Università degli Studi di Padova

Dipartimento di Matematica "Tullio Levi-Civita"

Corso di Laurea Magistrale in Matematica

Del Pezzo Surfaces and points in the plane

Candidato:

Federico Mangano

mat.1218975

Relatori:

Jonas Bergström

Olof Bergvall

Orsola Tommasi

Anno accademico 2020/2021- **25 Giugno 2021**

Abstract

This thesis will focus on the study of the relationship that exists between Del Pezzo surfaces, a kind of surface defined as "a smooth birationally trivial surface V on which the sheaf ω_V^{-1} is ample" and counting points in the projective plane $\mathbb{P}_k^2$ built over a finite field k.

The result allowing us to to link the two concepts says that a Del Pezzo surface of degree d bigger that 1 is isomorphic to the blowup up of 9-d points in $\mathbb{P}_k^2$.

Once we have settled the relationship between the two concepts the results will revolve around counting n-tuples of points in $\mathbb{P}_k^2$ both from a theoretical and computational point of view.

In particular the case of 8-tuples, corresponding to Del Pezzo surfaces of degree 1, will be the one around which most of the work will revolve, culminating with the statement of a degree 8 monic polynomial expressing the number of 8-tuples of points in general position as a function of the dimension of the base field.

The work concludes by considering further instances of counting points in a projective plane, in particular in the case of points on which the Frobenius morphism acts in a specific way.

Contents

1 Introduction

Del Pezzo surfaces were first introduced by Pasquale Del Pezzo, an Italian mathematician that in his two notes "Sulle superficie dell'ordine n immerse negli spazi di n+1 dimensioni" [13] and "Sulle superficie dell'n^{mo} ordine immerse nello spazio di n dimensioni" [14] laid the foundations for the definition and study of such surfaces. His work was full of marvelous theorems and observation but, as it's common for mathematics coming from before the 20th century, relies on a notation and a mindset that is now considered outdated and therefore unfit to be used as a direct source for a modern approach to the topic.

The definition we'll use for them is "a smooth birationally trivial surface V on which the sheaf ω_V^{-1} is ample". This definition is on itself not as interesting, for the purpose of the results we want to get about counting Del Pezzo surfaces, as others that stem from it. In particular the most interesting for this work will link Del Pezzo surfaces of degree ≤ 7 to the blow-up of points in $\mathbb{P}^2_k$. Moreover counting n-tuples of points also connects with the cohomology of Del Pezzo surfaces.

The goal of this work will be to obtain a polynomial depending on the cardinality of a finite field $\mathbb{F}_q$ and counting the number of 8-tuples of points in general position in the projective space $\mathbb{P}^2_{\mathbb{F}_q}$, and by this also Del Pezzo surfaces of degree 1, as was already done for surfaces of degree 2 in several works, for example in [3]. To do this we'll need to consider different topics in algebraic geometry and algebra.

More in detail, structurally the thesis will be made of two big topics that will then converge in the core section.

We'll therefore start by laying the theoretical foundation, as long as they differ from the one that can be found in an introductory curse on algebraic geometry, for the definition of Del Pezzo surface that will then be studied on themselves giving results that describe them under many different points of view. Del Pezzo surfaces will be defined by their sheaf, as blowups of points in the projective plane, in the case in case of low degrees we'll describe them more in detail in the blowup space, and their exceptional curves will be described and enumerated.

The focus will then move to algebra, first by describing finite fields and their algebraic closure, and them by tackling the problem of counting point sin the projective plane $\mathbb{P}^2_{\mathbb{F}_q}$ built from a finite field. *This counting will also constitute the biggest part of results obtained independently from the sources,*

although they will not be original. Moreover the problem of counting n-tuples by means of a computer will be considered and with that in mind strategies to both compute results and do it faster will be elaborated.

In the one that will constitute the sixth section this two topics will converge, with the goal of obtaining a function of the cardinality of the base field that counts 8-tuples in general position and therefore Del Pezzo surfaces of degree 1 in the case of finite field.

This will constitute the main original result but will not represent the end of the thesis, in fact the reasoning that led to it, or to be more precise to the decision to use a finite, and therefore not algebraically closed, field as the base one , lead to further development an example of which is given.

This is the study of the action of the Frobenius morphism on n-tuples of points in the projective plane built over the closure of a finite field, and will be the focus of the last section, *that again even if the results are not original was developed autonomously.*

But even if we called it final this section will not be the one to conclude the work, this because a big role in obtaining the main result was held by algorithms is SageMath. *This autonomously written code* will therefore, along with the bibliography and some longer proof that disrupt the flow of the main sections, be collected and transcribed in the appendix.

2 Preliminary topics in algebraic geometry

This section will contain a number of definition and theorems that are needed to define Del Pezzo surfaces and prove results about them.

2.1 Sheaves: some definitions

The results here are taken from [9] and therefore notation and terminology have to be considered as given in there, in particular in chapter 2.

Definition 2.1.1 ([9], pg 153)
Let X be a noetherian scheme, i.e. a scheme that can be covered by open affine subsets Spec A_i (a locally noetherian scheme) for A_i a noetherian ring and such that it's also quasi-compact. Quasi-compact means that every open covering of X, seen as a topological space and not a locally ringed space, contains a finite open subcovering.An invertible sheaf $\mathcal{L}$ on X is said to be ***ample*** *if for every coherent sheaf $\mathcal{F}$ on X there is an integer $n_0 > 0$ (depending of $\mathcal{F}$) such that for every $n \geq n_0$ the sheaf $\mathcal{F} \otimes \mathcal{L}^n$, for $\mathcal{L}^n$ the n-fold tensor power of $\mathcal{L}$ with itself, is generated by its global sections.*

A sheaf $\mathcal{L}$ on X is said to be ***very ample relative to*** *Y (where X is a scheme over Y) if there is an immersion $i : X \to \mathbb{P}^n_Y$ for some n such that $\mathcal{L} \simeq i^*\mathcal{O}(1)$*

Definition 2.1.2 ([9], pg 175)
Let $f : X \to Y$ be a morphism of schemes. We consider the diagonal morphism $\Delta : X \to X \times_Y X$, this is an isomoprhism onto its image, $\Delta(X)$ is a locally closed subscheme of $X \times_Y X$ i.e. a closed subscheme of an open subset W of $X \times_Y X$.

Let $\mathcal{I}$ be the sheaf of ideal of $\Delta(X)$ in W. Then we define the ***sheaf of relative differentials of*** *X* ***over*** *Y to be the sheaf $\Omega_{X/Y} = \Delta^*(\mathcal{I}/\mathcal{I}^2)$ on X.*

We can notice how $\mathcal{I}/\mathcal{I}^2$ has a natural structure of $\mathcal{O}_{\Delta(X)}$-module. Then since Δ induces an isomorphism of X to $\Delta(X)$, $\Omega_{X/Y}$ has a natural structure of $\mathcal{O}_X$-module. Furthermore $\Omega_{X/Y}$ is quasi-coherent; if Y is noetherian and f a morphism of finite type then $X \times_Y X$ is also noetherian and therefore $\Omega_{X/Y}$ is coherent.

Definition 2.1.3 ([9], pg 180)
Let X be a nonsingular variety over k. We define the ***canonical sheaf of*** *X to be $\omega_X = \bigwedge^n \Omega_{X/k}$, the n-th exterior power of the sheaf of differential, where*

$n = dim\ X$. It is an invertible sheaf on X. If X is projective and nonsingular, we define the ***geometric genus of*** *X to be $p_g = dim_k \Gamma(X, \omega_X)$, this is a non-negative integer.*

An invertible sheaf is said to be anticanonical if its inverse is a canonical sheaf.

Definition 2.1.4 ([9], pg 182)
Let Y be a non-singular subvariety of a non-singular variety X over k. The locally free sheaf $\mathcal{I}/\mathcal{I}^2$, where $\mathcal{I}$ is the sheaf of ideals defining Y as a subscheme, takes the name of ***conormal sheaf of*** *Y* ***in*** *X. Its dual $\mathcal{N}_{Y/X} = Hom_{\mathcal{O}_Y}(\mathcal{I}/\mathcal{I}^2, \mathcal{O}_Y)$ is called the* ***normal sheaf of*** *Y* ***in X*** *and it's locally free of rank $r = codim(Y, X)$.*

Definition 2.1.5 ([9], pg.110)
We define the group $\tilde{M}(U)$ to be the set of functions $s : U \to \bigsqcup_{\mathfrak{p} \in U} M_{\mathfrak{p}}$ such that for each $\mathfrak{p} \in U$, $s(\mathfrak{p}) \in M_{\mathfrak{p}}$ and such that s is locally a fraction m/f with $m \in M$ and $f \in A$. To be precise, we require that for each $\mathfrak{p} \in U$ there is a neighbourhood V of $\mathfrak{p}$ in U, and there are elements $m \in M$ and $f \in A$ such that for each $q \in V$, $f \notin q$, and $s(q) = m/f$ in $M_{\mathfrak{p}}$ We make $\tilde{M}$ into a sheaf by using the obvious restriction maps.

Theorem 2.1.6 (The adjunction and addition formulas)
Let Y be a non-singular subvariety of a non-singular variety X over k.

Adjunction formula: [[9], II.8.20] $\omega_Y \simeq \omega_X \otimes \bigwedge^r \mathcal{N}_{Y/X}$;

Addition formula: [[9], II.5.12] Let S be a graded ring and $x = Proj\ S$. We can assume that S is generated by $S(1)$ as an S_0-algebra. For any graded S-module M, $\tilde{M}(n) \simeq \tilde{M(n)}$. In particular $\mathcal{O}_X(n) \otimes \mathcal{O}_X(m) \simeq \mathcal{O}_X(n+m)$;

Proof.

- We can take the highest exterior powers of the locally free sheaves in the exact sequence

$$0 \to \mathcal{I}/\mathcal{I}^2 \to \Omega_{X/k} \otimes \mathcal{O}_Y \to \Omega_{Y/k} \to 0.$$

  We thus find that $\omega_X \otimes \mathcal{O}_Y \simeq \omega_Y \otimes \bigwedge^r (\mathcal{I}/\mathcal{I}^2)$ taking the determinant of the exact sequence. Formation of the highest exterior power commutes with taking the dual sheaf and so $\omega_Y \simeq \omega_X \otimes \bigwedge^r \mathcal{N}_{Y/X}$;

- This follows from the fact that $(M \tilde{\otimes}_S N) \simeq \tilde{M} \otimes_{\mathcal{O}_X} \tilde{N}$ for any two graded S-modules M and N, when S is generated by $S(1)$. Indeed, for any $f \in S(1)$ we have $(M \otimes_S N)_{(f)} = M_{(f)} \otimes_{S_{(f)}} N_{(f)}$;

□

Corollary 2.1.7 (Adjunction formula for divisors, [[9], II.8.20)
In the adjuction formula if $r = 1$ then Y can be considered a divisor, we can take $\mathcal{L}$ as the associated invertible sheaf on X. Then $\omega_Y \simeq \omega_X \otimes \mathcal{L} \otimes \mathcal{O}_Y$.

Proof. If $r = 1$ we have that $\mathcal{I}_Y \simeq \mathcal{L}^{-1}$ and so $\mathcal{I}/\mathcal{I}^2 \simeq \mathcal{L}^{-1} \otimes \mathcal{O}_Y$ and $\mathcal{N}_{Y/X} \simeq \mathcal{L} \otimes \mathcal{O}_Y$. So applying the previous result with $r = 1$ we obtain $\omega_Y \simeq \omega_X \otimes \mathcal{L} \otimes \mathcal{O}_Y$. □

Note 2.1.8 ([9], II.8.20.1)
To obtain the canonical sheaf of $X = \mathbb{P}^n$ one can take the exact sequence

$$0 \to \Omega_{X/Y} \to \mathcal{O}_X(-1)^{n+1} \to \mathcal{O}_X \to 0$$

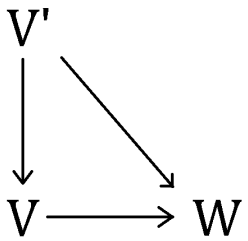
and by taking the highest exterior power find out that $\omega_X \simeq \mathcal{O}_X(-n-1)$.

2.2 Core theorems on birational maps

The definition of Del Pezzo surface we are working towards contains two requirements, we took care of the theory underlying the first one in the previous subsection and in this we'll work from the second. This is birational triviality and we'll state other theorems regarding birational maps that will be needed in the proves regarding Del Pezzo surfaces.

We therefore list, without proof that, given how such results are quite lengthy, three important results on birational maps.

Theorem 2.2.1 (Resolution of singularities of a map, [12], 21.1)
Let V be a smooth projective surface over a field k, W a projective variety and $f : V \to W$ some birational map. Then there exists a resolution of f, i.e. we can draw the following graph for h a morphism and g a birational morphism



in which g decomposes as an iteration of blowing ups of closed points which lie over point where f is not defined.

Theorem 2.2.2 (Structure theorem for birational morphism, [12], 21.4)
Let $f : V \to W$ be a birational morphism of smooth projective surfaces over a field k. Then f is an iteration of blowing up of closed points. In other words, there exists a sequence of surfaces and morphisms

$$V = V_0 \to^{f_1} V_1 \to^{f_2} V_2 \cdots \to^{f_r} V_r = W$$

such that $f_i : V_{i-1} \to V_i$ is the blowing up of a closed point $x_i \in V_i$ and such that $f = f_r \circ f_{r-1} \circ \cdots \circ f_1$.

Even if the proof is omitted it contains an important lemma that we formulate on its own:

Lemma 2.2.3 ([12], 21.4.1)
Let $f : V \to W$ as in the theorem and let the rational map f^{-1} be not defined at the closed point $x \in W$. Then f decomposes into a product $V \to^{f'} W' \to^{h} W$ where h is the blowing up of x, and f' is some morphism.

2.3 Intersection theory

More specific description of Del Pezzo surfaces of low degree require a study of intersection numbers and therefore this subsection becomes important to fix these results.

Theorem 2.3.1 (Bertini's theorem[9], II.8.18)
Let X be a nonsingular closed subvariety of $\mathbb{P}^n_k$, where k is an algebraically closed field. Then there exists a hyperplane $H \subseteq \mathbb{P}^n_k$, not containing X, and such that the scheme $H \cap X$ is regular at every point, i.e. its local rings are regular everywhere. Furthermore, the set of hyperplanes with this property forms an open dense subset of the complete linear system $|H|$, i.e. the set of all effective divisors linearly equivalent do H, considered as a projective space. If $\dim X \geq 2$ then the schemes $H \cap X$ are irreducible and nonsingular.

Corollary 2.3.2 ([9], II.8.18.1)
This result continues to hold even if X has a finite number of singular points, because the set of hyperplanes containing any one of them is a proper closed subset of $|H|$.

Definition 2.3.3 ([9], pg.357)
We say that, for C and D curves on X and $P \in C \cap D$, C and D ***meet transversally*** *at P if the local equations $, g$ of C, D at P generate the maximal ideal m_P of $\mathcal{O}_{P,X}$.*

Lemma 2.3.4 ([9], V.1.2)
Let $C_1, \ldots, C_r$ be irreducible curves on the surface X, and let D be a very ample divisor, i.e. $\mathcal{L}(D)$, the associated invertible sheaf, is very ample. Then almost all curves D' in the complete linear system $|D|$ are irreducible, non singular and meet each of the C_1 transversally.

Proof. We embed X in a projective space $\mathbb{P}^n$ using the very ample divisor D. We can apply Bertini's theorem to X and the curves $C_1, \ldots C_r$. We conclude that most $D' \in |D|$ are irreducible nonsingular curves in X, and that the intersections $C_i \cap D$ are nonsingular, i.e. points with multiplicity one, which means that the C_i and D' meet transversally. Since we didn't assume nonsingularity for the C_i we need to use Bertini's corollary. □

Definition 2.3.5 (Invertible sheaf corresponding to a Cartier divisor, [9], pg.144)
$\mathcal{L}(D)$ is the sub-$\mathcal{O}_X-$module of the sheaf of total quotient rings generated by $f_i^{-1}(U_i)$ where $\{(U_i, f_i)\}_i$ represent D.

Lemma 2.3.6 ([9], V.1.3)
Let C be an irreducible singular curve on X, and let D be any curve meeting C transversally. Then

$$card(C \cap D) = deg_C(\mathcal{L}(D) \otimes \mathcal{O}_C).$$

Proof. Here deg_C denotes the degree of the invertible sheaf $\mathcal{L}(D) \otimes \mathcal{O}_C$ on C. We use the fact that $\mathcal{L}(-D)$ is the sheaf of ideals of D on X. Therefore, tensoring with $\mathcal{O}_C$, we have the exact sequence

$$0 \to \mathcal{L}(-D) \otimes \mathcal{O}_C \to \mathcal{O}_C \to \mathcal{O}_{C \cap D} \to 0$$

where now $C \cap D$ denotes the scheme theoretic intersection. Thus $\mathcal{L}(D) \otimes \mathcal{O}_C$ is the invertible sheaf on C corresponding to the divisor $C \cap D$. Since the intersection is transversal, the degree of $C \cap D$ is just the number of points in it.

□

Theorem 2.3.7 (Definition of intersection number, [9], V.1.1)
There is a unique pairing $Div\ X \times Div\ X \to \mathbb{Z}$, denoted by (C, D) for any two divisors C, D such that:

1. *If C and D are non singular curves meeting transversally, then we have that $(C, D) = card(C \cap D)$, the number of points of $C \cap D$;*

2. *It is symmetric: $(C, D) = (D, C)$;*

3. *It is additive: $(C_1 + C_2, D) = (C_1, D) + (C_2, D)$;*

4. *It depends only on the linear equivalence classes: $C_1 \sim C_2$ implies $(C_1, D) = (C_2, D)$.*

Proof. As a first thing we can show uniqueness. We can fix an ample divisor H on X. If we consider two divisors C, D on X we can find an integer $n > 0$ such that $C + nH, D + nH$ and nH are very ample. Indeed we can first chose $k > 0$ such that $\mathcal{L}(C + kH), \mathcal{L}(D + kH)$ and $\mathcal{L}(kH)$ are generated by global section. This is possible by the definition itself of ampleness . We can then choose $l > 0$ such that lH is very ample. Taking $n = k + l$ it follows that $C + nH, D + nH$ and nH are all very ample. We can now use the first of the lemmas and choose nonsingular curves

$$\begin{array}{rl} C' \in |C + nH| & \\ D' \in |D + nH| & \textbf{transversal to C'} \\ E' \in |nH| & \textbf{transversal to D'} \\ F' \in |nH| & \textbf{transversal to C' and E'.} \end{array}$$

Then $C \sim C' - E'$ and $D \sim D' - F'$ so by the properties of the theorem we have

$$(C, D) = card(C' \cap D') - card(C' \cap F') - card(E' \cap D') + card(E' \cap F').$$

This proves that the intersection number is uniquely determined by these properties.

Regarding existence we can use the same method and check that everything is well defined. To simplify matters, we proceed in two steps. Let $\mathfrak{B} \subseteq Dvi\ X$ be the set of very ample divisor. Then $\mathfrak{B}$ is a cone, in the sense that the sum of two very ample divisors is again very ample. For $C, D \in \mathfrak{B}$ we define the intersection number (C, D) as follows: by the first lemma choose $C' \in |C|$ nonsingular and $D' \in |D|$ nonsingular and transversal to C'. Define $(C, D) = card(C' \cap D')$. To prove this is well-defined first fix C' and let $D'' \in |D|$ be another non-singular curve, transversal to C'. Then by the second lemma

$$card(C' \cap D') = deg\mathcal{L}(D') \times \mathcal{O}_{C'}$$

and the same for D''. But $D' \sim D''$ so $\mathcal{L}(D') \simeq \mathcal{L}(D'')$ so these two numbers are the same. Thus our definition is independent of D'. Now suppose $C'' \in$

$|C|$ is another nonsingular curve. By the previous step we may assume D' is transversal to both C' and C'' and by the same argument we see that $card(C' \cap D') = card(C'' \cap D'')$. So now we have a well-define pairing $\mathfrak{B} \times \mathfrak{B} \to \mathbb{Z}$ which is clearly symmetric and by definition only depends on the linear equivalence classes of the divisors. It also follows from the second lemma that this is additive since $\mathcal{L}(D_1 + D_2) \simeq \mathcal{L}(D_1) \otimes \mathcal{L}(D_2)$ and the degree is additive on a curve. Finally this pairing on $\mathfrak{B} \times \mathfrak{B}$ satisfies the first condition by construction. To define the intersection pairing on all of $Div\ X$ let C and D be any two divisors. Then as above we can write $C \sim C' - E$ and $D \sim D' - F'$ where C', D', E', F' are all in $\mathfrak{B}$. So we define

$$(C, D) = (C', D') - (C', F') - (E', D') + (E', F').$$

If, for example, we used $C \sim C'' - E''$ with C'', E'' also very ample, then

$$C' + E'' \sim C'' + E'$$

so by what we have shown for the pairing in $\mathfrak{B}$ we have

$$(C', D') + (E'', D') = (C'', D') + (E', D')$$

and the same happened for F' in place of D'.Thus the resulting two expressions for (C, D) are the same. This shows that the intersection pairing (C, D) is well-defined on all of $Div\ X$. It satisfies also the other 3 properties by construction and by the corresponding properties on $\mathfrak{B}$, the first one again follows from the first lemma. □

Proposition 2.3.8 ([9], V.1.4)
If C and D are curves with no common irreducible component and $P \in C \cap D$ we define ***the intersection multiplicity*** $(C, D)_P$ *as $len(\mathcal{O}_{P,X}/(f, g))$ for f, g local equations of C, D at P.*

The following formula then holds

$$(C, D) = \sum_{P \in C \cap D} (C, D)_P.$$

Proof. As in the proof of the second lemma let $\mathcal{L}(D)$ be the invertible sheaf corresponding to D. Then we have the exact sequence

$$0 \to \mathcal{L}(-D) \otimes \mathcal{O}_C \to \mathcal{O}_C \to \mathcal{O}_{C \cap D} \to 0$$

where we consider $C \cap D$ as a scheme. Now the scheme $C \cap D$ has support at the points of $C \cap D$ and for any such P its structure sheaf is the k-algebra $\mathcal{O}_{P,X}/(f, g)$. Therefore

$$dim_k\ H^0(X, \mathcal{O}_{C \cap D}) = \sum_{P \in C \cap D} (C, D)_P.$$

On the other hand we can compute H^0 from the cohomology sequence of the exact sequence above, and thus obtain

$$dim\ H^0(X, \mathcal{O}_{C\cap D}) = \chi(\mathcal{O}_C) - \chi(\mathcal{L}(-D) \otimes \mathcal{O}_C)$$

. And so we proved that the expression $\sum(C, D)_P$ depends only on the linear equivalence classes. By replacing C and D by difference of nonsingular curves, all transversal to each other as in the proof of the theorem, we see this is equal to the intersection number. □

Definition 2.3.9 ([9], V.1.4.1)
*If D is any divisor on the surface X we can define the **self intersection number** (D, D). This, even for a nonsingular curve, cannot be directly calculated as in the proposition. However we can use linear equivalence and we can also notice how*

$$C^2 = deg(\mathcal{L}(C) \otimes \mathcal{O}_C).$$

Note 2.3.10 ([9], V.1.4.4)
*Using self intersection we can define a new numerical invariant of a surface. Let ω_X be the canonical sheaf of the surface X. Any divisor K in the linear equivalence class corresponding to ω_X is called a **canonical divisor**. K^2, the self intersection of the canonical divisor, depends only on X.*

Proposition 2.3.11 (Adjunction formula, [9], V.1.5)
This is a reformulation of the adjunction formulas 2.1.6 and 2.1.7 in the particular case of curves and that focuses more on the degrees of the two sides of the equality.

If C is a nonsingular curve of genus g on a surface X, and if K is the canonical divisor on X, then

$$2g - 2 = (C, (C + K)).$$

Proof. We have from the adjunction formula that for $r = 1$, $\omega_C \simeq \omega_X \otimes \mathcal{L}(C) \otimes \mathcal{O}_C$. The degree of ω_C is $2g - 2$ and on the other hand

$$deg_C(\omega_X \otimes \mathcal{L} \otimes \mathcal{O}_C) = (C, C + K)$$

as we showed above. □

This allows us to quickly compute the genus of a curve if we know the degree and vice versa. For example a curve of degree d in $\mathbb{P}^2$ gives us

$$2g - 2 = d * (d - 3) \Rightarrow g = \frac{1}{2}(d - 1)(d - 2)$$

, if we instead consider a curve of type (a,b) on a quadric surface then $C+K$ has type $(a-2, b-2)$ and so

$$2g-2 = a*(b-2)+(a-2)(b) \Rightarrow g = ab-a-b+1$$

We conclude the subsection with the statement and proof of Riemann-Roch theorem, first for curves and then in a more general fashion:

Theorem 2.3.12 (Riemann-Roch for curves, [9], IV.1.3)
Let D be a divisor on a curve X of genus g. Then

$$l(D) - l(K-D) = deg\ D + 1 - g$$

. Here $l(D) = dim_k\ H^0(X, \mathcal{L}(D))$ (and so is equal to $dim|D|+1$).

Proof. The divisor $K-D$ corresponds to the invertible sheaf $\omega_X \otimes \mathcal{L}(D)^V$, we then have (we need to use Serre duality) that $H^0(X, \omega_X \otimes \mathcal{L}(D)^V)$ is dual to $H^1(X, \mathcal{L}(D))$ and thus we turned the problem into proving

$$\chi(\mathcal{L}(D)) = deg\ D + 1 - g$$

where for any coherent sheaf $\mathcal{F}$

$$\chi(\mathcal{F}) = \sum (-1)^i dim_k H^i(X, \mathcal{F})$$

is the Euler characteristic that in this case becomes

$$\chi(\mathcal{F}) = dim_k H^0(X, \mathcal{F}) - dim_k H^1(X, \mathcal{F}).$$

We first consider $D=0$, then we obtain

$$dim_k H^0(X, \mathcal{O}_X) - dim_k H^1(X, \mathcal{O}_X) = 0 + 1 - g$$

that is true because $dim H^0(X, \mathcal{O}_X) = k$ for any projective variety and $dim_k H^1(X, \mathcal{O}_X) = g$.

Now let D be any divisor and P any point. We'll show that the formula is true for D if and only if it's true for $D+P$. Since any divisor can be reached from 0 in a finite number of steps by adding or subtracting points this will prove the result for all D. We can consider P as a closed subscheme of X. Its structure sheaf is a skyscraper sheaf, i.e. a sheaf of the form $i_{x,*}A$ for any point x of X where $i_x : x \to X$ is the inclusion of a point into X and A is an abelian group. This sheaf sits at P, that we denote by $k(P)$ and its sheaf of ideals is $\mathcal{L}(-P)$, therefore we have the exact sequence

$$0 \to \mathcal{L}(-P) \to \mathcal{O}_X \to k(P) \to 0.$$

We can now tensor with $\mathcal{L}(D+P)$ to get

$$0 \to \mathcal{L}(D) \to \mathcal{L}(D+P) \to k(P) \to 0$$

($\mathcal{L}(D+P)$ is locally free of rank 1 so tensoring by it doesn't affect $k(P)$). Now from the additivity of the Euler characteristic and from $\chi(k(P)) = 1$ we get

$$\chi(\mathcal{L}(D+P)) = \chi(\mathcal{L}(D)+1),$$

on the other hand $deg\,(D+P) = deg\ D+1$ and so our formula is true for D if and only if it's true for $D+P$. □

Theorem 2.3.13 (Riemann-Roch,[9], V.1.6)
If D is any divisor on the surface X then

$$l(D) - s(D) + l(K-D) = \frac{1}{2}(D, D-K) + 1 + p_a,$$

*for p_a the arithmetic genus, $l(D) = dim_k H^0(X, \mathcal{L}(D))$ and $s(D)$ is defined as $dim\ H^1(X, \mathcal{L}(D))$ and takes the name of **superabundance**. In this context we have that $p_a = \chi(\mathcal{O}_X) - 1$.*

Proof. We have that (again coming from Serre duality)

$$l(K-D) = dim\ H^0(X, \mathcal{L}(D)^V \otimes \omega_X) = dim\ H^2(x, \mathcal{L}(D))$$

that tells us that the left side of the equation is nothing but the Euler characteristic and turns the goal into proving

$$\chi(\mathcal{L}(D)) = \frac{1}{2}(D, D-K) + 1 + p_a.$$

Both sides only depend on the linear equivalence class of D and so we can, as we already did in other proofs, set $D = C - E$ for two nonsingular curves. Now we can compute. The ideal sheaves of C and E are $\mathcal{L}(-C)$ and $\mathcal{L}(-D)$ and we obtain the exact sequences, by tensoring,

$$0 \to \mathcal{L}(C-E) \to \mathcal{L}(C) \to \mathcal{L}(C) \otimes \mathcal{O}_E \to 0$$

and

$$0 \to \mathcal{O}_X \to \mathcal{L}(C) \to \mathcal{L}(C) \otimes \mathcal{O}_C \to 0$$

but the Euler characteristic is additive on short exact sequences and so we have

$$\chi(\mathcal{L}(C-E)) = \chi(\mathcal{O}_X) + \chi(\mathcal{L}(C) \otimes \mathcal{O}_C) - \chi(\mathcal{L}(C) \otimes \mathcal{O}_E).$$

Now $\chi(\mathcal{O}_X) = 1 + p_a$ and using the Riemann-Roch theorem for curves we get

$$\chi(\mathcal{L}(C) \otimes \mathcal{O}_C) = (C, C) + 1 - g_C$$

and

$$\chi(\mathcal{L}(C) \otimes \mathcal{O}_E) = (C, E) + 1 - g_E$$

we can now compute the genus using the adjunction formula 2.3.11 to get

$$g_C = \frac{1}{2}(C, (C + K)) + 1$$

$$g_E = \frac{1}{2}(E, (E + K)) + 1$$

and combining everything we obtain

$$\chi(\mathcal{L}(C - E)) = \frac{1}{2}(C - E, C - E - K) + 1 + p_a$$

as we wanted. □

2.4 The Picard group

Closely related to divisors is the Picard group, and similarly this will be used in the proofs of many properties regarding Del Pezzo surfaces.

Definition 2.4.1 ([9], pg.143)
*For any ringed space X we define the **Picard Group** of X, **Pic X**, to be the group of isomoprhism classes of invertible sheaves of X under the operation $\otimes$. There is an identity element, since $\mathcal{O}_X \otimes \mathcal{L} \simeq \mathcal{L}$ moreover the tensor product is associative. It is true that if $\mathcal{L}$ and $\mathcal{M}$ are invertible sheaves on a ringed space X so is $\mathcal{L} \otimes \mathcal{M}$ If $\mathcal{L}$ is any invertible sheaf on X then there exists an invertible sheaf $\mathcal{L}^{-1}$ on X such that $\mathcal{L} \otimes \mathcal{L}^{-1} \simeq \mathcal{O}_X$ We call this sheaf the **inverse** of L. All of this shows that Pic is indeed a group.*

Theorem 2.4.2 ([12], 20.9)
Let $f : Y \to Y'$ be the blowup map of a closed point, and W' the exceptional divisor. f induces an embedding of Picard groups $f^* : Pic\ V \to Pic\ V'$ (corresponding to the homomorphism f^* of the divisor group) which preserves the intersection numbers:

$$(f^*L_1, f^*L_2) = (L_1, L_2)$$

for all $L_1, L2 \in Pic\, V$, moreover

$$(W, W') = -d \quad d = [k(x) : k] \quad (f^*L, W') = 0$$

for all $L \in Pic\, V$ (we write W' instead of $\mathcal{O}_{V'}(W')$).

The full proof of this is lengthy and requires several other theorems and so it's unfit to be put in such a work. However the same can't be said about the first statement and some corollaries:

Proof. The sheaf $f^*(L)$ is invertible on V' for every invertible sheaf L on V;Let D an effective divisor. As a particular case of invertible image we have that taking $L = \mathcal{O}_V(D)$ it immediately follows from the definition that $f^*(\mathcal{O}_V(D))$ is canonically isomorphic to $\mathcal{O}_{V'}(f^*(D))$. Therefore the maps f^* on the groups Div and Pic correspond. □

Corollary 2.4.3
Under the conditions of the theorem we have

$$Pic\, V' = f^*(Pic\, V) \oplus \mathbb{Z}w$$

for w the class of $\mathcal{O}_{V'}(W')$ and the subgroups $f^*(Pic\, V)$ and $\mathbb{Z}w$ determine one another uniquely as orthogonal complements with respect to the intersection number.

Proof. We already proved a similar result for the Div group:

$$Div\, V' = f^*(Div\, V) \oplus \mathbb{Z}W'.$$

The kernel of the canonical homomorphism $Div\, V' \to Pic\, V'$ is completely contained in $f^*(Div\, V)$, because if $f^*(D) + aW'$ is a principal divisor, then

$$0 = (f^*(D) + aW', W') = -a.$$

Consequently, $Pic\, V' = f^*(Pic\, V) \oplus \mathbb{Z}w$. The second assertion also follows immediately from the corresponding lemma for Div. □

Proposition 2.4.4 ([12],20.10)
Under the conditions of the Lemma we have

$$\omega_{V'} = f^*(\omega_V) + w$$

where w is the class of the sheaf $\mathcal{O}_{V'}(W')$ in $Pic\, V'$.

Using the Picard group we are able to compute some intersection numbers corresponding to canonical divisors as defined in 2.3.10

Example 2.4.5
Let $X = \mathbb{P}^2$ implies $Pic\, \mathbb{P}^2 \simeq \mathbb{Z}$ generated by h, and $K = -3h$, so $K^2 = 9$.

If X is a quadric surface the Picard group is isomorphic to $\mathbb{Z} \oplus \mathbb{Z}$, K has type $(-2, -2)$ and $K^2 = (-2)^2 + (-2)^2 = 8$.

2.5 Weighted spaces

[[11], V.1.3] Weighted spaces are the ones where Del Pezzo surfaces of degree 1 and 2 live and so is good to have a proper definition of them. Let k be a field and $S = k[x_0, \dots, x_n]$ the polynomial ring in $n+1$ variables. Let $a_i \in \mathbb{N}$, we can define a grading of S by $deg\, x_i = a_i$. $ProjS$, i.e. the set of all homogeneous prime ideals of S that don't contain all of $S_+ := \bigoplus_{d>0} S_d$, is called **the weighted projective space of dimension n with weights a_i**. It's denoted by $\mathbb{P}_{(a_0,\dots,a_n)}$. The following properties hold:

- $\mathbb{P}_{(a_0,\dots,a_n)} \simeq \mathbb{P}_{(da_0,\dots,da_n)}$ and so we'll assume the weights to be coprime, if they are the space is said to be **well formed**;
- $\mathbb{P}_{(a_0,\dots,a_n)} \simeq \mathbb{P}^n/\mu_{a_0} \times \cdots \times \mu_{a_n}$ where μ_{a_i} is the group of a_u^{th} roots of unity and acts on $\mathbb{P}^n$ by multiplying the i-th coordinate;
- Let $\mathcal{O}(m)$ be the coherent sheaf associated to the graded module $S(m)$: $\mathcal{O}(m)$ is locally free $\iff$ $a_i | m$ for every i;
- $\mathbb{P}_{(a_0,\dots,a_n)}$ has isolated singularities $\iff$ the weights are pairwise relatively prime.

3 Introduction to Del Pezzo surfaces

The main sources that will be used with regards to Del Pezzo surfaces are Yuri I. Manin's "Cubic Forms, Algebra, Geometry, Arithmetic" [12], chapters 24, and Janos Kollar's "Rational curves on algebraic varieties" [11], chapter III.3.

3.1 Definition and basic properties

Theorem 3.1.1 ([12],24.1)
Let V be a smooth cubic surface over a field k, i.e a surface defined by a polynomial of degree 3 in $\mathbb{A}^3_k$. Then

1. *V is birationally trivial;*
2. *The anticanonical sheaf ω_V^{-1} is ample.More precisely $\omega_V^{-1} \simeq \mathcal{O}_V(1)$ under the usual projective embedding.*

Before going to the proof we need to state a lemma:

Lemma 3.1.2 ([9], II.8.20.3)
A hypersurface X of degree d in $\mathbb{P}^n$ for $n \geq 2$, has $\omega_X^n \simeq \mathcal{O}_X(n+1-d)$.

Proof. Taking $i : X \hookrightarrow \mathbb{P}^n$ as the inclusion of the smooth hypersurface of degree d into the projective space we can rewrite the case $r = 1$ of the adjunction formula 2.1.7 as

$$\omega_X \simeq i_* \omega_{\mathbb{P}^n} \otimes \mathcal{O}_X(d)$$

and from $\omega_{\mathbb{P}^n} \simeq \mathcal{O}_{\mathbb{P}^n}(-n-1)$ we get

$$\omega_X \simeq i_* \mathcal{O}_{\mathbb{P}^n}(-n-1) \otimes \mathcal{O}_X(d) = \mathcal{O}_X(-n-1+d).$$

The corresponding anticanonical sheaf is therefore

$$\omega_X^{-1} \simeq \mathcal{O}_X(-(-n-1+d)) = \mathcal{O}_X(n+1-d).$$

□

Proof of the theorem. 1. It can be proven, see [8]'s section 11, that on any smooth cubic surface lie 27 lines, moreover at least two of these, we can

call them D and D', are disjoint and if we consider any point on the cubic then there is a unique line passing through it, D and D'.

Is therefore possible to define two dominant rational maps (and so prove birationality):

$X \to D \times D'$ We can send every point a not in $D \cup D'$ to (a_1, a_2), the intersections of D and D' with the unique line through them and a. This map is clearly well defined away from $D \cup D'$;

$D \times D' \to X$ We can map the pair (a_1, a_2) to the unique intersection point between the line passing through them and X, this is well defined whenever the line through them is not contained in X, and this is an open condition.

We therefore have two rational maps that behave like inverse from an open set to an open set, id est birational maps. But it's well known that $\mathbb{P}^2$ is birational to $\mathbb{P}^1 \times \mathbb{P}^1$ and trivial that $D \times D' \simeq \mathbb{P}^1 \times \mathbb{P}^1$ and so by transitivity we proved birational triviality.

2. We can now turn our attention to the second claim. This comes from the lemma 3.1.2 In particular if we take the hypersurface V to have degree 3 we get

$$\omega_V \simeq \mathcal{O}_X(1+1-3) = \mathcal{O}_X(-1) \Rightarrow \omega_V^{-1} \simeq \mathcal{O}_X(1)$$

and this is exactly what a cubic surface in $\mathbb{P}^3$ is.

Here the embedding is the natural 3-rd Veronese embedding $\mathbb{P}^3 \to \mathbb{P}^{19}$ sending

$$[x_0 : x_1 : x_2 : x_3] \to [x_0^3 : x_1^3 : x_2^3 : x_3^3 : x_0^2 x_1 : \ldots x_2 x_3^2]$$

the set of all monomials of degree 3, this makes the cubic surfaces a linear subspace and we'll consider this embedding better later.

□

Definition 3.1.3 ([12],24.2)
A smooth birationally trivial surface V on which the sheaf ω_V^{-1} is ample is called a Del Pezzo surface.

We call $\mathbf{d}=(\omega_V, \omega_V)$, the self intersection number of the canonical sheaf, the degree of the Del Pezzo surface V. It coincides with the projective degree of $i(V)$ in $\omega_V^{-1} \simeq i^*(\mathcal{O}(1))$.

Lemma 3.1.4 ([12],24.3.1)
For every (smooth projective) surface V which is birationally trivial, the group $Pic\, V$ is free with a finite number of generators and

$$rk\ Pic\ V + (\Omega_V, \Omega_V) = 10.$$

Proof. Let $V \to V'$ be the blowup map of a closed point. It follows from the theorem 2.4.2 that the lemma is true for V if and only if it's true for V'. The theorems 2.2.1 and 2.2.2 then show that it suffices to verify the lemma on a single arbitrary surface, for instance $\mathbb{P}^2$. In this case we have $\omega_{\mathbb{P}^2} \simeq \mathcal{O}_{\mathbb{P}^2}(-3)$ and $Pic\, \mathbb{P}^2 \simeq \mathbb{Z}$ so the lemma holds and the proof is over. □

Theorem 3.1.5 ([12],24.3)
Let V be a Del Pezzo surface of degree d. Then:

1. $1 \leq d \leq 9$;
2. *Every irreducible curve with a negative self-intersection number on V is exceptional;*
3. *If V has no exceptional curves, then either $d = 9$ and V is isomorphic to $\mathbb{P}^2$, or $d = 8$ and V is isomorphic to $\mathbb{P}^1 \times \mathbb{P}^1$.*

Proof.

1. This is implied by the previous lemma once we notice that both (ω_V, ω_V), from the fact that ω_V^{-1} is ample, and $rk\ Pic\ V$ are at least equal to 1;
2. Let $D \subset V$ be an irreducible curve and $(D, D) < 0$. Because ω_V^{-1} is ample we get $(D, \omega_V^{-1}) > 0$ (this is the degree of the curve D, which divides n, if ω_V^{-1} induces a projective embedding of V and D). On the other hand
$$2p_a(D) - 2 = (D, D) - (D, \omega_V^{-1})$$
which is nothing but the modified version of the adjunction formula 2.3.11. Now $p_a(D) \geq 0$ being D irreducible and this leaves us with
$$(D, D) = -1 \quad p_a(D) = 0.$$
This is only possible if $D \simeq \mathbb{P}^1$ that proves that the curve is exceptional;
3. If there are no exceptional curves on V, then V is minimal and by (ii) it has no curves with negative self-intersection number. But $\mathbb{P}^2$ and $\mathbb{P}^1 \times \mathbb{P}^1$ are the only minimal rational surfaces for which this is true and are both, quite obviously, Del Pezzo surfaces.

□

3.2 Del Pezzo surfaces as blow-ups

Theorem 3.2.1 (Explicit description of Del Pezzo surfaces [12] 24.4)
Let V be a Del Pezzo surface of degree d:

1. *If $d = 9$, then V is isomorphic to $\mathbb{P}^2$:*
2. *If $d = 8$, then V is isomorphic to either $\mathbb{P}^1 \times \mathbb{P}^1$ or the preimage of $\mathbb{P}^2$ under a blowing up map of a point;*
3. *If $7 \geq d \geq 1$, then V is isomorphic to the preimage of $\mathbb{P}^2$ under a blowing up map of the union of $9 - d$ closed points, no three of them which lie on one line and no six of them which lie on a conic.*

Conversely every such surface for $d \geq 3$ is a Del Pezzo surface of the corresponding degree.

Note 3.2.2
With stronger requirements regarding general position we can extend the inverse statement also to degrees 1 and 2, to do so we need the surface to satisfy the requirements set it 3.4.6.

Proof. We already analysed the case of minimal surfaces in the previous theorem so let V be non-minimal. Then there exits a birational morphism $f : V \to W$ for W a minimal rational surface, W cannot be a non-trivial ruled surface, otherwise there would be an irreducible curve D on W with self intersection number -2 and $(f^{-1}(D), f^{-1}(D)) \leq -2$ contradicting the previous theorem as this is not exceptional (exceptional curves have self intersection number equal to -1). We are therefore left with $W = \mathbb{P}^2 \vee W = \mathbb{P}^1 \times \mathbb{P}^1$. In the latter case let $x \in W$ be a point where f^{-1} is not defined. From 2.2.3 we know that f can be split as $V \to^g W' \to W$ where the latter is the blowing up map of x. But for W' we have in turn a morphism $h : W' \to \mathbb{P}^2$ collapsing the inverse images of the two fibres of the projection of W on $\mathbb{P}^1$ and passing through x. The composed morphism $V \to^g W' \to^h \mathbb{P}^2$ gives us, also in this case, a birational morphism of V to $\mathbb{P}^2$. We can call, with a slight abuse of notation, this morphism f. Since under each blowing up map of a closed point the rank of the Picard group goes up by one (since $Pic\, V' \simeq Pic\, V \oplus \mathbb{Z}$), and the rank of this group for V is $10 - d$ we have that f splits into a product of $9 - d$ such transformations. Let $x_1, \ldots, x_s \in \mathbb{P}^2$ be all closed points where f^{-1} is not defined, then $r = s$ necessarily. If not $s < r$ and then one of the blowing up maps of the decomposition of f would have centre on the inverse image

of some x_i under the blowing up of the point itself. After such a transformation the proper image of D, an effective divisor, would have an intersection number equal to -2 and on V this number can only go down, thus giving us a contradiction (the only curves with negative self intersection in V have it equal to -1). We can now suppose that 3 points are collinear on the line D, then $(f^1(D), f^{-1}(D)) \leq -2$ given how the self intersection number becomes -2 from just blowing up these 3 points. In a similar fashion if we had a conic containing at least 5 points then this would again be converted into a curve with a self intersection number smaller or equal to -2. □

The inverse statement comes as a consequence of the following lemma, whose proof is quite long and complex and therefore will be omitted, as will the proof of the its corollary.

Lemma 3.2.3 ([12] 24.5)
If the surface V is obtained from $\mathbb{P}^2$ by means of a blowing up map centred at $r \leq 6$ closed points in general position regarding lines and conics, then the sheaf ω_V^{-1} is very ample and its sections yield a closed embedding of V in a projective space of dimension

$$dim H^0(V, \omega_V^{-1}) - 1 = (\omega_V, \omega_V) = 9 - r.$$

The set of exceptional curves is identified under this embedding with the set of lines in the containing space which lie on V. The image of V has degree $9 - r$.

Note 3.2.4 ([12] 24.5.1)
It's worth noticing that this theorem stops working for $n \geq 7$. This is exactly the reason why we need to be more careful, and consider cubic curves, while counting n-tuples points in general position for $n \geq 7$.

Corollary 3.2.5 ([12] 24.5.2)
Let $V' \to^f V$ be a birational morphism:

1. *If V' is a Del Pezzo surface, then so is V;*
2. *If V is a Del Pezzo surface and all curves in V' with a negative self-intersection are exceptional, V' is a Del Pezzo surface*

3.3 Del Pezzo surfaces of low degree

We start by noticing a fact about Del Pezzo surfaces of high degree:

Note 3.3.1 ([12] 24.4.1)
For $7 \geq d \geq 5$, all Del Pezzo surfaces turn out to be isomorphic if they have the same degree, this comes from the fact that the automorphisms of $\mathbb{P}^2$ act transitively on a system of ≤ 4 points in general position, and will be better explored in 5.4.2.

Regarding curves of low degree we first need to state a theorem and a lemma, whose proof will be omitted, listing some properties of canonical and anticanonical sheaves of Del Pezzo surfaces:

Theorem 3.3.2 ([11],III.3.2.5)
Let X be a Del Pezzo surface, we define $h^n := dim(H^n)$. Then

1. *$h^1(X, \mathcal{O}(\omega_k^{-m})) = 0$ for $m \geq 0$;*
2. *$h^0(X, \mathcal{O}(\omega_k^{-m})) = \frac{m(m+1)}{2} dim(\omega_X, \omega_X) + 1$ for $m \geq 0$.*

Proof. Both statements are stable under field extension so we can assume the field to be closed. Let $C \in |\omega_X^{-1}|$ be the general member in this class, this is irreducible and reduced and has genus 1 (see 2.3.4). We can consider the sequence

$$H^1(X, \mathcal{O}(\omega_k^{-m})) \to H^1(X, \mathcal{O}(\omega_k^{-(m+1)})) \to H^1(C, \mathcal{O}(\omega_k^{-(m+1)})) = 0$$

we can now prove the first statement inductively. The second derives from applying the Riemann-Roch theorem 2.3.13. □

Lemma 3.3.3 ([11], 3.4)
Let X be a Del Pezzo surface. Then

1. *$|\omega_X^{-m}|$ is free if $m * (\omega_X, \omega_X) \geq 2$;*
2. *r_j for $j \leq \alpha(\omega_X, \omega_X)$ generate $R(X, \omega_X^{-1})$;*
3. *$|\omega_X^{-1}|$ is very ample if $(\omega_X, \omega_X) \geq 3$*

*where $r_j := H^0(C, L)$ and $R(C, L) = \sum_{i \geq 0} r_i$ takes the name of **canonical ring**, and α is a function defined as $\alpha(1) = 3$, $\alpha(2) = 2$ and $\alpha(m) = 1$ for $m \geq 3$.*

Theorem 3.3.4 (Explicit description of Del Pezzo surfaces of low degree, [11] III.3.5)
Let X be a Del Pezzo surface over a field k, assume that the degree is at most 4. Then $X \simeq Proj\left(\sum_{m \geq 0} H^0(X, \mathcal{O}(\omega_X^{-m}))\right)$ can be described as follows:

1. *If* $deg = 1$, *then* $X \simeq X_6 \subset \mathbb{P}_{(1,1,2,3)}$;

2. *If* $deg = 2$, *then* $X \simeq X_4 \subset \mathbb{P}_{(1,1,1,2)}$;

3. *If* $deg = 3$, *then* $X \simeq X_3 \subset \mathbb{P}^3$;

4. *If* $deg = 4$, *then* $X \simeq X_{2,2} \subset \mathbb{P}^4$;

Conversely, any smooth weighted complete intersection, i.e. complete intersection in a weighted space, as the ones above is a Del Pezzo surface of the expected degree.

Note 3.3.5
We remind that a complete intersection is an algebraic variety whose ideal is generated by codim V *elements. And indeed the hypersurfaces above are such, being of codimension one and generated, as we'll see, by a single element. The same happens for the pencil of quadrics ,i.e being made by* 2 *polynomials that define varieties of codimension* $4-2=2$, *where in general a pencil is a family of geometric objects with a common property.*

Proof. This proof is a personal version of the one given by Kollar, in particular changes were made to make more explicit the reason why we chose polynomials of a certain degree or some particular weighted spaces.

We can start by defining

$$\begin{array}{ccc} X & \hookrightarrow & \mathbb{P} \\ & \uparrow & \\ & via & (\omega_k^{-1}) \end{array}$$

Consider: $R(X) = \bigoplus_{n\geq 0} H^0(\mathcal{O}((\omega_k^{-n}))$ where $R(X)$ is the ring of all functions on X given by $(\omega_k^{-1}$ and each of the summand is made of restricted homogeneous polynomials from $\mathbb{P}$

To understand X, i,e, get equations for X in $\mathbb{P}$, we want to find relationships in $R(X)$

We can start with the case of degree 2, we know from the lemma that the anticanonical ring is generated by $H^0(\mathcal{O}((\omega_k^{-1}))$ and $H^0(\mathcal{O}((\omega_k^{-2}))$. We now compute the dimension of these spaces using the definitions we gave in theorem 3.3.2:

1. $h^0(X, \mathcal{O}((\omega_k^{-1})) =: h^0(\mathcal{O}((\omega_k^{-1}))) = 3 \leftarrow$, with $H^0(\mathcal{O}((\omega_k^{-1})))$ generated by x, y, z (polynomials of degree 1 in 3 variables);

2. $h^0(X, \mathcal{O}((\omega_k^{-2}))) = 7$ but from x, y, z we can only get 6 polynomials that are homogeneous of degree 2, i.e. $x^2, y^2, z^2, xz, xy, yz$ so there is another element in the base of $H^0(\mathcal{O}((\omega_k^{-2})))$, we can call it "$t$".

So the anticanonical ring is generated by x, y, z, t. This implies that X is isomorphic to an hypersurface X' in the weighted projective space $\mathbb{P}_{(1,1,1,2)}$ (3 generators come from $H^0(\mathcal{O}((\omega_k^{-1})))$ and one from $H^0(\mathcal{O}((\omega_k^{-2}))))$. Now we can continue computing $h^0(X, \mathcal{O}((\omega_k^{-n})))$

- $h^0(\mathcal{O}((\omega_k^{-3})) = 13$ and indeed we can build 13 polynomials of degree 3 (keeping in mind that t has degree 2) from x, y, z, t, i.e $\binom{3-1+3}{3} = 10$ (multiset binomial coefficient $\left(\binom{n}{k}\right) = \binom{n+k-1}{k}$ counting the ways to chose k elements in a set of n but allowing repetitions) made only from x, y, z and 3 that include t;

- $h^0(\mathcal{O}((\omega_k^{-4})) = 21$. In a way similar as before we can check that from x, y, z, t we can build $\binom{3-1+4}{4} = 15$ polynomial that are homogeneous of degree 4 made only from x, y, z and $\binom{3-1+2}{2} = 6$ that include t and some of x, y, z, plus t^2. We therefore have 1 extra polynomial and this concludes our search.

The extra polynomial in $H^0(\mathcal{O}((\omega_k^{-4}))$ tells us there is a relationship between these elements and so X' is given by a degree 4 polynomial.

In a similar fashion we know that for $(\omega_X, \omega_X) = 1$ the anticanonical ring is generated by:

- $h^0(\mathcal{O}((\omega_k^{-1}))) = 2$ with $H^0(\mathcal{O}((\omega_k^{-1})))$ generated by x, y (polynomials of degree 1 in 2 variables);

- $h^0(X, \mathcal{O}((\omega_k^{-2}))) = 4$ but from x, y we can only get 3 polynomials that are homogeneous of degree 2, i.e. x^2, y^2, xy so there is another element in the base of $H^0(\mathcal{O}((\omega_k^{-2})))$, we can call it "$t$";

- $h^0(\mathcal{O}((\omega_k^{-3})) = 7$ but from x, y, t we can only get 6 polynomials that are homogeneous of degree 3, i.e. $x^3, x^2y, y^2x, y^3, xt, yt$ so there is another element in the base of $H^0(\mathcal{O}((\omega_k^{-3})))$, we can call it "$k$".

So the anticanonical ring is generated by x, y, t, k. This implies that X is isomorphic to an hypersurface X' in $\mathbb{P}_{(1,1,2,3)}$. Now we can continue computing $h^0(X, \mathcal{O}((\omega_k^{-n})))$:

- $h^0(\mathcal{O}((\omega_k^{-4})) = 11$ and we can build $\binom{2-1+4}{4} = 5$ homogeneous polynomials of degree 4 from just x, y. There are $\binom{2-1+2}{2} = 3$ elements that contain t and some of x and y. Then there is t^2 and to end we have $\binom{2-1+1}{1} = 2$ elements that contain k, and the sum is indeed 11;

- $h^0(\mathcal{O}((\omega_k^{-5})) = 16$. Here we have $\binom{2-1+5}{5} = 6$ polynomials homogeneous of degree 5 made only from x, y. There are $\binom{2-1+3}{3} = 4$ polynomials of the form t*polynomial in x, y of degree 3. We can build $\binom{2-1+2}{2} = 3$ polynomials that include k and some of x, y. The family of polynomials including t^2 contains only t^2x and t^2y and finally we have yk. The total is indeed 16;

- $h^0(\mathcal{O}((\omega_k^{-5})) = 22$.Here we have $\binom{2-1+6}{6} = 7$ polynomials homogeneous of degree 6 made only from x, y. We can consider then a polynomial made of t and a polynomial of degree 4 in x, y, there are $\binom{2-1+4}{4} = 5$ of them. The set of polynomials in x, y of degree 2 multiplied by t^2 contains $\binom{2-1+2}{2} = 3$ elements. We then have t^3. There are $\binom{2-1+3}{3} = 4$ polynomials of degree 3 in x, y that we can multiply by k. Of course we have k^2. We can finally consider the polynomials containing $k * t$ and these are $k * t * x$ and $k * t * y$. The total is 23. We therefore have 1 extra polynomial and this concludes our search.

The extra polynomial in $H^0(\mathcal{O}((\omega_k^{-4}))$ tells us there is a relationship between these elements and so X' is given by a degree 6 polynomial. If $deg = 3$ (respectively 4) then ω_X^{-1} is very ample and gives an embedding $X \to \mathbb{P}^3$ (resp. $\mathbb{P}^{\not 4}$) whose image has degree 3 (resp. 4). If $deg = 3$ then the image must be a cubic surface. If $deg = 4$ we can again compute h^0:

- $h^0(\mathcal{O}((\omega_k^{-1})) = 5$, so H^0 is generated by x, y, z, t, r;

- $h^0(\mathcal{O}((\omega_k^{-2})) = 13$, however $\binom{5-1+2}{2} = 15$, we therefore have 2 extra polynomials.

As in the previous cases this means that the image in $\mathbb{P}^4$ is generated by 2 degree 2 polynomials, i.e. a pencil of quadrics. □

3.4 Exceptional curves in a Del Pezzo surface

Definition 3.4.1 ([12] 23.7)
Let $r \geq 1$ be an integer. We consider a composed object $\{N_r, \omega_r, (,)\}$, where

i) $N_r = \mathbb{Z}^{r+1} = \bigoplus_{i=0}^{r} \mathbb{Z} l_i$ *for* (l_i) *a chosen basis;*

ii) $\omega_r = (-3, 1, \ldots, 1) \in N_r$*;*

iii) $(,)$ *is a bilinear form* $N_r \times N_r \to \mathbb{Z}$ *given by:*

$$(l_0, l_0) = 1 \quad (l_i, l_i) = -1 \; if \; i \geq 1 \quad (l_i, l_j) = 0 \; if \; i \neq j.$$

We define the subsets $R_r, I_r \subset N_r$ *by the condition*

iv) $R_r = \{I \in N_r | (I, \omega_r) = 0, \; (I, l) = -2\}$;

v) $I_r = \{I \in N_r | (I, \omega_r) = (I, l) = -1\}$

Proposition 3.4.2 ([12] 25.1)
Let V *be a Del Pezzo surface of degree* d *which is not isomorphic to* $\mathbb{P}^1 \times \mathbb{P}^1$*, let* $r = 9 - d$ *(which is also the number of points we need to blowup to obtain the Del Pezzo surface form* $\mathbb{P}^2$*). There exists in the Picard group* $PicV$ *a free basis* $(l_0, l_1, \ldots, l_r)$ *such that:*

1. $\omega_V = -3l_0 + \sum_{i=1}^{r} l_i$*;*
2. $(l_0, l_0) = 1, \; (l_i, l_i) = -1, \;$ *for* $i \geq 1$*, and* $(l_i, l_j = 0)$ *for* $i \neq j$.

Proof. Let $f : V \to \mathbb{P}^2$ be the blowing up map centered at the r point and defining the Del Pezzo surface. Let l_0 be the class of $f^*(\mathcal{O}_{\mathbb{P}^2}(1))$ and l_i, for $i \geq 1$, the classes of the sheaves $\mathcal{O}_V(D_i)$ for D_i the inverse image of the blown up points. They constitute a basis for $Pic\, V$ from the fact that $Pic\, V = f^* Pic\, \mathbb{P}^2 \oplus \mathbb{Z}w$. We can then use the formula $\omega_V = f^*(\omega_{\mathbb{P}^2}) + w$, and consider that $\omega_{\mathbb{P}^2} \simeq \mathcal{O}_{\mathbb{P}^2}(-3)$, to get that indeed $\omega_V = -3l_0 + \sum_{i=1}^{r} l_i$. To compute the self intersection numbers we can use the formulas of theorem 2.4.2. □

Corollary 3.4.3 ([12] 25.1.1)
The object $\{Pic\; V, \omega_V, intersection\; number\}$ *is, up to isomoprhism, only dependent on* r *and coincides with the object* $\{N_r, \omega_r, (,)\}$.

We can now consider an exceptional curve $D \subset V$. We have that the class l of $\mathcal{O}_V$ in $Pic\, V$ is such that

$$(l, \omega_V) = (l, l) = -1,$$

all such classes take the name of **exceptional classes**. The isomoprhism we stated in the corollary above identifies the set of exceptional classes in $Pic\, V$ with the subset $I_r \subset N_r$. Let

$$l = al_0 - \sum_{i=1}^{r} b_i l_i \in N_r.$$

$l \in N_r$ implies (we are solving a Diophantine equation)

$$3a - \sum_{i=1}^{r} b_i = 1 \tag{1}$$

$$a^2 - \sum_{i=1}^{r} b_i^2 = -1. \tag{2}$$

Note 3.4.4 ([12] pg.134)
If we want to describe I_r for $r \leq 8$ we can use two easy arguments. The first one is to notice how $I_r = I_8 \cap (\bigoplus_{i=1}^{r} \mathbb{R} l_i)$ so that we suffice to compute I_8. The second one is to introduce in the equations (1) and (2) the auxiliary "unknown" $b_9 = 1$ which reduces the question to solving the system:

$$3a - \sum_{i=1}^{9} b_i = 0 \tag{3}$$

$$a^2 - \sum_{i=1}^{9} b_i^2 = -2 \tag{4}$$

$$b_9 = 1. \tag{5}$$

Theorem 3.4.5 ([12] 26.1)
All the solutions of the system made of equations (1) and (2) are obtained by all possible permutations of the b_i as in the rows of the following table:

a	b_1	b_2	b_3	b_4	b_5	b_6	b_7	b_8
0	−1	0	0	0	0	0	0	0
1	1	1	0	0	0	0	0	0
2	1	1	1	1	1	0	0	0
3	2	1	1	1	1	1	1	0
4	2	2	2	1	1	1	1	1
5	2	2	2	2	2	2	1	1
6	3	2	2	2	2	2	2	2

Proof. We can prove that for $r = 9$ the system made of equations (3) and (4) is equivalent to

$$3a - \sum_{i=1}^{9} b_i = 0 \tag{6}$$

$$a \sum_{i=1}^{9} (a - 3b_i)^2 = 18. \tag{7}$$

We can than look for the explicit solutions to the second equation (there are not many of them in the integers if we forget the order) and see which are also solutions of the first one, the actual computations are quite long so will be put in the appendix 8.3. □

Theorem 3.4.6 (On exceptional curves on a Del Pezzo surface,[12] 26.2) *Let V be a Del Pezzo surface of degree $1 \leq d \leq 7$, and let $f : V \to \mathbb{P}^2$ be its representation as a blowing up map of $r = 9 - d$ points in $\mathbb{P}^2$, then the following assertions hold:*

i) The map $D \to (\text{class of } \mathcal{O}_V(D)) \in Pic\, V$ establishes a one to one onto correspondence between exceptional curves on V and exceptional classes in the Picard group. These classes generate the Picard group;

ii) The image $f(D)$ in $\mathbb{P}^2$ of an arbitrary exceptional curve $D \subset V$ is of one of the following types:

   a) One of the points x_i;

   b) A line passing through two of the points;

   c) A conic passing through five of the points;

   d) A cubic passing through seven of the points x_i such that one of them is a double point;

   e) A quartic passing through eight of the points x_i such that three of them are double points;

   f) A quintic passing through eight of the points x_i such that six of them are double points;

   g) A sextic passing through eight of the points x_i such that seven of them are double points are one is a triple point.

iii) The number of exceptional curves on V for each n-tuple of points is given by the following table

8	7	6	5	4	3	2
240	56	27	16	10	6	3

Proof. i) Let L be the exceptional sheaf on V, that is,

$$(L, L) = (L, \omega_V) = -1.$$

We can apply the Riemann-Roch theorem 2.3.13 to it, taking into account that $p_a(V) = 0$, discard H^1 and replace H^2 by its dual group. We then find

$$dim\ H^0(V, L) \geq$$

$$\frac{1}{2}(L, L) - \frac{1}{2}(\omega_V, L) + 1 - dim\ H^0(V, \omega_V \otimes L^{-1}) = 1 - dim\ H^0(V, \omega_V \otimes L^{-}1).$$

But

$$(\omega_V^{-1}, \omega_V \otimes L^{-1}) = -d - 1 < 0,$$

now the sheaf ω_V^{-1} is ample and so $\omega_V \otimes L^{-1}$ has no non-zero sections. Thus $dim\ H^0(V, L) \geq 1$. Let s be a non-zero section of L, and D the divisor of its zeros, and let $D = \sum a_i D_i,\ a_i > 0$ be its decomposition into irreducible components. Now $1 = (\omega_V - 1, D) = \sum a_i(\omega_V^{-1}, D_i)$ and from the ampleness of ω_V^{-1} it follows that $(\omega_V^{-1}, D_i) > 0$. D can therefore have only one irreducible component which has multiplicity one. From the condition on L it follows that $p_a(D) = 0,\ (D, D) = -1$, therefore D is an exceptional curve and $L \simeq \mathcal{O}_V(D)$. Two different exceptional curve belong to different exceptional classes:

$$\mathcal{O}_V(D_1) \simeq \mathcal{O}_V(D_2) \Rightarrow (D_1, D_2) = (D_1, D_1)$$

but the latter is equal to -1 whilst the first is ≥ 0 if $D_1 \neq D_2$. The last of the assertions of i) is obtained by induction on r, starting with $r = 3$. For $r = 2$ we have, with the notation we introduced in 3.4.2, that $Pic\ V$ is generated by the classes of $l_0 - l_1 - l_2, l_1, l_2$ that are all exceptional;

ii) We use again with the notation of 3.4.2. Suppose that $f(D)$ is not a point. If the class l of $\mathcal{O}_V(D)$ is of the form $al_0 - \sum_{i=1}^{2} b_i l_i$ then $b_i = (D, l_i)$ so that the point x_i becomes a b_i-multiple point of $f(D)$ under the

collapsing of a curve of the class l_i into x_i. Because $D = f^{-1}(f(D))$ we have

$$class\ f^*(f(D)) = l + \sum_{i=1}^{r} b_i l_i = a l_0,$$

from which we get that the degree of $f(D)$ is given by the expression

$$(f(D), \mathcal{O}_{\mathcal{P}^2}(1)) = (f^*(f(D)), l_0) = a.$$

Now it becomes clear that the list a)-g) is a direct translation in geometric language of the table in 3.4.5, where a is the degree of the curve and b_i is the multiplicity of the point so for example the 9-uple (3,2,1,1,1,1,1,0) means "curve of degree 3, passing through 7 points one of which is a double point".

iii) This is simply a matter of computing how many n-tuples of points are there in a set of k-point, for example if we have 7 points from the table in 3.4.5 we know that we have to count

- Singular points: for a total of $\binom{7}{1} = 7$;
- Lines through two points:for a total of $\binom{7}{2} = 21$;
- Conics through five points: for a total of $\binom{7}{5} = 21$;
- Cubic passing through seven points; for a total of $\binom{7}{7} * \binom{7}{1} = 7$, the first factor counts how many sets of seven points are there, the second how many sets of one point (we have to assign the double point) are there in seven points.

and the total is indeed 56.

□

4 Preliminary topics in algebra

4.1 On the existence of finite fields

These are classical results of algebra (in particular we'll follow Dummit and Foote, Abstract Algebra [6]) but it's indeed worth mentioning them in some detail, given how important finite field and their closure are for our desired result. By reviewing this topic we set the ground to discuss the algebraic closure of them and the role of the Frobenius morphism.

The first result we'll take into consideration a personal formulation and proof of a standard result, telling us that the only possible fields have order, i.e. number of elements, a prime power:

Theorem 4.1.1
The order of a finite field F is equal to p^n for some prime integer p and integer n.

Proof. We can consider the map

$$P : \mathbb{Z} \to F \quad s.t. \quad P(z) = 1_F * z := 1_F + 1_F + \dots 1_F \ (n \ times)$$

now we know that $Im(P) \simeq \mathbb{Z}/ker(P)$, but the image is a subring of F and a subring of an integral domain (and a field is an integral domain) is an integral domain. This because a subring contains the additive identity 0_F and so $a * b = 0_F$ in the subring implies $a * b = 0_F$ in the integral domain and therefore one of a or b is equal to 0. So we get that $ker(P)$ has to be a prime ideal of $\mathbb{Z}$. The prime ideals of $\mathbb{Z}$ are of the form $p\mathbb{Z}$ for some prime integer p and so $Im(P)$ (the so called prime subfield) is a subfield of order p of F that therefore, being a vector space over it, has to have order p^n for some integer n. □

For the second result we can consider the base field $\mathbb{F}_p$, we remind that this is $\mathbb{Z}/p\mathbb{Z}$ for p a prime integer, id est the set $\{0, 1, 2, \dots, p-1\}$ endowed with the product $a *_{\mathbb{F}_p} b = a *_{\mathbb{Z}} b \pmod p$ $a *_{\mathbb{F}}$ making $\mathbb{Z}/p\mathbb{Z} \setminus \{0\}$ into an abelian group. We now consider the splitting field for the polynomial $x^{p^n} - x$ over $\mathbb{F}_p$. i.e. the smallest field containing all the roots of the polynomial $x^{p^n} - x$ seen as an element of $\mathbb{F}_p[x]$. This polynomial is separable (has no multiple root); to prove this we can take advantage of the following proposition

Proposition 4.1.2 ([6], 13.5.33)
A polynomial $f(x)$ has a multiple root α if and only if α is also a root of $D_x f(x)$ (the formal derivative of f)

Proof. Suppose that α is a multiple root of $f(x)$, then over the splitting field we can write

$$f(x) = (x-\alpha)^n g(x)$$

for some polynomial $g(x)$ and $n \geq 2$, we can now take the formal derivative and get

$$D_x f(x) = n(x-\alpha)^{n-1} g(x) + (x-\alpha)^n D_x g(x)$$

and α is clearly a root of this.

Vice versa suppose that $f(x)$ and $D_x f(x)$ have a common root and suppose that

$$f(x) = (x-\alpha)h(x)$$

, taking the derivative we obtain

$$D_x f(x) = h(x) + (x-\alpha)D_x h(x)$$

, if we compute it in α we get that

$$0 = D_x f(\alpha) = h(\alpha)$$

and so

$$h(x) = (x-\alpha)g(x) \Rightarrow f(x) = (x-\alpha)^2 g(x)$$

and therefore α is a multiple root of $f(x)$. □

Proposition 4.1.3 ([6], pg 549-550)
A finite field $\mathbb{F}_{p^n}$ is the splitting field of the polynomial $x^{p^n} - x$ over $\mathbb{F}_p$.

Proof. We want to apply the proposition 4.1.2 to $x^{p^n} - x$. We can consider the derivative of it, i.e. $(p^n)x^{p^n-1} - 1$.Given that we are working in a field of characteristic p, as $\mathbb{F}_p$ is, this is equivalent to -1, this polynomial has no root so in particular has no common root with $x^{p^n} - x$ that therefore is separable.

Now that we know this is separable we get that it has $deg(x^{p^n} - x) = p^n$ distinct roots. Let α and β be two roots, then $\alpha^{P_n} = \alpha$ and $\beta^{P_n} = \beta$, therefore

$$(\alpha\beta)^{p^n} = \alpha\beta \quad and \quad (\alpha^{-1})^{p^n} = \alpha^{-1}$$

. Moreover we also have that

$$(\alpha+\beta)^{p^n} = \alpha^{p^n} + \binom{p^n}{1}\alpha^{p^n-1}\beta + \ldots \binom{p^n}{i}\alpha^{p^n-i}\beta^i + \cdots + \beta^{p^n}$$

but given that $\binom{p^n}{i} = \frac{p^n!}{i!(p^n-i)!}$ we get that all the coefficients but the first and last one are multiples of p^n and therefore are 0. This leaves us with

$$(\alpha+\beta)^{p^n} = \alpha^{p^n} + \beta^{p^n} = \alpha + \beta$$

. This proves that the p^n roots of $x^{p^n} - x$ form a field and, given that $\forall e \in \mathbb{F}_p$ $e^{p^n} = e$, this is exactly the splitting field of $x^{p^n} - x$ and as such has degree n over the base field.

On the other hand we can consider a finite field $\mathbb{F}$ of characteristic p, if this has dimension n over its prime subfield then it has p^n elements. The multiplicative group $\mathbb{F}^X$ of a field is made of all but the 0 element and so has order $p^n - 1$ telling us that $\alpha^{p^n-1} = 1$ for any element of $\mathbb{F}^x$ and therefore $\alpha^{p^n} = \alpha$ and it's a root of $X^{p^n} - x$, proving that $\mathbb{F}$ is contained into the splitting field of this polynomial. But we proved that the splitting field itself has order p^n and therefore the two fields are the same. Therefore we proved that finite fields of order p^n exist for any prime integer p and integer n and are unique up to isomorphism, each of them being isomorphic to the splitting field of $x^{p^n} - x$ over $\mathbb{F}_p$, such a field will be denoted by $\mathbb{F}_{p^n}$ which is coherent with the fact that $\mathbb{F}_p$ is the splitting field of $x^p - x \in \mathbb{F}_p[x]$. □

4.2 On the closure of finite fields

(This subsection will mostly be based on [10] rewritten to be coherent with [6]). Algebraically closed spaces are the usual choice to work with in algebraic geometry. In our case this remains true, this because once we defined the algebraic closure of a finite field we'll be able, with the help of the Frobenius morphism, to go back to finite field but also being able to use results about algebraically closed fields.

We start by underling some properties of $\mathbb{F}_{q^n}$, here personally rewritten and proved in a single note.

Note 4.2.1
The field $\mathbb{F}_{q^n}$ is normal over $\mathbb{F}_q$. This comes from the fact that its elements are the roots of $x^{p^n} - x$, so given an irreducible polynomial in $\mathbb{F}_q$ either this is a divisor of $x^{p^n} - x$ and therefore splits completely or no root of it is contained in $\mathbb{F}_{p^n}$ which is exactly the definition of a normal extension. It's also separable: the minimal polynomials of its elements are divisors of $x^{p^n} - x$ that is separable and so are its divisors, therefore it's a Galois extension of $\mathbb{F}_q$. Moreover the Frobenius automoprhism of the base field $\mathbb{F}_p$, i.e. $\sigma_q : alpha \to \alpha^p$, belongs to the Galois group given how $\forall e \in \mathbb{F}_q$ $e^p = e$. This is also the smallest p such that this equation is true, and the same happens for every multiple of p and only for them, therefore we get that

$$Gal(\mathbb{F}_{q^n}/\mathbb{F}_q) =< \sigma_q \simeq \mathbb{Z}/n\mathbb{Z}$$

i.e. is cyclic of order n (given that $\alpha^{q^n} = \alpha$ $\forall \alpha \in \mathbb{F}_{q^n}$) generated by σ_q.

We can now take advantage of the fundamental theorem of Galois Theory

Theorem 4.2.2 ([6], 14.2.14)
Let K/F be a Galois extension and set $G = Gal(K/F)$. Then there is a bijection

$$\left\{\begin{array}{cc} & K \\ Subfields\ E & | \\ of\ K & E \\ containing\ F & | \\ & F \end{array}\right\} \longleftrightarrow \left\{\begin{array}{cc} & 1 \\ Subgroups\ H & | \\ of\ G & H \\ & | \\ & G \end{array}\right\}$$

given by the correspondence

$$\begin{array}{ccc} E & \longrightarrow & \left\{\begin{array}{c} The\ fixed\ field \\ of\ H \end{array}\right\} \\ \left\{\begin{array}{c} The\ elements\ of\ G \\ fixing\ E \end{array}\right\} & \longleftarrow & H \end{array}$$

which are inverse of each other. Under this correspondence

1. *If E_1, E_2 correspond to H_1, H_2, respectively, then*

$$E_1 \subseteq E_2 \iff H_2 \leq H_1;$$

2. *$[K : E] = |H|$ and $[E : F] = |G : H|$, the index of H in G*

$$\begin{array}{ll} K & \\ | & \} \quad |H| \\ E & \\ | & \} \quad |G : H| \\ F & \end{array};$$

3. *K/E is always Galois, with Galois group $Gal(K/E) = H$:*

$$\begin{array}{ll} K & \\ | & H; \\ E & \end{array}$$

4. *E is Galois over F if and only if H is a normal subgroup in G. If this is the case, then the Galois group is isomorphic to the quotient group*

$$Gal(E/F) \simeq G/H.$$

More generally, even if H is not necessarily normal in G, the isomoprhism of E (into a fixed algebraic closure of F containing K) which fix F are in one to one correspondence with the cosets $\{\sigma H\}$ of H in G;

5. *If E_1, E_2 correspond to H_1, H_2, respectively, then the intersection $E_1 \cap E_2$ corresponds to the group $< H_1, H_2 >$ generated by H_1 and H_2 and the composite field E_1E_2 corresponds to the intersection $H_1 \cap H_2$. Hence the lattice of subfields of K containing F and the lattice of subgroups of G are "dual" (the lattice diagram for one is the lattice diagram for the other turned upside down).*

6.

From this we get that every subfield of $\mathbb{F}_{q^n}$ corresponds to a subgroup of $\mathbb{Z}/n\mathbb{Z}$ and these are of the form $\mathbb{Z}/m\mathbb{Z}$ for $m|n$ which translates into the fact that the only way for $\mathbb{F}_{q^m}$ to be a subfield of $\mathbb{F}_{q^n}$ is for m to divide n. Another crucial theorem is the following:

Theorem 4.2.3 ([6], 13.4.25-26)
Let $p(x)$ be an irreducible element of degree n of $\mathbb{F}_q[x]$ and α be a root of it over some extension. Then there is some $\mathbb{F}_{q^{(m)}}$ in which $p(x)$ splits .

Proof. In the previous subsection we showed that any finite extension of $\mathbb{F}_q$ of degree m is isomorphic to $\mathbb{F}_{q^m}$. The splitting field of $p(x)$ over $\mathbb{F}_q$ has finite degree (it can be proved to be at most $n!$) and so it's one of the $\mathbb{F}_{q^m}$.

□

Theorem 4.2.4 (Closure of a finite field, [10], 2.1)
The closure of a finite field $\mathbb{F}_{q^n}$, that as usual we'll indicate by $\overline{\mathbb{F}_p}$ is equal to

$$\Gamma(q) = \cup_{i=1}\mathbb{F}_{q^{i!}}.$$

This field is not finite.

Moreover we can express the algebraic closure also as

$$\overline{\mathbb{F}_p} = \cup_{i=1}\mathbb{F}_{q^i}.$$

Proof. We proved that $\mathbb{F}_{q^n} \subseteq_{as\ a\ subfield} \mathbb{F}_{q^m} \iff n|m$ and of course $n|n!$ so $\mathbb{F}_{q^n} \subseteq \mathbb{F}_{q^{n!}}$, and given that $\{n!|n \in \mathbb{N}\} \subset \mathbb{N}$ we have that

$$\overline{\mathbb{F}_p} = \cup_{i=1}\mathbb{F}_{q^i} \subseteq \overline{\mathbb{F}_p} = \cup_{i=1}\mathbb{F}_{q^{i!}}\overline{\mathbb{F}_p} = \cup_{i=1}\mathbb{F}_{q^i}$$

and so actually we have the equality.

Now if $\cup_{i=1}\mathbb{F}_{q^i}$ turns out to be algebraically closed then it would be the algebraic closure of each of its subfields, in particular of every $\mathbb{F}_{q^n}$.

We are now left to prove that indeed this is an algebraically closed field: let $\alpha, \beta \in \Gamma(q)$, then by definition we have that $\alpha \in \mathbb{F}_{q^{i_a!}}$ and $\beta \in \mathbb{F}_{q^{i_b!}}$ for some i_a, i_b, and so they are both in $\mathbb{F}_{q^{i!}}$ for $i = i_a * i_b$, but this is implies they are roots of $x^{q^{i!}} - x$ and so algebraic over $\mathbb{F}_q$ as are both $\alpha + \beta$, and $\alpha\beta$ and α^{-1} (for $\alpha \neq 0$) being elements of the same field and this proves that $\Gamma(q)$ is indeed a field and moreover it's algebraic over $\mathbb{F}_q$.

Let $f(x) \in \Gamma(q)[x]$, this has a finite number of coefficients $c_1, \ldots, c_n$ each in $\mathbb{F}_{q^{c_i!}}$ and so they all are in $\mathbb{F}_{q^{\prod_{i=1}^n c_n!}}$. The splitting field of $f(x)$ is a finite extension of $\mathbb{F}_{q^{\prod_{i=1}^n c_n!}}$ and therefore also of $\mathbb{F}_p$ and therefore is equal to $\mathbb{F}_{q^k}$ and again for this field it holds

$$\mathbb{F}_{q^k} \subset \mathbb{F}_{q^{k!}} \subset \Gamma(q)$$

thus proving this is algebraically closed.

Regarding infinity we have that $\mathbb{F}_{q^m}$ has q^m elements and given that $m > n$ implies $\mathbb{F}_{q^m} \not\subset \mathbb{F}_{q^n}$ and for each $k \in \mathbb{N}$ there is n_k s.t. $q^{n_k} > k$ and so $\Gamma(q) \supset \mathbb{F}_{q^{n_k}}$ has more than k elements. □

5 Counting n-tuples in $\mathbb{F}_q$

5.1 Counting n-tuples in $\mathbb{P}^2_{\mathbb{F}_{111}}$ for $n \leq 5$

The main result of this work regards counting n-tuples of points in the projective space of dimension 2 over our base finite field of choice $\mathbb{K}$, id est the space $\mathbb{P}^2_{\mathbb{K}}$ that from now on will mostly be denoted just by $\mathbb{P}^2$. The whole section was obtained independently of any previous counting result.

The actual numbers we will investigate are hard to compute formally and so we will just do explicit computation for the cases of n-tuples for $n < 6$. This will still be useful given that the sage code in the end, that will be the one to compute the number of 8-tuples in general position, heavily relies on the number of 4-tuples to give results in an acceptable time frame, even if this relation will not be immediately clear.

The first thing we want to do is count elements in $\mathbb{P}^2$ itself and to do so we'll reduce them to a "standard" form (where standard here means fitting a standard I have personally set).

Proposition 5.1.1 (Standard form of point in $\mathbb{P}^2$)
We can consider an element $(a : b : c) \in \mathbb{P}^2$ such that $a \neq 0_{\mathbb{K}}$, then we can multiply by a^{-1} to obtain an equivalent element of the form $(1 : d : e)$, if $a = 0$ then we are dealing with an element of the form $(0 : b : c)$ that is a similar fashion (for $b \neq 0$) can be written as $(0 : 1 : d)$ and finally if the element is of the form $(0 : 0 : c)$ then it's equivalent to $(0 : 0 : 1)$. These three subsets of elements are indeed distinct and any element of $\mathbb{P}^2$ can be written uniquely in this form.

Counting n-tuples for n=1,2 In this section we want to count n-tuples of points, it turns out that the most natural way to do it gives us n-tuples of *ordered* points, if we want to obtain the corresponding *unordered* result we suffice to divide by $n!$, and so from now on every n-tuple will be assumed to be ordered.

We can now easily count the equivalence classes in $\mathbb{P}^2$ given that, if we define $k := |\mathbb{K}|$, the set $\{(1 : d : e) | d, e \in \mathbb{K}\}$ has k^2 elements, the set $\{(0 : 1 : e) | e \in \mathbb{K}\}$ has k elements and the set $\{(0 : 0 : 1)\}$ has a single element and therefore $|\mathbb{P}^2| = k^2 + k + 1$. The theory above can be turned into a practical algorithm to generate the actual elements of the projective plane given the base field $\mathbb{F}_{q^n}$, see algorithm 8.1.

This simple result allows us to give formulas for the number of 1, 2-tuples of points of $\mathbb{P}^2$:

Proposition 5.1.2
For $n = 1, 2$ there are no restrictions about general position of distinct points and so

$n = 1$ *There are* $\binom{k^2+k+1}{1} = k^2 + k + 1 = n_1$ 1*-tuples of points in* $\mathbb{P}^2$*;*

$n = 2$ *There are* $(k^2 + k + 1)(k^2 + k) = n_2$ 2*-tuples of points in* $\mathbb{P}^2$*;*

Counting n-tuples for $n = 3$ Extending the above results allows us to compute the number of n-tuples of distinct points in $\mathbb{P}^2$ simply as $\binom{k^2+k+1}{n} * n!$, however in this count are included points in special position i.e. n-tuples where there are more than 3 point on the same line of $\mathbb{P}^2$.

We therefore need to remove these and to do so we need to formalise the concept of "collinearity": if we move to the cone associated to $\mathbb{P}^2$ in $\mathbb{K}^3$ our point become affine lines and the concept of "collinearity" becomes "coplanarity", and a line is coplanar to two other ones $\iff$ it's contained in the plane generated by these and this happens $\iff$ it's a linear combination of them. But a linear combination of lines corresponds to a linear combination of the points and so we obtain that P_3 is collinear with P_1 and P_2 $\iff$ it can be written as a linear combination of the two with coefficients in $\mathbb{K}$.

As a first step in the solution of this problem we state another standard form result:

Theorem 5.1.3
Given $P_1, P_2 \in \mathbb{P}^2_{\mathbb{K}}$, $P_1 \neq P_2$ and consider that standard map (that maps the cone over a projective variety to the variety itself)

$$\theta : \mathbb{A}^3_{\mathbb{K}} \setminus \{0, 0, 0\} \to \mathbb{P}^2_{\mathbb{K}} \; s.t. \; \theta((a, b, c)) = (a : b : c).$$

We can now define the set

$$\{bP_1 + cP_2 | b, c \in \mathbb{K}\} := \theta(\{b + \theta^{-1}(P_1) + c * \theta^{-1}(P_2) | b, c \in \mathbb{K}\})$$

and the map

$$F : \{P_1 + aP_2 | a \in \mathbb{K}\} \cup \{P_2\} \hookrightarrow \{bP_1 + cP_2 | b, c \in \mathbb{K}\}$$

s.t. $F(P_1 + aP_2) = P_1 + aP_2$.This map is a bijection and we'll indicate any of the two sets as $< P_1, P_2 >$.

Proof. We need to check injectivity and surjectivity

Injectivity:

$$e_1 := P_1 + aP_2 \simeq P_1 + bP_2 =: e_2 \iff P_1 + aP_2 = k * (P_1 + bP_2) \iff$$

$$\iff (1-k)P_1 = (kb-a)P_2 \iff P_1 \simeq P_2 \vee (1 = k \wedge kb = a)$$

but the first case is impossible given that P_1 and P_2 are not in the same equivalence class by construction and the second implies $b = a$ and therefore $e_1 = e_2$ and the map is injective;

Surjectivity: We can consider $aP_1 + bP_2$, if $a = 0$ then this is nothing but $bP_2 \simeq P_2 = F(P_2)$, if not we have that $aP_1 + bP_2 \simeq \frac{1}{a}(aP_1 + bP_2) = P_1 + \frac{a}{b}P_2 = P_1 + cP_2 = F(P_1 + cP_2)$ and therefore we just proved the map is also surjective.

□

In the same fashion as when we counted points in $\mathbb{P}^2$ we see that the domain of F, and by bijectivity the whole generated line, contains q points of the form $P_1 + aP_2$ each coming from one of to the q possible values of a, and P_2 for a total of $k + 1$ points . But in this count we included both P_1 and P_2 and removing them leaves us with $k - 1$ other points, i.e. with $k - 1$ points that are collinear with the given pair.

Proposition 5.1.4
The case of 3*-tuples is the first one where we have to consider collinearity and gives us the following:*

$n = 3$ *Given a* 2*-tuple* (P_1, P_2) *there are* $q - 1$ *other points that are collinear with it and so* $q^2+q+1-2-(q-1)$ *ways to chose a third point that is not collinear (there are* $q^2 + q + 1 - 2$ *points different from* P_1, P_2 *and* $q - 1$ *of them are collinear) and so* $n_3 = n_2 * (q^2) = (q^2 + q + 1)(q^2 + q)(q^2) = (q^2 + q + 1)(q^2 + q)(q^2)$ 3*-tuples of points in general position.*

Counting n-tuples for $n = 4$ If we try counting 4-tuples we discover that a new problem arises: the intersection of lines/planes. We can start with a "good" 3-tuple (P_1, P_2, P_3) and we can try to add a fourth point such that no 3 points in the 4-tuples are collinear, this translates to $P_4 \not\in < P_1, P_2 >$, $P_4 \not\in < P_1, P_3 >$, $P_4 \not\in < P_1, P_3 >$. Each of this conditions "removes" $q - 1$ points but theoretically this 3 sets may not be distinct. However it turns

out they are and to see it we can go back into $\mathbb{K}^3$. Here "a point is in both $< P_a, P_b >$ and $< P_c, P_d >$" translates to "a line is in both $< l_a, l_b >$ and $< l_c, l_d >$" (where l_n is cone over P_n, i.e. a line), but $< l_a, l_b >$ and $< l_c, l_d >$ are distinct planes in $\mathbb{K}^3$ and so they intersect in a single line. In the case of $< l_1, l_2 >$, $< l_1, l_3 >$ and $< l_2, l_3 >$ it's trivial to notice that any two contain the common generator that therefore is the unique line (and so point in $\mathbb{P}^2$) constituting the intersection. But the generators are not part of the set of $q-1$ collinear points and therefore we get that to add a fourth point we have indeed $q^2+q+1-3-3(q-1) = q^2-2q+1$ points to chose from.

Proposition 5.1.5
As we showed above to count 4-tuples we need to consider the different possibilities for collinearity:

$n = 4$ *There are* $n_4 = n_3 * (q^2 - 2q + 1)$ *different 4-tuples of points in general position.*

Counting n-tuples for $n = 5$ We have now to consider the case of 5-tuples and here we get a new "problem" : the one arising from disjoint pairs of couples of points, which is also the last problem regarding general position in the sense of a linear subspaces of $\mathbb{P}^2$. 5-tuples are built starting from 4-tuples and in a 4-tuple we can indeed find 4 different points and so 2 planes in $\mathbb{K}^3$ with no common generator. E.g. the 4-tuple (P_1, P_2, P_3, P_4) can give us the planes $< l_1, l_2 >$ and $< l_3, l_4 >$ that have no common generator. In this case the unique line (and so the also the unique point) constituting the intersection of the two is indeed in the set C of $q-1$ points collinear with P_1, P_2 and also in the one of the points collinear with P_3, P_4. We therefore counted this point at least two times, and the same can be said for any other pair of distinct planes, we can generalise this behaviour by stating the following correspondence:

pair of lines with disjoint generators $\rightarrow$ point counted an additional time

that is not $1-1$ (the same point can be counted an arbitrary number of times with the right choice of base field and n-tuple).

However to translate this into counting we need to know exactly how many times each multiply counted points is "removed". Suppose that we have a point (line) p that is collinear with 3 pairs, if we remove it, for what we said above, the 3 spanned spaces need to be disjoint and therefore the 3 planes have to be generated by 6 disjoint points/lines. This assures us that, at least until we want to build $(2k+1)$-tuples, there is no intersection point counted k times. We can now state the counting result for 5-tuples:

Proposition 5.1.6
To count 5*-tuples we need to consider the different possibilities for collinearity and the points counted too many times:*

$n = 5$ *Given a* 4*-tuples to add a* 5*th point we have to check this is not collinear with any of the* $\binom{4}{2} * 2 = 6$ *unordered pairs of points, for each pair there are* $q - 1$ *collinear points for a "total" of* $6 * (q - 1)$*. Now if we chose* 2 *points out of the four we are left with two other points and we can form* 2 *pairs of pairs that, as we said above, give us a single point counted too many times. There are* $\frac{\binom{4}{2}}{2} = 3$ *such pairs of pairs and so we have* $q^2 + q + 1 - 4 - 6(q - 1) + 3 = q^2 - 5q + 6$ *elements we can chose from, therefore we have that there are* $n_5 = n_4 * (q^2 - 5q + 6)$ *different* 5*-tuples of points in general position.*

These calculation are implemented in algorithms 8.3 and 8.4 and act as a safety mechanism for the more general ones giving results that are for sure correct.

5.2 Counting n-tuples for $n = 6$

If we want to count n-tuples for $n = 6$ it's not enough to consider general position only with regards to lines but we also need to take into account conics, defined as homogeneous polynomials of degree 2.

Counting how many conics are there in a given space, how many of these are degenerate and how many points are in each of them is relatively easy, as it's proving how a conic intersects with lines and with some work even the intersection with other conics can be figured out.

However it's clear that obtaining an explicit formula, even if possible, is a lengthy process given how we have to consider all possible intersection between conics and lines, and the final formula will be quite complicated in itself.

So from this point on we'll not try coming up with closed formulas but only think about the problem in a computational way.

Toward the computations: checking if 6 **points lie on a conic** As they teach in any linear algebra course if we have 3 vectors they are independent if and only if the resulting matrix has rank 3. We can do something similar with conics: we remind that the k-th **Veronese** embedding $\mathbb{P}^n \to \mathbb{P}^N$

for $N = \binom{k+n}{n} - 1$ is defined as sending $(x_0 : \cdots : x_n) \to (x_0^k : x_0^{k-1}x_1 : x_0^{k-1}x_2 : \cdots : x_n^k)$ the set of every monomial of degree k. This embedding therefore sends hypersurfaces of degree k to hyperplanes, i.e. linear spaces. In the case of $n = 2$, $k = 2$ we have that $N = \binom{4}{2} - 1 = 5$ and so we have that 6 points are independent with regard to conics, i.e. don't lie on the same one, if and only if the matrix that has as rows the evaluation of monomials of degree 2 in a given point has rank 6, given that this translates to 6 vectors being linearly independent in $\mathbb{P}^N$. This works in any dimension, a set of points belongs to an hypersurface of degree k if and only if the projective embedding of the vectors through the k-th Veronese embedding spans a matrix of rank less than maximal (of course this only works if the number of points is at most $N + 1$).

5.3 Counting n-tuples for $n > 6$

Now we may wonder if there are other possibilities for points not to be in general position that we want to consider.

We start by noticing how the space of polynomials of degree 3 has dimension $\binom{2+3}{3} = 10$, and the Veronese embedding goes to $\mathbb{P}^9$, so we need n to be at least 10 to find points not in general position. Trivially increasing the degree will also increase this number so these simple, i.e. of the form "points lying on a curve", requirements can be ignored (given that our goal is to study Del Pezzo surfaces and in particular count 8-tuples).

The situation is different if we want to consider singular, irreducible, curves. The simplest one is a singular, irreducible cubic. First thing first they exist (an example is $zx^2 - y^3 = 0$) and moreover we have that the condition "8 points lie on the same singular cubic and the singularity is in one of them" gives exactly 10 requirements, i.e. 7 requirements of the form "the point satisfies the same cubic equation" and 3 of the form "the derivatives of said equation go to 0 in the 8-th point" (we remind that the derivatives being 0 is exactly the condition for a point to be singular). The two sets of requirements are independent because the cubic is irreducible , we know that a polynomial is irreducible if and only if it doesn't share zeroes with its derivative as we showed in 4.1.2.

We can therefore define the following three functions

$$c : (x, y, z) \to (x^3, y^3, z^3, x^2y, x^2z, y^2x, y^2z, z^2x, z^2y, xyz)$$

$$cx : (x, y, z) \to (3x^2, 0, 0, 2xy, 2xz, y^2, 0, z^2, 0, yz)$$

$$cy : (x, y, z) \to (0, 3y^2, 0, x^2, 0, 2yx, 2yz, 0, z^2, xz)$$
$$cz : (x, y, z) \to (0, 0, 3z^2, 0, x^2, 0, y^2, 2zx, 2zy, xy)$$

We can now take x_i in the n-tuple $(x_1, x_2, \ldots, x_8)$ and check if the $10x10$ matrix that has as rows $cx(x_i), cy(x_i), cz(x_i), c(x_j)$ for $j \neq i$ has rank less then 10, if this happens for at least 1 of the x_i then the points are not in general position.

We can moreover prove that further enquires are not needed. To do so we start with two well known lemmas:

Lemma 5.3.1 ([16], 3)
A plane curve of degree n has at most $\frac{(n-1)(n-2)}{2}$ singular points.

Lemma 5.3.2 (Bézout's theorem, reformulated from [15], 2.2.1.)
Let X and Y be two plane projective curves defined over a field F that do not have a common component. Then the total number of intersection points of X and Y with coordinates in an algebraically closed field E which contains F, counted with their multiplicities, is equal to the product of the degrees of X and Y.

These two together are the backbone of the proof that the ones we listed are the only possible conditions to check for 8 points. We can moreover use them to do the computation explicitly for low degrees. First thing first we need a table for the dimension of the space of curves of degree n and for the number of derivatives of degree $n-1$. We also need to know the total number of possible singular points. In these we use the multiset binomial coefficient we reminded the definition in the proof of 3.3.4.

Degree of the curve	Total number of singular points
3	$\binom{3-1}{3-2} = 1$
4	$\binom{4-1}{4-2} = 3$
5	6
6	10
7	15

Degree of the derivative	Total number of derivatives
0	$\left(\binom{3}{0}\right) = 1$
1	$\left(\binom{3}{1}\right) = 3$
2	6
3	10
4	15

Degree of the curves	Dimension of the space of curves
3	$\binom{3}{3} - 1 = 9$
4	$\binom{3}{4} - 1 = 14$
5	20
6	27

We can now start to check that no other condition is possible in the case of low degrees of the curve.

Cubic An irreducible cubic has at most 1 singularity and we already tackled this case.

Quartic An irreducible quartic has at most 3 singularities. If all 3 are double points then we have $(8-3)*1+3*3=14$ conditions that are not enough to force us to consider this (they would need to be more than the dimension of the space that is 14). This comes from the fact that for 5 points we have to consider 1 derivative (the 0-th derivative) and for 3 points we have to consider the 3 first derivatives.

If one of the points is a triple point than it's the only one given that any line through it and another singular point would have an intersection multiplicity $> 3+2=5>4=4*1$, the number that comes from Bézout. If this is the case we have $7+6*1=13$ conditions so we are fine.

There is no point of multiplicity 4 given that a line through it and another point of the curve would have multiplicity of intersection $4+1=5>4*1$.

Quintic An irreducible quintic has at most 6 singularities. If all 6 are double points we get $2+6*3=20$ conditions that are few enough (less or equal than 20).

Now suppose that one is a triple point, and suppose that there are 4 other singularities, then if we take the conic through these 5 points the intersection multiplicity would be $3+2*4=11$ that is bigger than $5*2=10$ coming from Bézout. So at most 3 other points can be singular, and they all need to be double points (if one was triple the multiplicity of intersection with a line would be $3+3=6>5*1=5$). This gives us $4+3*3+1*6=19$ conditions.

For a linear intersection reason if a point of multiplicity 4 exists then it would be the only singular point and give us $7*1+1*10=17$ conditions.

Sextic An irreducible sextic has at most 10 singularities. If all 8 points are double points we get $8*3 = 24$ conditions that are few enough (less than 27).

Now if the singular point of highest multiplicity has it equal to 3 there can only be at most 3 such points, if we had 4 the multiplicity of the intersection with a conic would be $3*4+1 = 13 > 2*6 = 12$, moreover the other points can't all be double given that $3*3+4 = 13$, but $3*3+2+1 = 12$ is fine. This case, 3 triple, one double, 4 regular, that is the "worst" we can do for triple points, gives a number of conditions equal to $1*4+3*1+6*3 = 25$.

We may wonder if removing some triple point and adding more double ones would improve this number. For 2 triple points and 5 double ones we can consider the singular cubic passing through these with the singularity in one of the triple points (that we know exists since these are $6+1*3 = 9$ conditions) that gives us a multiplicity of the intersection equal to $5*2+3+3*2 = 19$ ($3*2$ because one triple point is a double point for the cubic) but this is equal to $19 > 18 = 3*6$ so 5 double points are too many. But for 2 triple point and 4 double ones we have $2*1+4*3+2*6 = 26$ which are no enough conditions. Finally for only 1 triple point and 7 double ones we have $7*3+6 = 27$.

If the point of highest multiplicity has it equal to 4 we can have that the other singular points can only be double ones. How many of them can we take? If we took 6 double points then the cubic passing through these 6 and having the singularity in the one of multiplicity 4 would have a multiplicity of intersection equal to $2*6+4*2 = 20 > 18 = 3*6$. If we take 1 point of multiplicity 4, 5 double points and 2 of multiplicity one we have a number of conditions equal to $2*1+5*3+1*10 = 27$.

For a reason that comes down to a linear intersection, if a point of multiplicity 5 exists then it would be the only singular point and give us $7*1+1*15 = 22$ conditions.

We therefore showed for curves of dimension up to 6 that the only possible way for points not to be in general position is for 3 of them to be on a line, 6 on a conic and 8 on a singular cubic with the singularity in one of them, given that any other condition is either not restrictive enough to be avoided (whenever we have less conditions that the dimension of the space) or impossible. With similar calculation the same is true for any higher dimensional curve.

These results give rise to the algorithm 8.5 that is the one, with some modifications, we'll use to count 8-tuples in general position.

5.4 Towards the computation: points in special position and the projective linear group

What we said until now works well in theory, however a slightly different approach to the topic will give us some result that speed up computation and this subsection will be devoted to these results. These theorems are not specifically taken from any book even if they can be found , they rather are a personal restatement of mine of these results.

We start with a definition:

Definition 5.4.1
We denote by PGL the projective general linear group, i.e. given how $\mathbb{P}^2 = (\mathbb{K}^3 \setminus \{0\})/k*$ *we can define* $PGL(3) = GL(3)/k*$ *where* $a \in k*$ *acts by* $\begin{pmatrix} a & 0 & 0 \\ 0 & a & 0 \\ 0 & 0 & a \end{pmatrix}$ *on the set of* $3x3$ *matrices.*

Theorem 5.4.2
Let S *be the set of points* $(P_1, \dots, P_4)$ *in general position in* $\mathbb{P}^2$.

1. *There is a natural bijection*

$$PGL(3) \to S.$$

Moreover this action is free and transitive;

2. *This bijection implies that to each configuration of general points corresponds an invertible matrix that sends the first* 4 *points in a chosen* 4*-tuple of points in general position. If we pair any of these maps with an* n*-tuple in special position, i.e. starting with the chosen* 4 *points, we then get a* $1-1$ *correspondence with points in general position.*

Proof. 1. We can consider the map

$$\begin{array}{ccc} PGL(3) & \to & S \\ \begin{pmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_3 \\ a_3 & b_3 & c_3 \end{pmatrix} & \to & \left(\begin{bmatrix} a_1 \\ a_2 \\ a_3 \end{bmatrix}, \begin{bmatrix} b_1 \\ b_2 \\ b_3 \end{bmatrix}, \begin{bmatrix} c_1 \\ c_2 \\ c_3 \end{bmatrix}, \begin{bmatrix} a_1+b_1+c_1 \\ a_2+b_2+c_2 \\ a_3+b_3+c_3 \end{bmatrix} \right) \end{array}$$

We notice that this is simply the image under the given elements of $PGL(3)$ of the vectors $\begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$

- This is injective: if $M = (A\ B\ C)$ and $N = (A'\ B'\ C')$ have the same image then we have that, for $a, b, c, d \in \mathbb{K}$ the base field, $a * A = A'$, $b * B = B'$, $c * C = C'$, $d * (A + B + C) = A' + B' + C'$ that implies $d * A + d * B + d * C = a * A + b * B + c * C$ but A, B, C are independent vectors so this can only happen if $a = b = c = d$ and so $N = d * M$ and the two matrices belong to the same class in $PGL(3)$;
- This is surjective: any 4 points in $\mathbb{P}^2$ are linearly dependent and so if we consider the vectors A, B, C, D we can write $D = a * A + b * B + c * C$, if we then take the element $(a * A\ b * B\ c * C)$ this is mapped exactly to $(a * A, b * B.c * C, D) \simeq (A, B, C, D)$:
- The elements of $PGL(3)$ preserve collinearity: this because any element of $PGL(3)$ is a linear transformation, therefore it preserves linear combinations (collinear points remain collinear) and being invertible if the image of a set of points is a collinear set of points then so is the starting set;
- The group action is free: any element of $\mathbb{P}^2$ can be written as a linear combination of elements of the base, but we showed that any matrix g in $SGL(3)$ acts freely on elements x of the base, i.e. $g * x = h * x$ implies $g = h$, and so has to do it on the general point;
- The group action is transitive: the map we defined sends

  $$\begin{bmatrix}1\\0\\0\end{bmatrix}, \begin{bmatrix}0\\1\\0\end{bmatrix}, \begin{bmatrix}0\\0\\1\end{bmatrix}, \begin{bmatrix}1\\1\\1\end{bmatrix} \quad \text{to} \quad \begin{bmatrix}a_1\\a_2\\a_3\end{bmatrix}, \begin{bmatrix}b_1\\b_2\\b_3\end{bmatrix}, \begin{bmatrix}c_1\\c_2\\c_3\end{bmatrix}, \begin{bmatrix}a_1+b_1+c_1\\a_2+b_2+c_2\\a_3+b_3+c_3\end{bmatrix},$$

  moreover it's invertible and so the inverse sends

  $$\begin{bmatrix}a_1\\a_2\\a_3\end{bmatrix}, \begin{bmatrix}b_1\\b_2\\b_3\end{bmatrix}, \begin{bmatrix}c_1\\c_2\\c_3\end{bmatrix}, \begin{bmatrix}a_1+b_1+c_1\\a_2+b_2+c_2\\a_3+b_3+c_3\end{bmatrix} \quad \text{to} \quad \begin{bmatrix}1\\0\\0\end{bmatrix}, \begin{bmatrix}0\\1\\0\end{bmatrix}, \begin{bmatrix}0\\0\\1\end{bmatrix}, \begin{bmatrix}1\\1\\1\end{bmatrix},$$

  and the composition allows us to go from each element of S to any other, that is the definition of transitivity.

2. We already said that there is a map, depending on the element, of $SGL(3)$ that sends any given element of S to $\begin{bmatrix}1\\0\\0\end{bmatrix}, \begin{bmatrix}0\\1\\0\end{bmatrix}, \begin{bmatrix}0\\0\\1\end{bmatrix}, \begin{bmatrix}1\\1\\1\end{bmatrix}$ and vice versa, moreover this map preserves collinearity and it's injective

(being linear) and therefore bijective (being defined on a finite set), so any n-tuple in general position is sent to an n-tuple in general position starting with the 4 special points, and vice versa each such "special" n-tuple corresponds to a given general one once we fixed the map for the first 4 points. It also preserves general position regarding cubic and conic equations being linear.
We can therefore only study the special case.

□

An easier case gives rise to the following theorem:

Theorem 5.4.3
Let $S' = \{(v_1, v_2, v_3) | v_i \in \mathbb{K}^3, Span(\{v_1, v_2, v_3\}) = \mathbb{K}^3\}$. *The map*

$$S \to GL(3)$$

$$(v_1, v_2, v_3) \to \begin{bmatrix} v_1 & v_2 & v_3 \end{bmatrix}$$

is a bijection. Moreover the action of $GL(3)$ *on* S' *is free and transitive*

Proof. The proof it totally equivalent to the one of the projective case: We can consider the map

$$\begin{array}{ccc} GL(3) & \to & S' \\ \begin{pmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_3 \\ a_3 & b_3 & c_3 \end{pmatrix} & \to & \left(\begin{bmatrix} a_1 \\ a_2 \\ a_3 \end{bmatrix}, \begin{bmatrix} b_1 \\ b_2 \\ b_3 \end{bmatrix}, \begin{bmatrix} c_1 \\ c_2 \\ c_3 \end{bmatrix} \right) \end{array}$$

This is simply the image under the given elements of $GL(3)$ of the vectors $\begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$

- This is injective: if $M = (A\ B\ C)$ and $N = (A'\ B'\ C')$ have the same image then we have, trivially, that, $A = A'$, $B = B'$ and $C = C'$;
- This is surjective: we can trivially send the vectors A, B, C to $(A\ B\ C)$ and the image under the map will be made by the three vectors we started with :
- The elements of $GL(3)$ preserve collinearity: any element of $GL(3)$ is a linear transformation, therefore it preserves linear combinations (collinear points remain collinear) and being invertible if the image of a set of points is a collinear set of points then so is the starting set;

- The group action is free: any element of $\mathbb{P}^2$ can be written as a linear combination of elements of the base, but we showed that any matrix g in $GL(3)$ acts freely on elements x of the base, i.e. $g * x = h * x$ implies $g = h$, and so has to do on the general point;
- The group action is transitive: the map we defined sends

$$\begin{bmatrix}1\\0\\0\end{bmatrix}, \begin{bmatrix}0\\1\\0\end{bmatrix}, \begin{bmatrix}0\\0\\1\end{bmatrix} \rightarrow \begin{bmatrix}a_1\\a_2\\a_3\end{bmatrix}, \begin{bmatrix}b_1\\b_2\\b_3\end{bmatrix}, \begin{bmatrix}c_1\\c_2\\c_3\end{bmatrix},$$

moreover it's invertible and so the inverse sends

$$\begin{bmatrix}a_1\\a_2\\a_3\end{bmatrix}, \begin{bmatrix}b_1\\b_2\\b_3\end{bmatrix}, \begin{bmatrix}c_1\\c_2\\c_3\end{bmatrix} \rightarrow \begin{bmatrix}1\\0\\0\end{bmatrix}, \begin{bmatrix}0\\1\\0\end{bmatrix}, \begin{bmatrix}0\\0\\1\end{bmatrix},$$

and the composition allows us to go from each element of S' to any other, that is the definition of transitivity.

□

We can now suppose we want to check which n-tuples in $\mathbb{P}^2$ satisfy a given property, doing it naively requires us to iterate through roughly $(\mathbb{P}^2)^n$ such n-tuples. We can however reduce this number by a good amount simply by "forcing" the first 4 points to be

$$P_1 = [1:0:0] \quad P_2 = [0:1:0] \quad P_3 = [0:0:1] \quad P_4 = [1:1:1]$$

that reduces the number of n-tuples to $(\mathbb{P}^2)^{n-4}$, this because by the multiplying by the right element of $PGL(3)$ any $8-$tuples can be turned into one starting with the special points.

Of course this is not enough to count all the n-tuples, we also need to multiply the number on n-tuples we find starting with the 4 special points with the number of ways we can send points to the special ones, i.e. the number of invertible matrices. We therefore need to find the cardinality of $PGL(3, \mathbb{F}_q)$ This cardinality should be equal to n_4 given how we proved that there is a $1-1$ correspondence with n-tuples in general position.

Regarding $PGL(3, \mathbb{F}_q)$ cardinality we can first compute the cardinality of $GL(3, \mathbb{F}_q)$ and then divide by $q-1$ (that is the cardinality of each equivalence class in $\mathbb{P}^2_{\mathbb{F}_q}$). $GL(3, \mathbb{F}_q)$ is the set of invertible $3x3$ matrices, to find its cardinality we can notice how each of the elements is made by 3 independent

vectors of length 3 (and different from 0). The first vector can be chosen in $q^3 - 1$ ways given that we simply need to chose 3 of the elements of $\mathbb{F}_q$ and remove the vector $(0, 0, 0)$. For the second one we have the additional requirement of it not being a multiple of the first one, given that there are q multiples (including 0) of it, we are left with $q^3 - q$ vectors. Similarly for the third one we have to remove the linear combination of the first two and therefore their number is equal to q^2 leaving us with $q^3 - q^2$ elements. We can conclude that

$$|GL(3, \mathbb{F}_q)| = (q^3 - 1)(q^3 - q)(q^3 - q^2)$$

and

$$|PGL(3, \mathbb{F}_q)| = \frac{(q^3 - 1)(q^3 - q)(q^3 - q^2)}{q - 1} = (q^2 + q + 1)(q^3 - q)(q^3 - q^2).$$

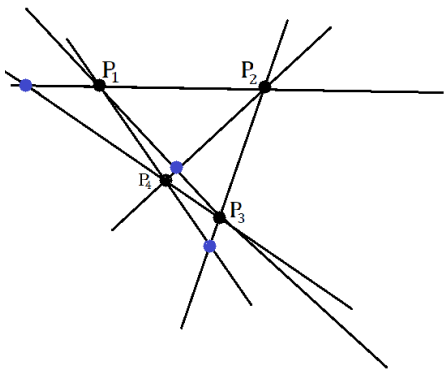
But now we can regroup these factors in the following way:

$$(q^2 + q + 1)(q^3 - q)(q^3 - q^2) = (q^2 + q + 1)(q^2 + q)(q - 1)(q - 1)(q^2) =$$

$$= (q^2 + q + 1)(q^2 + q)(q^2)(q^2 - 2q + 1) = n_4$$

as we were supposed to get.

Example 5.4.4 (5-tuples)
We can assume the first 4 *points are indeed in the special position we said. We now suffice to chose* P_5 *away from the lines between the points.*



there are 6 *such lines and, as we said several times,* $q+1$ *points on each of them. The number of ways we can therefore chose* P_5 *is equal to*

$$|\mathbb{P}^2_{\mathbb{F}_q}| - 6|L(\mathbb{F}_q)| + 2 * 4 + 3 = q^2 - 5q + 6$$

where $2 * 4$ *comes from the fact that each "base point" is removed* 3 *times instead of* 1*, the* 3 *comes from the* 3 *intersection points counted* 2 *times. This allows us to conclude that we have a number of general* 5*-tuples equal to* $|PGL(3, \mathbb{F}_q)| * N = (q^2 + q + 1)(q^3 - q)(q^3 - q^2)(q^2 - 5q + 6)$.

This has been implemented in the algorithm 8.6 that improves the previous one. Further computational improvements have been made in the algorithm 8.7 and a parallelized version, in order to split the computation over n computers and speed by a factor close to n the computations, has been given in algorithm 8.8.

5.5 Points in a conic or a singular cubic

Even if explicit computations are lengthy something we can do is study how many points there are on a conic in $\mathbb{P}^2$ or on a singular cubic. This will be useful to compute some coefficient of the polynomial describing the number of 8-tuples in 6.0.5.

We can start by noticing that given a conic (non degenerate so no point, double lines or intersecting lines) and a line the two intersect in at most two points from Bézout's theorem 5.3.2.

The case of a single point intersection is not only possible but we can prove there is a tangent line to any point of a conic: as we said computing the intersection means computing solutions to a 2nd degree equation, for such an equation the condition of having a single solution counted two times is linear and a linear equation over a field has always a solution. We can therefore set up an equation giving as inputs the conic and the wanted point of tangency and always find a coefficient defining a line that is tangent to the conic in the given point.

Now if we consider a point p_0 in a given conic we can build all the lines passing through it, there are $q + 1$ such lines and each of them intersects the conic in two points, but the unique tangent line, which proves that the conic contains q more points. Vice versa if we take any other point in the conic and build a line through it an p_0 then this would be one of the q that we defined. This proves there is a bijection between lines passing through p_0 and point in the conic and moreover that **a conic in $\mathbb{P}^2_{\mathbb{F}_q}$ contains q+1 points.**

In a totally similar fashion if we take a line through the singular point of a cubic then this meets the cubic in a single other point, and through any other point of the cubic we can build the line passing through the singularity and it. A conic has either 1 or 2 tangents at the singular point over a finite

field, in particular if the singularity is a cusp there is only 1 tangent, if it's a node and the tangents at it are defined over $\mathbb{F}_q$ there are 2 and if the tangents are defined over $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$ of course it has none but again we can build a line through the singularity and the singularity only and so we again have 1 special line. There are $q^2 + 1 - q - 1 = q^2 - q$ lines over $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$, as we'll better show in 7. These are more than the ones over $\mathbb{F}_q$, which shows that most of the times a singular cubic will have $q+1$ points, and it will have q only if the sinularity is a node whose tangent are defined over $\mathbb{F}_q$.

6 Del Pezzo surfaces of degree 1

Now we know about Del Pezzo surfaces, their link with points in the plane and how to count these. The ground is therefore set to work towards the main enumeration result for Del Pezzo surfaces of degree 1.

In section 3 we came to the conclusion that degree 1 Del Pezzo surfaces are isomorphic to degree 6 hypersurfaces in the weighted space $\mathbb{P}_{(1,1,2,3)}$. But we also know that they are isomorphic to the blowup of 8 points in general position of $\mathbb{P}^2$ and there is a correspondence between surfaces up to isomorphism and blowing ups. To be more precise there is an isomoprhism between the set of ordered 8-tuples in general position in $\mathbb{P}^2$ and the moduli space of Del Pezzo surfaces of degree 1 with geometric marking, i.e. to any 8-tuple we are associating a class of isomorphic degree 1 Del Pezzo surfaces with the same geometric marking. So we have that by counting 8-tuples in general position we are also counting Del Pezzo surfaces of degree 8 and vice versa.

Given the importance of the concept of geometric marking is better to give a formal definition:

Definition 6.0.1 ([5])
Given $r = 9 - d$ points $P_1, \dots, P_r \in \mathbb{P}^2$ in general position, the Del Pezzo surface $\pi : X \to \mathbb{P}^2$ of degree d obtained by blowing up these points has basis for the Picard group

$$Pic(X) = \mathbb{Z}L \oplus \mathbb{Z}E_1 \oplus \cdots \oplus \mathbb{Z}E_r$$

where $L = \pi^*\mathcal{O}(1)$ is the strict transform of a line in $\mathbb{P}^2$ and E_i is the exceptional curve which is the inverse image of P_i . Such a basis coming from a blowup is called a ***geometric marking****.*

We also realised that trying to obtain some closed formula, even for 6 points in general position, is very complicated which made us make the decision to compute such numbers by means of a Sage algorithm.

Luckily it can be proven that there is a function, depending on the cardinality of the base field, counting the number of $8-$tuples in general position in the projective plane over a finite field. Moreover this function is actually a **monic polynomial of degree** 8.

The main result we'll take advantage of is the following:

Theorem 6.0.2
Let $C_{2,8}^{gp}$ be the set 8-tuples in general position in $\mathbb{P}^2$.

- *The number of points of $C^{gp}_{2,8}$ over $\mathbb{F}_q$ is a polynomial $P(q)$ of q;*
- *The degree of $P(q)$ in q is equal to 8 (this is the polynomial describing the number of points once we divide by the dimension of $PGL(3)$);*
- *Since $C^{gp}_{2,8}$ is connected we have that $P(q)$ is monic.*

This is a consequence, even if it requires some work, of theorem 1.2 in [4]

Even with this result we are not done yet, this because in the case of some particular fields we have that Del Pezzo surfaces behave differently from any other finite field. This happens when the characteristic of the base field is 2 or 3 and may imply a different behaviour also regarding the polynomial.

Some examples of the difference in behaviour are given in the appendix 8.2.

The difference in behaviour is a necessary but not sufficient condition for the polynomial to be different in the 3 cases (characteristic 2, characteristic 3, any other characteristic) but is indeed reflected by the proper computations that show that no degree 8 monic polynomial over the integers passes through the points that come out of direct computation .

Note 6.0.3
We may now wonder why we did state theorems about algebraically closed fields if we are working with finite fields that are not algebraically closed (we know that the algebraic closure is infinite). The answer lies in the Frobenius morphism, i.e. the map sending $\mathbb{P}^2_{\mathbb{F}_q} \ni (x_1, x_2, x_3) \to (x_1^q, x_2^q, x_3^q)$, that we'll see in the next section has the property that

$$x_1^q = x_1 \iff x_1 \in \mathbb{F}_q$$

and so we get that if we only consider the n-tuples fixed by Frobenius we go back to the finite case.

Now we could finally state the final lemma regarding the number of 8-tuples in $\mathbb{P}^2$ over a finite field and in general position. But first it's better if we state some preliminary results that will make the core lemma more concise.

Lemma 6.0.4
The coefficient of x^7 in the polynomial, and this remains true regardless of the characteristic of the base field, is -84.

Proof. We can consider the space X of 8-tuples in general position in $\mathbb{P}^2_{\mathbb{F}_q}$, we have the following trivial inclusion that gives rise to an inequality that is itself trivial:

$$X \subset (\mathbb{P}^2)^8 \Rightarrow |X| \leq |(\mathbb{P}^2_{\mathbb{F}_q})^8| = |\mathbb{P}^2_{\mathbb{F}_q}|^8 = (q^2+q+1)^8 = x^{16} + 8x^{15} \dots$$

Now to get the cardinality of X we can work by the standard method of addition ad subtraction, i.e the one that is used to count elements in sets with intersection. We start by removing all possible ways 8 points can be in a position that is not general, i.e.:

- There are $\binom{8}{3} = 56$ ways 3 points can be collinear;
- There are $\binom{8}{6} = 28$ ways 6 points can lie on the same non-singular conic;
- There are $\binom{8}{1} = 56$ ways 8 points can lie on a singular cubic with the singularity in one of them;

Now each of this condition generates an hyperspace that has codimension 1, moreover they are independent and generate irreducible hyperspaces which tells us that their contribution to the counting is of order $16 - 1 = 15$. We should take into consideration the fact that there are intersections between this possible non-general configurations, but an intersection of two hypersurfaces has codimension 2 and therefore with the same reasoning contributes for a factor of $a * x^14$ and so on with further passages of the add-subtract method.

Therefore we have that

$$|X| = x^{16} + 8x^{15} - (28 + 56 + 8)x^{15} \cdots = x^{16} - 84x^{15} \dots .$$

But we can divide by $|PGL(3)| = x^3(x^5 - x^3 - x^2 + 1)$ and get that the result starts as

$$x^8 - 84x^7 \dots$$

□

Proposition 6.0.5
The coefficient of x^6 in the polynomial, and this remains true regardless of the characteristic of the base field, is 3151.

Proof. As can be found in [3] the polynomial, after dividing by the cardinality of $PGL(3)$ counting $7-$tuples of points in general position starts as

$$q^6 - 35q^5 + 490q^4 \dots .$$

We can now consider 7-tuples of points in a position even more restrictive, so that any line through 2 of these meets any conic through two of these in exactly 2 distinct point, any cubic in 3, any other line in 1, any conic meets any other conic in 4, any cubic in 6 and any singular cubic meets any other singular cubic in 7 ($9-2$ coming from the 2 double points).

It can be proven that the polynomial enumerating these is different from the one enumerating $7-$uples in general position by coefficients of monomial of degree less then 4, therefore this also starts as

$$q^6 - 35q^5 + 490q^4 \dots .$$

Knowing this it becomes easy enough to count how many choices we have for an 8-th point.

This has to lie away from:

- Any of the $\binom{7}{2}$ lines through 2 of the 7 points, each containing $q+1-2 = q-1$ points apart from the starting ones;
- Any of the $\binom{7}{5}$ conics through 5 of the 7 points, each containing $q+1-5 = q-4$ points apart from the starting ones;
- Any of the 8 cubics through it and the 7 starting points and having a singularity in one of these, each containing either $q-6$ or $q-7$ points, depending if the cubic contains q or $q-1$ points, apart from the starting ones.

but these curves have intersections, that by hypothesis are all general, and moreover also from construction no triple intersection can be found. We need therefore to add the intersection points back in given that we removed each of these 2 times.

- Each of the $\binom{7}{2}$ lines intersects in a single point, away from the 7 starting ones, $\binom{7-2}{2}$ other lines, for a total of 210 intersection points to be divided by two from the ordering of the two lines, and so there are 105 points counted two times this way;
- For each of the $\binom{7}{2}$ we have $\binom{5}{5}$ ways to chose 5 other points in the 7 and therefore a conic having 2 intersection with it away from the 7-tuple. We also have $\binom{5}{4}$ ways to chose 4, to be multiplied by the $\binom{2}{1}$ ways to chose the fifth in the ones defining the lines, these give us conics with a single intersection away from the 7-tuple. At the end we have 252 intersection points between conics and lines;

- For each of the $\binom{7}{2}$lines we have 8 ways to chose a singular conic passing through a 7-tuple, each sharing 2 points of it with the line and therefore giving us $3-2=1$ intersection points away from it. The total of intersection points amounts therefore at 168;

- Each of the $\binom{7}{5}$ conics shares at least 3 points in the 7-tuples with any other conic defined over it and therefore at most 1 away from the 7-tuple. There ones that share only 3 are the only ones we need to count and there are $\binom{5}{3}$ to choose the common points and $\binom{2}{2}$ to chose the other 2. This gives us a total of 210 210 intersection points to be divided by two from the ordering of the two conics, and so there are 105 points counted two times this way;

- For each of the $\binom{7}{5}$ conics we have 8 ways to chose a singular conic passing through a 7-tuple, each sharing 5 points of it with the line and therefore giving us $6-5=1$ intersection points away from it. The total of intersection points amounts therefore at 168;

- In the case of two singular cubics they intersect in 7 points but two of them are singular and so this amount to all the 9 possible intersections therefore adding nothing to the count.

Summing all of this we get that we have between $q^2-49q+945$ and $q^2-49q+953$ ways to chose the 8-th point, where 945 comes from the case where every singular cubic has $q+1$ points and 953 from the case in which every singular cubic has q points. And so the possible range polynomial describing the ways to chose an $8-$tuple can be described, at least for the starting coefficients, by the following polynomial multiplications

$$(q^6-35q^5+490q^4)(q^2-49q+945)=q^8-84q^7+3150q^6$$

and

$$(q^6-35q^5+490q^4)(q^2-49q+953)=q^8-84q^7+3158q^6$$

that moreover confirms that the coefficient of q^7 is indeed -84.

However we know that neither of these cases is true and so the number has to lie in between, it can moreover be proven, as it is in [2] that the coefficients of the final polynomial has to come from a particular table. If we apply this result to our candidate coefficients we get that the possible ones have to be equal to the sums of elements in a subset of the following set

$$N6=[8,28,70,168,112,160,210,560,1134,700,1050,2688,35,84,567,1344]$$

that is actually a bit bigger than needed, but the only ones that satisfy this property, as can be check by algorithm 8.10 are 3151, 3156 and 3157. But counting the number of points in a singular cubic we also noticed how in most cases such curve has $q+1$ points and this allows us to convince ourselves that the right coefficient is 3151.

A more formal method would involve computing the actual polynomial for 7-tuples in "very general" position and then classify cubics.

□

Proposition 6.0.6
The following are the tables for the number of points in general position for base finite fields of order smaller than 24 *in the cases of characteristic* 2*:*

q	N	$k = \|PGL(3)/$	N/k
2	0	168	0
4	0	60480	0
8	0	16482816	0
16	1552090595328000	4277145600	362880

of characteristic 3:

q	N	$k = \|PGL(3)\|$	N/k
3	0	5616	0
9	0	42456960	0

and of every other characteristic:

q	N	$k = \|PGL(3)\|$	N/k
5	0	372000	0
7	0	5630688	0
11	0	212427600	0
13	0	810534816	0
17	0	6950204928	0
19	81933697456128000	16934047920	4838400

Proposition 6.0.7
In the case of characteristic of the base field $\neq 2, 3$ *by using algorithm 8.9 we*

can interpolate the polynomial through the 6 *points and having the coefficient of* x^8, x^7 *and* x^6 *as we computed.*
This will count the number 8*-tuples in general position of* $\mathbb{P}^2$ *in this case for any* q*.*

$$q^8 - 84q^7 + 3151q^6 - 70224q^5 + 1024329q^4 - 9906756q^3 +$$

$$+60545309q^2 - 208027416q + 301030730.$$

This turns out to be a refinement of corollary 1.6 in [1].

7 Going further: the Frobenius morphism and n-tuples in $\mathbb{P}^2_{\overline{\mathbb{F}_q}}$

As we proved in section 4 the closure of any finite field is not finite anymore, however algebraically closed fields are widely used in algebraic geometry.

If we want to work with algebraically closed fields, in particular with the algebraic closure of $\mathbb{F}_q$, we need, in some sense, to lower our expectations and turn our focus on something more specific than simply counting n-tuples of points.

In particular we'll study the implication for an n-tuples of points to have the property of getting permuted , through an element of $S(n)$, the n-th symmetric group, by the Frobenius endomorphism.

First thing first we can settle the definition of the morphism:

Definition 7.0.1 (Frobenius endomorphism, [6], 13.5.35)
*Given a finite ring $\mathbb{F}_q$ the **Frobenius endomorphism** F is defined as the map $\mathbb{F}_q \to \mathbb{F}_q$ such that $Frob(x) = x^q$. This is a ring morphism given that*

$$Frob(xy) = (xy)^q = x^q y^q \ , \ Frob(1) = 1^q = 1$$

and

$$Frob(x+y)^q = x^q + y^q + \sum_{i=1}^{q-1} \binom{p}{i} x^i y^{q-1}$$

however the terms of the sum on the right are all multiples of p and therefore equal to 0 telling us $Frob(x+y)^q = x^q + y^q$.

If $\mathbb{F}_q$ is a finite ring we define the Frobenius endomorphism on $\mathbb{A}^n_{\mathbb{F}_{q^m}}$ as

$$Frob((x_1, \dots, x_n)) = (x_1^q, \dots, x_n^q)$$

and on $\mathbb{P}^n_{\mathbb{F}_{q^m}}$ as

$$Frob((x_1 : \cdots : x_n)) = (x_1^q : \cdots : x_n^q).$$

It's worth noticing that we need to specify q given that it changes what the endomorphism is, for example $\mathbb{F}_{2^6} = \mathbb{F}_{4^3}$ but if we express the field in the first way the morphism is $x \to x^2$ whilst in the second case is $x \to x^4$.

Our goal now is to count n-tuples of points in general linear position in $\mathbb{P}^2_{\overline{\mathbb{F}_q}}$ fixed by a given element of $S(n)$, condition that not only will imply the

finiteness of the number of such n-tuples but also turn the problem into one about a finite field. The next theorem will be a key part on counting collinear points from now on, and it's mostly original work, at least in the proof.

Theorem 7.0.2
For a line L in $\mathbb{P}^2_{\overline{\mathbb{F}_q}}$ the following are equivalent:

1) L is defined over $\mathbb{F}_{q^n}$;

2) $P_1 \in L \Rightarrow F^n(P_1) \in L \ \forall P_1 \in \overline{\mathbb{F}_q}$;

3) $\exists P_1, P_2, P_3, P_4 \in \overline{\mathbb{F}_q}$ such that $P_1 = F^n(P_3)$ $P_2 = F^n(P_4)$, $P_1, P_2, P_3, P_4 \in L$.

Proof. The proof is actually quite straightforward:

1) $\Rightarrow$ 2) If L is defined over $\mathbb{F}_{q^n}$ then $L =< P_1, P_2 >$, $P_1, P_2 \in \mathbb{P}^2_{\mathbb{F}_{q^n}}$. Now $a \in L \Rightarrow a = P_1 + x_a * P_2$, x_a in $\overline{\mathbb{F}_q}$ and so $F^n(a) = F(P_1 + x_a * P_2) = F^n(P_1) + F^n(x_a) * F^n(P_2)$, but F^n acts as the identity on $\mathbb{P}^2_{\mathbb{F}_{q^n}}$ and is an automorphism of $\overline{\mathbb{F}_q}$ and so actually $F(a) = P_1 + x_{F(a)} * P_2 \in < P_1, P_2 >= L$;

2) $\Rightarrow$ 3) Trivial given that we can take arbitrary $P_1, P_2 \in L$ and set $P_3 = F(P_2)$;

3) $\Rightarrow$ 1) Let $P_3 = F^n(P_2)$ and $P_1, P_2, P_3 \in L$. A line is defined by any of its two points and so we have $< P_1, P_2 >= L =< P_3, P_4 >$. Now F(L)$=<$ $F^n(P_1), F^n(P_2) >=< P_3, P_4 >= L$ and so L is fixed by F^n and therefore defined over its fixed field that is $\mathbb{F}_{q^n}$.

□

Frobenius and $S(1)$ The case of 1-permutations (elements of $S(1)$) is trivial: $S(1)$ has only one element and this is the identity, therefore we have $F(P_1) = P_1,\ P_1 \in \mathbb{P}^2_{\overline{F}_q}$, but this means that P_1 is in the fixed field of F, or to be precise is an element of $\mathbb{P}^2_K$ where$\mathbb{K}$ is the fixed field of F, and this implies $K = \mathbb{F}_q$, given that in the subsection about finite fields we defined $\mathbb{F}_{q^n}$ as the field made of roots of $x^{q^n} - x$ and so K is the fixed field of $F \iff \forall x \in K$ $x^q = x \iff x^q - x = 0$ and this is exactly the equation defying $\mathbb{F}_q$.. This tells us that $P_1 \in \mathbb{P}^2_{F_q}$ and the number of the 1-tuples fixed by F is nothing but $|\mathbb{P}^2_{F_q}| = q^2 + q + 1$.

Proposition 7.0.3
For F the Frobenius endomorphism of $\mathbb{P}^2_{\overline{F}_q}$:

- *There are q^2+q+1 1-tuples of $\mathbb{P}^2_{\overline{F}_q}$ on which F acts like the permutation* (1).

Frobenius and $S(2)$ The group $S(2)$ has $2! = 2$ elements that are the identity permutation $(1)(2)$ and the permutation $(1, 2)$.

- Suppose that for $P_1, P_2 \in \mathbb{P}^2_{\overline{F}_q}$ F acts like $(1)(2)$:

Total number: If this is the case then P_1, P_2 again are in the fixed field $\mathbb{F}_q$ and so the number of 2-tuples on which F acts this way is the number of 2-tuples in this space, i.e. what we called $n_2 = (q^2+q+1)(q^2+q)$.

- The other case is a bit more interesting: so we can consider $P_1, P_2 \in \mathbb{P}^2_{\overline{F}_q}$ such that $F(P_1) = P_2$ and $F(P_2) = P_1$.

Total number: In this case we get that $F^2(P_1) = F(P_2) = P_1$ and $F^2(P_2) = F(P_1) = P_2$ and so actually $P_i \in \mathbb{P}^2_{F_{q^2}}$, moreover $P_1 \neq P_2$ and so they are not in $\mathbb{P}^2_{F_p}$ The couple is totally defined by P_1 being P_2 its image and so the number of such couples, that being couples are always in general position, is the number of points in the space $\mathbb{P}^2_{F_{q^2}} \setminus \mathbb{P}^2_{F_p}$:

$$|\mathbb{P}^2_{F_{q^2}} \setminus \mathbb{P}^2_{F_p}| = |\mathbb{P}^2_{F_{q^2}}| - |\mathbb{P}^2_{F_p}| = q^4 + q^2 + 1 - q^2 - q - 1 = q^4 - q.$$

Proposition 7.0.4
For F the Frobenius endomorphism of $\mathbb{P}^2_{\overline{F}_q}$:

- *There are $(q^2+q+1)(q^2+q)$ 2-tuples of $\mathbb{P}^2_{\overline{F}_q}$ on which F acts like the permutation* $(1)(2)$*;*
- *There are $q^4 - q$ 2-tuples of $\mathbb{P}^2_{\overline{F}_q}$ on which F acts like the permutation* $(1\ 2)$ *and the same number on which it acts like ;*

Frobenius and $S(3)$ The group $S(3)$ has $3! = 6$ elements, these are $(1)(2)(3)$, $(1)(2\ 3)$, $(2)(1\ 3)$, $(3)(1\ 2)$, $(1\ 2\ 3)$ and $(1\ 3\ 2)$. It's quite trivial to notice how, for the purpose of counting 3-tuples fixed by any of these, the permutations $(1\ 2\ 3)$ and $(1\ 3\ 2)$ and the permutations $(1)(2\ 3)$, $(2)(1\ 3)$,

(3)(1 2) behave the same and so we only have 3 permutations that are structurally different.

- (1)(2)(3) is the identity that we know means that, for $P_i \in \mathbb{P}^2_{\overline{F}_q}$, $P_i \in \mathbb{P}^2_{F_q}$ giving a number of such n-tuples equal to $n_3 = (q^2+q+1)(q^2+q)(q^2)$.
- We can now consider the 3-tuples permuted as (1)(2 3) by F. This means that for $P_i \in \mathbb{P}^2_{\overline{F}_q}$ $F(P_1) = P_1$, $F(P_2) = P_3$ and $F(P_3) = P_2$, the first equation tells us that $P_1 \in \mathbb{F}_q$, while if the apply F to the other two we obtain $F^2(P_2) = F(P_3) = P_2$ and $F^2(P_2) = F(P_3) = P_2$ and so we get that actually $P_3, P_2 \in \mathbb{P}^2_{F_{q^2}}$. Such a 3-tuples is totally defined by P_1 and P_2 given that $P_3 = F(P_2)$. We can as a first thing count the number of such triplets and then remove the collinear ones

Total number: There are q^2+q+1 ways to chose a point in $\mathbb{P}^2_{\mathbb{F}_q}$ and $q^4+q^2+1-(q^2+q+1) = q^4-q$ ways to chose one in $\mathbb{P}^2_{\mathbb{F}_{q^2}} \setminus \mathbb{P}^2_{\mathbb{F}_q}$ for a total of $(q^2+q+1)(q^4-q)$ ways to chose a 3-tuple ;

Collinear ones: We want now to count how many collinear triplets there are in this set

1. Each line defined over $\mathbb{F}_q$ is completely characterized by two of its points P_1, P_2 given that it can be written as $<P_1, P_2>$. There are $n_2 = (q^2+q+1)(q^2+q)$ ways to chose two points but each line over $\mathbb{F}_q$ contains $q+1$ points so in the above calculation every line is counted $\binom{q+1}{2}$ times and so the number of distinct lines is $\frac{\frac{(q^2+q+1)(q^2+q)}{2}}{\frac{(q+1)q}{2}} = q^2+q+1$;
2. As we proved talking about collinear triplets, and used in counting the lines over $\mathbb{F}_q$, given a line $< P_1, P_2 >$ this has $q+1$ solutions in $\mathbb{P}^2_{\mathbb{F}_p}$ and so, for $L(K)$ = solutions of L over $\mathbb{P}^2_K$, we get $|L(\mathbb{F}_{q^2})| - |L(\mathbb{F}_p)| = q^2+1-(q+1) = q^2-q$ solutions in $\mathbb{P}^2_{\mathbb{F}_{q^2}} \setminus \mathbb{P}^2_{\mathbb{F}_q}$ corresponding to choosing the point P_2 and $|L(\mathbb{F}_p)| = q+1$ solutions in $\mathbb{P}^2_{\mathbb{F}_q}$ corresponding to choosing the point P_1. This gives us a total of $(q^2-q)(q+1) = q^3-q$ triplets on each line.

We therefore have $(q^2+q+1)(q^3-q)$ collinear triplets.

The total number of general triples turns out to be

$$(q^2+q+1)(q^4-q)-(q^2+q+1)(q^3-q) = (q^2+q+1)(q^4-q^3) = q^6-q^3.$$

- The final case is the one of the 3-tuples permuted as (1 2 3) permutation Let (P_1, P_2, P_3) with $P_i \in q^2_{\overline{\mathbb{F}_q}}$ and such that $F(P_1) = P_2$, $F(P_2) = P_3$, $F(P_3) = P_1$. In other words F acts like the permutation (1 2 3) on the triplet.

  The fact that P_1, P_2, P_3 are all distinct proves that they don't belong to $\mathbb{P}^2_{\mathbb{F}_q}$, but at the same time $F^3(P_i) = F^2(P_{i+1}) = F(P_{i+2}) = P_{i+3} = P_i$ (where $i \in \mathbb{Z}/3\mathbb{Z}$) and by the same reasoning we have that $P_i \in \mathbb{P}^2_{\mathbb{F}_{q^3}}$ and in particular $P_i \in \mathbb{P}^2_{\mathbb{F}_{q^3}} \setminus \mathbb{P}^2_{\mathbb{F}_q}$. The triplet is completely characterized by choosing $P_i \in \mathbb{P}^2_{\mathbb{F}_{q^3}} \setminus \mathbb{P}^2_{\mathbb{F}_q}$. We can also wonder what happens for $F^2(P_i)$ and if it's possible to have $F^2(P_i) = P_i$, but we see that $F^2(P_i) = P_i \Rightarrow F(P_i) = F(F^2(P_i)) = F^3(P_i) = P_i$ and this is not possible if $P_i \notin \mathbb{P}^2_{\mathbb{F}_q}$.

Total number: We showed how $P_1 \neq F(P_1) \neq F^2(P_1) \iff P_1 \in \mathbb{P}^2_{\mathbb{F}_{q^3} \setminus \mathbb{F}_q}$ and so to count the triplets permuted by F as (1 2 3) we suffice to count how many points are there in $\mathbb{P}^2_{\mathbb{F}_{q^3} \setminus \mathbb{F}_q}$. This is simply

$$|\mathbb{P}^2_{\mathbb{F}_{q^3} \setminus \mathbb{F}_q}| = |\mathbb{P}^2_{\mathbb{F}_{q^3}| - |\mathbb{F}_q}| = (q^3)^2 + q^3 + 1 - (q^2 + q + 1) = q^6 + q^3 - q^2 - q.$$

Collinear ones: We need to count the number of lines defined over $\mathbb{F}_q$ and multiply it by the number of solutions of the equation lying in $\mathbb{F}_{q^3}$ but not in $\mathbb{F}_q$.

1. The fact that the points are collinear means that the line on which they lie is defined over $\mathbb{F}_q$, this because the line is fixed by Frobenius, and there are $q^2 + q + 1$ such lines:
2. We want now to count the points satisfying the equation of the line, there are

   $$|L(\mathbb{F}_{q^3} \setminus \mathbb{F}_q)| = |L(\mathbb{F}_{q^3})| - |L(\mathbb{F}_q)| = q^3 + 1 - (q + 1) = q^3 - q$$

   solutions.

The total number of collinear triplets is therefore $(q^2+q+1)(q^3-q)$.

At the end we get that the number of $3-tuples$ of $\overline{F_q}$ on which F acts as the permutation (1 2 3) is equal to

$$(q^6 + q^3 - q^2 - q) - (q^2 + q + 1)(q^3 - q) = q^6 - q^5 - q^4 + q^3.$$

Proposition 7.0.5
For F the Frobenius endomorphism of $\mathbb{P}^2_{\overline{F}_q}$:

- *There are* $(q^2+q+1)(q^2+q)(q^2)$ 3*-tuples of* $\mathbb{P}^2_{\overline{F}_q}$ *on which* F *acts like the permutation* $(1)(2)(3)$*;*
- *There are* q^6-q^3 3*-tuples of* $\mathbb{P}^2_{\overline{F}_q}$ *on which* F *acts like the permutation* $(1)(2\,3)$*, the same is true for the permutations* $(2)(1\,3)$ *and* $(3)(1\,2)$*;*
- *There are* $q^6-q^5-q^4+q^3$ 3*-tuples of* $\mathbb{P}^2_{\overline{F}_q}$ *on which* F *acts like the permutation* $(1\,2\,3)$*, the same is true for the permutation* $(1\,3\,2)$*.*

From these computations it becomes clear the role of the cycles in the permutations, this can be turned into a proper statement

Proposition 7.0.6 (Frobenius and cycles)
If the Frobenius morphism acts on a set of elements $P_1,\dots P_n$*,* $P_i \in \mathbb{P}^2_{\overline{F}_q}$ *as a cycle then* $P_i \in \mathbb{P}^2_{F_{q^n}}$

Frobenius and $S(4)$ In $S(4)$ the distinct cycles, up to renaming of the variables, are 5, equivalent to the 5 ways to write 4 as a sum of naturals (that are $1+1+1+1$, $1+1+2$, $2+2$, $1+3$, 4) i.e. $(1)(2)(3)(4)$, $(1)(2)(3\,4)$, $(1\,2)(3\,4)$, $(1)(2\,3\,4)$ and $(1\,2\,3\,4)$.

- In the case of $(1)(2)(3)(4)$ we again have that $P_i \in \mathbb{P}^2_{\overline{F}_q} \Rightarrow P_i \in \mathbb{P}^2_{F_q}$ and so there are $n_4 = n_3 * (q^2-2q+1) = (q^2+q+1)(q^2+q)(q^2)(q^2-2q+1)$ 4-tuples of points on which F acts this way.
- Regarding the permutation $(1)(2)(3\,4)$:

Total number: Such 4-tuples are completely characterized by the choice of the first three points (the fourth is the image under Frobenius of the third), the points have to be chosen such that the first two lie in $\mathbb{P}^2_{\mathbb{F}_q}$ and the third in $\mathbb{P}^2_{\mathbb{F}_{q^2}} \setminus \mathbb{P}^2_{\mathbb{F}_q}$ for a total of

$$\left(q^2+q+1\right)\left(q^2+q\right)\left(q^4-q\right)$$

points.

Collinear ones:
1. If the collinear points are P_1, P_2, P_3 then again we have that the line containing them is defined over $\mathbb{F}_q$ (it is the unique line passing through P_1 and P_2) and given how $P_4 = F(P_3)$ we have that it actually passes through every of the 4 points. There are (q^2+q+1) lines defined over $\mathbb{F}_q$ and in each of them we have $q+1$ ways to chose P_1, q ways to chose P_2 and

$(q^2+1-(q+1)) = q^2-q$ ways to chose P_3 for a total of $(q+1)(q)(q^2-q) = q^4-q^2$;

2. If the collinear points are P_1, P_3, P_4 then we have to multiply the number q^2+q+1 of lines over $\mathbb{F}_q$ by the $q+1$ ways to chose P_1, the $(q^2+q+1-(q-1))$ ways to chose P_2 such that it's not collinear and the q^2-q ways to chose P_3 for a total of $(q+1)(q^2)(q^2-q) = q^5-q^3$ The same happens if the points are P_2, P_3, P_4 .

- The 4-tuples on which F acts as (1 2)(3 4) are characterized by the choice of P_1 and P_3 in $\mathbb{P}^2_{\mathbb{F}_{q^2}} \setminus \mathbb{P}^2_{\mathbb{F}_p}$

Total number: There are $(q^4-q)(q^4-q-1)$ such 4-tuples corresponding to choosing 2 elements in $\mathbb{P}^2_{\mathbb{F}_{q^2}}$.

Collinear ones: If we take any three points we are actually taking all four given how $P_2 = F(P_1)$, $P_4 = F(P_3)$ and the lines are defined over the fixed field of F , and so there are q^2+q+1 of them. We need therefore to count how many couple of points on the same line are there in $\mathbb{P}^2_{\mathbb{F}_{q^2}} \setminus \mathbb{P}^2_{\mathbb{F}_p}$, and turns out this number is $(q^2-q)(q^2-q-1)$.

- We can consider the permutation (1)(2 3 4), that is characterized by the choice of P_1 and P_2

Total number: There are q^2+q+1 ways to chose an element of $\mathbb{P}^2_{\mathbb{F}_q}$ and $(q^6+q^3+1-q^2-q-1) = (q^6+q^3-q^2-q)$ ways to chose an element in $\mathbb{P}^2_{\mathbb{F}_{q^3}} \setminus \mathbb{P}^2_{\mathbb{F}_q}$ for a total of $(q^2+q+1)(q^6+q^3-q^2-q)$ 4-tuples

Collinear ones: Thanks to the theorem about collinear lines we know that again the lines are defined over $\mathbb{F}_q$ (we have that $P_1 = F(P_1)$ and $P_3 = F(P_2)$). On each of the q^2+q+1 lines over $\mathbb{F}_q$ we can take P_2, P_3, P_4 on the line in q^3-q ways and P_1 not on it in q^2 ways, for a total of $(q^2)(q^3-q)$ 4-tuples where the last 3 points are collinear . If we chose P_1 on the line (and there are $q+1$ ways to do so) to find a 4-tuples not in general position we are forced to take all the 4 points on the line for a total of $(q+1)(q^3-q)$ 4-tuples of collinear points. The fact we are forced to take all 4 points come from the fact that, containing both P_2 and $F(P_2)$ it has to be defined over $\mathbb{F}_q$ and so contain also $F(P_3) = P_4$.

- At last we consider the permutation (1 2 3 4) that is completely characterized by P_1

Total number: We simply need to count how many points are in $\mathbb{P}^2_{\mathbb{F}_{q^4}} \setminus \mathbb{P}^2_{\mathbb{F}_{q^2}}$, and there are $q^8 - q^2$ such points (we need to remove $\mathbb{P}^2_{\mathbb{F}_{q^2}}$ given how $P_1 \neq P_3$ and $P_2 \neq P_4$) and removing this, given the inclusion $\mathbb{F}_q \subset \mathbb{F}_{q^2}$ we are also removing the former.

Collinear ones: If we take any 3 points P_i, P_j, P_k out of the 4 then we'll have that, up to renaming them, $P_i = F(P_j)$, $P_k = F(P_i)$ and so the line containing them is defined over $\mathbb{F}_q$, and also contains the fourth point and there are $q^2 + q + 1$ of them. Each of these lines has $q^4 - q^2$ solutions in $\mathbb{P}^2_{\mathbb{F}_{q^4}} \setminus \mathbb{P}^2_{\mathbb{F}_{q^2}}$.

Proposition 7.0.7
For F the Frobenius endomorphism of $\mathbb{P}^2_{\overline{F}_q}$:

- *There are n_4 4-tuples of $\mathbb{P}^2_{\overline{F}_q}$ on which F acts like the permutation* $(1)(2)(3)(4)$*;*
- *There are*

  $$(q^2+q+1)(q^2+q)(q^4-q)-(q^2+q+1)(q^4-q^2)-2*(q^2+q+1)(q^5-q^3)$$

  4-tuples of $\mathbb{P}^2_{\overline{F}_q}$ on which F acts like the permutation $(1)(2)(3\ 4)$*, the same is true for the permutations* $(1)(3)(2\ 4)$*,* $(1)(4)(3\ 2)$*,* $(3)(2)(1\ 4)$*,* $(4)(2)(3\ 1)$ *and* $(3)(4)(1\ 2)$*;*
- *There are* $(q^4-q)(q^4-q-1)-(q^2+q+1)(q^2-q)(q^2-q-1)$ *4-tuples of $\mathbb{P}^2_{\overline{F}_q}$ on which F acts like the permutation* $(1\ 2)(3\ 4)$*, the same is true for the permutations* $(1\ 3)(2\ 4)$ *and* $(1\ 4)(3\ 2)$*.*
- *There are* $(q^2+q+1)(q^6+q^3-q^2-q)-(q^2+q+1)(q^2)(q^3-4)-(q^2+q+1)(q+1)(q^3-q)$ *4-tuples of $\mathbb{P}^2_{\overline{F}_q}$ on which F acts like the permutation* $(1)(2\ 3\ 4)$*, the same is true for the permutations* $(1)(2\ 4\ 3)$*,* $(2)(1\ 3\ 4)$*,* $(2)(1\ 4\ 3)$*,* $(3)(2\ 1\ 4)$*,* $(3)(4\ 1\ 2)$*,* $(4)(2\ 3\ 1)$ *and* $(4)(3\ 2\ 1)$*.*
- *There are* $(q^8-q^2)-(q^2+q+1)(q^4-q^2)$ *4-tuples of $\mathbb{P}^2_{\overline{F}_q}$ on which F acts like the permutation* $(1\ 2\ 3\ 4)$*, the same is true for the permutations* $(1\ 2\ 4\ 3)$*,* $(1\ 3\ 2\ 4)$*,* $(1\ 3\ 4\ 2)$*,* $(1\ 4\ 3\ 2)$ *and* $(1\ 4\ 2\ 3)$*.*

Frobenius and $S(5)$ With the case of $S(4)$ it became clear how going from $S(n)$ to $S(n+1)$ increases greatly the number of different cases and the length of the equation of the solution, this is not totally unexpected

given how $Card(S(n)) = n!$. Moreover we notice how the underlying method became standardized way more than in the case of counting n-tuples in $\mathbb{P}^2_{\mathbb{F}_q}$. Given this two observations from now on we'll avoid writing too much explicit computations but we'll reduce to highlight any eventual new property of an n-tuple of $\mathbb{P}^2_{\mathbb{F}_q}$ on which F acts like a given permutation of $S(n)$ and write the resulting number of 5-tuples.

Now, the main difference between 4-tuples and 5-tuples is that now in some cases we have that the lines containing collinear points may not be defined over $\mathbb{F}_q$, therefore we'll be particularly careful in this regard, and we'll devote a proposition to the problems coming from this. This is also an original result, or at least was obtained autonomously.

Proposition 7.0.8 (Points on lines over a finite field)
We'll divide this proposition in two parts, one where we look for solutions into a field extension and one where we look for solutions into a subfield:

Extensions: *Suppose we have that the line is defined over $\mathbb{F}_q$, then we showed that this can be expressed as the set $\{a + x * b | x \in \mathbb{K}\} \cup \{a\}$ where a, b are points in $\mathbb{P}^2_{\mathbb{F}_q}$ and K is the field such that $\mathbb{P}^2_{\mathbb{K}}$ is where we want to look for solutions. Given that there are q^n elements in $\mathbb{F}_{q^n}$ we get that the set of solutions has exactly $q^n + 1$ elements. We notice that this can only work if $\mathbb{K}$ is an extension of $\mathbb{F}_q$, so that the linear combinations are elements of $\mathbb{P}^2_{\mathbb{K}}$;*

Subfields : *For $K \subset \mathbb{F}_q$, a subfield, we can't use the previous method given how it's not sure anymore that $a + x * b$ will belong to $\mathbb{P}^2_K$, even if $x \in K$.*

A line in $\mathbb{P}^2$ can also be expressed by an equation $ax + by + cz = 0$ with $(a, b, c) \in K^3$, where we look at solutions $(x, y, z) \in K^3$. The set of solutions is a vector space over K of dimension $3 - d$ where d is the dimension of the span of $\{a, b, c\}$, again over K.

A linear vector space over K of dimension n has $card(K)^n$ elements, if we projectivise this (that is a cone) we get that the image has $\frac{card(K)^n - 1}{card(K) - 1}$, where we remove the zero point and divide by $card(K) - 1 = card(K^x)$ the cardinality of the multiplicative subgroup. If $d = 1$ then the line is actually defined over K (a, b, c are linearly dependent i.e. $a = l * b = k * c$ with l, k in K and dividing by a we obtain an equivalent formulation that is rational over K), so the proper lines in a field, id est the ones that are not defined over any subfield, have either 1 or 0 solutions over a given subfield depending on the dimension of the span of $\{a, b, c\}$.

We can now count $5-$tuples permuted as elements of $S(5)$.

Proposition 7.0.9 (5-tuples and elements of $S(5)$)
We list every of the 7 *unique, up to renaming, permutations.*

- *In the case of* $(1)(2)(3)(4)(5)$ *we already accounted for collinear triplets in the computation of* $n_5 = (q^2+q+1)(q^2+q)(q^2)(q^2-2q+1)(q^2-5q+6)$*;*
- *We can consider* $(1)(2)(3)(4\,5)$*: there are* $(q^2+q+1)(q^2+q)(q^+q-1)(q^4-q)$ *such* 5*-tuples. We now have several cases:*
  - *If the collinear points are* P_1, P_2, P_3*, it's possible to have that only these* 3 *are collinear and the line they belong to is defined over* $\mathbb{F}_q$*. In each of the* q^2+q+1 *lines there are* $(q+1)(q)(q-1)(q^4-q^2)$ *such* 4*-tuples, where* $q^4-q^2 = (q^4+q^2+1-(q^2-q))-(q^2+q+1-(q+1))$*;*
  - *If the points are* P_1, P_2, P_4 *then the line they belong to is defined over* $\mathbb{F}_q$ *and actually also* P_5 *belongs to the line. In each of the* q^2+q+1 *lines there are* $(q+1)(q)(q^2)(q^2-q)$ *such 4-tuples, and the same is true for* P_1, P_3, P_4, P_5 *and for* P_2, P_3, P_4, P_5*;*
  - $P_1, P_4, P_5 \in L \Rightarrow L$ *defined over* $\mathbb{F}_q$*. In each of the* q^2+q+1 *lines there are* $(q^2)(q^2-1)(q+1)(q^2-q)$ *such* 4*-tuples, and the same is true for* P_2, P_4, P_5 *and for* P_3, P_4, P_5*;*
  - $P_1, P_2, P_3, P_4 \in L \Rightarrow L$ *defined over* $\mathbb{F}_q$ *and also* $P_5 \in L$ *so actually we are only left with the case of all* 5 *points collinear. In each of the* q^2+q+1 *lines there are* $(q+1)(q)(q-1)(q^2-q)$ *such* 4*-tuples.*

  Every other 3*-tuples or* 4*-tuples reduces to one of the above cases.*
- *For* $(1)(2\,3)(4\,5)$ *there are* $(q^2+q+1)(q^4-q)(q^4-q-1)$ *such* 5*-tuples. Regarding collinearity the cases, up to renaming, are*
  - $P_1, P_2, P_3 \in L \Rightarrow L$ *defined over* $\mathbb{F}_q$*, on each of the* q^2+q+1 *lines there are* $(q+1)(q^2-q)(q^4-q^2)$ *such* 4*-tuples. the same is true for* P_1, P_4, P_5*;*
  - $P_1, P_2, P_4 \in L \Rightarrow L$*, given that* P_1*,* P_2*,* P_4 *are in* $\mathbb{P}^2_{\mathbb{F}_{q^2}}$*, it's defined over* $\mathbb{F}_{q^2}$*, but not over* $\mathbb{F}_q$*, or it's defined over* $\mathbb{F}_q$ *and so all* 5 *points belong to it, this last case will be treated in his own regard so we focus on the first one.From proposition 7.0.8 we get that if this is the case then* $d = 2$ *and there is only one solution in* $\mathbb{F}_q$*, from this we have that on each of the* q^4-q *lines there are* $(1)(q^2)(q^2-1)$ *such* 5*-tuples, where* $q^4-q-1 = q^4+q^2+1-(q^2-q-1)-1$*. The same is true for* P_1, P_2, P_5*,* P_1, P_3, P_5*, and* P_1, P_3, P_4*. To end it's worth noticing that* $F(< P, Q >) =< F(P), F(Q) >$ *given that,*

with the usual abuse of notation $< P, Q >= \{q + xQ | x \in \mathbb{F}_{|\mathbb{F}^\times|}\}$, *but* $F(q + xQ) = F(P) + F(x)F(Q)$, $F(x) \in \mathbb{F}_{|\mathbb{F}^\times|}$ *we get that indeed* $F(L) =< F(P), F(Q) >$. *Applying this to our* 5*-tuples we get that*

$$P_3 = F(P_2), P_5 = F(P_3), P_1 = F(P_1)$$

tells us that P_1, P_2, P_4 *collinear* $\iff$ P_1, P_3, P_4 *;*

- $P_2, P_3, P_4 \in L \Rightarrow L$ *defined over* $\mathbb{F}_q$ *and also* P_5 *belongs to the same line, on each of the* q^2+q+1 *lines there are* $(q^2)(q^2-q)(q^2-q-1)$ *such* 4*-tuples;*
- $P_1, P_2, P_3, P_4 \in L \Rightarrow L$ *defined over* $\mathbb{F}_q$ *and also* P_5 *belong to the same line, on each of the* $q^2 + q + 1$ *lines there are* $(q + 1)(q^2 - q)(q^2 - q - 1)$ *such* 5*-tuples.*

Every other 3*-tuples or* 4*-tuples reduces to one of the above cases.*

- *For* $(1)(2)(3\,4\,5)$ *we have that the number on* 5*-tuples is* $(q^2+q+1)(q^2+q)(q^6+q^3-q^2-q)$. *Regarding collinearity we have:*
  - $P_1, P_2, P_3 \in L \Rightarrow L$ *defined over* $\mathbb{F}_q$ *and actually* $P_4, P_5 \in L$. *In each of the* q^2+q+1 *lines there are* $(q+1)(q)(q^3-q)$ *such* 5*-tuples;*
  - $P_1, P_3, P_4 \in L \Rightarrow L$ *defined over* $\mathbb{F}_q$ *and actually* $P_5 \in L$. *In each of the* $q^2 + q + 1$ *lines there are* $(q + 1)(q^2)(q^3 - q)$ *such* 5*-tuples and the same happens for* P_2, P_3, P_4, P_5*;*
  - $P_3, P_4, P_5 \in L \Rightarrow L$ *defined over* $\mathbb{F}_q$. *In each of the* q^2+q+1 *lines there are* $(q^2)(q^2-1)(q^3-q)$ *such* 5*-tuples.*

Every other 3*-tuples or* 4*-tuples reduces to one of the above cases.*

- *For* $(1\,2)(3\,4\,5)$ *we have that* $(q^4 - q)(q^6 + q^3 - q^2 - q)$ 5*-tuples satisfy the requirement. Regarding collinearity:*
  - $P_1, P_2, P_3 \in L \Rightarrow L$ *defined over* $\mathbb{F}_q$ *and actually* $P_4, P_5 \in L$. *Therefore on each of the* $q^2 + q + 1$ *lines there are* $(q^2 - q)(q^3 - q)$ *such* 5*-tuples;*
  - $P_1, P_3, P_4 \in L \Rightarrow L =< P_1, P_4 >=< P_1, P_3 >$ *and so* $F^2(L) =< F^2(P_1), F^2(P_4) >=< P_1, P_3 >= L$ *and so either* L *is defined over* $\mathbb{F}_{q^2}$ *but not over* $\mathbb{F}_q$*, or it's defined over* $\mathbb{F}_q$ *and actually* $P_2, P_5 \in L$. *The first case is however not possible given that* $\mathbb{F}_{q^2}$ *is not a subfield of* $\mathbb{F}_{q^3}$*, the second one will be treated on its own;*
  - $P_3, P_4, P_5 \in L \Rightarrow L$ *defined over* $\mathbb{F}_q$. *Therefore on each of the* $q^2 + q + 1$ *lines there are* $(q^4 - q^2)(q^3 - q)$ *such* 5*-tuples.*

Every other 3*-tuples or* 4*-tuples reduces to one of the above cases.*

- *For* $(1)(2\,3\,4\,5)$ *we have that the total number of such* 5*-tuples is* $(q^2+q+1)(q^8-q^2)$
  - $P_1, P_2, P_3 \in L \Rightarrow L$ *defined over* $\mathbb{F}_q$ *and actually* $P_4, P_5 \in L$. *Therefore on each of the* q^2+q+1 *lines there are* $(q+1)(q^4-q^2)$ *such* 5*-tuples;*
  - $P_1, P_2, P_4 \in L \Rightarrow L$ *defined over* $\mathbb{F}_{q^2}$*, this comes from the fact that the cycle* $(2\,3\,4\,5)$ *defined by* F *contains the subcycles* $(2\,4)$ *and* $(3\,5)$ *defined by* F^2*. Therefore on each of the* q^4-q *lines there are* $(1)(q^4-q^2)$ *such* 5*-tuples. Again we get that in this case also* P_1, P_3, P_5 *are collinear;*
  - $P_2, P_3, P_4 \in L \Rightarrow L$ *defined over* $\mathbb{F}_q$ *and so also* $P_5 \in L$*. Therefore on each of the* q^2+q+1 *lines there are* $(q^2)(q^4-q^2)$ *such* 5*-tuples.*

  Every other 3*-tuple or* 4*-tuple reduces to one of the above cases.*

- *For* $(1\,2\,3\,4\,5)$ *we have that the total number of such lines is* $(q^{10}+q^5-q^2-q)$*. Regarding collinearity:*
  - $P_1, P_2, P_3 \in L \Rightarrow L$ *defined over* $\mathbb{F}_q$ *and actually* $P_4, P_5 \in L$. *Therefore on each of the* q^2+q+1 *lines there are* (q^5-q) *such* 5*-tuples;*
  - $P_1, P_2, P_4 \in L \Rightarrow L =< P_1, P_4 >=< P_2, P_4 >$ *, that implies that* $F^2(L) =< F^2(P_2), F^2(P_4) >=< P_4, P_1 >= L$ *and so either* L *is defined over* $\mathbb{F}_{q^2}$ *but not over* $\mathbb{F}_q$*, or it's defined over* $\mathbb{F}_q$ *and actually* $P_2, P_5 \in L$*. We notice that also in this cases, similarly than in the case of* $(1\,2)(3\,4\,5)$*,* $\mathbb{F}_{q^2}$ *is not a subfield of* $\mathbb{F}_{q^5}$ *and so this case actually gives us no* 5*-tuple. .*

  Every other 3*-tuples or* 4*-tuples reduces to one of the above cases.*

A note on the equivalence of the counting methods As the last part of this subsection we can make a statement about the different methods we used to count n-tuples of points.

Note 7.0.10
In section 5 we computed the number of n*-tuples in general position, for* $n < 6$*, and now we did the same for* n*-tuples that are permuted in a given way by Frobenius. But some permutations give us back* $n-$*tuples in general position.*

As an example we can consider 4-tuples in general position, these are 4-tuples that are permuted as (1)(2)(3)(4) by Frobenius. So we can check that counting permutations permuted as (1)(2)(3)(4) gives back what we called n4 as a result.

- *The number of n-tuples is* $\binom{q^2+q+1}{4} * 4!$*;*
- *The number of lines over* $\mathbb{F}_q$ *is as always* q^2+q+1*;*
- *The 4-tuples of 3 collinear points and one not collinear to the three in each of these lines are* $\binom{q+1}{3} * 3!(q^2+q+1-(q+1)) * 4$ *(given that there are 4 position in which the external point may be in the 4-tuple);*
- *The number of 4-tuples of collinear points is equal to* $\binom{q+1}{4} * 4!$*.*

This gives a total of

$$(q^2+q+1)\left(\binom{q+1}{3} * 3!(q^2+q+1-(q+1)) * 4 - \binom{q+1}{4} * 4!\right)$$

non-general 4-tuples. We now have to check, here $\stackrel{?}{=}$ *means "is the left side equal to the right one?", if*

$$n_4 = (q^2+q+1)(q^2+q)(q^2)(q^2-2q+1) \stackrel{?}{=}$$

$$\stackrel{?}{=} (q^2+q+1)(q^2+q)(q^2+q-1)(q^2+q-2) -$$
$$-(q^2+q+1)\left(\binom{q+1}{3}(q^2) * 3! * 4 - \binom{q+1}{4} * 4!\right) \iff$$

$$(q^2+q)(q^2)(q^2-2q+1) \stackrel{?}{=} (q^2+q)(q^2+q-1)(q^2+q-2) -$$
$$-\left(4 * (q+1)(q)(q-1)(q^2) - (q+1)(q)(q-1)(q-2)\right) \iff$$

$$(q^2)(q^2-2q+1) \stackrel{?}{=} (q^2+q-1)(q^2+q-2) -$$
$$-\left(4 * (q-1)(q^2) - (q-1)(q-2)\right) \iff$$

$$(q^2)(q^2-2q+1) \stackrel{?}{=} (q^2+q-1)(q^2+q-2) -$$
$$-\left(4 * (q-1)(q^2) - (q-1)(q-2)\right) \iff$$

$$q^4-2q^3+q^2 \stackrel{?}{=} (q^4+2q^3-2q^2-3q+2) - (4q^3-3q^2-3q+2) \iff$$

$$\iff q^4-2q^3+q^2 \stackrel{?}{=}$$

$$\stackrel{?}{=} q^4+2q^3-2q^2-3q+2-4q^3+3q^2+3q-2 = q^4-2q^3+q^2$$

as we wanted to prove.

Frobenius and $S(n)$, for $n > 5$ Subsequent cases behave in a very similar fashion as long as we simply require the general position to only regard lines. General position regarding conics or polynomials of even bigger degree is unfit to be discussed in the simple case of finite fields, and even more so in this more complicated set-up. The path to follow would therefore be to consider the algorithms used to count n-tuples of points in a finite field and adapt them.

8 Appendix

8.1 Sage code

$\mathbb{P}^2$ generator for a finite set

Algorithm 8.1

```
P2=[]
def P_2(n):
  P2.append((0,0,1))
  for i in GF(n):
          P2.append((0,1,i))
  for i in GF(n):
          for j in GF(n):
              P2.append((1,i,j))
```

Comments 8.1.1

P2=[] *<—- defines an empty set called "P2"*

def $P_2(n)$ *<—— defines a function called "P_2" that has an integer as input*

P2.append ($(0,0,1)$***)*** *<—- adds the element* $(0,0,1)$ *to the set "P2"*

for i ***in*** $GF(n)$ *<—- does what will be in the indented instructions below for every element of* $GF(n)$*, this is Sage notation for* $\mathbb{F}_n$ *and so* n *has to be a prime power*

Reducing to standard form elements of $\mathbb{P}^2$

Algorithm 8.2

```
def Red(v):
if v[0]=0
   if v[1]=0
      v=(0,0,1)
   else v=(0,1, v[2]/v[1])
else v=(1,v[1]/v[0],v[2]/v[0])
```

Comments 8.2.1

def Red(v***):*** *<—-v has to be an element of* $\mathbb{P}^2$*, i.e. we need to create it in such a way that Sage knows how to define operations e.g. by the function* P_2 *and successive operations.*

Counting n-tuples for low n ($1st$ algorithm)

Algorithm 8.3

```
def SC(k,n):
     n1=(k^2+k+1)
     n2=n1*(k^2+k)
     n3=n2*k^2
     n4=n3*(k^2-2*k+1)
     n5=n4*(k^2-5*k+6)
     if n==1:
       print ('There are', n1, '1-tuples in general position')
     if n==2:
       print ('There are', n2, '2-tuples in general position')
     if n==3:
       print ('There are', n3, '3-tuples in general position')
     if n==4:
       print ('There are', n4, '4-tuples in general position')
     if n==5:
       print ('There are', n5, '5-tuples in general position')
```

Comments 8.3.1
def SC(k,n) *<—- k is the order of the finite base field, n is the same as the one in n-tuple.*

Counting unordered n-tuples for low n ($1st$ algorithm)

Algorithm 8.4

```
def SC(k,n):
     n1=(k^2+k+1)
     n2=n1*(k^2+k)/2
     n3=n2*k^2/3
     n4=n3*(k^2-2*k+1)/4
     n5=n4*(k^2-5*k+6)/5
     if n==1:
       print ( n1, 'unordered 1-tuples in general position')
     if n==2:
       print ( n2, 'unordered 2-tuples in general position')
     if n==3:
       print ( n3, 'unordered 3-tuples in general position')
     if n==4:
       print ( n4, 'unordered 4-tuples in general position')
```

```
if n==5:
  print ( n5, 'unordered 5-tuples in general position')
```

Even if this algorithms are nothing but a specific polynomial evaluate they still has their own uses, the main being that they can be used to check if more complex algorithms, at least for low n, work as intended.

Counting n-tuples in finite fields

Algorithm 8.5
The following problem (counting n-tuples of $\mathbb{P}^2_{F_q}$) requires, if we don't want simply to implement the one we defined in the theoretical part, an algorithm that is way more complex than the ones we've used until now and so it's better, for clarity, to break it down into small components.

Building $\mathbb{P}^2_{\mathbb{F}_q}$

```
P2=[]
def P_2(q,n,S):
 S.append((0,0,1))
 for i in GF(q^n):
          S.append((0,1,i))
 for i in GF(q^n):
          for j in GF(q^n):
              S.append((1,i,j))
```

*This function takes as inputs **q and n** such that $\mathbb{F}_{q^n}$ is the field we are working in (with q prime), and **S**=P2. The only output is P2=$\mathbb{P}^2_{\mathbb{F}_{q^n}}$.*

Building the sets of 3-tuples and 6-tuples of indices

```
I3=[]
I6=[]
I8=[]
def IG(k):
  global I3
  global I6
```

```
  I3=[]
  I6=[]
  I8=[]
  I=[]
  for f in range(k):
              I.append(f)
  for g in Subsets(I,3):
     I3.append(g)
  if k>5:
    for h in Subsets(I,6):
       I6.append(h)
  if k>7:
    for y in Subsets(I,8):
       I8.append(y)
```

This takes as input simply a set ***P*** *and the target length* ***k*** *of the k-tuple. The output are the sets* ***I3, I6 and I8*** *that are made of n-tuples, for* $n = 3, 6, 8$*, in the set of indices* $(0, .., k-1)$*.*

Checking if three elements of $\mathbb{P}^2$ are collinear over a field

```
def coll(x,y,z):
    A=[x,y,z]
    M = matrix(A)
    if M.determinant()==0:
        return 'true'
```

The inputs are ***x,y,z****, three elements of* $\mathbb{P}^2$ *we want to check if they are collinear by checking the determinant of the matrix having them as lines. The output is either "true" if the three are collinear or nothing. This as the previous is another function that will only be used nested.*

Defining the function "cone" that is needed to check if points lie on the same conic

```
def cone(v):
    t=[]
    t.append(v[0]^2)
```

```
    t.append(v[1]^2)
    t.append(v[2]^2)
    t.append(v[0]*v[1])
    t.append(v[2]*v[1])
    t.append(v[0]*v[2])
    return(t)
```

The input is a 3*-tuple* $\boldsymbol{v}$*, i.e. an element of* $\mathbb{P}^2_{\mathbb{F}_q}$*, . The output is a vector of length* 6 *whose coordinates are the possible monomials of degree* 2 *computed in* v*.*

Checking if six elements of $\mathbb{P}^2$ lie on the same conic over a field

```
def conic(x1,x2,x3,x4,x5,x6):
    A=[cone(x1),cone(x2),cone(x3),cone(x4),cone(x5),cone(x6)]
    M = matrix(A)
    if M.determinant()==0:
        return 'true'
```

The inputs are ***x1,x2,x3,x4,x5,x6****, six elements of* $\mathbb{P}^2$ *we want to check if they lie on the same conic. The output is either "true" if the six lie on the same conic or nothing, to check this we are putting the* 6 *images of the points under the Veronese embedding in a* $6x6$ *matrix and checking the determinant.*

Defining the function "cube" that is needed to check if points lie on the same cubic

```
def cube(v):
    t=[]
    t.append(v[0]^3)
    t.append(v[1]^3)
    t.append(v[2]^3)
    t.append(v[0]^2*v[1])
    t.append(v[0]^2*v[2])
    t.append(v[1]^2*v[0])
    t.append(v[1]^2*v[2])
    t.append(v[2]^2*v[1])
    t.append(v[2]^2*v[0])
```

```
    t.append(v[0]*v[1]*v[2])
    return(t)
```

The input is a 3*-tuple* $\boldsymbol{v}$*, i.e. an element of*$\mathbb{P}^2_{\mathbb{F}_q}$*, . The output is a vector of length* 10 *whose coordinates are the possible monomials of degree* 3 *computed in* v*.*

Defining the function "dxcube" that is needed to check if points lie on a singular cubic

```
def dxcube(v):
    t=[]
    t.append(3*v[0]^2)
    t.append(0)
    t.append(0)
    t.append(2*v[0]*v[1])
    t.append(2*v[0]*v[2])
    t.append(v[1]^2)
    t.append(0)
    t.append()
    t.append(v[2]^2)
    t.append(v[2]*v[1])
    return(t)
```

The input is a 3*-tuple* $\boldsymbol{v}$*, i.e. an element of* $\mathbb{P}^2_{\mathbb{F}_q}$*. The output is a vector of length* 10 *whose coordinates are derivatives in the first variable of the possible monomials of degree* 3 *computed in* v*.*

Defining the function "dycube" that is needed to check if points lie on a singular cubic

```
def dycube(v):
    t=[]
    t.append(0)
    t.append(3*v[1]^2)
    t.append(0)
    t.append(v[0]^2)
    t.append(0)
```

```
    t.append(2*v[1]*v[0])
    t.append(2*v[1]*v[2])
    t.append(v[2]^2)
    t.append(0)
    t.append(v[0]*v[2])
    return(t)
```

The input is a 3*-tuple* $\boldsymbol{v}$*, i.e. an element of* $\mathbb{P}^2_{\mathbb{F}_q}$*. The output is a vector of length* 10 *whose coordinates are derivatives in the second variable of the possible monomials of degree* 3 *computed in* v*.*

Defining the function "dzcube" that is needed to check if points lie on a singular cubic

```
def dzcube(v):
    t=[]
    t.append(0)
    t.append(0)
    t.append(3*v[2]^2)
    t.append(0)
    t.append(v[0]^2)
    t.append(0)
    t.append(v[1]^2)
    t.append(2*v[2]*v[1])
    t.append(2*v[2]*v[0])
    t.append(v[0]*v[1])
    return(t)
```

The input is a 3*-tuple* $\boldsymbol{v}$*, i.e. an element of* $\mathbb{P}^2_{\mathbb{F}_q}$*. The output is a vector of length* 10 *whose coordinates are derivatives in the third variable of the possible monomials of degree* 3 *computed in* v*.*

Checking if eight elements of $\mathbb{P}^2$ lie on the same singular cubic over a field with the singularity in one of them

```
def SIcubic(x1,x2,x3,x4,x5,x6,x7,x8):
    v1='false'
    v=[x1,x2,x3,x4,x5,x6,x7,x8]
```

```
    for a in range(8):
        x=v[a]
        A=[]
        A.append(dxcube(x))
        A.append(dycube(x))
        A.append(dzcube(x))
        for t in range(8):
         if t!=a:
           y=v[t]
           A.append(cube(y))
        M = matrix(A)
        if M.determinant()==0:
             v1='true'
    return v
```

The inputs are ***x1,x2,x3,x4,x5,x6,x7,x8****, eight elements of* $\mathbb{P}^2$ *we want to check if they lie on the same singular cubic with the singularity in one of them. The output is either 'true' if they do or 'false', again we are checking if the* $10x10$ *matrix of the image of the* 8 *points under the functions has determinant equal to* 0*. This as the previous ones is another function that will only be used nested.*

Counting all the n-tuples in $\mathbb{P}^2_{\mathbb{F}_q}$

```
t=1
def TOT(P,k):
      global t
      t=1
      s=len(P)
      t=binomial(s,k)
      return t
```

This takes as input a set $\boldsymbol{P}$ *and* $\boldsymbol{k}$ *that is the length of the vectors and returns the number of all* n*-tuples of* $\boldsymbol{P}$ *of the given length, that are trivially get by using the binomial coefficient.*

Checking if a given n-tuple is in general position

```
b=0
def check(s,k):
        global b
        IG(k)
        q=0
        for i8 in I8:
            a0=i8[0]
            a1=i8[1]
            a2=i8[2]
            a3=i8[3]
            a4=i8[4]
            a5=i8[5]
            a6=i8[6]
            a7=i8[7]
            if SIcubic(s[a0],s[a1],s[a2],s[a3],\\
            \\ s[a4],s[a5],s[a6],s[a7])=='true':
                 q=1
                 break
        if k>5:
          if q==0:
            for i6 in I6:
                a0=i6[0]
                a1=i6[1]
                a2=i6[2]
                a3=i6[3]
                a4=i6[4]
                a5=i6[5]
                if conic(s[a0],s[a1],s[a2],\\
                \\ s[a3],s[a4],s[a5])=='true':
                        q=1
                        break
        if q==0:
            for i3 in I3:
                a0=i3[0]
                a1=i3[1]
                a2=i3[2]
                if coll(s[a0],s[a1],s[a2])=='true':
                        q=1
                        break
        b=b+q
        return b
```

The input are $\boldsymbol{k}$*, the length of the target* n*-tuple we want to check general position of,* $\boldsymbol{s}$ *that is the* n*-tuple itself and, even if it's not an input of the function itself,* $\boldsymbol{b}$*, that starts as* 0*. The output we get is the value* $\boldsymbol{b}$*, either increased by* 1 *if* v *contains points not in general position or equal to before if it doesn't. This is the last algorithm that we'll only use nested. To check this we are taking all possible sub* 3*-tuples of elements, as got by* $I3$*, and checking if these* 3 *points are not collinear, using* $I6$ *to check if the* $6-$*tuples of points are non on the same conics and* $I8$ *to check if the* $8-$*tuples are not a singular cubic.*

Counting n-tuple in general position

```
def Count(S,k):
    global b
    b=0
    for s in Subsets(S,k):
          check(s,k)
    g=t-b
    print('There are ', g , ' unordered', \\
    \\ k ,'-tuples in general position')
    print('There are ', g*factorial(k) , ' ordered', \\
    \\ k,'-tuples in general position')
```

This is the final function, its inputs are $\boldsymbol{S}$*=*$P2$ *and* $\boldsymbol{k}$ *the length of the target vector. The output is* $\boldsymbol{g}$*: the number of general* n*-tuples of* $\mathbb{P}^2_{\overline{F}_q}$ *satisfying the starting requirements. To do so we are taking every* $n-$*tuples are putting it as input of check.*

Comments 8.5.1
if $\boldsymbol{z==A}$*<—if* z *is equal to* A*.*

global $\boldsymbol{t}$*<—tells the algorithm to take* t *not as a local variable but as the global variable we defined previously.*

break*<—interrupts the for cycle and forces sage to go to the operation after it.*

import itertools*<—-imports the library itertools that contains functions we need to use.*

The double dash *indicates a linebreak that has to be removed in the actual sage code.*

Counting n-tuples in finite fields faster

Algorithm 8.6
The above algorithm indeed works but has to downside of requiring to go through roughly q^{n*k} k-tuples. We can however take advantage of what we said in subsection 5.4 to bring this down to $q^{n*(k-4)}$. We only need to modify slightly two sub-algorithms and add another one:

Counting all the n-tuples in $\mathbb{P}^2_{\mathbb{F}_q}$

```
t=1
def TOT(P,q,n,k):
   global t
   t=1
   y=q^n
   s=len(P)
   if k<4:
     t=binomial(s,k)*factorial(k)
   else:
     t=binomial(s,k-4)
     t=t*(y^2+y+1)*(y^3-y)*(y^3-y^2)*factorial(k-4)
     return t
```

*This takes as input a set **P** and **k** that is the length of the vectors and returns the number of all n-tuples of **P** of the given length, starting with the the 4 special points, in general position.*

Fusing two vectors into one

```
def fuse(s,t):
    global sn
    sn=[]
    for v in s:
        sn.append(v)
    for v in t:
        sn.append(v)
    return sn
```

This takes as input a vector $\boldsymbol{s}$ *and gives as output a vector that starts with* $(1,0,0)$, $(0,1,0)$, $(0,0,1)$, $(1,1,1)$ *and end with* s *itself.*

Counting n-tuple in general position

```
sn=[]
def Count(S,q,n,k):
    global b
    b=0
    y=q^n
    v=[(1,0,0),(0,1,0),(0,0,1),(1,1,1)]
    if k<4:
      for s in Subsets(S,k):
          check(s,k)
      l=b*factorial(k)
    else:
      for r in Subsets(S,k-4):
          check(fuse(v,r),k)
      l=b*(y^2+y+1)*(y^3-y)*(y^3-y^2)*factorial(k-4)
    g=t-l
    print('There are ', g/factorial(k) , ' unordered',\\
    \\ k,'-tuples in general position')
    print('There are ', g , ' ordered', \\
    \\ k ,'-tuples in general position')
```

This is the final function, its inputs are $\boldsymbol{S}$*=P2, the values* $\boldsymbol{q,n}$ *defining the base field and* $\boldsymbol{k}$ *the length of the target vector. The output are the numbers of general* n*-tuples of* $\mathbb{P}^2_{\overline{F}_q}$ *satisfying the starting requirements, both ordered and unordered. The speed up is obtained by only checking* $n-$*tuples starting with the* 4 *special points and then multiplying the result by* $|PGL(3)|$.

Counting n-tuples in finite fields even faster

Algorithm 8.7
With a bit of work we can improve the algorithm even more by trying to avoid doing the same computation several times, e.g. currently for every step we are checking that $(1,0,0)$, $(0,0,1)$, $(0,1,1)$ *are not collinear, or we are including the* 4 *special point into the set of ones we can chose an additional* $(k-4)$*-tuple from, by removing this redundancy we are reducing by a good*

amount the number of n-tuples to check. We can moreover add a counter for general linear and linear+conic position.

Building the sets of 3-tuples and 6-tuples of indices

```
I2R=[]
I2S=[]
I3=[]
I3R=[]
I6=[]
I8=[]
def IG(k):
  global I2S
  global I2R
  global I3
  global I3R
  global I6
  global I8
  I2R=[]
  I2S=[]
  I3=[]
  I3R=[]
  I6=[]
  I8=[]
  I=[]
  IS=[]
  IR=[]
  for f1 in range(k):
              I.append(f1)
  for g3 in Subsets(I,3):
     I3.append(g3)
  if k>4:
     for f2 in range(4):
               IS.append(f2)
     for f3 in range(k-4):
               IR.append(f3+4)
     for g2s in Subsets(IS,2):
               I2S.append(g2s)
     for g2r in Subsets(IR,2):
```

```
                I2R.append(g2r)
    for g3r in Subsets(IR,3):
                I3R.append(g3r)
    for a in range(4):
        A=[a]
        for b in I2R:
           I3R.append(fuse(A,b))
  if k>5:
    for g6 in Subsets(I,6):
       I6.append(g6)
  if k>6:
    for g7 in Subsets(I,7):
       I6.append(g7)
  if k>7:
    for y in Subsets(I,8):
       I8.append(y)
```

This takes as input simply a set $\boldsymbol{P}$ *and the target length* $\boldsymbol{k}$ *of the* k*-tuple. The output are sets of indices in* $(0,..,k-1)$ *with the special properties, when used in check to allow us to avoid considering result we already know, for example given that the vector* v *starts as* $[(1,0,0),(0,1,0),(0,0,1),(1,1,1)...]$ *we don't want the set of sub* $3-$*tuples to contain* $(0,1,2)$ *given that we already know the first* 3 *components are in general position.*

Checking if a special 5-tuple is in general position

```
b1=0
def check1(s,a):
        global b1
        q1=0
        for i2 in I2S:
                a0=i2[0]
                a1=i2[1]
                if coll(s[a0],s[a1],a)=='true':
                        q1=1
                        break
        b1=b1+q1
        return b1
```

The inputs are $\boldsymbol{s}$*, the* 4*-tuple of points in the special position and* $\boldsymbol{a}$*, and*

element we want to check if it's in general position regarding to the first 4*, even if it's not an input of the function itself,* ***b1, b2, b3****, that start as* 0*. The output we get is the value* ***b1****, either increased by* 1 *if* v *contains points not in general position or equal to before if it doesn't. This will be used to greatly reduce the number of computations to make, by being sure that no single point can be collinear with* 2 *of the special points we are cutting down on the sub* $n-$*tuples to check.*

Checking if an n-tuple is in general position

```
b1=0
b2=0
b3=0
def check2(s,k):
        global b1
        global b2
        global b3
        q1=0
        q2=0
        q3=0
        for i3 in I3R:
                a0=i3[0]
                a1=i3[1]
                a2=i3[2]
                if coll(s[a0],s[a1],s[a2])=='true':
                        q1=1
                        q2=1
                        q3=1
                        break
        if q2==0:
          if k>5:
            for i6 in I6:
                a0=i6[0]
                a1=i6[1]
                a2=i6[2]
                a3=i6[3]
                a4=i6[4]
                a5=i6[5]
                if conic(s[a0],s[a1],s[a2],\\
```

```
                \\ s[a3],s[a4],s[a5])=='true':
                        q2=1
                        q3=1
                        break
        if q3==0:
         if k>7:
          for i8 in I8:
            a0=i8[0]
            a1=i8[1]
            a2=i8[2]
            a3=i8[3]
            a4=i8[4]
            a5=i8[5]
            a6=i8[6]
            a7=i8[7]
            if SIcubic(s[a0],s[a1],s[a2],s[a3],\\
            \\ s[a4],s[a5],s[a6],s[a7])=='true':
                 q3=1
                 break
        b1=b1+q1
        b2=b2+q2
        b3=b3+q3
        return b1
        return b2
        return b3
```

The inputs are ***s****, an £*n*£-tuple of points we want to check are in general position and* ***k*** *the length of such* n*-tuple and, even if it's not an input of the function itself,* ***b1, b2, b3****, that start as* 0*. The output we get is the value* ***b1****, either increased by* 1 *if* v *contains points not in general position or equal to before if it doesn't. This only works if we know that any point that is not one of the first* 4 *is in general position regarding the first* 4*.*

Counting n-tuple in general position

```
sn=[]
def Count(S,q,n,k):
    IG(k)
    global b1
```

```
global b2
global b3
l1=0
l2=0
l3=0
y=q^n
s=len(S)
v=[(0,0,1),(0,1,0),(1,0,0),(1,1,1)]
V1=copy(S)
V1.remove((1,0,0))
V1.remove((0,1,0))
V1.remove((0,0,1))
V1.remove((1,1,1))
if k<4:
  b1=0
  for s in Subsets(S,k):
      check(s,k)
  l1=b1*factorial(k)
  l2=t
  l3=t
if k>4:
  V2=copy(V1)
  for r1 in V1:
      b1=0
      b2=0
      b3=0
      check1(v,r1)
      if b1==1:
         V2.remove(r1)
  s2=len(V2)
  l1=l1+binomial(s-4,k-4)-binomial(s2,k-4)
  l2=l2+binomial(s-4,k-4)-binomial(s2,k-4)
  l3=l3+binomial(s-4,k-4)-binomial(s2,k-4)
  b1=0
  b2=0
  b3=0
  for r2 in Subsets(V2,k-4):
         check2(fuse(v,r2),k)
  l1=l1+b1
  l2=l2+b2
  l3=l3+b3
```

```
      l1=l1*(y^2+y+1)*(y^3-y)*(y^3-y^2)*factorial(k-4)
      l2=l2*(y^2+y+1)*(y^3-y)*(y^3-y^2)*factorial(k-4)
      l3=l3*(y^2+y+1)*(y^3-y)*(y^3-y^2)*factorial(k-4)
    g1=t-l1
    g2=t-l2
    g3=t-l3
    print('There are ', g1/factorial(k) , ' unordered',\\
    \\ k,'-tuples in general linear position')
    print('There are ', g1 , ' ordered',\\
    \\ k ,'-tuples in general linear position')
    print('There are ', g2/factorial(k) , ' unordered',\\
    \\ k,'-tuples in general linear and conic position')
    print('There are ', g2 , ' ordered', \\
    \\ k ,'-tuples in general linear and conic position')
    print('There are ', g3/factorial(k) , ' unordered', \\
    \\ k,'-tuples in general position')
    print('There are ', g3 , ' ordered',\\
    \\ k ,'-tuples in general position')
```

This is the final function, its inputs are $\boldsymbol{S}$*=P2, the values* $\boldsymbol{q,n}$ *defining the base field and* $\boldsymbol{k}$ *the length of the target vector. The output are the numbers of general* n*-tuples of* $\mathbb{P}^2_{\overline{F}_q}$ *satisfying the starting requirements, . So this counts* n*-tuples in linear, linear+conic and linear+conic+cubic general position both ordered and unordered. In here we first remove points not in general linear position with the* 4 *special ones thanks to check*1*, count the how many* $n-$*tuples contain these, and then check general position on the other using the faster check*2

Compact form

```
def Active(q,n,k):
            P2=[]
            P_2(q,n,P2)
            TOT(P2,q,n,k)
            Count(P2,q,n,k)
```

The above function is simply a compact way to do computations, taking as inputs $\boldsymbol{q,n}$ *defining the base field and* $\boldsymbol{k}$ *defining the* k*-tuple.*

Parallel computing for counting n-tuples

Algorithm 8.8
The problem of counting n-tuples seems to have a computational complexity around $k^1 1$ where k is the dimension of the base field. Therefore to compute the case of $k = 23$ the standard method would require roughly 3 months. To solve this the best choice is to parallelize the computation: if we split them into n computers we cut the time by roughly n. In the specific case $n = 7$ was chosen.

When doing this is important to put the set $P2$ in the code we import on Sage or anyway check that this is the same for all the computers we are using. This because it's not clear how Sage deals with ordering and creating a set and therefore we may end up doing the computations on some points several times and skip others.

The only algorithms to change are Count and Active.

Counting n-tuple in general position

```
sn=[]
def PCount(S,q,n,k,p):
    IG(k)
    global b1
    global b2
    global b3
    l1=0
    l2=0
    l3=0
    y=q^n
    s=len(S)
    v=[(0,0,1),(0,1,0),(1,0,0),(1,1,1)]
    V1=copy(S)
    V1.remove((1,0,0))
    V1.remove((0,1,0))
    V1.remove((0,0,1))
    V1.remove((1,1,1))
    if k<4:
      b1=0
      for s in Subsets(S,k):
          check(s,k)
```

```
  l1=b1*factorial(k)
  l2=t
  l3=t
if k>4:
  V2=copy(V1)
  for r1 in V1:
      b1=0
      b2=0
      b3=0
      check1(v,r1)
      if b1==1:
         V2.remove(r1)
  s2=len(V2)
  l1=l1+binomial(s-4,k-4)-binomial(s2,k-4)
  l2=l2+binomial(s-4,k-4)-binomial(s2,k-4)
  l3=l3+binomial(s-4,k-4)-binomial(s2,k-4)
  b1=0
  b2=0
  b3=0
  d=ceil(s2/7)
  V3=[]
  for i in range(d*(p-1),min(d*p,s2)):
      V3.append(V2[i])
  for r2 in Subsets(V2,k-4):
        if r2[0] in V3:
           check2(fuse(v,r2),k)
  b1=b1*(y^2+y+1)*(y^3-y)*(y^3-y^2)*factorial(k-4)
  b2=b2*(y^2+y+1)*(y^3-y)*(y^3-y^2)*factorial(k-4)
  b3=b3*(y^2+y+1)*(y^3-y)*(y^3-y^2)*factorial(k-4)
  l1=l1*(y^2+y+1)*(y^3-y)*(y^3-y^2)*factorial(k-4)
  l2=l2*(y^2+y+1)*(y^3-y)*(y^3-y^2)*factorial(k-4)
  l3=l3*(y^2+y+1)*(y^3-y)*(y^3-y^2)*factorial(k-4)
print('b1=',b1,'b2=',b2,'b3=',b3 )
print('initial l1,l2,l3=',l1)
```

In the above we split $Subset(V2, k-4)$ *in 7 pieces,* $\boldsymbol{p}$ *denotes what piece we are computing and goes from* 1 *to* 7*. On each of the* 7 *parallel instances of sage we compute a different* p*. The outputs are the initial* $l1$ *(that is equal to* $l2$ *and* $l3$*), that is the difference between the number of subsets of dimension* 4 *of* $V1$ *and* $V2$*, and some partial* $b1, b2, b3$*. To get the final result we have simply to do* $t - (ln + \sum_{i=1}^{7} b_{n,i})$ *for* $n = 1, 2, 3$ *to get, respectively, how many*

points are in linear, linear+conic and general position.

This version of count only checks a given fraction of the set of n-tuples, in this particular version one seventh, and ignores the others.

Compact form

```
def PActive(P2,q,n,k,p):
            TOT(P2,q,n,k)
            PCount(P2,q,n,k,p)
```

Obtaining and checking the final polynomial

Algorithm 8.9
The problem of computing and checking the final polynomial once we have the points is not a complicated one but given that some code has been written it has to be reported too.

Reducing the variables from 9 to 6

```
def Mspit(v,w,s,n,m):
for p in range(len(v)):
    w1=w[p]-v[p]^8+n*v[p]^7-m*v[p]^6
    s.append(w1)
```

This takes as inputs two vectors $\boldsymbol{v}$ *is the vector of points on which we apply the function (the "*x*") and* $\boldsymbol{w}$ *is the vector of results (the "*y*"), a target set* $\boldsymbol{s}$ *and numbers* $\boldsymbol{n,m}$*. The output is the set* s *whose elements are the ones of* w *on which we applied some calculations, in particular these allow us to interpolate an* 8*th degree polynomial through only* 6 *points, by fixing the coefficients for* x^8*,* x^7 *and* x^6*.*

Interpolating a polynomial

```
def inter(v,w):
   RR=[]
   for p in range(len(v)):
```

```
        RR.append((v[p],w[p]))
    f1 = R.lagrange_polynomial(RR)
    return(f1)
```

This takes as inputs two vectors $\boldsymbol{v}$ *is the vector of points on which we apply the function (the "x") and* $\boldsymbol{w}$ *is the vector of results (the "y"). The output is the polynomial of the lowest degree passing through the points.*

Checking if a given number can be obtained as sum of elements in subsets of a set

Algorithm 8.10
To make a very educated guess on the coefficient of x^6 *in the polynomial describing the number of* $8-$*tuples in general position we need to check if given candidate coefficients can be obtained as the sums of the elements of some subsets of a given set.*

```
def sums(S,n):
    for a in Subsets(S):
        c=0
        for b in a:
           c=c+b
        if c==n:
           print(a)
           break
```

This takes as input a set of numbers $\boldsymbol{S}$ *and a target number* $\boldsymbol{n}$ *and gives as output the first subset of* S *whose sum is equal to* n *if it exits. To do so it simply takes any subset and checks what the sum of the elements in it is.*

8.2 Some results of fields of characteristic $2, 3$

With regards to characteristic 2 we can look into section 4 of [1] to find some interesting difference in behaviour with other characteristics:

Proposition 8.2.1 ([1] ,4.1)
Let k be a field. Any Del Pezzo surface S of degree 2 over k can be written in the form

$$w^2 + f_2(x, y, z) * w = f_4(x, y, z) \subset \mathbb{P}(1, 1, 1, 2) \quad deg\ f_i = i$$

(as we already partially proved in 3.3), where w is the variable with weight 2.

The anticanonical map $\pi : S \to \mathbb{P}^2$ is given by $[x : y : z : w] \to [x : y : z]$ and realises S as a double cover of $\mathbb{P}^2$. The behaviour in characteristic 2 is slightly different as shown in [7]. The morphism is separable for any characteristic.

For char k$\neq$ 2 we can choose the equations such that $f_2(x, y, z) = 0$. If we do so the double cover is ramified over the smooth quartic curve $B : f_4(x, y, z) = 0$. If char $k = 2$ the branch curve B is the plane conic $f_2(x, y, z) = 0$ that can be reducible or non-reduced.

In both cases we define the ramification curve to be $R = \pi^{-1}(B)_{red}$ i.e. the reduced subscheme underlying $\pi^{-1}(B)$.

Lemma 8.2.2 ([1] , Lemma 4.1)
Let S be a Del Pezzo surface of degree 2 over an algebraically closed field (as the closure of a finite field) k with ramification curve R.

- *If char $k \neq 2$ then R is irreducible smooth and of genus 3;*
- *If char $k = 2$ then R has at most 2 irreducible components, and each of these has genus 0.*

Proof. If char k$\neq$ 2 then the result is clear, as $R \simeq B$ is a smooth plane quartic.

Let now char $k = 2$. Here $\pi^{-1}(B)$ has the equation

$$\pi^{-1}(B) : f_2(x, y, z) = 0 \quad w^2 = f_4(x, y, z) \subset S$$

it is now enough to consider the different possibilities for B:

1. If B is a smooth plane conic $R = \pi^{-1}(B)$ is irreducible and reduced, but may be singular. The morphism $R \to B$ is purely inseparable of degree 2, if we consider $N \to R$ as the normalization of R we have that $N \to B$ remains purely inseparable of degree 2 and so $g(N) = g(B)$ and thus $g(R) = 0$;

2. $B = L_1 \cup L_2$ gives us that each $R_i := \pi^{-1}(L_i)$ is irreducible and reduced and the map $R_i \to L_i$ purely inseparable of degree 2, as before we obtain that $g(R_i) = 0$:

3. $B = L^2$ a double line gives that $\pi^{-1}(B)$ is non-reduced, but $R \to L$ is still purely inseparable of degree 2 and again $g(R) = 0$.

□

One has to notice that the blowing up of 8 points can be obtained also by first blowing up 7 points (that in our case gives us a Del Pezzo surface of degree 2) and then blow up one point of this and so the fact that Del Pezzo surfaces of degree 2 behave in a different way for characteristic 2 reflects also for ones of degree 1.

Regarding characteristic 3 the difference in behaviour regards exceptional curves as stated in the following:

Proposition 8.2.3 (4.4.6 [17])
Let $R1, \ldots, R8$ *be* 8 *points in* $\mathbb{P}^2$ *in general position. We can define the following curves:*

- $L1$ *is the line through* $R1$ *and* $R2$*;*
- $L2$ *is the line through* $R3$ *and* $R4$*;*
- $C1$ *is the conic through* $R1$*,* $R3$*,* $R5$*,* $R6$ *and* $R7$*;*
- $C2$ *is the conic through* $R1$*,* $R4$*,* $R5$*,* $R6$ *and* $R8$*;*
- $C3$ *is the conic through* $R2$*,* $R3$*,* $R5$*,* $R7$ *and* $R8$*;*
- $C4$ *is the conic through* $R2$*,* $R4$*,* $R6$*,* $R7$ *and* $R8$*;*
- $D1$ *is the quartic through all eight points, singular in* $R1$*,* $R7$ *and* $R8$*;*
- $D2$ *is the quartic through all eight points, singular in* $R2$*,* $R5$ *and* $R6$*;*
- $D3$ *is the quartic through all eight points, singular in* $R3$*,* $R6$ *and* $R8$*;*

- *$D4$ is the quartic through all eight points, singular in $R4$, $R5$ and $R7$.*

Assume that the characteristic of k is not 3. Then the ten curves $L1, L2, C1, \ldots C4, D1, \ldots, D$ are not concurrent.

8.3 Computations for 3.4.5

We remind that we are looking for solutions to the system of equations

$$3a - \sum_{i=1}^{9} b_i = 0 \tag{8}$$

$$a\sum_{i=1}^{9}(a - 3b_i)^2 = 18. \tag{9}$$

$$b_9 = 1. \tag{10}$$

We can start with equation (9), which means looking for 9 perfect squares in $\mathbb{Z}$ whose sum is 18, we get the following possible solutions

16	1	1	0	0	0	0	0	0
9	9	0	0	0	0	0	0	0
9	4	4	1	0	0	0	0	0
9	4	1	1	1	1	1	0	0
4	4	4	4	1	1	0	0	0
4	4	4	1	1	1	1	1	1

Now we know that $b_9 = 1$ and so we have the following possibilities for a

$$(a - 3b_9) = 16 \iff a = -1, 7$$

$$(a - 3b_9) = 9 \iff a = 0, 6$$

$$(a - 3b_9) = 4 \iff a = 1, 5$$

$$(a - 3b_9) = 1 \iff a = 2, 4$$

$$(a - 3b_9) = 0 \iff a = 3.$$

We can similarly compile the following table that, starting from the fact that $a - 3b = c \iff 3b = a - c$ tells us if it's possible, starting from a given a,

to get certain values of c

	-4	-3	-2	-1	0	1	2	3	4
7	1	*NO*	*NO*	2	*NO*	*NO*	3	*NO*	*NO*
6	*NO*	1	*NO*	*NO*	2	*NO*	*NO*	3	*NO*
5	*NO*	*NO*	1	*NO*	*NO*	2	*NO*	*NO*	3
4	0	*NO*	*NO*	1	*NO*	*NO*	2	*NO*	*NO*
3	*NO*	0	*NO*	*NO*	1	*NO*	*NO*	2	*NO*
2	*NO*	*NO*	0	*NO*	*NO*	1	*NO*	*NO*	2
1	-1	*NO*	*NO*	0	*NO*	*NO*	1	*NO*	*NO*
0	*NO*	-1	*NO*	*NO*	0	*NO*	*NO*	1	*NO*
-1	*NO*	*NO*	-1	*NO*	*NO*	0	*NO*	*NO*	1

so a solution is possible if an only if, given a corresponding to a given perfect square all other perfect squares in the solution have a root that is possible in the above table.
This means that the solutions we have are exactly

a	b_1	b_2	b_3	b_4	b_5	b_6	b_7	b_8
0	-1	0	0	0	0	0	0	0
0	1	0	0	0	0	0	0	0
1	1	1	0	0	0	0	0	0
2	0	0	0	1	1	1	1	1
3	0	0	1	1	1	1	1	1
3	2	2	1	1	1	1	1	1
3	2	0	1	1	1	1	1	1
4	2	2	2	1	1	1	1	1
5	1	1	2	2	2	2	2	2
6	1	2	2	2	2	2	2	2
6	3	2	2	2	2	2	2	2

We can now check if $3a = 1 + \sum_{i=1}^{8} b_i$ and this forces us to exclude the following 9-tuples:

$$(0,1,0,0,0,0,0,0,0),\ (3,0,0,1,1,1,1,1,1),$$

$$(3,2,2,1,1,1,1,1,1),\ (6,1,2,2,2,2,2,2,2)$$

and so we get indeed that the solutions are, up to permutation of b_i

a	b_1	b_2	b_3	b_4	b_5	b_6	b_7	b_8
0	-1	0	0	0	0	0	0	0
1	1	1	0	0	0	0	0	0
2	1	1	1	1	1	0	0	0
3	2	1	1	1	1	1	1	0
4	2	2	2	1	1	1	1	1
5	2	2	2	2	2	2	1	1
6	3	2	2	2	2	2	2	2

References

[1] Daniel Loughran Barinder Banwait, Francesc Fitè. Del pezzo surfaces over finite fields and their frobenius traces. *Mathematical Proceedings of the Cambridge Philosophical society*, 2019(167):35–60, 2019.

[2] Olof Bergvall. Cohomology of complements of toric arrangements associated to root systems, 2020.

[3] Olof Bergvall. Equivariant cohomology of the moduli space of genus three curves with symplectic level two structure via point counts. *European Journal of Mathematics*, 6(6):262–320, 2020.

[4] Olof Bergvall. On the cohomology of the space of seven points in general linear position. *Research in number theory*, 2020(6):Article 48, 2020.

[5] Olof Bergvall and Frank Gounelas. Cohomology of moduli spaces of del pezzo surfaces, 2019.

[6] Richard M. Foote David S. Dummit. *Abstract Algebra*. John Wilet and Sons, Inc., 2004.

[7] Igor V. Dolgachev Francois R. Cossec. *Enriques surfaces I*. Birkhauser, 76. Birkhauser Boston, Inc., Boston, MA, 1989.

[8] Andreas Garthmann. *Algebraic Geometry*. Online self publishing, https://www.mathematik.uni-kl.de/ gathmann/de/alggeom.php, 2019.

[9] Robin Hartshorne. *Algebraic Geometry*. Springer, 1977.

[10] George E. Schnibben Joel V. Brawley. *Infinite algebraic extensions of finite fields*. American mathematical society, 1989.

[11] Janos Kollar. *Rational curves on algebraic varieties*. Springer, 2001.

[12] Yuri Ivanovich Manin. *Cubic Forms, Algebra, Geomtry, Arithmetic*. Elsevier science publishers, 1986.

[13] Pasquale Del Pezzo. Sulle superficie di ordine n immerse nello spazio di n+1 dimensioni. *Rendiconto dell' Accademia delle Scienze Fisiche e Matematiche*, 1885(24):212–216, 1885.

[14] Pasquale Del Pezzo. Sulle superficie dell'n-mo ordine immerse nello spazio di n dimensioni. *Rendiconto del Circolo Matematico di Palermo*, 1887(1):241–271, 1887.

[15] Joe Harris Phillip Griffiths. *Principles of algebraic geometry*. Wiley, 1978.

[16] Robert J. Walker. *Algebraic Curves*. Princeton University Press, 1950.

[17] Rosa Linde Winter. Geometry and arithmetic of del pezzo surfaces of degree 1. *Doctoral thesis*, 2021(2021):1–207, 2021.