/2$
$\mathcal{O}_1$	real chords of $\mathcal{C}_3$	$\mathcal{L}_6(2) = \mathcal{L}_1(2)^\perp$	$q(q+1)/2$
$\mathcal{O}_2$	tangent lines of $\mathcal{C}_3$	$\mathcal{L}_2(2)$	$q+1$
$\mathcal{O}_3$	imaginary chords of $\mathcal{C}_3$	$\mathcal{L}_8(2)$	$q(q-1)/2$
$\mathcal{O}_3^\perp$	imaginary axes of Γ	$\mathcal{L}_9(2) = \mathcal{L}_8(2)^\perp$	$q(q-1)/2$
$\mathcal{O}_4$	unisecants contained in osc. pl.	$\mathcal{L}_3(2) \cup \mathcal{L}_4(2)$	$q+1$, q^2-1
$\mathcal{O}_5$	unisecants not contained in osc. pl.	$\mathcal{L}_5(2)$	$q(q-1)(q+1)$
$\mathcal{O}_5^\perp$	external lines in osc. pl.	$\mathcal{L}_7(2) = \mathcal{L}_5(2)^\perp$	$q(q-1)(q+1)$

22.3 every point $Q \in \mathrm{PG}(N,q)$ not belonging to any subspace of dimension $\rho-1$ generated by the points of $\mathcal{S}$, such that the number of subspaces of dimension ρ generated by the points of $\mathcal{S}$ and containing Q, counted with multiplicity, is at least μ. The multiplicity m_T of a subspace T is computed as the number of distinct sets of $\rho+1$ independent points contained in $T \cap \mathcal{S}$.

Example 99. Let $\mathcal{C}_2 : \mathcal{Z}(X_0X_1 - X_2^2)$ be a non-degenerate conic. The conic has $(q+1)$ points and no 3 points are collinear. $\mathcal{C}_2$ is a $(1, \frac{(q-1)}{2})$-saturating $(q+1)$-set.

23.1 Any 3 points of $\mathcal{C}_2$ generate $\mathrm{PG}(2,q)$.

23.2 A subspace of dimension $\rho-1$ generated by the points of $\mathcal{C}_2$ is a point of $\mathcal{C}_2$. Therefore any point $P \in \mathrm{PG}(2,q) \setminus \mathcal{C}_2$ is a point which does not belong to any subspace of dimension $\rho-1$ generated by the points of $\mathcal{C}_2$.

23.3 Let Q be the point in $\mathrm{PG}(2,q)$ not belonging to $\mathcal{C}_2$. If Q is an external point,

Table 4.6 The description of G-orbits of lines over the finite field with characteristic 3.

Line classes	Description	G-orbits	Sizes
$\mathcal{O}_1^\perp$	real axes of Γ	$\mathcal{L}_1(3)$	$q(q+1)/2$
$\mathcal{O}_1$	real chords of $\mathcal{C}_3$	$\mathcal{L}_6(3) = \mathcal{L}_1(3)^\perp$	$q(q+1)/2$
$\mathcal{O}_2$	tangent lines of $\mathcal{C}_3$	$\mathcal{L}_2(3)$	$q+1$
$\mathcal{O}_3$	imaginary chords of $\mathcal{C}_3$	$\mathcal{L}_8(3)$	$q(q-1)/2$
$\mathcal{O}_3^\perp$	imaginary axes of Γ	$\mathcal{L}_9(3) = \mathcal{L}_8(3)^\perp$	$q(q-1)/2$
$\mathcal{O}_4$	unisecants contained in osc. pl.	$\mathcal{L}_3(3)$	$q(q+1)$
$\mathcal{O}_5$	unisecants not contained in osc. pl.	$\mathcal{L}_4(3) \cup \mathcal{L}_5(3)$	$q(q^2-1)/2$, $q(q^2-1)/2$
$\mathcal{O}_5^\perp$	external lines in osc. pl.	$\mathcal{L}_6(3) \cup \mathcal{L}_7(3) = \mathcal{L}_4(3)^\perp \cup \mathcal{L}_5(3)^\perp$	$q(q^2-1)/2$, $q(q^2-1)/2$
$\mathcal{O}_7$	axis of Γ	$\mathcal{L}_{10}(3)$	1
$\mathcal{O}_8$	ext lines meeting the axis of Γ	$\mathcal{L}_{11}(3) \cup \mathcal{L}_{12}(3) \cup \mathcal{L}_{13}(3)$	$(q^2-1)/2$, $(q^2-1)/2$, $q(q^2-1)/2$

Table 4.7 The matrix representation of ten G-orbits of lines over the finite field with characteristic > 3

Orbit	Representative	Orbit	Representative
$\mathcal{L}_1$	$\begin{bmatrix} . & \alpha & \beta \\ \alpha & \beta & . \end{bmatrix}$	$\mathcal{L}_6 = \mathcal{L}_1^\perp$	$\begin{bmatrix} \alpha & . & . \\ . & . & \beta \end{bmatrix}$
$\mathcal{L}_2$	$\begin{bmatrix} \alpha & \beta & . \\ \beta & . & . \end{bmatrix}$	$\mathcal{L}_7 = \mathcal{L}_4^\perp$	$\begin{bmatrix} \alpha & . & \beta \\ . & \beta & \beta \end{bmatrix}$
$\mathcal{L}_3$	$\begin{bmatrix} \alpha & . & \beta \\ . & \beta & . \end{bmatrix}$	$\mathcal{L}_8 = \mathcal{L}_5^\perp$	$\begin{bmatrix} \alpha & \beta & \beta \\ \beta & \beta & -\beta \end{bmatrix}$
$\mathcal{L}_4$	$\begin{bmatrix} . & \alpha & \beta \\ \alpha & \beta & \beta \end{bmatrix}$	$\mathcal{L}_9$	$\begin{bmatrix} \alpha & \beta & \alpha b \\ \beta b & \alpha b & \beta b \end{bmatrix}$
$\mathcal{L}_5$	$\begin{bmatrix} \alpha & \beta & \beta \\ \beta & \beta & \alpha u^3 + 3u(1-u)\beta \end{bmatrix}$	$\mathcal{L}_{10} = \mathcal{L}_9^\perp$	$\begin{bmatrix} \gamma\beta & \gamma'\alpha & -\beta \\ \gamma'\alpha & -\beta & -\alpha \end{bmatrix}$

where $u \in \mathbb{F}_q \setminus \{0\}$ satisfying $u^2 - u + 1 \in \triangle$ and $b \in \triangle$. γ, γ' are square or non-square depends on whether $-3 \in \square$ or not.

then Q is on $(q-1)/2$ bisecant line of $\mathcal{C}_2$. If Q is an internal point, then Q is on $(q+1)/2$ bisecant line of $\mathcal{C}_2$. For $\mu = (q-1)/2$ is smallest number for the lines containing 2 points of the conic. Therefore, $\mathcal{C}_2$ is a $(1, \frac{(q-1)}{2})$-saturating $(q+1)$-set.

Now, we can give the relation between multiple covering codes and saturating sets. An $[n,k]R_0$ code C with $R_0 = \rho + 1$ *corresponds* to a (ρ,μ)-saturating n-set $\mathcal{S}$ in $\mathrm{PG}(n-k-1,q)$ if C admits a parity check matrix whose columns are homogenous coordinates of the points in $\mathcal{S}$.

Proposition 100. *A linear $[n,k]R_0$ code* C *corresponding to a (ρ,μ)-saturating n-set $\mathcal{S} \in \mathrm{PG}(n-k-1,q)$ is a $(\rho+1,\mu)$-MCF-code.*

The connection between projective geometry and the coding theory is (ρ,μ)-

Table 4.8 a, b are non-squares and $u \in \mathbb{F}_q \setminus \{0, 1, \infty\}$ satisfying $u^2 - u + 1$ is a non-square.

Orbit	Representative
$\mathcal{L}_1$	$(e_1 \otimes e_1 \otimes e_2 + e_1 \otimes e_2 \otimes e_1 + e_2 \otimes e_1 \otimes e_1) \otimes e_1 +$ $(e_1 \otimes e_2 \otimes e_2 + e_2 \otimes e_1 \otimes e_2 + e_2 \otimes e_2 \otimes e_1) \otimes e_2$
$\mathcal{L}_1^\perp$	$(e_1 \otimes e_1 \otimes e_1) \otimes e_1 + (e_2 \otimes e_2 \otimes e_2) \otimes e_2$
$\mathcal{L}_2$	$(e_1 \otimes e_1 \otimes e_1) \otimes e_1 +$ $(e_1 \otimes e_1 \otimes e_2 + e_1 \otimes e_2 \otimes e_1 + e_2 \otimes e_1 \otimes e_2) \otimes e_2$
$\mathcal{L}_3$	$(e_1 \otimes e_1 \otimes e_1) \otimes e_1 + (e_1 \otimes e_2 \otimes e_2) \otimes e_2 +$ $(e_2 \otimes e_1 \otimes e_2 + e_2 \otimes e_2 \otimes e_1) \otimes e_2$
$\mathcal{L}_4$	$(e_1 \otimes e_1 \otimes e_2 + e_1 \otimes e_2 \otimes e_1 + e_2 \otimes e_1 \otimes e_1) \otimes e_1 +$ $(e_1 \otimes e_2 \otimes e_2 + e_2 \otimes e_1 \otimes e_2 + e_2 \otimes e_2 \otimes e_1 + e_2 \otimes e_2 \otimes e_2) \otimes e_2$
$\mathcal{L}_4^\perp$	$(e_1 \otimes e_1 \otimes e_1) \otimes e_1 + (e_1 \otimes e_2 \otimes e_2) \otimes e_2 +$ $(e_2 \otimes e_1 \otimes e_2 + e_2 \otimes e_2 \otimes e_1 + e_2 \otimes e_2 \otimes e_2) \otimes e_2$
$\mathcal{L}_5$	$(e_1 \otimes e_1 \otimes e_1 + e_2 \otimes u^3 e_2 \otimes e_2) \otimes e_1 + (e_1 \otimes e_1 \otimes e_2 + e_1 \otimes e_2 \otimes e_1) \otimes e_2 +$ $(e_1 \otimes e_2 \otimes e_2 + e_2 \otimes e_1 \otimes e_1 + e_2 \otimes e_1 \otimes e_2 + e_2 \otimes e_2 \otimes e_1 + e_2 \otimes (3u - 3u^2) e_2 \otimes e_2) \otimes e_2$
$\mathcal{L}_5^\perp$	$(e_1 \otimes e_1 \otimes e_1) \otimes e_1 + (e_1 \otimes e_1 \otimes e_2 + e_1 \otimes e_2 \otimes e_1 + e_1 \otimes e_2 \otimes e_2) \otimes e_2 +$ $(e_2 \otimes e_1 \otimes e_1 + e_2 \otimes e_1 \otimes e_2 + e_2 \otimes e_2 \otimes e_1 - e_2 \otimes e_2 \otimes e_2) \otimes e_2$
$\mathcal{L}_6$	$(e_1 \otimes -be_1 \otimes e_1 + e_1 \otimes e_2 \otimes e_2 + e_2 \otimes e_1 \otimes e_2 + e_2 \otimes e_2 \otimes e_1) \otimes e_1 +$ $(e_1 \otimes -be_1 \otimes e_2 + e_1 \otimes -be_2 \otimes e_1 + e_2 \otimes -be_1 \otimes e_1 + e_2 \otimes e_2 \otimes e_2) \otimes e_2$
$\mathcal{L}_6^\perp$	$(e_1 \otimes -be_1 \otimes e_1 + e_1 \otimes e_2 \otimes e_2 + e_2 \otimes e_1 \otimes e_2 + e_2 \otimes e_2 \otimes e_1) \otimes e_1 +$ $(e_1 \otimes -ae_1 \otimes e_2 + e_1 \otimes -ae_1 \otimes e_2 + e_2 \otimes -ae_1 \otimes e_1 + e_2 \otimes e_2 \otimes e_2) \otimes e_2$

saturating sets are linear $(\rho+1, \mu)$-MCF codes and vice versa by Proposition 100.

Definition 101. A (ρ, μ)-saturating n-set in $\mathrm{PG}(N, q)$ is called *minimal* if it does not contain a (ρ, μ)-saturating $(n-1)$-set in $\mathrm{PG}(N, q)$.

For $\rho = 2$ and $N = 3$,

Theorem 102. *(Bartoli, Davydov, Marcugini & Pambianco, 2020) Let*

$$\mu = \frac{q^2 - 3q + 2}{6} \text{ if } q \not\equiv 0 \ (mod\, 3),$$

the twisted cubic $\mathcal{C}_3$ is a is a minimal $(2, \mu)$-saturating $(q+1)$-set.

Definition 103. An $[n, k]R_0$ code C is called (R_0, μ) *almost-perfect* multiple covering off the farthest-off points ((R_0, μ)-APMCF code) if each $x \in \mathbb{F}_q^n$ with $d(x, \mathrm{C}) = R_0$ belongs to exactly μ spheres centered in codewords of C.

Theorem 104. *Let μ be as in Theorem 102. Let* C *be the code associated with the twisted cubic $\mathcal{C}_3$. Then the code* C *is a $[q+1, q-3, 5]3$ quasi perfect* generalized doubly extended Reed-Solomon *(GDRS for short) code of covering radius $R_0 = 3$ and, moreover,* C *is a $(3, \mu)$-MCF code.*

Proof. Since twisted cubic is a NRC and NRC in $\mathrm{PG}(N, q)$ is a $[q+1, q-N, N+2]$

GDRS code. $(2,\mu)$ saturating set is a $(3,\mu)$-MCF code. □

There is also another link between codes and twisted cubic. Generalized Reed Solomon codes are MDS, hence their weight enumerators are known and they depend on sizes of the finite field, the length and dimension. The coset leader weight enumerator of an MDS code depends on the geometry of the associated projective system of the dual code. The twisted cubic is $[q+1, q-3, 5]$ code and the coset leader weight enumerators of this code depends on the classification of the points, lines and planes of $\mathrm{PG}(3,q)$ under the action of the stabiliser of the twisted cubic. The parity check matrix H of the $[q+1, q-3, 5]$ code is $4 \times (q+1)$. The columns of H are the points of the twisted cubic. Therefore, H is the normal rational curve of degree three in $\mathbb{F}_q$ and the columns are non-zero and no pair of columns is dependent. To determine $\theta_i = \theta_i(q)$ which are the number of vectors in $\mathbb{F}_q^4$ that are a linear combination of some set of i columns of H but not less. Generally, we want to determine θ_i the number of points in $\mathrm{PG}(3,q)$ that lie in a projective space of dimension $i-1$ that intersects $\mathcal{C}_3$ in exactly i points, not for smaller i. Therefore, we have the following questions:

24.1 θ_1: How many points on the twisted cubic $\mathcal{C}_3$?

24.2 θ_2: How many points, not counted in θ_1, are on a line containing two points of the twisted cubic $\mathcal{C}_3$?

24.3 θ_3: How many points are the on a plane which is a plane contining three points of the twisted cubic, not counted in θ_1 and θ_2?

The answers of the above questions are easy over $\mathbb{F}_q$, so $\theta_1 = (q+1)$, $\theta_2 = q(q+1)/2$, and $\theta_3 = q(q+1)^2/2$. For more results on $\mathrm{PG}(3,q)$ and $\mathrm{PG}(3,q^n)$ see (Blokhuis et al., 2021).

5. CONCLUSION AND FUTURE WORK

In the first part of my thesis, we revisit the completeness problem left open in 1967 by Segre in his seminal work (Segre, 1962). In 1980s, Pellegrino gave a long proof obtained in a series of papers that are difficult to find in the literature. Moreover, these papers are written in Italian. We contribute to the literature with an alternative short proof to the problem left open by Segre. We noticed that the existence of a line containing two internal H-free points might not happen which is mentioned in (Hirschfeld, 1993). Finally, we give examples of small arcs containing at least $(q+1)/2$ points from a conic.

In 1977, (Bruen & Hirschfeld, 1977) the lines of $\mathrm{PG}(3,q)$ were separated into disjoint line classes under the action of the stabiliser group G of the twisted cubic. Although the G-orbits of points and planes are well-known, the line classes which are a single orbit, or which are a union of orbits are not known. Hence, in the second part of my thesis, we study the classification of line orbits under the action of G. We classify lines contained in the osculating planes, lines meeting the twisted cubic, imaginary chords, and axes of the twisted cubic. For the classified G-orbits of lines, we determine the plane and point orbit distributions of lines.

The remaining G-orbits of lines partition the class $\mathcal{O}_6$ consisting of external lines to $\mathcal{C}_3$ which are not imaginary chords and which are not contained in osculating planes. There are in total $q(q-1)(q^2-1)$ such lines. As far as we know the G-orbits of these lines are not classified yet. We conjecture that there are $2q-2$ or $2q-4$ G-orbits contained in $\mathcal{O}_6$ depending on whether q is 1 or 5 modulo 6. For reasons of clarity, we state our conjecture in terms of the total number of G-orbits of lines in $\mathrm{PG}(3,q)$, i.e. including the 10 G-orbits which we already know.

Conjecture 105. *The number of line orbits under the action of G is $9+(2q-1)$, if $q \equiv 1 \pmod 6$, G is $9+(2q-3)$ if $q \equiv 5 \pmod 6$.*

As future work, we want to finish the classification of G-orbits of lines in $\mathrm{PG}(3,q)$. After the classification of the line classes $\mathcal{O}_6$, we get a complete classification of G-orbits of lines in $\mathrm{PG}(3,q)$, for q odd and not divisible by 3.

BIBLIOGRAPHY

Ball, S. (2012). On sets of vectors of a finite vector space in which every subset of basis size is a basis. *J. Eur. Math. Soc. (JEMS)*, *14*(3), 733–748.

Ball, S. & De Beule, J. (2012). On sets of vectors of a finite vector space in which every subset of basis size is a basis II. *Des. Codes Cryptogr.*, *65*(1-2), 5–14.

Ball, S. & Lavrauw, M. (2018). Planar arcs. *J. Combin. Theory Ser. A*, *160*, 261–287.

Ball, S. & Lavrauw, M. (2019). Arcs in finite projective spaces. *EMS Surv. Math. Sci.*, *6*(1), 133–172.

Bamberg, J., Betten, A., Cara, P., De Beule, J., Lavrauw, M., & Neunhöffer, M. (2018). *FinInG – Finite Incidence Geometry, Version 1.4.1.*

Bartoli, D., Davydov, A. A., Marcugini, S., & Pambianco, F. (2020). On planes through points off the twisted cubic in PG$(3,q)$ and multiple covering codes.

Blokhuis, A., Pellikaan, R., & Szőnyi, T. (2021). The extended coset leader weight enumerator of a twisted cubic code.

Bose, R. C. (1947). Mathematical theory of the symmetrical factorial design. *Sankhyā*, *8*, 107–166.

Brieskorn, E., K. H. (1986). *Plane Algebraic Curves.* Birkhauser Verlag. Basel, Boston, Stuttgart.

Bruen, A. A. & Hirschfeld, J. W. P. (1977). Applications of line geometry over finite fields. I. The twisted cubic. *Geometriae Dedicata*, *6*(4), 495–509.

Bruen, A. A., Thas, J. A., & Blokhuis, A. (1988). On M.D.S. codes, arcs in PG(n,q) with q even, and a solution of three fundamental problems of B. Segre. *Invent. Math.*, *92*(3), 441–459.

Casse, L. R. A. (1969). A solution to Beniamino Segre's "Problem $I_{r,q}$" for q even. *Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Nat. (8)*, *46*, 13–20.

Davydov, A. A., Marcugini, S., & Pambianco, F. (2021). Twisted cubic and orbits of lines in PG$(3,q)$.

GAP (2018). *GAP – Groups, Algorithms, and Programming, Version 4.9.2.* The GAP Group.

Günay, G. & Lavrauw, M. (2021). On pencil of cubics on the projective line over finite fields of characteristic>3. *arXiv:2104.04756.*

Günay, G. & Lavrauw, M. (2021). On planar arcs of size (q + 3) / 2. *Journal of Combinatorial Designs.*

Hall, Jr., M. (1975). Ovals in the Desarguesian plane of order 16. *Ann. Mat. Pura Appl. (4)*, *102*, 159–176.

Harris, J. (2013). *Algebraic Geometry: A First Course.* Graduate Texts in Mathematics. Springer New York.

Hirschfeld, J. (1998). *Projective Geometries Over Finite Fields.* Oxford mathematical monographs. Clarendon Press.

Hirschfeld, J., James William Peter, H., & Hirschfeld, R. (1979). *Projective Geometries Over Finite Fields.* Oxford mathematical monographs. Clarendon Press.

Hirschfeld, J., Korchmáros, G., & Torres, F. (2013). *Algebraic Curves over a Finite Field.* Princeton Series in Applied Mathematics. Princeton University Press.

Hirschfeld, J. & Storme, L. (1998). The packing problem in statistics, coding theory

and finite projective spaces. *Journal of statistical planning and inference*, *72*(1-2), 355–380.

Hirschfeld, J. W. P. (1993). American mathematical society. *Mathematical Reviews*.

Hirschfeld, J. W. P. & Korchmáros, G. (1996). On the embedding of an arc into a conic in a finite plane. *Finite Fields Appl.*, *2*(3), 274–292.

Hirschfeld, J. W. P. & Korchmáros, G. (1998). On the number of rational points on an algebraic curve over a finite field. volume 5 (pp. 313–340). Finite geometry and combinatorics (Deinze, 1997).

Hirschfeld, J. W. P. & Storme, L. (2001). The packing problem in statistics, coding theory and finite projective spaces: update 2001. In *Finite geometries*, volume 3 of *Dev. Math.* (pp. 201–246). Kluwer Acad. Publ., Dordrecht.

Hirschfeld, J. W. P. & Thas, J. A. (1991). *General Galois geometries*. Oxford Mathematical Monographs. The Clarendon Press, Oxford University Press, New York. Oxford Science Publications.

Korchmáros, G. & Sonnino, A. (2003). Complete arcs arising from conics. volume 267 (pp. 181–187). Combinatorics 2000 (Gaeta).

Lavrauw, M. (2020a). On linear systems of conics over finite fields [slides].

Lavrauw, M. (2020b). Tensors in finite geometry [slides].

Lavrauw, M. & Popiel, T. (2020). The symmetric representation of lines in $\mathrm{PG}(\mathbb{F}^3 \otimes \mathbb{F}^3)$. *Discrete Math.*, *343*(4), 111775, 22.

Lavrauw, M., Popiel, T., & Sheekey, J. Combinatorial invariants for nets of conics in $\mathrm{PG}(2,q)$. *Des. Codes Cryptogr.*

Lavrauw, M. & Sheekey, J. (2015). Canonical forms of $2\times3\times3$ tensors over the real field, algebraically closed fields, and finite fields. *Linear Algebra Appl.*, *476*, 133–147.

Lombardo-Radice, L. (1956). Sul problema dei k-archi completi in $s_{\{}2,q\}$. ($q = p^t$, p primo dispari.). *Bollettino dell'Unione Matematica Italiana*, *11*(2), 178–181.

Maruta, T. & Kaneta, H. (1991). On the uniqueness of $(q+1)$-arcs of $\mathrm{PG}(5,q)$, $q = 2^h$, $h \geq 4$. *Math. Proc. Cambridge Philos. Soc.*, *110*(1), 91–94.

Newstead, P. E. (1981). Invariants of pencils of binary cubics. *Math. Proc. Cambridge Philos. Soc.*, *89*(2), 201–209.

Nunemacher, J. (1991). Mathematics and its history. by john stillwell. *The American Mathematical Monthly*, *98*(6), 569–574.

O'Keefe, C. M. & Penttila, T. (1991). Hyperovals in $\mathrm{PG}(2,16)$. *European J. Combin.*, *12*(1), 51–59.

Pellegrino, G. (1981a). Complete arcs of order $(q+3)/2$ in the Galois planes $S_{2,q}$ with $q \equiv 3 \pmod 4$. *Rend. Circ. Mat. Palermo (2)*, *30*(2), 311–320.

Pellegrino, G. (1981b). Sui campi di galois, di ordine dispari, che ammettono terne di quadrati (non-quadrati) consecutivi. *Boll. Un. Mat. Ital.*, *5*(17B), 1482–1495.

Pellegrino, G. (1982a). Complete arcs of order $(q+3)/2$ in Galois planes $S_{2,q}$, with $q \equiv 1 \pmod 4$. *Rend. Mat. (7)*, *2*(1), 59–66.

Pellegrino, G. (1982b). Sulle sostituzioni lineari, sui campi finiti di ordine dispari, che conservano oppure scambiano il carettere quadratico degli elementi transformati. *Boll. Un. Mat. Ital.*, *6*(19B), 211–223.

Pellegrino, G. (1992). On complete arcs in the plane $\mathrm{PG}(2,q)$, with q odd, containing $(q+3)/2$ points of a conic. *Rend. Mat. Appl. (7)*, *12*(3), 649–674.

Pellegrino, G. (1993a). Complete arcs, containing $(q+1)/2$ points of a conic, in Galois planes of odd order. *Rend. Circ. Mat. Palermo (2)*, *42*(2), 273–308.

Pellegrino, G. (1993b). Complete arcs, containing $(q+1)/2$ points of a conic, in Galois planes of odd order. *Rend. Circ. Mat. Palermo (2)*, *42*(2), 273–308.

Segre, B. (1954). Sulle ovali nei piani lineari finiti. *Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Nat. (8)*, *17*, 141–142.

Segre, B. (1955a). Curve razionali normali e k-archi negli spazi finiti. *Ann. Mat. Pura Appl. (4)*, *39*, 357–379.

Segre, B. (1955b). Ovals in a finite projective plane. *Canadian J. Math.*, *7*, 414–416.

Segre, B. (1959). Le geometrie di Galois. *Ann. Mat. Pura Appl. (4)*, *48*, 1–96.

Segre, B. (1962). Ovali e curve σ nei piani di Galois di caratteristica due. *Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Nat. (8)*, *32*, 785–790.

Segre, B. (1967). Introduction to Galois geometries. *Atti Accad. Naz. Lincei Mem. Cl. Sci. Fis. Mat. Natur. Sez. Ia (8)*, *8*, 133–236.

Segre, B. & Bartocci, U. (1971). Ovali ed altre curve nei piani di Galois di caratteristica due. *Acta Arith.*, *18*, 423–449.

Storme, L. & Thas, J. A. (1993). M.D.S. codes and arcs in $\mathrm{PG}(n,q)$ with q even: an improvement of the bounds of Bruen, Thas, and Blokhuis. *J. Combin. Theory Ser. A*, *62*(1), 139–154.

Thas, J. A. (1968). Normal rational curves and k-arcs in Galois spaces. *Rend. Mat. (6)*, *1*, 331–334.

Vandendriessche, P. (2019). Classification of the hyperovals in $\mathrm{PG}(2,64)$. *Electron. J. Combin.*, *26*(2), Paper No. 2.35, 12.

Voloch, J. F. (1991). Complete arcs in Galois planes of nonsquare order. In *Advances in finite geometries and designs (Chelwood Gate, 1990)*, Oxford Sci. Publ. (pp. 401–406). Oxford Univ. Press, New York.

Wall, C. (1983). Pencils of real binary cubics. *Mathematical Proceedings of the Cambridge Philosophical Society*, *93*(3), 477–484.

Weil, A. (1948). *Sur les courbes algébriques et les variétés qui s'en déduisent.* Actualités Sci. Ind., no. 1041 = Publ. Inst. Math. Univ. Strasbourg **7** (1945). Hermann et Cie., Paris.