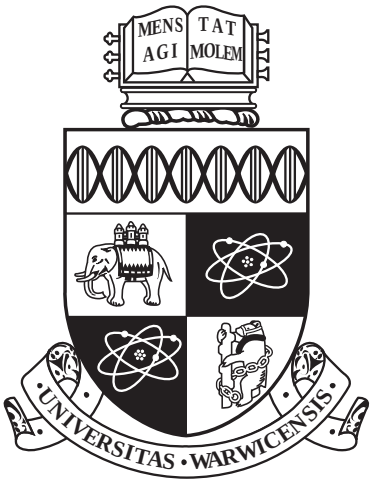

Cubic Surfaces over Finite Fields

by

Jenny Anne Cooley

Thesis

Submitted to the University of Warwick

for the degree of

Doctor of Philosophy

Warwick Mathematics Institute

June 2014

THE UNIVERSITY OF
WARWICK

Contents

Acknowledgments

Many people have helped me complete this PhD. The first I would like to mention are my family. From forwarding mail and making furniture to pep talks and wake-up calls, they have been there for me all the way. A weekend at home complete with Sunday roast never failed to refresh me and leave me morally prepared for the weeks to come. In particular I would like to thank my parents Roy and Anne for encouraging my love for mathematics and learning in general from a very young age. My good friends Chris Cherng, Bec Drysdale, Nicky McConkey, Chris Pettitt, Nat Shiers and Colette Wood were there for lunches, dinners, days out and holidays. Anisha Patel is a constant source of inspiration to me, and I have often left our conversations reinvigorated about work and life in general! The University of Warwick Latin and Ballroom Dancesport Club and the University of Warwick Big Band both provided much appreciated hours of fun and distraction. I would also particularly like to thank Malik Refaat for breakfast dates, jazz breaks and being generally very supportive while I was writing my thesis.

Warwick Mathematics Institute is a fantastic work environment. This is in no small part due to the Head of Department Colin Sparrow and also Nav Patel, Carole Fisher, Hazel Graley, Rimi Singh and all the other brilliant support staff. The department has also been full of lots of wonderful number theorists! Samuele Anni, Florian Bouyer, Heline Deconinck, Stephanos Papanikolpoulos, Vandita Patel, Jeroen Sijsling, Damiano Testa and Chris Williams are all people with whom I have greatly enjoyed discussing mathematics, but are also good friends that have that have been the source of a lot of fun! Several academics and fellow students from other institutes have provided much inspiration, encouragement and food for

thought along the way. These include Manjul Bhargava, Julio Brau, Martin Bright, Dan Loughran, Dave Mendes da Costa, Rachel Newton, Sarah Zerbes and especially the mad and brilliant Efthymios Sofos!

I would also like to thank my PhD examiners Tim Dokchitser and Damiano Testa for a very enjoyable viva. The effort they both put into reading my thesis, and the interest they took in my work and how it could be taken further is very much appreciated.

My final and biggest thank you must go to my incredible supervisor Professor Samir Siksek. During the last four years Samir has taken on the roles of mentor, educator, colleague, food critic, comedian, political commentator, personal trainer, travel agent, counsellor, clown and purveyor of fine chocolates! He was always ready for a chat or to give a hand explaining a difficult concept and our meetings were a perfect mix of two thirds maths, one third jokes. I am very grateful for the care he has taken over guiding my studies and the belief he has shown in me.

A huge thank you to all of you; I could not have done it without you.

Declarations

Chapter 1 covers material that is known and found elsewhere in the literature, though the examples given in that chapter are my own. Chapters 2, 3, 4, 5 and 6 are my own work unless otherwise stated. The material in Chapter 2 has appeared in an article in Archiv der Mathematik [6]. The material in Chapter 3 forms the basis of a preprint [7] on the `ArXiv`.

Abstract

It is well-known that the set of rational points on an elliptic curve forms an abelian group. When the curve is given as a plane cubic in Weierstrass form the group operation is defined via tangent and secant operations. Let S be a smooth cubic surface over a field K. Again one can define tangent and secant operations on S. These do not give $S(K)$ a group structure, but one can still ask for the size of a minimal generating set.

In Chapter 2 of the thesis I show that if S is a smooth cubic surface over a field K with at least 4 elements, and if S contains a skew pair of lines defined over K, then any non-Eckardt K-point on either line generates $S(K)$. This strengthens a result of Siksek [20].

In Chapter 3, I show that if S is a smooth cubic surface over a finite field $K = \mathbb{F}_q$ with at least 8 elements, and if S contains at least one K-line, then there is some point $P \in S(K)$ that generates $S(K)$.

In Chapter 4, I consider cubic surfaces S over finite fields $K = \mathbb{F}_q$ that contain no K-lines. I find a lower bound for the proportion of points generated when starting with a non-Eckardt point $P \in S(K)$ and show that this lower bound tends to $\frac{1}{6}$ as q tends to infinity.

In Chapter 5, I define c-invariants of cubic surfaces over a finite field $K = \mathbb{F}_q$ with respect to a given K-line contained in S, give several results regarding these c-invariants and relate them to the number of points $|S(K)|$.

In Chapter 6, I consider the problem of enumerating cubic surfaces over a finite field, $K = \mathbb{F}_q$, with a given point, $P \in S(K)$, up to an explicit equivalence

relation.

Chapter 1

Introduction

In this chapter we will state some well-known and useful results before giving an outline of the rest of the thesis.

1.1 Plane curves

The definitions and results in this section can be found in Silverman's book *The arithmetic of elliptic curves* [21], or are specialisations of such.

A *plane curve* over a field K in an affine plane $\mathbb{A}^2_K$ is the locus of points of a nonzero, non-constant polynomial $f \in K[x, y]$. A plane curve over K in a projective plane $\mathbb{P}^2_K$ is the locus of points of a nonzero, non-constant homogeneous polynomial $F \in K[X, Y, Z]$. A plane curve in $\mathbb{A}^2_K$ defined by $f(x, y) = 0$ may be completed in $\mathbb{P}^2_K$ to become the curve defined by $Z^d f(\frac{X}{Z}, \frac{Y}{Z}) = 0$ where d is the degree of f.

We denote the algebraic closure of K by $\overline{K}$. Let $C : f(x, y) = 0$ be a plane curve defined over a field K in $\mathbb{A}^2_K$. A point $P \in C(\overline{K})$ is *singular* if and only if

$$\frac{\partial f}{\partial x}(P) = \frac{\partial f}{\partial y}(P) = 0.$$

Likewise, for a projective plane curve $C : F(X, Y, Z) = 0$, $P \in C(\overline{K})$ is singular if and only if

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

A curve C is *smooth* or *non-singular* if it is non-singular at all $P \in C(\overline{K})$.

Lemma 1.1. Let C be a plane curve over K in $\mathbb{A}^2_K$ defined by $f(x, y) = 0$. The point $P = (0, 0)$ is on the curve and singular if and only if the linear and constant terms of f are zero.

Proof. Note that we can write f as follows

$$f(x,y) = a + b_1x + b_2y + \ldots (\text{higher order terms}),$$

where $a, b_1, b_2 \in K$. Therefore

$$\frac{\partial f}{\partial x}(0,0) = b_1, \ \frac{\partial f}{\partial y}(0,0) = b_2.$$

Recall that C is singular at P if and only if $\frac{\partial f}{\partial x}(P) = \frac{\partial f}{\partial y}(P) = 0$. Therefore C is singular at $(0,0)$ if and only if $b_1 = b_2 = 0$. □

The next theorem, which can be found in [10, Chapter 1], concerns intersections between plane curves. First we make a definition and set some notation. Let C and D be two projective plane curves defined over a field K. The *intersection multiplicity* of C and D at a point $P \in \mathbb{P}^2_K$, denoted by $(C \cdot D)_P$, is defined as follows:

- $(C \cdot D)_P := \infty$ if P lies on a common component of C and D.
- $(C \cdot D)_P := 0$ if $P \notin C \cap D$.
- $(C \cdot D)_P := k$ if $P \in C \cap D$ but P does not lie on a common component of C and D. We may compute k in the following way. Remove any common components from C and D to obtain the curves C' and D' respectively. Choose projective coordinates such that the point $[1:0:0]$ does not lie on $C' \cup D'$, nor on any line joining distinct points of $C' \cup D'$, nor on any line tangent to C' or D' at a point in $C' \cap D'$. We denote by F and G the defining polynomials of C' and D' respectively. Then for $P = [a:b:c]$ we define k to be the largest integer such that $(bZ - cY)^k$ divides the resultant of F and G, $\mathrm{Res}_{F,G}(Y,Z)$ [12].

In particular, the intersection multiplicity of a plane curve C and a line ℓ at a point $P \in C \cap \ell$ will be $(C \cdot \ell)_P = 1$ if ℓ cuts C at P and ℓ does not lie tangent to C at P, and $(C \cdot \ell)_P \geq 2$ if ℓ lies tangent to C at P. Further, if $C \cap D = \{P_1, \ldots, P_s\}$, we write $C \cdot D = n_1P_1 + \cdots + n_sP_s$ where $n_i = (C \cdot D)_{P_i}$.

Theorem 1.2 (Bézout's Theorem)**.** *Let C and D be distinct projective plane curves of degrees d and e respectively and having no common components. Let $C \cap D = \{P_1, \ldots, P_s\}$. Then*

$$\sum_{i=1}^{s} (C \cdot D)_{P_i} = de.$$

1.1.1 Elliptic Curves

One possible definition of an *elliptic curve* is a smooth plane curve defined over a field K in $\mathbb{P}^2_K$ defined by a homogeneous cubic polynomial $F(X,Y,Z) = 0$ with a choice of rational point $\mathcal{O}$. It is always possible to transform this into a non-singular Weierstrass equation

$$YZ^2 + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3,$$

where $\mathcal{O}$ becomes the point at infinity $(0:1:0)$ [21].

Let E be an elliptic curve defined over a field K in $\mathbb{P}^2_K$ given by a Weierstrass equation. By Bézout's Theorem (Theorem 1.2) any line in $\mathbb{P}^2_K$ intersects E exactly three times counting multiplicities, thus we can define the following binary operation on the points of E. Let $P, Q \in E(\overline{K})$ be two distinct points and m the line joining P and Q. Then $m \cdot E = P + Q + R$ with $R \in E(\overline{K})$. We define the *secant operation* to be $P * Q = R$. Let $P \in E(\overline{K})$ and let m be the tangent line to E at P. Then $m \cdot E = 2P + R$. We define the *tangent operation* to be $P * P = R$. These two operations together form a commutative binary operation on $E(\overline{K})$, which is closed on $E(L)$ for L a subfield of $\overline{K}$ that contains K.

This operation can be made into an Abelian group operation as follows. Let $\mathcal{O} = (0:1:0)$ and for a point $P \in E(\overline{K})$ we define the inverse element of P to be $-P = P * \mathcal{O}$. Therefore the abelian group operation on $E(\overline{K})$ along with identity element $\mathcal{O} \in E(\overline{K})$ is $(P, Q) \mapsto (P * Q) * \mathcal{O}$.

The following three results can be found in Cohen's book *A course in Computational Algebraic Number Theory* [5, Chapter 7]. The first gives us information on the group of rational points of an elliptic curve defined over $\mathbb{Q}$.

Theorem 1.3 (The Mordell-Weil Theorem)**.** *Let E be an elliptic curve over $\mathbb{Q}$. Then $E(\mathbb{Q})$ is a finitely generated Abelian group. In other words,*

$$E(\mathbb{Q}) \simeq E(\mathbb{Q})_{\text{tors}} \oplus \mathbb{Z}^r,$$

where r is a non-negative integer called the rank *of the curve and $E(\mathbb{Q})_{\text{tors}}$ is the torsion subgroup of $E(\mathbb{Q})$, which is a finite Abelian group.*

The second gives a precise statement of the possibilities for the torsion subgroup of an elliptic curve defined over $\mathbb{Q}$.

Theorem 1.4 (Mazur)**.** *Let E be an elliptic curve over $\mathbb{Q}$. The torsion subgroup $E(\mathbb{Q})_{\text{tors}}$ of E can be isomorphic only to one of the* 15 *following groups:*

$$\begin{array}{ll} \mathbb{Z}/m\mathbb{Z} & \text{for } 1 \le m \le 10 \text{ or } m = 12, \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z} & \text{for } 1 \le m \le 4 \end{array}$$

In particular, its cardinality is at most 16.

The third result concerns the structure of $E(K)$ for E an elliptic curve defined over a finite field $K = \mathbb{F}_q$.

Proposition 1.5. *If E is an elliptic curve over a field $\mathbb{F}_q$, then $E(\mathbb{F}_q)$ is either cyclic or isomorphic to a product of two cyclic groups. Furthermore, in the case where it is not cyclic, if we write $E(\mathbb{F}_q) \simeq \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z}$ with $d_1|d_2$, then $d_1|q-1$.*

So, for an elliptic curve E defined over a field K, the size of a minimal generating set of points for $E(K)$ is 1 or 2 if K is a finite field and r, $r+1$ or $r+2$ if $K = \mathbb{Q}$.

The following theorem gives bounds on the number of rational points of an elliptic curve defined over a finite field [21, Chapter V]. It is a special case of the Hasse-Weil bound.

Theorem 1.6 (Hasse)**.** *Let E be an elliptic curve defined over $\mathbb{F}_q$. Then*

$$|\#E(\mathbb{F}_q) - q - 1| \le 2\sqrt{q}.$$

This thesis is concerned with generalisations of some of these concepts and theorems to cubic surfaces.

1.2 Cubic surfaces

A *cubic surface* over a field K is a variety in $\mathbb{P}^3_K$ defined by a homogeneous cubic polynomial $F \in K[X,Y,Z,W]$. Let S be a cubic surface defined over a field K in $\mathbb{P}^3_K$. A point $P \in S(\overline{K})$ is *singular* if and only if

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

A cubic surface S is said to be *smooth* if it is non-singular at all $P \in S(\overline{K})$.

Theorem 1.7. (Cayley-Salmon) *Every non-singular cubic surface over an algebraically closed field contains exactly* 27 *lines.*

Every line ℓ on the surface meets exactly 10 *other lines, which break up into* 5 *pairs ℓ_i, ℓ_i' ($i = 1,\dots,5$) such that ℓ, ℓ_i and ℓ_i' are coplanar, and $(\ell_i \cup \ell_i') \cap (\ell_j \cup \ell_j') = \varnothing$ for $i \neq j$.*

Proof. For a proof see [10, V.4] or [19, Section IV.2]. □

Example 1.8. A cubic surface over $\mathbb{Q}$ defined by

$$XQ_1(X,Y,Z,W) + YQ_2(X,Y,Z,W) = 0,$$

where Q_1 and Q_2 are homogeneous quadratic polynomials, contains the line $X = Y = 0$.

Let S be a smooth cubic surface in $\mathbb{P}^3$ over a field K, defined by a homogeneous cubic polynomial $F \in K[X,Y,Z,W]$. Throughout this thesis, for a point $P \in S(\overline{K})$, we shall denote the tangent plane to S at P by Π_P. This is given by $\Pi_P : (\nabla F)(P) \cdot \underline{\mathbf{x}} = 0$, where $\underline{\mathbf{x}} = (X : Y : Z : W)$. We shall write Γ_P for the plane curve $S \cdot \Pi_P$.

Example 1.9. A cubic surface defined by

$$S : F(X,Y,Z,W) = XW^2 + Q(X,Y,Z)W + C(X,Y,Z) = 0,$$

where Q is a homogeneous quadratic polynomial and C is a homogeneous cubic polynomial, contains the point $P = (0:0:0:1)$. We compute

$$(\nabla F)(P) \cdot \underline{\mathbf{x}} = X,$$

which shows that Π_P is the plane $X = 0$. Conversely, suppose the tangent plane at $P = (0:0:0:1)$ is $\Pi_P : X = 0$. Then S is given by

$$S : F'(X,Y,Z,W) = L'(X,Y,Z)W^2 + Q'(X,Y,Z)W + C'(X,Y,Z) = 0,$$

where L', Q' and C' are homogeneous linear, quadratic and cubic polynomials respectively. We know that $\Pi_P : (\nabla F')(P) \cdot \underline{\mathbf{x}} = L'(X,Y,Z) = 0$ so $L'(X,Y,Z)$ must be a multiple of X. Scaling F' we obtain

$$S : XW^2 + Q''(X,Y,Z)W + C''(X,Y,Z) = 0,$$

with Q'' a homogeneous quadratic polynomial and C'' a homogeneous cubic polynomial. This example will prove useful because any cubic surface S' defined over K and containing a smooth K-point P' is isomorphic over K to a surface of this form.

Lemma 1.10. *Let S be a smooth cubic surface defined over a field K and $P \in S(\overline{K})$. Then the cubic curve Γ_P does not contain any multiple components.*

Proof. Since the degree of Γ_P is 3, if there is a multiple component it must be a line. Suppose that this is the case and Π_P contains the line ℓ as a multiple component. By applying a suitable projective linear transformation we can take Π_P to $X = 0$ and ℓ to $X = Y = 0$. Then the equation of S must be of the form

$$S : F = XQ(X, Y, Z, W) + Y^2 L(X, Y, Z, W) = 0,$$

where Q is a homogeneous quadratic polynomial and L is a homogeneous linear polynomial. Let $P' \in S(\overline{K})$ satisfy $X = Y = Q(X, Y, Z, W) = 0$. This is a singular point because

$$\begin{aligned}
\frac{\partial F}{\partial X} &= Q + X\frac{\partial Q}{\partial X} + Y^2\frac{\partial L}{\partial X} \\
\frac{\partial F}{\partial Y} &= X\frac{\partial Q}{\partial Y} + 2YL + Y^2\frac{\partial L}{\partial Y} \\
\frac{\partial F}{\partial Z} &= X\frac{\partial Q}{\partial Z} + Y^2\frac{\partial L}{\partial Z} \\
\frac{\partial F}{\partial Z} &= X\frac{\partial Q}{\partial W} + Y^2\frac{\partial L}{\partial W}
\end{aligned}$$

all vanish when $X = Y = Q(X, Y, Z, W) = 0$. This contradicts the smoothness of S, and so Γ_P cannot contain a multiple component. □

Lemma 1.11. *Let S be a smooth cubic surface over a field K defined by the equation $F(X, Y, Z, W) = 0$. Let $P \in S(\overline{K})$. Then Γ_P is a cubic curve with a singularity at P.*

Proof. By applying a suitable projective linear transformation we can take P to $(0 : 0 : 0 : 1)$ and Π_P to $X = 0$. Then, as in Example 1.9,

$$F = XW^2 + Q(X, Y, Z)W + C(X, Y, Z),$$

where Q and C are homogeneous quadratic and cubic polynomials respectively. We now have that $\Gamma_P = S \cdot \Pi_P$ is the curve in the plane $X = 0$ given by

$$Q(0, Y, Z)W + C(0, Y, Z) = 0.$$

We dehomogenise, setting $W = 1$ to obtain $P = (0, 0, 0)$ and $\Gamma_P : Q(0, y, z) + C(0, y, z) = 0$ in the affine plane $x = 0$. By Lemma 1.1, the point P is a singular point of Γ_P if and only if there are no linear terms in $Q(0, y, z) + C(0, y, z)$. But Q and C are homogeneous of degrees 2 and 3 respectively. Hence Γ_P is singular at P. □

Lemma 1.12. *Let S be a smooth cubic surface defined over a field K and let $P \in S(\overline{K})$. If Γ_P is absolutely irreducible, then P is the only singular point in $\Gamma_P(\overline{K})$.*

Proof. Suppose there is a second singular point on Γ_P, which we denote P', $P \neq P'$. Let ℓ be the line joining P and P'. The line ℓ intersects both P and P' with multiplicity at least 2, therefore $\ell \subset S$ and hence $\ell \subset \Gamma_P$. So Γ_P has a linear component. This is a contradiction with the irreducibility of Γ_P. □

The curve $\Gamma_P = \Pi_P \cdot S$ is a degree 3 plane curve that is singular at P. Therefore it is either nodal or cuspidal at P. If Γ_P is reducible then it is the union of a line and an irreducible conic, or of three distinct lines. Figures 1.1 to 1.9 illustrate the possibilities for Γ_P.

We follow [20] in classifying points. A $\overline{K}$-line ℓ is called an *asymptotic line* (c.f. [25, Section 2]) at $P \in S(\overline{K})$ if $(\ell \cdot S)_P \geq 3$, where $(\ell \cdot S)_P$ is the intersection multiplicity of ℓ and S at P. As S is a cubic surface, for an asymptotic line ℓ at P, either $(\ell \cdot S)_P = 3$ or $\ell \subset S$. The asymptotic lines at P are contained in Π_P.

Any line contained in S and passing through P is an asymptotic line through P. The number of distinct asymptotic $\overline{K}$-lines at P is either 1, 2 or infinite. If S has either one or infinitely many asymptotic lines at P then we shall call P a *parabolic* point.

If P is non-parabolic, then Γ_P has a node at P. Figures 1.1 to 1.3 show the possibilities for Γ_P when P is a non-parabolic point in $S(K)$. The lines in the figures represent lines in S, with solid lines being K-lines and dashed lines being lines defined over a specified finite extension of K.

If P is parabolic and the number of distinct asymptotic $\overline{K}$-lines at P is 1, then the curve Γ_P has a cusp at P. Note that if such a P lies on a line $\ell \subset S$ then $\Gamma_P = \ell \cup C$ where C is an irreducible conic and ℓ lies tangent to C as in Figure 1.6 on page 10. Otherwise Γ_P is an irreducible cubic curve with a singularity at P as in Figure 1.5 on page 10.

The case where there are infinitely many asymptotic lines at P is special: in this case Γ_P decomposes as a union of three $\overline{K}$-lines passing through P lying on S. In this case the point P is known as an *Eckardt point*. See Figures 1.7 to 1.9 on page 10.

Example 1.13. Let S be a smooth cubic surface defined over a field K containing the point $P = (0 : 0 : 0 : 1)$, which has tangent plane $\Pi_P : X = 0$. Then S has equation

$$S : F(X, Y, Z, W) = XW^2 + G(X, Y, Z)W + H(X, Y, Z) = 0$$

where G and H are homogeneous quadratic and cubic polynomials respectively, both defined over K. If $G \neq 0$ then P is non-Eckardt. Suppose G satisfies

$$G(0, Y, Z) = \alpha(\beta_1 Y + \gamma_1 Z)(\beta_2 Y + \gamma_2 Z)$$

with $\alpha \in K$ and $\beta_1,\ \beta_2,\ \gamma_1,\ \gamma_2 \in L$ where L is a quadratic extension of K. Also suppose $(\beta_1 Y + \gamma_1 Z)$ and $(\beta_2 Y + \gamma_2 Z)$ are linearly independent. Then Γ_P is a cubic curve with a node at P. Further, if $\beta_1,\ \beta_2,\ \gamma_1,\ \gamma_2 \in K$ then P is a split node, i.e. the two tangent lines at P are defined over K, otherwise it is a non-split node so the two tangent lines at P are Galois conjugates over a quadratic extension of K. When P is a split node there are two subcases that can occur. The first occurs if exactly one of $(\beta_1 Y + \gamma_1 Z)$, $(\beta_2 Y + \gamma_2 Z)$ divides $H(0, Y, Z)$. Then Γ_P is the union of a K-line and a conic as shown in Figure 1.2 and the equation of the line in Π_P is the common factor of $G(0, Y, Z)$ and $H(0, Y, Z)$. The second subcase is when $(\beta_1 Y + \gamma_1 Z)(\beta_2 Y + \gamma_2 Z)$ divides $H(0, Y, Z)$, in which case Γ_P is the union of three K-lines as shown in Figure 1.3.

Example 1.14. Let S be a smooth cubic surface defined over a field K containing the point $P = (0 : 0 : 0 : 1)$ and with $\Pi_P : X = 0$. Then S has equation

$$S : F(X, Y, Z, W) = XW^2 + G(X, Y, Z)W + H(X, Y, Z) = 0,$$

where G and H are homogeneous quadratic and cubic polynomials defined over K respectively. Suppose G satisfies

$$G(0, Y, Z) = \alpha(\beta Y + \gamma Z)^2,$$

with $\alpha,\ \beta,\ \gamma \in K$. This implies that there is a double tangent line to Γ_P at $P = (0 : 0 : 0 : 1)$ with equation $X = \beta Y + \gamma Z = 0$, i.e. Γ_P has a cusp at P. If $(\beta Y + \gamma Z)$ divides $H(0, Y, Z)$ then Γ_P splits into a line and a conic as shown in Figure 1.6, otherwise Γ_P is a irreducible cubic curve with a cusp at P as in Figure 1.5.

Example 1.15. Let S be a smooth cubic surface defined over a field K with equation

$$S : XW^2 + H(X, Y, Z) = 0,$$

where H is a homogeneous cubic polynomial. The surface S contains the point $E = (0 : 0 : 0 : 1)$ with tangent plane $\Pi_E : X = 0$. The curve $\Gamma_E : H(0, Y, Z) = 0$ is the union of three lines in S that all intersect at E, so E is an Eckardt point. If $H(0, Y, Z)$ splits into three linear components over K then the three lines through

E in S are K-lines as shown in Figure 1.7. If $H(0, Y, Z)$ splits into one linear and one quadratic component over K, then E lies on one K-line in S and two Galois conjugate lines in S that are defined over a quadratic extension of K as in Figure 1.8. If $H(0, Y, Z)$ is irreducible over K then E lies on three lines in S that are all Galois conjugate and each is defined over a cubic extension of K as in Figure 1.9.

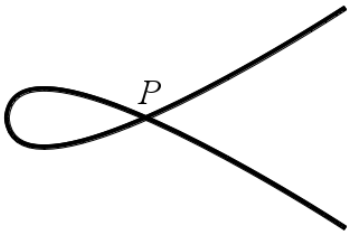

Figure 1.1: Γ_P is an irreducible cubic curve with a node at P.

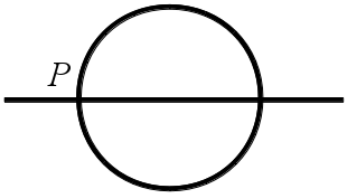

Figure 1.2: P is a single point of intersection of a K-line and a conic.

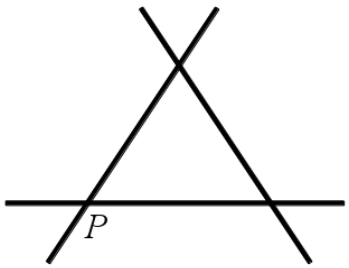

Figure 1.3: Γ_P is the union of three K-lines of which P is the intersection of two.

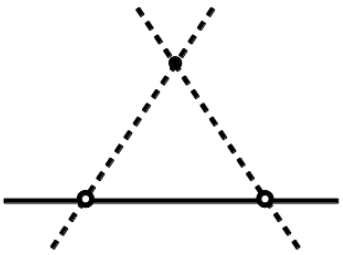

Figure 1.4: Γ_P is the union of one K-line and two Galois conjugate lines defined over a quadratic extension of K. P is the point of intersection of the two Galois conjugate lines.

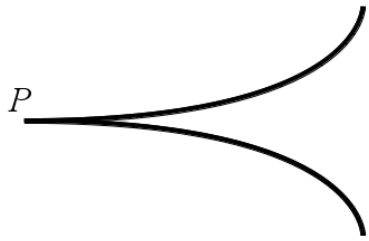

Figure 1.5: Γ_P is an irreducible cubic curve with a cusp at P.

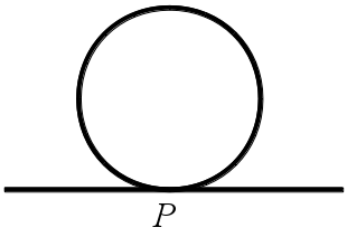

Figure 1.6: P is a double point of intersection of a K-line and a conic.

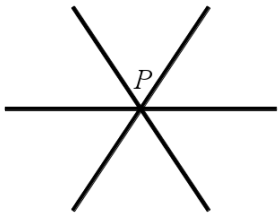

Figure 1.7: P is an Eckardt point lying on three K-lines.

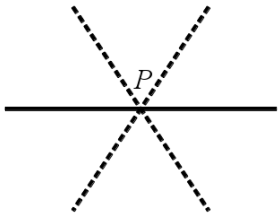

Figure 1.8: P is an Eckardt point lying on a K-line and two Galois conjugate lines defined over a quadratic extension of K.

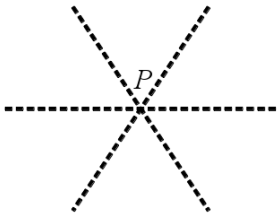

Figure 1.9: P is an Eckardt point lying on three Galois conjugate lines each defined over a cubic extension of K.

We continue to follow [20] in defining the *Gauss map* on $S(\overline{K})$ to be the map that takes a point P to its tangent plane Π_P. We define γ_ℓ to be the restriction of the Gauss map to a K-line $\ell \subset S$. Before discussing some further properties of the Gauss map we state the following lemma, the proof of which is taken from [20].

Lemma 1.16. *Let $P \in S(\overline{K})$. The curve Γ_P contains every $\overline{K}$-line on S that passes through P.*

Proof. By Euler's Homogeneous Function Theorem we know that $P \cdot (\nabla F)(P) = 0$. The line ℓ has a parametrisation of the form $sP + t\underline{\mathbf{v}}$ with $(s : t) \in \mathbb{P}^1$. Thus the polynomial $F(sP + t\underline{\mathbf{v}})$ vanishes identically. However, the coefficient of ts^2 in this

polynomial is $(\nabla F)(P)\cdot\underline{\mathbf{v}}$. This shows that ℓ is also contained in Π_P, and hence in Γ_P. □

We now know that if $P \in \ell \subset S$ then $\ell \subset \Pi_P$. In particular this implies that if three of the 27 lines in S intersect in a single point then these three lines must be coplanar, i.e. the point is an Eckardt point. Since Γ_P has degree 3, we cannot have more than three lines in S meeting in a single point. Lemma 1.16 also shows that the image of γ_ℓ is contained in the pencil of planes through ℓ, which in turn is isomorphic to $\mathbb{P}^1_K$. Hence we can consider the Gauss map of S at ℓ as a map $\gamma_\ell : \ell \to \mathbb{P}^1_K$.

The proof of the following lemma can be found in the proof of [20, Lemma 2.2].

Lemma 1.17. *Let S be a smooth cubic surface. Given a K-line $\ell \subset S$, the map γ_ℓ has degree 2.*

Proof. By a projective transformation defined over K we may suppose that ℓ passes through the point $(0:0:0:1)$, that the tangent to S at the point is $X = 0$ and that ℓ is the line $X = Y = 0$. Then

$$S : F(X,Y,Z,W) = XQ + YR = 0,$$

where Q and R are homogeneous quadratic polynomials in $K[X,Y,Z,W]$. Suppose that $P \in \ell(\overline{K})$. Then $X(P), Y(P) = 0$. Recall that $\Pi_P : (\nabla F)(P)\cdot\underline{\mathbf{x}} = 0$. We have

$$\begin{aligned}
\frac{\partial F}{\partial X} &= Q + X\frac{\partial Q}{\partial X} + Y\frac{\partial R}{\partial X}\\
\frac{\partial F}{\partial Y} &= X\frac{\partial Q}{\partial Y} + R + Y\frac{\partial R}{\partial Y}\\
\frac{\partial F}{\partial Z} &= X\frac{\partial Q}{\partial Z} + Y\frac{\partial R}{\partial Z}\\
\frac{\partial F}{\partial Z} &= X\frac{\partial Q}{\partial W} + Y\frac{\partial R}{\partial W},
\end{aligned}$$

so

$$(\nabla F)(P) = (Q(0:0:Z:W) : R(0:0:Z:W) : 0 : 0).$$

Now the map $\gamma_\ell \to \mathbb{P}^1_K$ can be written as $P \mapsto (Q(P) : R(P))$. The fact that S is smooth implies that Q and R do not simultaneously vanish along the line ℓ. Thus γ_ℓ has degree 2. □

The next three results can be found in [15, Chapter 1] and [16, Section 7].

Lemma 1.18. *Let S be a smooth cubic surface. If ℓ_1, ℓ_2 and ℓ_3 are three distinct coplanar lines in S and ℓ' is a fourth line in S, then ℓ' meets exactly one of ℓ_1, ℓ_2, ℓ_3.*

Three coplanar lines in a cubic surface can be referred to as a *triangle of lines*. This configuration is illustrated in Figure 1.10.

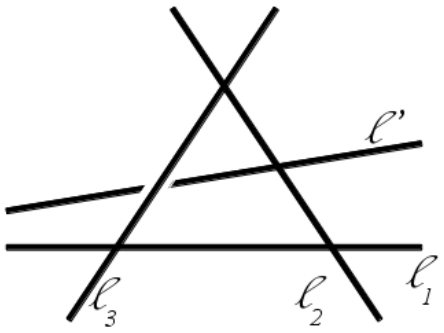

Figure 1.10: A triangle of lines intersected by a fourth line in S.

Proof. Let Π be the plane containing ℓ_1, ℓ_2, ℓ_3. The curve $\Pi \cdot S$ has degree 3 therefore $\ell' \notin \Pi$, hence ℓ' intersects Π in a point $P \in \Pi \cdot S = \ell_1 \cup \ell_2 \cup \ell_3$. Suppose P lies on more than one of ℓ_1, ℓ_2, ℓ_3. Then, without loss of generality $P = \ell_1 \cdot \ell_2$. Hence by Lemma 1.16 we have ℓ_1, ℓ_2, $\ell' \subset \Pi_P$. But ℓ_1, ℓ_2, ℓ' are not coplanar, therefore ℓ' meets exactly one of ℓ_1, ℓ_2, ℓ_3. □

We now restate the second part of The Cayley-Salmon Theorem (Theorem 1.7).

Proposition 1.19. *Let S be a smooth cubic surface. Given a line $\ell \subset S$, there exist exactly five pairs of lines in S that meet ℓ, which we denote (ℓ_i, ℓ_i'), $i = 1, \ldots, 5$. These lines satisfy*

(i) ℓ, ℓ_i and ℓ_i' are coplanar for $i = 1, \ldots, 5$,

(ii) $(\ell_i \cup \ell_i') \cap (\ell_j \cup \ell_j') = \varnothing$ for $i \neq j$.

See Figure 1.11 on page 13.

Proof. See [16, Proposition 7.3]. □

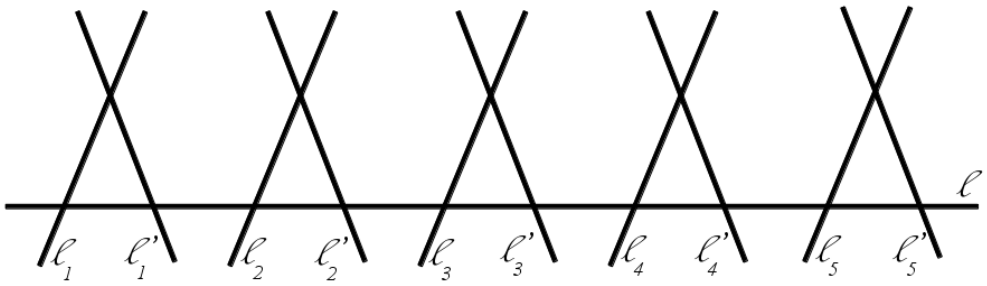

Figure 1.11: Every line in S is intersected by five pairs of lines in S.

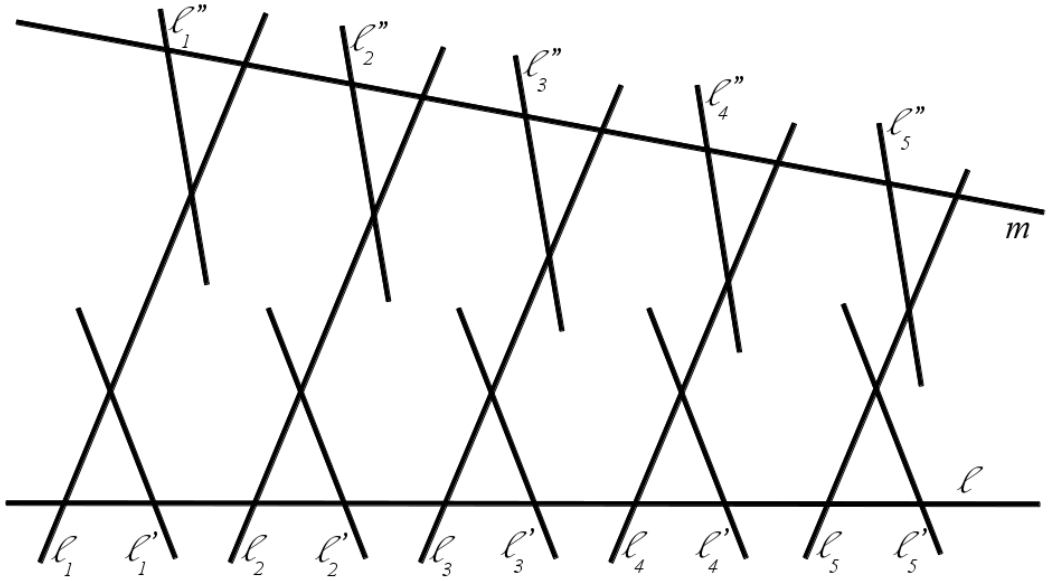

Figure 1.12: The configuration of lines intersecting a skew pair of lines in S.

Lemma 1.20. *Let S be a smooth cubic surface. Let ℓ and m be two disjoint, i.e. skew, lines in S. Then there are precisely five lines $\ell_1, \ldots, \ell_5 \subset S$ that intersect both ℓ and m, a further five lines $\ell'_1, \ldots, \ell'_5 \subset S$ that intersect ℓ and five lines $\ell''_1, \ldots, \ell''_5 \subset S$ such that the pairs (ℓ_i, ℓ'_i) and (ℓ_i, ℓ''_i) are coplanar for $i = 1, \ldots, 5$.*

This is illustrated in Figure 1.12 on page 13.

Proof. Follows from Lemma 1.18 and Proposition 1.19. □

The following lemma, proved in [20], gives useful information on the geometry of Γ_P for $P \in \ell(\overline{K})$.

Lemma 1.21. *Let ℓ be a K-line contained in S.*

(i) If $\mathrm{char}(K) \neq 2$ then γ_ℓ is separable. Precisely two points in $\ell(\overline{K})$ are parabolic and so there are at most two Eckardt points on ℓ.

(ii) *If* $\mathrm{char}(K) = 2$ *and* γ_ℓ *is separable then there is precisely one point* $P \in \ell(\overline{K})$ *which is parabolic and so at most one Eckardt point on* ℓ*.*

(iii) *If* $\mathrm{char}(K) = 2$ *and* γ_ℓ *is inseparable then every point* $P \in \ell(\overline{K})$ *is parabolic and the line* ℓ *contains exactly* 5 *Eckardt points.*

The following theorem, which can be found in Swinnerton-Dyer's papers [23] and [24], gives a precise statement for the possible number of rational points on a cubic surface defined over a finite field. It is another special case of the Hasse-Weil bound.

Theorem 1.22. *Let* S *be a smooth cubic surface defined over a finite field* $K = \mathbb{F}_q$*. Then the number of points of* $S(K)$ *is given by*

$$|S(K)| = q^2 + mq + 1,$$

where m *is an integer satisfying* $-2 \leq m \leq 5$ *if* $q = 2, 3$ *or* 5*, and* $-2 \leq m \leq 7$*,* $m \neq 6$ *otherwise.*

1.3 The Mordell-Weil Problem for cubic surfaces

Following Manin [14] and Segre [18] one can define a secant and tangent process for generating new rational points from old. This process is somewhat analogous to the group operation on the rational points of an elliptic curve as discussed in Section 1.1.1. The *secant operation* is defined as follows. Let P, $Q \in S(K)$ and $P \neq Q$. Let ℓ be the line joining P and Q. If $\ell \notin S$ then ℓ intersects S in exactly three points counting multiplicities, i.e. $\ell \cdot S = P + Q + R$ where $R \in S(K)$. If R is distinct from P and Q then we say we have generated R from P and Q. For the *tangent operation* let Π_P be the tangent plane to S at P. Let ℓ be any K-line lying in Π_P. If $\ell \notin S$ then $\ell \cdot S = 2P + R$. If $R \neq P$ then we have generated R from P.

Segre used the secant and tangent processes in [18] to show that a cubic surface defined over $\mathbb{Q}$ may have precisely $0, 1, 3$ or infinitely many rational points and that there are no other possibilities.

The set of rational points on a cubic surface is not a group. In fact the secant and tangent process is not even a binary operation: one can see that $P \circ P$ is not well-defined and $P \circ Q$ for $P \neq Q$ is not everywhere defined. However one can still pose questions about the size of a minimal generating set of points. This is the *Mordell-Weil Problem* for cubic surfaces. Problems of this type were first studied by Segre in [18], and by Manin in his book *Cubic Forms* [14]. Manin found that

the structure given to certain equivalence classes of points of a cubic surface with respect to these secant and tangent operations was a *commutative Moufang loop*. We follow a different direction in this thesis inspired initially by the approach in Siksek's paper [20]. Beyond the definitions above, there is no overlap with Manin's work.

In order to study this problem we define the *span* of a set of points in $S(K)$ as follows. Let Σ be a set of K-points on S. We define $\mathrm{Span}(\Sigma)$ as the minimal set of points in $S(K)$ containing Σ that is closed under the secant and tangent operations so we have $\Sigma \subseteq \mathrm{Span}(\Sigma) \subseteq S(K)$. We will write $\mathrm{Span}(P_1, \ldots, P_n)$ in place of $\mathrm{Span}(\{P_1, \ldots, P_n\})$ for ease of notation.

Chapters 2, 3 and 4 are concerned with the Mordell-Weil Problem for cubic surfaces over finite fields and, in particular, generalisations of the following result.

Theorem 1.23 (Siksek [20, Theorem 1])**.** *Let K be a field with at least 13 elements. Let S be a smooth cubic surface over K. Suppose S contains a pair of skew lines both defined over K. Let $P \in S(K)$ be a point on either line that is not an Eckardt point. Then*

$$Span(P) = S(K).$$

We also mention the following result.

Theorem 1.24 (Siksek [20, Theorem 2])**.** *Let $p_1, \ldots, p_s$, $(s \geq 1)$, be distinct primes such that*

(i) $p_i \equiv 1 \pmod 3$,

(ii) *2 is a cube modulo p_i.*

Let $M = \prod p_i$ and let $S = S_M/\mathbb{Q}$ be the smooth cubic surface given by

$$S_M : X^3 + Y^3 + Z(Z^2 + MW^2) = 0.$$

Then the size of a minimal generating set of $\mathbb{Q}$-points for $S(\mathbb{Q})$ is at least $2s$.

Observe that these surfaces have a $\mathbb{Q}$-line with equation $X + Y = Z = 0$.

1.4 Results

In Chapter 2 the main result is Theorem 2.1, which extends Theorem 1.23 to fields with at least four elements. Theorem 2.2 gives a slightly weaker result for $\mathbb{F}_3$.

Theorem 2.1. *Let K be a field with at least 4 elements. Let S be a smooth cubic surface over K. Suppose S contains a skew pair of lines both defined over K. Let P be any K-rational point on either line that is not Eckardt. Then*

$$\mathrm{Span}(P) = S(K).$$

Theorem 2.2. *Let $K = \mathbb{F}_3$. Let S be a smooth cubic surface over K. Suppose S contains a skew pair of lines ℓ and ℓ' defined over K and that ℓ and ℓ' each contain at most one K-rational Eckardt point. Then there exists a point $P \in \ell(K) \cup \ell'(K)$ such that* $\mathrm{Span}(P) = S(K)$.

Theorem 2.2 was partly proved using an exhaustive enumeration in the computer algebra package `MAGMA` [13]. The implementation of the secant and tangent operations on a cubic surface is given in Section 2.2.

My work based on Chapter 2 has appeared in Archiv der Mathematik [6].

The main result of Chapter 3 is Theorem 3.1, which gives a complete solution to the Mordell-Weil Problem for cubic surfaces that contain a rational line when the surface is defined over a finite field with at least eight elements.

Theorem 3.1. *Let $K = \mathbb{F}_q$ be a finite field with $q \geq 8$. Let S be a smooth cubic surface defined over K containing at least one K-rational line. Then there exists a point $P \in S(K)$ such that* $\mathrm{Span}(P) = S(K)$.

The main idea behind the proof of Theorem 3.1 is to generate a little over half of the rational points on such a cubic surface and then show using a pigeonhole principle that the rest of the rational points can be generated.

Theorem 3.4. *Let S be a smooth cubic surface over $K = \mathbb{F}_q$. Let $T \subseteq S(K)$ be such that $\ell(K) \subseteq T$ for all K-lines ℓ contained in S, and $|T| > \frac{1}{2}|S(K)| + \frac{q+1}{2}$. Then*

$$\mathrm{Span}(T) = S(K).$$

Using a `MAGMA` computation, we proved the following result by an exhaustive enumeration.

Theorem 3.2. *Let $K = \mathbb{F}_2$. Let S be a smooth cubic surface over K. Suppose S contains a line ℓ defined over K that does not contain any K-rational Eckardt points. Then there exists a point $P \in \ell(K)$ such that* $\mathrm{Span}(P) = S(K)$.

This result also appeared in [6]. The rest of the contents of Chapter 3 appear in my `arXiv` preprint [7].

Chapter 4 concerns the Mordell-Weil Problem for cubic surfaces over finite fields that do not contain any rational lines. The main result of this chapter is Theorem 4.1, which does not give a solution to the Mordell-Weil Problem but does give a lower bound for the proportion of the rational points on such a cubic surface that can be generated from a single rational point. This may prove to be the first step in a more complete solution to the Mordell-Weil problem for cubic surfaces over finite fields in general.

Theorem 4.1. *Let S be a smooth cubic surface defined over a finite field $K = \mathbb{F}_q$ containing no rational lines. Let $P \in S(K)$ be a non-Eckardt point. Let*

$$n = [(2q+3)/6],$$

where $[x]$ denotes the nearest integer to x. Then

$$\frac{|\mathrm{Span}(P)|}{|S(K)|} \geq \frac{2nq - 3n^2 + 3n}{2(q^2+7q+1)}.$$

This lower bound on $\frac{|\mathrm{Span}(P)|}{|S(K)|}$ tends to $\frac{1}{6}$ as q tends to infinity.

Theorems 2.2 and 3.2 have stronger hypotheses than the theorems that hold for larger fields. There is evidence to show that statements with as weak hyptheses as Theorems 2.1 and 3.1 will not hold over small finite fields. Examples 1.25, 1.26 and 1.27 illustrate this. For these examples we used the method of Clebsch [4] for computing the lines. Details of this method can be found in [22] and an implementation in `MAGMA` is given below.

The method of Clebsch involves computing the first minors of a 4×4 matrix. The function `minor` takes as its inputs a 4×4 matrix H and two integers $i, j \in \{1,2,3,4\}$. The output is the first minor of H that is found by taking the determinant of the 3×3 matrix obtained by removing the i^{th} row and j^{th} column, multiplied by the corresponding cofactor.

```
minor:=function(H,i,j);
        I:=Exclude([1..4],i);
        J:=Exclude([1..4],j);
        S:=Submatrix(H,I,J);
        return (-1)^(i+j)*Determinant(S);
end function;
```

We then define the function `clebsch` which takes as its input a homogeneous cubic polynomial U in four variables x_1, x_2, x_3, x_4 defined over a field K and outputs the

K-lines of the cubic surface $S : U = 0$.

```
clebsch:=function(U);
        P:=Parent(U);
```

Here P is the polynomial ring where U is defined, i.e. $K[x_1, x_2, x_3, x_4]$. We next need to compute the Hessian matrix

$$H := \left(\frac{\partial^2 U}{\partial x_i \partial x_j} \right)_{i,j \in \{1,2,3,4\}}$$

and its determinant Δ.

```
        H:=Matrix( [ [ Derivative(Derivative(U,P.i),P.j) : i in
[1..4]] : j in [1..4]]);
        delta:=Determinant(H);
```

We then compute the sum

$$\Theta := \sum_i \sum_j U_{ij} \Delta_i \Delta_j, \quad i, j \in \{1, 2, 3, 4\},$$

where $\Delta_i = \frac{\partial \Delta}{\partial x_i}$ and U_{ij} is the minor of H obtained by removing the i^{th} row and j^{th} column multiplied by the corresponding cofactor, i.e. $U_{ij} = \texttt{minor(H, i, j)}$. We also compute the sum

$$T := \sum_i \sum_j U_{ij} \Delta_{ij}, \quad i, j \in \{1, 2, 3, 4\},$$

where $\Delta_{ij} := \frac{\partial^2 \Delta}{\partial x_i \partial x_j}$.

```
        theta:=&+[
minor(H,i,j)*Derivative(delta,P.i)*Derivative(delta,P.j) : i,j in
[1..4]];
        T:=&+[ minor(H,i,j)*Derivative(Derivative(delta,P.i),P.j) :
i,j in [1..4]];
```

We now compute $F := \Theta - 4\Delta T$. This is Clebsch's degree 9 covariant that meets the surface in the 27 lines. The irreducible linear components of this intersection are the K-lines of S.

```
        F:=theta-4*delta*T;
        PP:=ProjectiveSpace(P);
        S:=Scheme(PP,[U,F]);
```

```
        I:=IrreducibleComponents(S);
        assert &+[Degree(J) : J in I] eq 27;
        return [J : J in I | Degree(J) eq 1];
end function;
```

Example 1.25. Let S be the smooth cubic surface over $K = \mathbb{F}_2$ defined by

$$X^3 + X^2Y + X^2Z + X^2W + XW^2 + Y^3 + Z^3 = 0.$$

This surface has precisely three K-points, all of which are Eckardt. Therefore $\mathrm{Span}(P) = P$ for all $P \in S(K)$.

Example 1.26. Let S be the smooth cubic surface over $K = \mathbb{F}_2$ defined by

$$X^2W + XW^2 + Y^2Z + YZ^2 = 0.$$

This surface contains fifteen K-lines and fifteen K-points. All of the K-points are Eckardt, so $\mathrm{Span}(P) = P$ for all $P \in S(K)$.

Example 1.27. Let S be the smooth cubic surface over $K = \mathbb{F}_2$ defined by

$$X^2W + XYZ + XW^2 + Y^2Z + YZ^2 = 0.$$

This surface contains nine K-lines and thirteen K-points. Four of the K-points of S are Eckardt points and $|\mathrm{Span}(P)| \in \{1, 2, 5\}$ for all $P \in S(K)$.

In Chapter 5, for a cubic surface S defined over a finite field K and containing a K-line ℓ, we introduce the *c-invariants* of S with respect to ℓ. The c-invariants are integers that give information on the intersection of S with the pencil of K-planes through ℓ. This theory was initially developed to lower the bound on the minimal size of field in Theorem 3.1. Although this strategy did not provide a stronger result than Theorem 3.1, it did yield the following results. The first states the number of K-points on S in terms of the c-invariants.

Theorem 5.1. *Let S be a smooth cubic surface defined over $K = \mathbb{F}_q$ containing a K-line, ℓ, and let $c_1, \ldots, c_7$ be the c-invariants of S with respect to ℓ. Then*

$$c_1 + c_2 = c_3 + c_4$$

and

$$|S(K)| = q + 1 + c_1(q-1) + c_2(2q-1) + c_3(q+1) + c_4 + c_5q + 2c_6q.$$

The second gives relations on the c-invariants obtained from the geometry of S.

Proposition 5.2. *Let S be a smooth cubic surface defined over $K = \mathbb{F}_q$ containing a K-line, ℓ, and let $c_1, \ldots, c_7$ be the c-invariants of S with respect to ℓ. Then we have the following relations between the c_i.*

When $\mathrm{char}(K) = 2$ *and γ_ℓ is inseparable*

$$\begin{aligned} c_1 = c_2 = c_3 = c_4 = 0, \\ c_5 + c_6 + c_7 = q + 1, \\ c_6 + c_7 \leq 5. \end{aligned}$$

When $\mathrm{char}(K) = 2$ *and γ_ℓ is separable*

$$\begin{aligned} c_5 + c_6 + c_7 = 1, \\ c_1 + c_2 = c_3 + c_4 = \tfrac{q}{2}, \\ c_2 + c_4 + c_6 + c_7 \leq 5. \end{aligned}$$

When $\mathrm{char}(K) \neq 2$ *and there are no parabolic points in $\ell(K)$*

$$\begin{aligned} c_5 = c_6 = c_7 = 0, \\ c_1 + c_2 = c_3 + c_4 = \tfrac{q+1}{2}, \\ c_2 + c_4 + c_6 + c_7 \leq 5. \end{aligned}$$

When $\mathrm{char}(K) \neq 2$ *and there are exactly two parabolic points in $\ell(K)$*

$$\begin{aligned} c_5 + c_6 + c_7 = 2, \\ c_1 + c_2 = c_3 + c_4 = \tfrac{q-1}{2}, \\ c_2 + c_4 + c_6 + c_7 \leq 5. \end{aligned}$$

From these we obtain an expression linking the c-invariants to the quantity m given in the Hasse-Weil Bound (Theorem 1.22).

Corollary 5.4. *In the notation of Theorem 5.1 and Theorem 1.22*

$$m = 2 - c_1 + c_3 + c_6 - c_7.$$

From Corollary 5.4 we obtain the following theorem, which is a strengthening of Proposition 5.2.

Theorem 5.9. *Let S be a smooth cubic surface defined over $K = \mathbb{F}_q$ containing a K-line ℓ. Let $c_1, \ldots, c_7$ be the c-invariants of S with respect to ℓ and let m be the surface invariant satisfying $|S(K)| = q^2 + mq + 1$. Then we have the following relations between the c_i and m.*

$$
\begin{aligned}
&c_5 + c_6 + c_7 = q + 1 - 2N,\\
&c_1 + c_2 = c_3 + c_4 = N,\\
&c_2 + c_4 + c_6 + c_7 \leq 5\\
&c_4 + c_7 \leq 4m = 2 - c_1 + c_3 + c_6 - c_7,
\end{aligned}
$$

where

$$
N = \begin{cases}
0 & \text{if } \gamma_\ell \text{ is inseparable}\\
\frac{q-1}{2} & \text{if } \mathrm{char}(K) \neq 2 \text{ and there are two parabolic points in } \ell(K)\\
\frac{q}{2} & \text{if } \mathrm{char}(K) = 2 \text{ and } \gamma_\ell \text{ is separable}\\
\frac{q+1}{2} & \text{if } \mathrm{char}(K) \neq 2 \text{ and there are no parabolic points in } \ell(K).
\end{cases}
$$

Finally we obtain the following result on the nature of the 10 lines in S that intersect ℓ.

Lemma 5.8. *Let S be a cubic surface defined over a finite field $K = \mathbb{F}_q$ and containing a K-line ℓ. Then, of the ten $\overline{K}$-lines in S that intersect ℓ, at most eight can be defined over $\mathbb{F}_{q^2}$ but not K.*

Chapter 6 contains results regarding the computation of classes of pointed cubic surfaces (S, P) over a finite field K up to equivalence under linear transformations. These results were obtained during efforts to check whether for a given small finite field $K = \mathbb{F}_q$, $q \geq 5$, the set $S(K)$ could be generated via tangent and secant operations from any non-Eckardt point P, for all smooth cubic surfaces S over K. In particular we prove the following theorem.

Theorem 6.2. *Let S be a smooth cubic surface defined over $K = \mathbb{F}_5$ or $\mathbb{F}_7$ and containing a non-Eckardt point $P \in S(K)$ such that P is a cusp of Γ_P. Then*

$$\mathrm{Span}(P) = S(K).$$

Remark. Recall that a parabolic K-point on S is either an Eckardt point, or a cusp of Γ_P. The theorem implies that any non-Eckardt parabolic K-point on S generates $S(K)$.

Let (S, P) be a pointed cubic surface where S is defined over $K = \mathbb{F}_q$ and $P \in S(K)$ is a smooth point. Then (S, P) is equivalent to a pointed cubic surface (S', P') where S' is a cubic surface defined over K and P' is the point $(0:0:0:1)$ with tangent plane $\Pi_{P'} : X = 0$. By equivalent we mean that there is a K-linear transformation of variables taking (S, P) to (S', P'). We write $\mathcal{F}$ for the set of

all such pointed cubic surfaces and denote the subsets of $\mathcal{F}$ where the point P is an Eckardt point, cusp, split node and non-split node of Γ_P by $\mathcal{F}_E$, $\mathcal{F}_C$, $\mathcal{F}_{sN}$ and $\mathcal{F}_{nsN}$ respectively. We compute the subgroups of $\mathrm{GL}(4, K)$ that preserve the subsets $\mathcal{F}_E$ and $\mathcal{F}_C$, which we denote $\mathcal{G}_E$ and $\mathcal{G}_C$ respectively, and give generators for these subgroups. We believe this method would extend to finding the subgroups of $\mathrm{GL}(4, K)$ preserving $\mathcal{F}_{sN}$ and $\mathcal{F}_{nsN}$. Finding the generators of $\mathcal{G}_C$ allows us to define it as a subgroup of $\mathrm{GL}(4, K)$ in `MAGMA` [13]. We can then compute complete lists of inequivalent cusp pointed cubic surfaces under projective K-linear transformations. We give an implementation of this method in the computer algebra system `MAGMA`. We then test whether P generates $S(K)$ using the code given in Section 2.2. Using this we prove Lemma 6.2.

We also give an explanation of how to calculate the number of equivalence classes of a set $\mathcal{F}_i$ under a group action of $\mathcal{G}_i$ using Burnside's Lemma. The implementation in `MAGMA` is given.

Chapter 2

Cubic surfaces containing skew rational lines

In this chapter we discuss and in most cases solve the Mordell-Weil Problem for cubic surfaces defined over K that contain a pair of skew K-lines, where K is a field with at least three elements. The main results are the following two theorems. Figures are provided to aid the reader's intuition.

Theorem 2.1. *Let K be a field with at least 4 elements. Let S be a smooth cubic surface over K. Suppose S contains a skew pair of lines both defined over K. Let P be any K-rational point on either line that is not Eckardt. Then*

$$\mathrm{Span}(P) = S(K).$$

Theorem 2.2. *Let $K = \mathbb{F}_3$. Let S be a smooth cubic surface over K. Suppose S contains a skew pair of lines ℓ and ℓ' defined over K and that ℓ and ℓ' each contain at most one K-rational Eckardt point. Then there exists a point $P \in \ell(K) \cup \ell'(K)$ such that* $\mathrm{Span}(P) = S(K)$.

A stronger result for cubic surfaces over $\mathbb{F}_2$ is given in Chapter 3. Theorem 2.2 was proved using an exhaustive computer enumeration. This is not convenient for Theorem 2.1, despite the fact that the results of Siksek (Theorem 1.23) allow us to reduce our search to fields having at most 11 elements. To prove Theorem 2.1 by exhaustive enumeration over a finite field K we need to enumerate quadruples (S, ℓ, ℓ', P) up to projective equivalence, where S is a smooth cubic surface over K, ℓ and ℓ' are a skew pair of K-lines lying on S and $P \in \ell(K)$ is a non-Eckardt point. For each of these quadruples we would want to apply the tangent and secant process repeatedly to prove that $\mathrm{Span}(P) = S(K)$. Some effort was invested into

understanding the invariant theory needed for the enumeration, but the theory needed to make the enumeration practical for, say, $K = \mathbb{F}_{11}$ would be far more complicated than the theoretical proof of Theorem 2.1 given in Section 2.1.

2.1 Proof of Theorem 2.1

In the following Lemma 2.4 is a strengthening of Lemma 2.3 and Propositions 2.5 and 2.6 are used in the proofs of Lemmas 2.7 and 2.8. Theorem 2.1 is then a consequence of Lemmas 2.4, 2.7, 2.8 and 2.9.

Lemma 2.3. *Let K be a field with at least 4 elements and S a smooth cubic surface defined over K. Let ℓ be a K-line on S. Let $P \in \ell(K)$ be a point that does not lie on any other line belonging to S. Then*

$$\ell(K) \subseteq \Gamma_P(K) \subseteq \mathrm{Span}(P).$$

Proof. The curve Γ_P has degree 3. The line ℓ is an irreducible component of Γ_P, and there are no other lines in S passing through P. Thus $\Gamma_P = \ell \cup C$, where C is an irreducible conic.

Note that $C \cdot \ell = P + P'$ where P' is a point in $S(K)$. Note also that, since P' lies on both ℓ and C, any line $m \subset \Pi_P$, $m \neq \ell$ going through P' will be such that $m \notin S$ and will have a double intersection to Γ_P at P', i.e. Π_P is the tangent plane at P' and hence $\Gamma_{P'} = \Gamma_P$. See Figures 2.1 and 2.2. We want to show that $\Gamma_P(K) \subseteq \mathrm{Span}(P)$.

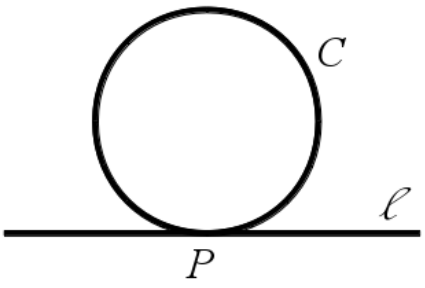

Figure 2.1: The case where $P = P'$.

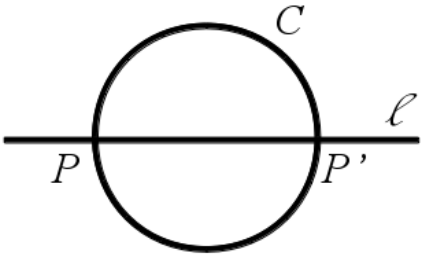

Figure 2.2: The case where $P \neq P'$.

Let $Q \in C(K)$, $Q \neq P, P'$. Let m be the line joining P and Q. Then $m \cdot S = 2P + Q$ as in Figure 2.3. Thus $Q \in \mathrm{Span}(P)$. Hence $C(K)\backslash\{P'\} \subseteq \mathrm{Span}(P)$. We now want to show that $\ell(K)\backslash\{P'\} \subseteq \mathrm{Span}(P)$. Fix $Q \in C(K)\backslash\{P, P'\}$, let $R \in \ell(K)\backslash\{P, P'\}$ and let m' be the line joining Q and R. Then $m' \cdot S = Q + R + R'$,

where $R' \in C(K)$. See Figure 2.4. Since Q, $R' \in C(K)\backslash\{P'\} \subseteq \mathrm{Span}(P)$, we have $R \in \mathrm{Span}(P)$. Thus $\Gamma_P(K)\backslash\{P'\} \subseteq \mathrm{Span}(P)$.

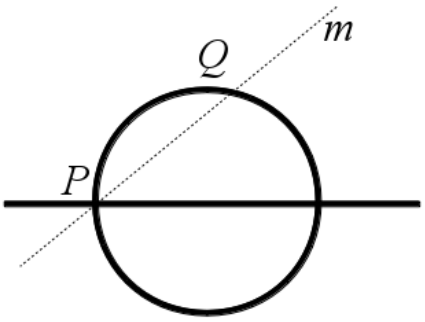

Figure 2.3: Tangent operation on P.

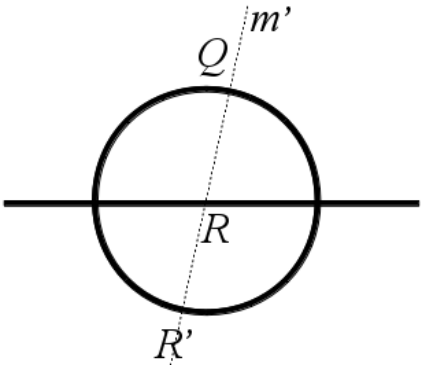

Figure 2.4: Secant operation on Q and R'.

If $P = P'$ then we have $\Gamma_P(K) \subset \mathrm{Span}(P)$ and we are done. Suppose now that $P \neq P'$. To complete the proof we must show that $P' \in \mathrm{Span}(P)$. As $P \neq P'$ but $\Gamma_P = \Gamma_{P'}$ it follows from Lemma 1.21 that γ_ℓ is separable and that therefore the line ℓ contains at most two Eckardt points. Since $|K| \geq 4$ the line ℓ has at least five K-rational points, and so there is some point $R \in \ell(K)$ that is neither Eckardt nor equal to P or P'. As noted above $\Pi_P = \Pi_{P'} \supset \ell \cup C$. As γ_ℓ has degree 2 by Lemma 1.17, we see that $\Pi_R \neq \Pi_P$. There are now two cases to consider. The first is when $\Gamma_R = \ell \cup C'$ where C' is an irreducible conic and the second is when Γ_R is a union of three lines as illustrated in Figures 2.5 and 2.6 respectively. For the first case we have

$$\Gamma_R(K)\backslash\{R'\} \subseteq \mathrm{Span}(R) \subseteq \mathrm{Span}(P),$$

where $\ell \cdot C' = R + R'$. Note that $P' \neq R'$ as $\Pi_{P'} = \Pi_P \neq \Pi_R = \Pi_{R'}$. Hence $P' \in \mathrm{Span}(P)$ and the proof is complete in this case.

Finally, we must consider the case where Γ_R is the union of three lines, which must include ℓ. Let the other two lines be ℓ' and ℓ'', where $\ell \cdot \ell' = R$, $\ell \cdot \ell'' = R'$ and $\ell' \cdot \ell'' = R''$. As R is not Eckardt, R, R' and R'' are distinct. Since ℓ and R are K-rational, so are the lines ℓ' and ℓ'' and the points R' and R''. First note that both R and R' are in $\mathrm{Span}(P)$ as they both lie on ℓ and are not equal to P'. Let $Q \in \ell''(K)$, $Q \neq R'$, R''. Let m be the line joining R and Q. As in Figure 2.7, $m \cdot S = 2R + Q$, and so $Q \in \mathrm{Span}(P)$. Thus

$$\ell''(K)\backslash\{R''\} \subseteq \mathrm{Span}(P)$$

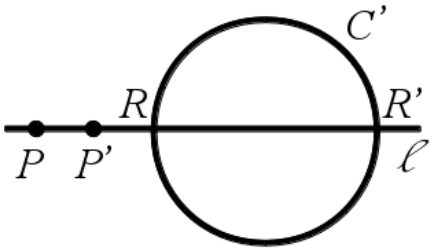

Figure 2.5: The case where $\Gamma_R = \ell \cup C'$.

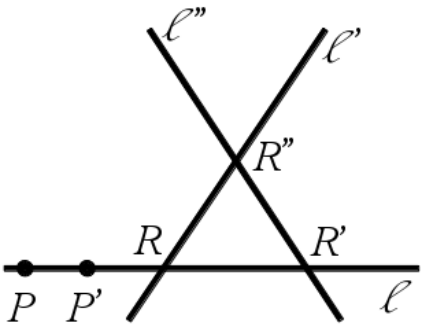

Figure 2.6: The case where Γ_R is the union of ℓ and two other K-lines.

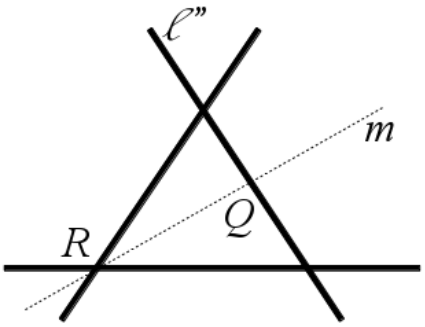

Figure 2.7: $\ell''(K) \subset \mathrm{Span}(R)$.

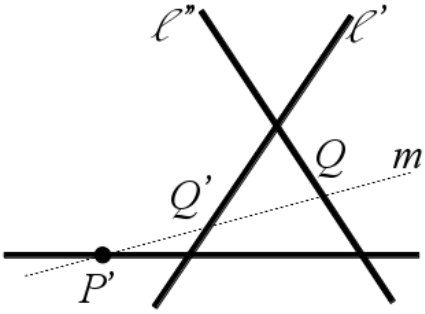

Figure 2.8: $P' \subset \mathrm{Span}(Q, Q')$

and likewise

$$\ell'(K) \backslash \{R''\} \subseteq \mathrm{Span}(P).$$

Take $Q \in \ell''(K)$ such that $Q \neq R'$, R''. Let m be the line joining P' and Q. Then

$$m \cdot S = P' + Q + Q',$$

where $Q' \in \ell'(K)$ and $Q' \neq R$, R'' as in Figure 2.8. Thus $P' \in \mathrm{Span}(P)$, completing the proof. □

The following lemma is a strengthening of Lemma 2.3.

Lemma 2.4. *Let K be a field with at least 4 elements and S a smooth cubic surface defined over K. Let ℓ be a K-line on S. Let $P \in \ell(K)$ and suppose that P is not an Eckardt point. Then*

$$\ell(K) \subseteq \Gamma_P(K) \subseteq \mathrm{Span}(P).$$

Proof. Let $P \in \ell(K)$ be a non-Eckardt point. If P does not lie on any other line contained in S then we can invoke Lemma 2.3. Thus we may suppose that P lies on some other line ℓ_2. This is necessarily a K-line because if it were not, its conjugate line would also pass through P, meaning that P were an Eckardt point, which would contradict the hypotheses of the lemma. Now $\Gamma_P = \ell \cup \ell_2 \cup \ell_3$, where ℓ_3 is also a K-line. As P is not Eckardt, ℓ_3 does not pass through P. Let $\ell \cdot \ell_3 = P'$ and $\ell_2 \cdot \ell_3 = P''$ as shown in Figure 2.9.

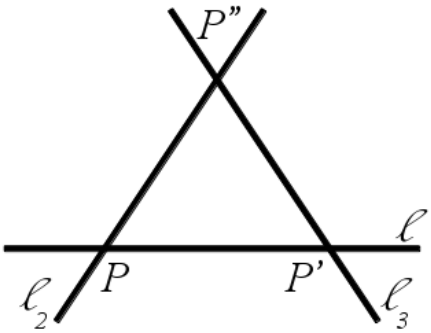

Figure 2.9: $\Gamma_P = \ell \cup \ell_2 \cup \ell_3$.

By executing a tangent operation on P we obtain

$$\ell_3(K) \backslash \{P', P''\} \subseteq \mathrm{Span}(P).$$

Since $\Gamma_{P'} = \Gamma_{P''}$ but $P' \neq P''$ we know that γ_{ℓ_3} is separable and so, by Lemma 1.21, there are at most two Eckardt points on ℓ_3. Since $\ell_3(K)$ has at least 5 points, we see that there is some $Q \in \ell_3(K) \backslash \{P', P''\}$ that is not Eckardt. We consider two cases. The first is where Q does not lie on any other line. Then by Lemma 2.3 we have

$$\ell_3(K) \subseteq \mathrm{Span}(Q) \subseteq \mathrm{Span}(P).$$

Thus P, P', $P'' \in \mathrm{Span}(P)$. By applying tangent operations to P', P'' we obtain

$$\ell(K) \cup \ell_2(K) \cup \ell_3(K) = \Gamma_P(K) \subseteq \mathrm{Span}(P, P', P'') = \mathrm{Span}(P).$$

The remaining case is when Q lies on some other K-line $\ell_4 \subset S$ and so $\Gamma_Q = \ell_3 \cup \ell_4 \cup \ell_5$.

Let $Q = \ell_3 \cdot \ell_5$, $Q' = \ell_3 \cdot \ell_4$ and $Q'' = \ell_4 \cdot \ell_5$ as in Figure 2.10. By applying

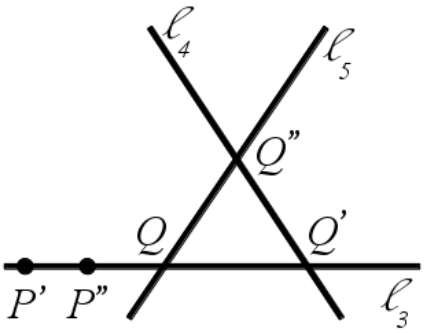

Figure 2.10: $Q \in \ell_4(K)$.

tangent operations to Q and Q' we obtain

$$(\ell_4(K) \cup \ell_5(K))\backslash\{Q''\} \subseteq \mathrm{Span}(Q, Q') \subseteq \mathrm{Span}(P).$$

Then by applying secant operations to the points of $(\ell_4(K) \cup \ell_5(K))\backslash\{Q''\}$ we obtain

$$P', P'' \in \mathrm{Span}((\ell_4(K) \cup \ell_5(K))\backslash\{Q''\}) \subseteq \mathrm{Span}(P),$$

which completes the proof. □

Proposition 2.5. *Let K be a field with at least 4 elements and S, a smooth cubic surface defined over K. Suppose S contains a skew pair of lines ℓ, ℓ' and there is a non-Eckardt point $P \in \ell(K)$ such that $\Pi_P \cdot \ell'$ is also non-Eckardt. Then*

$$\ell'(K) \subseteq \mathrm{Span}(\ell(K)).$$

Proof. Let $Q = \Pi_P \cdot \ell'$. Note that $Q \in \Gamma_P(K)$, thus $Q \in \mathrm{Span}(P) \subseteq \mathrm{Span}(\ell(K))$ by Lemma 2.4. By assumption Q is non-Eckardt. Applying Lemma 2.4 again we have

$$\ell'(K) \subseteq \mathrm{Span}(Q) \subseteq \mathrm{Span}(\ell(K)).$$

□

Proposition 2.6. *Let S be a smooth cubic surface defined over a field K. Suppose S contains a skew pair of K-lines ℓ, ℓ' and let $P \in \ell(K)$. Let Γ_P be the union of ℓ and an irreducible conic. Then the point $\ell' \cdot \Pi_P$ is not an Eckardt point.*

See Figure 2.11.

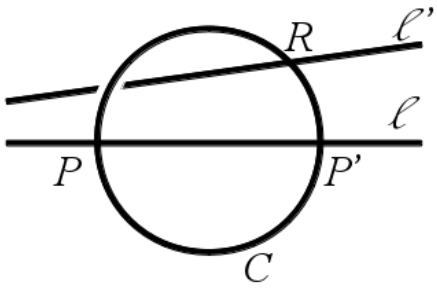

Figure 2.11: $\Gamma_P = \ell \cup C$, ℓ' is skew to ℓ.

Proof. Let $P \in \ell(K)$. Let $R = \ell' \cdot \Pi_P$. We must prove that R is not an Eckardt point so we suppose the contrary and proceed for a contradiction. Let ℓ_2 and ℓ_3 be the other two lines going through R. Let $Q = \ell \cdot \Pi_R$, then without loss of generality $Q = \ell \cdot \ell_2$. Note that ℓ_2 must be in the tangent plane to S at Q, so $\Pi_Q \neq \Pi_P$ since $\Gamma_P = \ell \cup C$. Note also that $R = \ell' \cdot \Pi_Q$, which implies that Π_Q is the unique plane containing ℓ and R. However, the plane Π_P also contains ℓ and R. But $\Pi_P \neq \Pi_Q$ so we have reached a contradiction and the point $R = \ell' \cdot \Pi_P$ cannot be an Eckardt point. □

Lemma 2.7. *Let K be a field with at least 7 elements and* $\mathrm{char}(K) \neq 2$. *Let S be a smooth cubic surface defined over K. Suppose S contains a skew pair of K-lines ℓ, ℓ'. Then*

$$\ell'(K) \subseteq \mathrm{Span}(\ell(K)).$$

Proof. By Lemma 1.21, there are at most two K-rational Eckardt points on each of ℓ, ℓ'. Hence

$$\#(\ell(K) \backslash \{\text{Eckardt points}\}) \geq 6.$$

The Gauss map on ℓ has degree 2 so

$$\#\gamma_\ell(\ell(K) \backslash \{\text{Eckardt points}\}) \geq 3.$$

Therefore we must have a non-Eckardt point $P \in \ell(K)$ which maps to a plane $\gamma_\ell(P)$ that intersects ℓ' in a non-Eckardt point Q. We invoke Proposition 2.5 to obtain $\ell'(K) \subseteq \mathrm{Span}(\ell(K))$, which completes the proof. □

Lemma 2.8. *Let K be $\mathbb{F}_4$, $\mathbb{F}_5$ or $\mathbb{F}_8$ and let S be a smooth cubic surface defined over K. Suppose S contains a skew pair of K-lines ℓ, ℓ'. Let $P \in \ell(K)$ be a point*

that is not Eckardt. Then

$$\ell_2(K) \subseteq \mathrm{Span}(\ell_1(K)),$$

where ℓ_1, ℓ_2 is a skew pair of K-lines in S that may or may not be equal to ℓ, ℓ'.

Proof. First note that for any non-Eckardt point $P \in \ell(K)$ we have $\ell(K) \subseteq \mathrm{Span}(P)$ by Lemma 2.4. Suppose $P \in \ell(K)$ is a point such that $\Gamma_P = C \cup \ell$ where C is an irreducible conic. Then $Q = \Pi_P \cdot \ell'$ is a non-Eckardt point by Proposition 2.6. We invoke Lemma 2.4 to obtain

$$\ell'(K) \subseteq \mathrm{Span}(Q) \subseteq \mathrm{Span}(P) \subseteq \mathrm{Span}(\ell(K)).$$

Therefore we may assume that all points in $\ell(K)$ lie on at least one K-line in S other than ℓ. Note that this excludes the case where $\mathrm{char}(K) = 2$ and γ_ℓ is inseparable, since in such cases we must have at least one non-Eckardt point in $\ell(K)$ and by Lemma 1.21 any such P must be parabolic, so Γ_P is the union of ℓ and an irreducible conic. Thus we may assume that γ_ℓ is separable and hence we must have four distinct points P, P', R, $R' \in \ell(K)$ with $\Gamma_P = \Gamma_{P'}$, $\Gamma_R = \Gamma_{R'}$. Let $\ell_1 \subset S$ be the K-line such that $\ell \cdot \ell_1 = P$ and $\ell_2 \subset S$ be the K-line such that $\ell \cdot \ell_2 = R$. Then $\ell_1 \subset \Pi_P$ and $\ell_2 \subset \Pi_R$, $\Pi_P \cdot \Pi_R = \ell$ and $P = \ell \cdot \ell_1 \neq R = \ell \cdot \ell_2$. This is illustrated in Figure 2.12. So

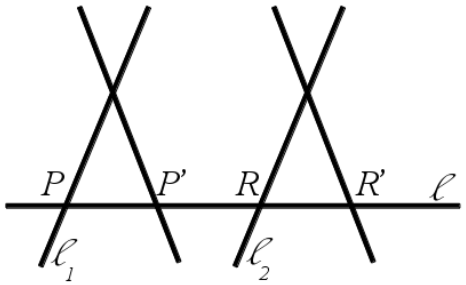

Figure 2.12: ℓ_1 is skew to ℓ_2.

ℓ_1 is skew to ℓ_2. Note that P is a non-Eckardt point on ℓ_1 so $\ell_1(K) \subseteq \mathrm{Span}(P)$ and likewise $\ell_2(K) \subseteq \mathrm{Span}(R) \subseteq \mathrm{Span}(P)$. Hence

$$\ell_1(K) \cup \ell_2(K) \subseteq \mathrm{Span}(P),$$

which completes the proof. □

The following lemma is stated in [20] with the hypothesis that K has at least 13 elements. Using our Lemma 2.4 and by modifying the proof we can strengthen

it as follows.

Lemma 2.9. *Let K be a field with at least 4 elements, and let S be a smooth cubic surface defined over K. Suppose S contains a pair of skew lines ℓ_1 and ℓ_2, both defined over K. If $\#K = 4$ then suppose also that at least one of ℓ_1 and ℓ_2 contains a non-Eckardt K-point. Then*

$$\mathrm{Span}(\ell_1(K) \cup \ell_2(K)) = S(K).$$

Note that for K with $\#K \geq 5$ we automatically have a non-Eckardt point on any K-line in S. The assumption that there is at least one non-Eckardt point in $\ell_1(K) \cup \ell_2(K)$ is one of the hypotheses of Theorem 2.1.

Proof. Let P be a K-point on S not belonging to either line; we will show that P belongs to the span of $\ell_1(K) \cup \ell_2(K)$. Let Π_1 be the unique plane containing ℓ_2 and P, and let Π_2 be the unique plane containing ℓ_1 and P. Since ℓ_1 and ℓ_2 are skew we know that $\ell_i \notin \Pi_i$ for $i = 1, 2$. We write $Q_i = \ell_i \cap \Pi_i$. Note that P, Q_1 and Q_2 are distinct points on S that also belong to the K-line $\ell = \Pi_1 \cap \Pi_2$. Suppose first that $\ell \notin S$. Then $\ell \cdot S = P + Q_1 + Q_2$. Thus $P \in \mathrm{Span}\left(\ell_1(K) \cup \ell_2(K)\right)$ as required.

Next suppose that $\ell \subset S$. If $|K| \geq 5$ we know from Lemma 1.21 that there are non-Eckardt K-points on both ℓ_1 and ℓ_2. If $|K| = 4$ then, by assumption, there is a non-Eckardt K-point on one of ℓ_1 and ℓ_2. Without loss of generality, $R \in \ell_2(K)$ is non-Eckardt.

Now $\ell \subset \Gamma_{Q_1}$. If Q_1 is not Eckardt then by Lemma 2.4 we may conclude that

$$P \in \ell(K) \subseteq \Gamma_{Q_1}(K) \subseteq \mathrm{Span}(Q_1) \subseteq \mathrm{Span}(\ell_1(K)).$$

Thus we may assume that Q_1 is Eckardt. Similarly Q_2 is Eckardt. Then $\Gamma_{Q_1} = \ell \cup \ell_1 \cup \ell_3$ where ℓ_3 is also K-rational. Now ℓ_2 must meet the tangent plane Π_{Q_1} in a unique point; this point is $Q_2 \in \ell$. Therefore, ℓ_2 and ℓ_3 are skew. Consider γ_{ℓ_2}. As Q_2 is Eckardt, it is a ramification point for γ_{ℓ_2}. Therefore $\gamma_{\ell_2}(Q_2) \neq \gamma_{\ell_2}(R)$. Note $\gamma_{\ell_2}(Q_2) \cdot \ell_3 = Q_1$, so $\gamma_{\ell_2}(R) \cdot \ell_3 = R'$ where R' is a K-point distinct from Q_1. Moreover, $R' \in \mathrm{Span}(R) \subseteq \mathrm{Span}(\ell_2(K))$. Finally, consider the line m that joins R' and P. This lies in Π_{Q_1}, but not on S, and so must intersect ℓ_1 in a K-point R''. See Figure 2.13. Hence $P \in \mathrm{Span}(\ell_1(K) \cup \ell_2(K))$ which completes the proof. □

We now restate Theorem 2.1.

Theorem 2.1. *Let K be a field with at least 4 elements. Let S be a smooth cubic surface over K. Suppose S contains a skew pair of lines both defined over K. Let*

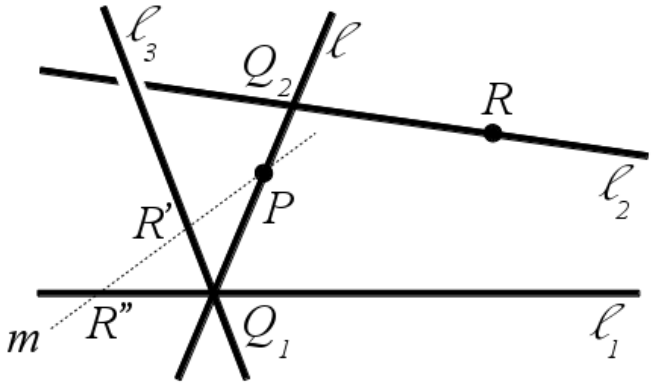

Figure 2.13: $P \in \mathrm{Span}(R', R'') \subseteq \mathrm{Span}(\ell_1(K) \cup \ell_2(K))$.

P be any K-rational point on either line that is not Eckardt. Then

$$\mathrm{Span}(P) = S(K).$$

Proof of Theorem 2.1. If K has 13 or more elements then we can invoke Siksek's Theorem 1.23. Thus we may restrict our attention to the cases $\#K = 4$, 5, 7, 8, 9 and 11. The proof follows from Lemmas 2.4, 2.7, 2.8 and 2.9. □

2.2 Proof of Theorem 2.2

In the proof of Theorem 2.2 we utilise the fact that the secant and tangent operations on a smooth cubic surface can be performed algorithmically. We describe an implementation of this method of point generation in the computer algebra package `MAGMA` [13].

As a secant operation on a cubic surface is not well defined for two points that lie on one of the 27 lines in the surface, it will be useful to have a function that tells us when this is the case. The function `lineOnSurface` takes as input a cubic surface S, denoted `CS` in the `MAGMA` code, defined over a field K and two distinct K-points P, Q on S. It outputs `true` if the K-line through P and Q lies on S, and `false` otherwise.

```
lineOnSurface := function(CS, P, Q);
```

We first assert that the K-points P and Q are distinct.

```
    assert P ne Q;
```

We then detect from S its defining polynomial F.

```
        DE:=DefiningEquations(CS);
        assert #DE eq 1;
        F:=DE[1];
```

We check that P and Q do indeed satisfy $F = 0$ and hence are on S.

```
        assert Evaluate(F,[P[i] : i in [1..4]]) eq 0;
        assert Evaluate(F,[Q[i] : i in [1..4]]) eq 0;
```

The following lines detect K, the field of definition for S.

```
        Kxyzw:=Parent(F);
        K:=BaseRing(Kxyzw);
```

We now parametrise the line passing through P and Q in terms of parameters s and t and find G, the defining polynomial of the intersection of S with this line.

```
        Kst<s,t>:=PolynomialRing(K,2);
        G:=Evaluate(F,[ s*P[i]+t*Q[i] : i in [1..4] ]);
```

Note that the coefficient of s^3 in G is $F(P) = 0$ and likewise the coefficient of t^3 is $F(Q) = 0$. Hence the line through P and Q is contained in S if and only if the coefficients of s^2t and st^2 are both zero.

```
        alpha:=MonomialCoefficient(G,s^2*t);
        beta:=MonomialCoefficient(G,s*t^2);
        if alpha eq 0 and beta eq 0 then
                return true;
        else
                return false;
        end if;
end function;
```

The function `secantspan` takes as input a cubic surface S (once again defined as `CS` in the `MAGMA` code) defined over a field K and two distinct points $P, Q \in S(K)$, and returns the set of points generated from P and Q using only the secant operation and not the tangent operation. This set will be $\{P, Q\}$ if the line through P and Q, ℓ, is contained in S, otherwise it will be $\{P, Q, R\}$ where $\ell \cdot S = P + Q + R$. As with `lineOnSurface` we start by confirming that $P \neq Q$, detecting the defining polynomial of S (which we denote by F), asserting that $P, Q \in S(K)$ and detecting the field K over which S is defined.

```
secantspan := function(CS, P, Q);
        assert P ne Q;
        DE:=DefiningEquations(CS);
        assert #DE eq 1;
        F:=DE[1];
        assert Evaluate(F,[P[i] : i in [1..4]]) eq 0;
        assert Evaluate(F,[Q[i] : i in [1..4]]) eq 0;
        Kxyzw:=Parent(F);
        K:=BaseRing(Kxyzw);
```

In the same way as in `lineOnSurface` we determine whether ℓ is in S. We do not call `lineOnSurface` because if $\ell \notin S$ we will require the coefficients of s^2t and st^2 to compute R. We then return $\{P, Q\}$ or $\{P, Q, R\}$ accordingly.

```
        Kst<s,t>:=PolynomialRing(K,2);
        G:=Evaluate(F,[ s*P[i]+t*Q[i] : i in [1..4] ]);
        alpha:=MonomialCoefficient(G,s^2*t);
        beta:=MonomialCoefficient(G,s*t^2);
        if alpha eq 0 and beta eq 0 then
                return {P,Q};
        else
                R:=CS![ beta*P[i]-alpha*Q[i] : i in [1..4] ];
                return {P,Q,R};
        end if;
end function;
```

We can now define the `span` function, which finds $\operatorname{Span}\Sigma$ for a non-empty set of points $\Sigma \subseteq S(K)$. The function `span` takes as input a cubic surface S, denoted `CS` in the `MAGMA` code, defined over a finite field K; a non-empty set $\Sigma \subseteq S(K)$, denoted `pts` in the code; and $S(K)$, denoted `CSpoints` in the code. We start by detecting the defining polynomial of S, denoted F.

```
span:=function(CS,pts,CSpoints);
        DE:=DefiningEquations(CS);
        assert #DE eq 1;
        F:=DE[1];
```

We then call `secantspan` to perform secant operations on any distinct pairs of points in Σ.

```
ptsnew:=pts;
for P,Q in pts do
        if P ne Q then
                ptsnew:=ptsnew join secantspan(CS,P,Q);
        end if;
end for;
```

In order to execute tangent operations we need to find $\nabla(F)(P)$, denoted in the code by `gFP`, for every point in Σ.

```
gF:=[Derivative(F,i) : i in [1..4] ];
for P in pts do
gFP:=[ Evaluate(g,[ P[i] : i in [1..4]  ] ) : g in gF  ];
```

We then find $\Gamma_P(K)$, denoted here by `GammaPpoints`.

```
GammaPpoints:=
[ Q: Q in CSpoints | &+[ gFP[i]*Q[i] : i in [1..4]   ]  eq 0 ];
```

Any points in $\Gamma_P(K)$ that do not lie on a line in S through P are generated from P by a tangent operation. These points are added to a placeholder set `ptsnew`. When we have done all the possible tangent and secant operations on the points of Σ the code will run again with `ptsnew` replacing Σ. One should perhaps note that this step only works when K is a finite field as otherwise there could be infinitely many points in $\Gamma_P(K)$.

```
for Q in GammaPpoints do
        if Q ne P then
                if lineOnSurface(CS,P,Q) eq false then
                        ptsnew:=ptsnew join {Q};
                end if;
        end if;
end for;
end for;
```

If `ptsnew` and Σ are the same then the algorithm has terminated. Otherwise the program iterates until process stabilises. This is guaranteed to terminate for when K is finite because $|S(K)|$ will be finite.

```
if ptsnew eq pts then
        return pts;
```

```
        else
                return $$(CS,ptsnew,CSpoints);
        end if;
end function;
```

Finally, the `isgenerator` function has an input of a cubic surface S, again denoted `CS` in the code, defined over a finite field K and a point $P \in S(K)$. It returns `true` if $\mathrm{Span}(P) = |S(K)|$ and `false` otherwise.

```
isgenerator:=function(CS,P);
        CSpoints:=Points(CS);
        CSpoints:={Q : Q in CSpoints};
        return span(CS,{P},CSpoints) eq CSpoints;
end function;
```

These programs were used in proving the following lemma.

Lemma 2.10. *Let $K = \mathbb{F}_3$ and let S be a smooth cubic surface defined over K. Suppose S contains a skew pair of K-lines ℓ, ℓ' and suppose ℓ contains exactly one K-rational Eckardt point. Then there exists a non-Eckardt point $R \in \ell(K)$ such that*

$$S(K) = \mathrm{Span}(R).$$

Proof. The lemma was proved by an exhaustive computer enumeration implemented in `MAGMA` [13]. By a projective change of coordinates we may first suppose that the line ℓ is defined by $X = Y = 0$ and that therefore the surface S has the form $XQ_1 + YQ_2$, where $Q_1 \in \mathbb{F}_3[X, Y, Z, W]$ and $Q_2 \in \mathbb{F}_3[Y, Z, W]$ are homogeneous quadratic forms. We may then by further projective changes of coordinates suppose that the K-rational Eckardt point on ℓ is the point $P = (0 : 0 : 0 : 1)$. We denote the other two lines in S passing through P by ℓ_1 and ℓ_2. The line ℓ' must intersect the plane Π_P in some K-point $Q \neq P$. As ℓ and ℓ' are skew, $Q \notin \ell$ and so without loss of generality $Q \in \ell_1$. The line ℓ_1 joins two K-points and is therefore a K-line. Hence ℓ_2 is also a K-line. By yet another change of coordinates that preserves ℓ and P, we may suppose that ℓ_1 and ℓ_2 have the equations $\ell_1 : X = Z = 0$ and $\ell_2 : X = Y + Z = 0$. Thus every cubic surface defined over $\mathbb{F}_3$ containing a skew pair of K-lines has a model that can be written in the form

$$X(aX^2 + bXY + cXZ + dY^2 + eY + fZ^2 + gW^2) + YZ(Y + Z)$$

where $a, \ldots, g \in \mathbb{F}_3$. Therefore the program was enumerated over $3^7 = 2187$ cubic surfaces. The program checked the surfaces for smoothness, then whether there was

a point $R \in \ell(K)$ such that $\mathrm{Span}(R) = S(K)$. In the cases where this failed, we verified that there was a second Eckardt point in $\ell(K)$. □

The proofs of the remaining cases in which there are no K-rational Eckardt points on either ℓ or ℓ' result from the following lemmas.

Lemma 2.11. *Let $K = \mathbb{F}_3$ and let S be a smooth cubic surface defined over K. Let ℓ be a K-line on S that does not contain any K-rational Eckardt points. Let $P \in \ell(K)$ be a point that does not lie on any other line belonging to S. Then*

$$\ell(K) \subseteq \Gamma_P(K) \subseteq \mathrm{Span}(P).$$

Proof. If P is a parabolic point then, as in the proof of Lemma 2.3, we know that $\Gamma_P(K) \subseteq \mathrm{Span}(P)$. Otherwise there is a point $P' \in \ell(K)$ such that $P' \neq P$ but $\Gamma_{P'} = \Gamma_P$. In this case, similarly to the proof of Lemma 2.3, we have

$$\Gamma_P(K) \backslash \{P'\} \subseteq \mathrm{Span}(P).$$

As $K = \mathbb{F}_3$ there are four points in $\ell(K)$: P, P', R and R'. If $\Gamma_R = \ell \cup C$ where C is an irreducible conic then $P' \in \mathrm{Span}(R) \subseteq \mathrm{Span}(P)$. Hence $\Gamma_P(K) \subseteq \mathrm{Span}(P)$. Otherwise $\Gamma_R = \Gamma_{R'}$ and is the union of 3 K-lines in S, which are ℓ, ℓ_2 and ℓ_3, where $\ell \cdot \ell_2 = R$, $\ell \cdot \ell_3 = R'$ and $\ell_2 \cdot \ell_3 = R''$. We know that $(\ell_2(K) \cup \ell_3(K)) \backslash \{R''\} \subseteq \mathrm{Span}(R, R')$ and $P' \in \mathrm{Span}((\ell_2(K) \cup \ell_3(K) \backslash \{R''\})$. Thus

$$\ell(K) \subseteq \Gamma_P(K) \subseteq \mathrm{Span}(P)$$

which completes the proof. □

Lemma 2.12. *Let $K = \mathbb{F}_3$ and let S be a smooth cubic surface defined over K. Suppose S contains a skew pair of K-lines, ℓ and ℓ', that contains no K-rational Eckardt points. Then there is a point $P \in \ell(K)$ such that*

$$\ell(K) \subseteq \Gamma_P(K) \subseteq \mathrm{Span}(P).$$

Proof. If there is a point in $\ell(K)$ that lies on no other line in S then the result follows from Lemma 2.11. Suppose that every point in $\ell(K)$ lies on exactly one other K-line in S. Since $K = \mathbb{F}_3$ there are 4 points in $\ell(K)$, which we denote P, P', R, R'. We have $\Gamma_P = \Gamma_{P'} = \ell \cup \ell_1 \cup \ell_2$ with $P = \ell \cdot \ell_1$, $P' = \ell \cdot \ell_2$ and $\Gamma_R = \Gamma_{R'}$ with $R = \ell \cdot \ell_3$, $R' = \ell \cdot \ell_4$. Let $P'' = \ell_1 \cdot \ell_2$. By the argument in the proof of Lemma 2.10 we know that ℓ' intersects precisely one of ℓ_1, ℓ_2 and one of ℓ_3, ℓ_4. Without loss

of generality suppose that ℓ' intersects ℓ_2 and ℓ_4. By our hypotheses ℓ' contains no K-rational Eckardt points, therefore the point $Q = \ell' \cdot \ell_2$ is non-Eckardt. Note that $Q \in (\ell_2(K) \backslash \{P', P''\}) \subseteq \mathrm{Span}(P)$. Let Q' be the remaining point in $\ell_2(K) \backslash \{P', P''\}$. Our aim is to show that P', $P'' \in \mathrm{Span}(P)$ since we can generate all the remaining points in $\ell(K)$ and $\ell_1(K)$ from P'' and P' respectively. If Q is a parabolic point then

$$P', P'' \in \ell_2(K) \subseteq \mathrm{Span}(Q) \subseteq \mathrm{Span}(P).$$

Likewise if $\Gamma_Q = \Gamma_{Q'}$ then

$$P', P'' \in \ell_2(K) \subseteq \mathrm{Span}(Q, Q') \subseteq \mathrm{Span}(P),$$

which completes the proof. □

Lemma 2.13. *Let $K = \mathbb{F}_3$ and let S be a smooth cubic surface defined over K. Suppose S contains a skew pair of K-lines ℓ and ℓ' that contains no K-rational Eckardt points. Then*

$$\ell'(K) \subseteq \mathrm{Span}(\ell(K)).$$

Proof. Let $P \in \ell(K)$. By Lemma 2.12 we know that $Q = \Pi_P \cdot \ell' \in \Gamma_P \subseteq \mathrm{Span}(P)$. We invoke Lemma 2.12 again to obtain

$$\ell'(K) \subseteq \mathrm{Span}(Q) \subseteq \mathrm{Span}(P) \subseteq \mathrm{Span}(\ell(K)).$$

□

Lemma 2.14. *Let $K = \mathbb{F}_3$ and let S be a smooth cubic surface defined over K. Suppose S contains a skew pair of K-lines ℓ_1 and ℓ_2, which contains no K-rational Eckardt points. Then*

$$\mathrm{Span}(\ell_1(K) \cup \ell_2(K)) = S(K).$$

Proof. This proof is similar to the proof of Lemma 2.9. Let P be a K-point on S not belonging to either line; we will show that P belongs to the span of $\ell_1(K) \cup \ell_2(K)$. Let Π_1 be the unique plane containing ℓ_2 and P, and Π_2 the unique plane containing ℓ_1 and P. Since ℓ_1 and ℓ_2 are skew we know that $\ell_i \notin \Pi_i$. Write $Q_i = \ell_i \cap \Pi_i$. Note that P, Q_1 and Q_2 are distinct points on S that also belong to the K-line $\ell = \Pi_1 \cap \Pi_2$. Suppose first that $\ell \notin S$. Then $\ell \cdot S = P + Q_1 + Q_2$. Thus $P \in \mathrm{Span}\left(\ell_1(K) \cup \ell_2(K)\right)$ as required.

Next suppose that $\ell \subset S$. This implies that $\ell \subset \Gamma_{Q_1}$ and, since Q_1 is not

Eckardt, then by Lemma 2.12,

$$P \in \ell(K) \subseteq \Gamma_{Q_1}(K) \subseteq \mathrm{Span}(Q_1) \subseteq \mathrm{Span}(\ell_1(K)),$$

which completes the proof. □

Theorem 2.2. *Let $K = \mathbb{F}_3$. Let S be a smooth cubic surface over K. Suppose S contains a skew pair of lines ℓ and ℓ' defined over K and that ℓ and ℓ' each contain at most one K-rational Eckardt point. Then there exists a point $P \in \ell(K) \cup \ell'(K)$ such that* $\mathrm{Span}(P) = S(K)$.

Proof of Theorem 2.2. The proof follows from Lemmas 2.12, 2.13, 2.14 and 2.10. □

Chapter 3

Cubic surfaces containing one rational line

In this chapter we discuss the results obtained for cubic surfaces containing one rational line over $K = \mathbb{F}_q$ where $q \geq 8$ or $q = 2$. Lemma 3.3 also works for infinite fields of characteristic 2.

The main result of this chapter is the following theorem.

Theorem 3.1. *Let $K = \mathbb{F}_q$ be a finite field with $q \geq 8$. Let S be a smooth cubic surface defined over K containing at least one K-rational line. Then there exists a point $P \in S(K)$ such that* $\mathrm{Span}(P) = S(K)$.

We also prove the following partial result for cubic surfaces over $\mathbb{F}_2$ via a computer enumeration. This is part of the paper [6], which forms the basis for Chapter 2.

Theorem 3.2. *Let $K = \mathbb{F}_2$. Let S be a smooth cubic surface over K. Suppose S contains a line ℓ defined over K that does not contain any K-rational Eckardt points. Then there exists a point $P \in \ell(K)$ such that* $\mathrm{Span}(P) = S(K)$.

In Theorem 1.24, we saw a family of cubic surfaces over $K = \mathbb{Q}$, each containing a K-line, for which there exists no point $P \in S(K)$ such that $\mathrm{Span}(P) = S(K)$, and in fact the number of points required to generate $S(K)$ is unbounded as S ranges through the cubic surfaces in this family. This indicates that the behaviour of the secant and tangent process over finite fields is notably different to that over $\mathbb{Q}$.

3.1 Types of K-planes through $\ell \subset S$

For a smooth cubic surface S defined over a field K by Lemma 1.18 we know that if S contains four K-lines then it must contain a skew pair. Due to Theorem 2.1 we need only prove Theorem 3.1 for cubic surfaces over K containing no more than three K-lines, all of which must be coplanar.

We note that any K-line ℓ in $\mathbb{P}^3_K$ is a copy of $\mathbb{P}^1_K$ and hence when $K = \mathbb{F}_q$ we have $|\ell(K)| = q + 1$. Proposition 1.19 states that there are exactly ten $\overline{K}$-lines in S intersecting any given $\overline{K}$-line in S. Thus there are at most 5 Eckardt points in $\ell(K)$. This along with Lemma 1.21 implies that when $q = 3$ or $q \geq 5$ we are guaranteed the existence of a non-Eckardt point in $\ell(K)$.

Let $K = \mathbb{F}_q$ and S, a cubic surface defined over K. Let $\ell \subset S$ be a K-line. There is a pencil of planes passing through ℓ, hence there is a bijection between rational points in $\mathbb{P}^1_K$ and K-planes through ℓ. Therefore there are exactly $q + 1$ distinct K-planes through ℓ. Let Π be any such plane and $\Gamma = \Pi \cdot S$. Then $\Gamma = \ell \cup C$ where C is some conic defined over K that may be absolutely irreducible or may decompose into two lines. The possible cases are enumerated below.

(1) C is absolutely irreducible and meets ℓ in two distinct K-points.

(2) C decomposes into two K-lines, m and m', and $m \cdot \ell \neq m' \cdot \ell$.

(3) C is absolutely irreducible and meets ℓ in two distinct points that are not K-points but are defined over $\mathbb{F}_{q^2}$ and are Galois conjugates.

(4) C decomposes into two Galois conjugate lines m and m' that are defined over $\mathbb{F}_{q^2}$ but not K. We have that $m \cdot m'$ is a K-point, that $m \cdot \ell \neq m' \cdot \ell$ and that $m \cdot \ell$ and $m' \cdot \ell$ are defined over $\mathbb{F}_{q^2}$ but are not K-points.

(5) C is absolutely irreducible and ℓ is tangent to C, so meeting C in exactly one K-point.

(6) C decomposes into two K-lines, m and m' with $m \cdot \ell = m' \cdot \ell$, and hence is an Eckardt point in $\ell(K)$.

(7) C decomposes into two Galois conjugate lines m, m', that are defined over $\mathbb{F}_{q^2}$ but not K. We have $m \cdot \ell = m' \cdot \ell$, and hence is an Eckardt point in $\ell(K)$.

Note that in case (7) we have $\Gamma(K) = \ell(K)$ since there are no K-points on m and m' other than the intersection point $m \cdot \ell = m' \cdot \ell = m \cdot m'$.

For the remainder of this thesis, given a K-line $\ell \subset S$, we will refer to a K-plane through ℓ as being "of type (n)", $n = 1, \ldots, 7$, when it falls into case (n)

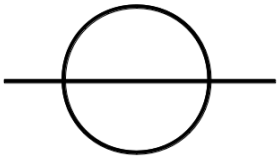

Figure 3.1: Case (1).

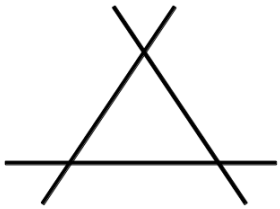

Figure 3.2: Case (2).

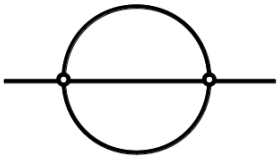

Figure 3.3: Case (3).

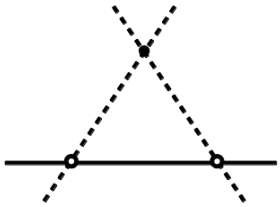

Figure 3.4: Case (4).

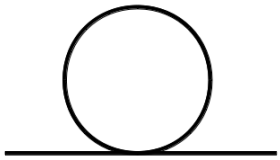

Figure 3.5: Case (5).

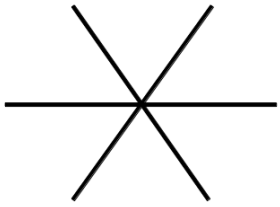

Figure 3.6: Case (6).

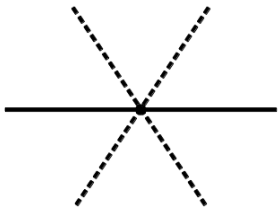

Figure 3.7: Case (7).

above. A cubic curve $\Gamma = \Pi \cdot S$, for some Π through ℓ, is also said to be of type (n) if Π is of type (n). A point $P \in \ell(K)$ is said to be of type (n) if Π_P is of type (n) and a plane conic $C \subset S$ intersecting ℓ is of type (n) if $\Gamma = C \cup \ell$ is of type (n).

In cases (5), (6) and (7) the conic C intersects the line ℓ in a single point. Such a point P is a parabolic point and Π is the tangent plane to S at P denoted Π_P. In fact these are the only possibilities for parabolic points in $\ell(K)$. The number of parabolic points on ℓ is determined by whether the Gauss map on ℓ is separable or inseparable as described in Chapter 1. We deal with the special case where $\mathrm{char}(K) = 2$ and γ_ℓ is inseparable separately.

3.2 Theorem 3.1 when γ_ℓ is inseparable

For S a smooth cubic surface defined over a field K of characteristic 2 and containing a K-line ℓ we can prove Theorem 3.1 directly without invoking a pigeonhole principle. This result also holds for infinite fields of characteristic 2.

Lemma 3.3. *Let K be a field of characteristic 2 containing at least 8 elements. Let S be a smooth cubic surface defined over K containing at least one K-line ℓ upon which the Gauss map γ_ℓ is inseparable. Let $P \in \ell(K)$ be a non-Eckardt point. Then*

$$\mathrm{Span}(P) = S(K).$$

Proof. Since γ_ℓ is inseparable every K-point on ℓ is parabolic. Therefore $\gamma_\ell(\ell(K)) \cong \mathbb{P}^1_K$, i.e. each plane in the pencil of K-planes through ℓ is Π_P for some $P \in \ell(K)$. Every plane containing ℓ and a point $R \in S(K)\backslash\ell(K)$ is a K-plane and so is Π_P for some $P \in \ell(K)$. Therefore every point $R \in S(K)\backslash\ell(K)$ is in $\Gamma_P(K)$ for some $P \in \ell(K)$. Hence

$$S(K) = \bigcup_{P \in \ell(K)} \Gamma_P(K).$$

By Proposition 1.19, there are at most five Eckardt points in $\ell(K)$. If more than one of these Eckardt points is of type (6) then we have more than three K-lines in S and hence a skew pair. Thus we apply Theorem 2.1 to obtain the result.

We may assume that there is at most one Eckardt point of type (6) in $\ell(K)$. Let $P \in \ell(K)$ be a non-Eckardt point. By Lemma 2.4 we have $\ell(K) \subset \Gamma_P(K) \subseteq \mathrm{Span}(P)$. Applying Lemma 2.4 again gives us that $\Gamma_Q(K) \subset \mathrm{Span}(P)$ for all non-Eckardt points $Q \in \ell(K)$. Hence if there are no Eckardt points of type (6) in $\ell(K)$ then we have $\bigcup_{P \in \ell(K)} \Gamma_P \subseteq \mathrm{Span}(P)$ so $\mathrm{Span}(P) = S(K)$.

Suppose that there is an Eckardt point of type (6) in $\ell(K)$, which we will denote E, and let the other two K-lines in S through E be denoted ℓ', ℓ''. Suppose there is a fourth K-line in S. Then by Lemma 1.18 there is a pair of skew K-lines in S, so we can invoke Theorem 2.1. We may assume that ℓ, ℓ', ℓ'' are the only K-lines in S.

By Lemma 2.4 we know that

$$\bigcup_{R \in \ell(K)\backslash\{E\}} \Gamma_R(K) \subseteq \mathrm{Span}(P).$$

Let $G := S(K)\backslash\Gamma_E(K)$ and let $Q \in \Gamma_E(K)\backslash\ell(K)$. Note that $G \subset \mathrm{Span}(\ell(K)) \subseteq \mathrm{Span}(P)$ by Lemma 2.4. We want to show that $Q \in \mathrm{Span}(P)$. It is sufficient to find two points R, $R' \in G$ such that Q, R and R' are collinear. Note that these points

cannot lie on a K-line in S since R, $R' \notin \Pi_E$ and therefore the line through Q, R and R' is not one of ℓ, ℓ' or ℓ''. Choose $P' \in \ell(K)$ that is non-Eckardt. Then P' is a point of type (5) and $\Gamma_{P'} = C \cup \ell$, where C is an absolutely irreducible conic over K.

The intersection $m = \Pi_Q \cdot \Pi_{P'}$ is a K-line not contained in S and hence intersects C in two points counting multiplicities which we will denote P_1, $P_2 \in C(\overline{K})$. In fact $m \cdot S = P_1 + P_2 + E$ since $E \in \ell \subset \Pi_P$ and $E \in \ell' \subset \Pi_Q$ so $E \in m = \Pi_P \cdot \Pi_Q$. Let $R \in C(K)$, $R \notin m(K)$. Let m' be the line joining Q and R. Note that $m' \notin S$ so $m' \cdot S = Q + R + R'$ for some $R' \in S(K)$. We know that $R \in \Pi_{P'}$, but $R \notin \Pi_Q \cdot \Pi_{P'}$ so $R \notin \Pi_Q$. See Figure 3.8. Therefore $R' \neq Q$ and hence $Q \in \mathrm{Span}(R, R') \subseteq \mathrm{Span}(P)$,

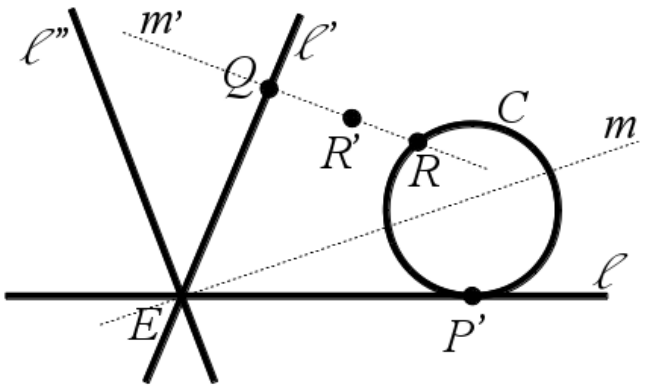

Figure 3.8: Special case of generating $P \in S(K) \backslash \ell(K)$ when γ_ℓ is inseparable. Observe that ℓ' and ℓ'' lie in a different plane to C.

from which the result follows. □

3.3 A pigeonhole principle for cubic surfaces over finite fields

The following theorem explains the pigeonhole principle required to prove Theorem 3.1 for the remaining cases where γ_ℓ is separable.

Theorem 3.4. *Let S be a smooth cubic surface over $K = \mathbb{F}_q$. Let $T \subseteq S(K)$ be such that $\ell(K) \subseteq T$ for all K-lines ℓ contained in S, and $|T| > \frac{1}{2}|S(K)| + \frac{q+1}{2}$. Then*

$$\mathrm{Span}(T) = S(K).$$

Proof. Suppose we wish to generate a point $Q \notin T$ and hence not lying on any K-line

in S. In order to generate Q we require points R, $R' \in T$ and a K-line m such that $m \cdot S = R + R' + Q$. Note that we may have $R = R'$, in which case Q is generated via a tangent operation on R. The points Q and R must be distinct since $R \in T$ and $Q \in T' = S(K) \backslash T$, and hence they uniquely determine m. Furthermore a point $R \in \Gamma_Q(K)$ can never belong to a pair of points R and R' that generate Q since then we would have $m \cdot S = 2Q + R + R'$, which would contradict the fact that m intersects S exactly three times counting multiplicities. We define the following sets of points in $S(K)$:

$$G = T \backslash \Gamma_Q(K),$$
$$B = T' \backslash \{Q\}.$$

The idea of the proof is as follows: we will define a map $\phi : G \to B$ and show that if Q cannot be generated from the points in G (and hence T) then ϕ is injective. We will show that if $|T| > \frac{1}{2}|S(K)| + \frac{q+1}{2}$ then $|G| > |B|$ contradicting the injectivity of ϕ. It will follow that $(S(K) \backslash T) \cup G \subseteq \mathrm{Span}(G)$ and since $\mathrm{Span}(G) \subseteq \mathrm{Span}(T)$ and $T \subseteq \mathrm{Span}(T)$ we will have $S(K) = \mathrm{Span}(T)$.

Suppose $Q \notin \mathrm{Span}(G)$. For any $R \in G$ let m be the unique K-line joining Q and R. Since $G = T \backslash \Gamma_Q(K)$ we know that $m \notin S$ by Lemma 1.16. Therefore $m \cdot S = Q + R + Q'$ where $Q' \in S(K)$, $Q' \neq Q$ and is uniquely determined by m. Since $Q \notin \mathrm{Span}(G)$ we must have $Q' \in B$. This defines an injective map $\phi : G \to B$ with $\phi(R) = Q'$ since two distinct points uniquely define a line in $\mathbb{P}^3_K$. See Figure 3.9.

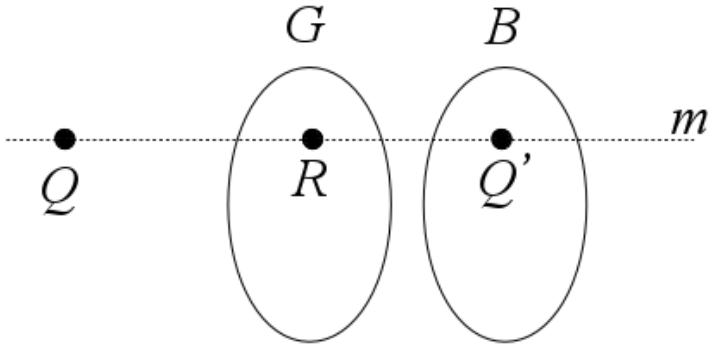

Figure 3.9: Generating $Q \in S(K)$ using a pigeonhole principle.

It now remains to show that if $|T| > \frac{1}{2}|S(K)| + \frac{q+1}{2}$ then $|G| > |B|$. Since Q is a K-point and does not lie on any K-lines in S we know that either Γ_Q is the union of three lines defined over a cubic extension of K that are Galois conjugates and

Form of Γ_Q	$\#\Gamma_Q(K)$
3 $\mathbb{F}_{q^3}$-lines and Q Eckardt	1
cusp at Q	$q+1$
split node at Q	q
non-split node at Q	$q+2$

Table 3.1: Size of $\Gamma_Q(K)$

that Q is an Eckardt point, or that Γ_Q is an irreducible cubic curve with a singular point at Q. Table 3.1 gives the possibilities for the size of $\Gamma_Q(K)$ taken from [11]. Recall that

$$|T| > \frac{1}{2}|S(K)| + \frac{q+1}{2},$$

and that

$$|\Gamma_Q(K)| \leq q+2.$$

From this we obtain the following chain of inequalities:

$$\begin{aligned}
|G| &= |T \backslash \Gamma_Q(K)| \\
&\geq |T| - (q+2) \\
&> \left(\tfrac{1}{2}|S(K)| + \tfrac{q+1}{2}\right) - (q+2) \\
&= |S(K)| - \left(\tfrac{1}{2}|S(K) + \tfrac{q+1}{2}\right) - 1 \\
&> |S(K) - |T| - 1 \\
&= |S(K) \backslash T| - 1 \\
&= |T' \backslash \{Q\}| \\
&= |B|,
\end{aligned}$$

which completes the proof. □

3.4 Proof of Theorem 3.1

It now remains to show that we can generate enough K-points on S to apply the pigeonhole principle. We will use the following lemmas.

Lemma 3.5. *Let S be a smooth cubic surface defined over a field K and containing at least one K-line. Then, if E is an Eckardt point in $S(K)$, E must lie on a K-line in S.*

Proof. Since E is a K-point, Π_E must be a K-plane. We know that Γ_E must split into three linear components over $\overline{K}$ and so we have the following three options.

1. Γ_E is the union of three K-lines in S,

2. Γ_E is the union of one K-line in S and two Galois conjugate lines in S that are defined over a quadratic extension of K,

3. Γ_E is the union of three Galois conjugate lines in S that are each defined over a cubic extension of K.

In the first two cases E lies on a K-line in S so we will consider the third case. Let $\ell \subset S$ be a K-line and suppose that there is an Eckardt point $E \in S(K)$ that does not lie on any K-line in S. Let $Q = \Pi_E \cdot \ell$. Note that $Q \in S(K)$ since it is the intersection of a K-line with a K-plane. But the only K-point in Γ_E is $E \notin \ell$, hence we reach a contradiction. □

Lemma 3.6. *Let S be a smooth cubic surface defined over a field K containing at least one K-line, ℓ, and no pair of skew K-lines. Let Π be a K-plane that passes through ℓ such that $\Gamma = \Pi \cdot S$ is of type (1), (3) or (5) and $\Gamma = C \cup \ell$. Let $P \in C(K) \backslash \ell(K)$. Then P does not lie on a K-line in S.*

Proof. Suppose $P \in C(K) \backslash \ell(K)$ lies on a K-line in S, which we will denote by m. By the hypotheses of the lemma, m cannot be skew to ℓ therefore m is coplanar to ℓ and hence contained in Π. Thus $m \cup \ell \cup C \subset \Gamma$. But Γ is a plane cubic curve so we arrive at a contradiction and P does not lie on a K-line in S. □

Lemma 3.7. *Let K be a field containing at least 4 elements. Let S be a smooth cubic surface defined over K containing exactly three K-lines, ℓ_1, ℓ_2 and ℓ_3, upon each of which the Gauss map γ_{ℓ_i} is separable and ℓ_1, ℓ_2, ℓ_3 meet in an Eckardt point E. Suppose that ℓ_2 contains no K-rational Eckardt point other than E. Then, up to relabelling of the three lines,*

$$\ell_2(K) \cup \ell_3(K) \subset \mathrm{Span}(\ell_1(K)).$$

Proof. We aim to generate a non-Eckardt point $R \in \ell_2(K)$ from $\ell_1(K)$ so we may invoke Lemma 2.4 to obtain $\ell_2(K) \subset \mathrm{Span}(\ell_1(K))$. Secant operations on the points of $\ell_1(K) \cup \ell_2(K)$ will then give the result.

Let $P \in \ell_1(K)$, $P \neq E$ be a non-parabolic point. We know that Γ_P must be of type (1) since ℓ_1, ℓ_2, ℓ_3 are the only K-lines in S, and $\Gamma_P = C \cup \ell_1$, with P' the K-point such that $C \cdot \ell_1 = P + P'$, $P \neq P'$.

We observe that secant operations on the points of $C(K)$ only generate K-points in Π_P. The tangent plane Π_Q of any point $Q \in C(K)$ will either contain the line ℓ_2 or meet it in exactly one K-point.

If we are in the case where $\ell_2 \subset \Pi_Q$ then for any point R in $\ell_2(K)$ the K-line m joining R and Q is not contained in S by Lemma 3.6. Therefore $\ell_2(K)$ is generated from Q via tangents operations and $\ell_2(K) \subset \mathrm{Span}(Q) \subseteq \mathrm{Span}(P) \subseteq \mathrm{Span}(\ell_1(K))$. $\ell_3(K)$ is then generated by secant operations on the points of $\ell_1(K)$ and $\ell_2(K)$, so $\ell_3(K) \subset \mathrm{Span}(\ell_1(K) \cup \ell_2(K)) \subseteq \mathrm{Span}(\ell_1(K))$, which completes the proof in this case.

Otherwise we are in the case where Π_Q meets ℓ_2 in exactly one K-point, which we will denote by R. If $Q = P$ or P' then $R = E$ and we cannot generate $\ell_2(K)$ from R. We suppose that $Q \neq P, P'$. Then $Q \notin \Pi_E$ so the K-line m joining Q and R is not equal to ℓ_1, ℓ_2 or ℓ_3 and hence $m \notin S$. Therefore $R \in \mathrm{Span}(Q) \subseteq \mathrm{Span}(P)$.

It remains to show that there is a choice of Q for which $R \neq E$. Note that the tangent line to C at a point $Q \in C(\overline{K})\backslash\{P, P'\}$ in Π_P is precisely the intersection $\Pi_P \cdot \Pi_Q$. There are exactly two points $Q_1, Q_2 \in C(\overline{K})$ such that the tangent lines to C at the Q_i in Π_P pass through E, i.e. Q_1 and Q_2 are the only points in $C(\overline{K})$ such that $\Pi_{Q_i} \cdot \ell_2 = E$. See Figure 3.10.

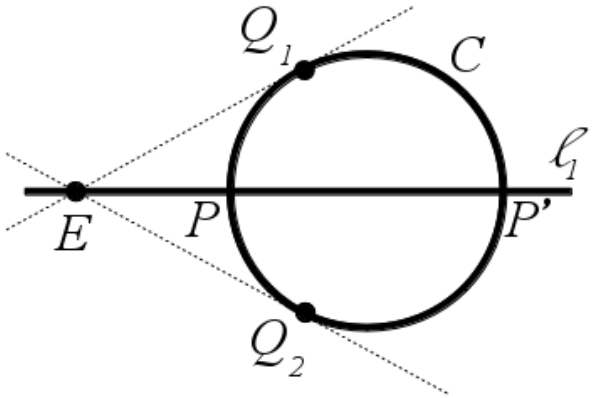

Figure 3.10: Tangent operations on Q_1 and Q_2 only generate E in $\ell_2(K)$.

Let $Q \in C(K)\backslash\{P, P', Q_1, Q_2\}$. Then Π_Q is a K-plane and intersects ℓ_2 in exactly one K-point, $R \neq E$. By Lemma 3.5 Q is not Eckardt, therefore by Lemma 2.4

$$R \in \mathrm{Span}(Q) \subseteq \mathrm{Span}(P) \subseteq \mathrm{Span}(\ell_1(K)).$$

By applying Lemma 2.4 we see that

$$\ell_2 \subset \mathrm{Span}(R) \subset \mathrm{Span}(\ell_1(K)).$$

We perform secant operations on the points of $\ell_1(K)$ and $\ell_2(K)$ to obtain

$$\ell_3(K) \subset \mathrm{Span}(\ell_1(K) \cup \ell_2(K)),$$

from which the result follows. □

Lemma 3.8. *Let K be a field containing at least 8 elements. Let S be a smooth cubic surface defined over K containing exactly three K-lines, ℓ_1, ℓ_2 and ℓ_3, that meet in a K-rational Eckardt point E. Then, up to relabelling the three lines, we have*

$$\ell_2(K) \cup \ell_3(K) \subset \mathrm{Span}(\ell_1(K)).$$

Proof. If the characteristic of K is 2, then the result follows from Lemmas 3.3 and 3.7. If any of ℓ_1, ℓ_2 and ℓ_3 contains no K-rational Eckardt points other than E then, after possibly relabelling ℓ_1, ℓ_2 and ℓ_3, the result follows from Lemma 3.7.

The case remains where each of ℓ_i, $i = 1, 2, 3$, contains precisely one K-rational Eckardt point of type (7) other than E, which we will denote by E_i respectively. To resolve this case we aim to show that one can choose a point $Q \in \Gamma_P(K)$ for some non-Eckardt point $P \in \ell_1(K)$ that generates a non-Eckardt point $R \in \ell_2(K)$ via a tangent operation. We find this choice of Q by avoiding points in the set $\{Q \in S(K) | \Pi_Q \cdot \ell_2 \text{ is Eckardt}\}$.

Let $P \in \ell_1(K)$ be a non-parabolic point. Then Γ_P is of type (1) since ℓ_1, ℓ_2 and ℓ_3 are the only K-lines in S, so $\Gamma_P = C \cup \ell_1$, denoting by P' the K-point such that $C \cdot \ell_1 = P + P'$. We want to prove the existence of a point in $Q \in C(K) \backslash \{P, P'\}$ such that a non-Eckardt point $R \in \ell_2(K)$ lies in Π_Q.

After a change of coordinates and dehomogenising, assume that $E_2 = (0, 0, 0)$, and let Π_P be the plane $x = 1$. Since E_2 lies on S we can write the equation of S as

$$L(x, y, z) + Q(x, y, z) + C(x, y, z) = 0,$$

where L, Q and C are respectively homogeneous linear, quadratic and cubic polynomials in x, y and z. We parametrise the plane $\Pi_P : x = 1$ by $(1, u, v)$ where u, v vary in $\overline{K}$. The line joining $E_2 = (0, 0, 0)$ to a point $(1, u, v)$ is parametrised by $t(1, u, v)$ where $t \in \overline{K}$. The line $t(1, u, v)$ intersects S in three points counting multiplicities, one of which is E_2. We denote the other two points by Q_1 and Q_2. For a given (u, v) we can find the values of t that yield E_2, Q_1 and Q_2 by solving the following equation:

$$L(t, tu, tv) + Q(t, tu, tv) + C(t, tu, tv) = 0.$$

If we let $l = L(1,u,v)$, $q = Q(1,u,v)$ and $c = C(1,u,v)$ then we can rewrite this as

$$tl + t^2q + t^3c = 0.$$

The solution at $t = 0$ corresponds to $E_2 = (0,0,0)$. The points Q_1 and Q_2 can be found by solving the quadratic equation in t

$$l + tq + t^2c = 0.$$

When $Q_1 = Q_2$ we have $E_2 \in \Pi_{Q_1}$. This corresponds exactly to the values of (u,v) such that

$$q^2 - 4c = 0.$$

In particular we wish to know for which values of (u,v) do we have $Q_1 = Q_2$ and $Q_1, Q_2 \in \Pi_P : x = 1$. To find these values we set $t = 1$ and we seek to find values of (u,v) that also satisfy

$$l + q + c = 0.$$

By rearranging and squaring both sides we obtain

$$q^2 = (l + c)^2,$$

from which

$$(l + c)^2 = 4c,$$

and therefore

$$(l - c)^2 = 0,$$

whch holds if and only if $l = c$ and $q = -2l$. Note that $l = c$ defines a plane cubic curve in Π_P and $q = -2l$ gives a plane quadratic curve in Π_P. The intersection of these two curves is contained in $S \cdot \Pi_P = \Gamma_P$. This intersection represents the points $Q \in \Gamma_P$ for which $E_2 \in \Pi_Q$. Recall that $\Gamma_P = C \cup \ell_1$. We therefore we have the following three possibilities:

1. $l = c$ and $q = -2l$ share a common quadratic component, which must be C,
2. $l = c$ and $q = -2l$ share a common linear component, which must be ℓ_1,
3. by Bezout's Theorem $l = c$ and $q = -2l$ intersect in at most six points.

We can eliminate the first two possibilities by noting that $P \in C \cap \ell_1$, and $E_2 \notin \Pi_P$. Therefore we must have at most six points in Γ_P that have E_2 in their tangent planes, and one of these points is E.

There are at most two points in $C(K)\backslash\{P, P'\}$ whose tangent planes intersect ℓ_2 at E (see Figure 3.10) and at most five points in $C(K)\backslash\{P, P'\}$ whose tangent planes intersect ℓ_2 at E_2. Therefore there are at least $q-8$ remaining points in $C(K)\backslash\{P, P'\}$. Recall that we are in the case where $\mathrm{char}(K) \neq 2$ so $q-8>0$ and we may choose $Q \in C(K)\backslash\{P, P'\}$ such that $\Pi_Q \cdot \ell_2 \neq E, E_2$. If Q lies upon a K-line, then this line is distinct from ℓ_1, ℓ_2 and ℓ_3, which contradicts the hypotheses of the lemma. Therefore by Lemma 3.5 Q is not an Eckardt point.

We consider the possibilities for Γ_Q. As Q does not lie on a K-line in S and Q is not an Eckardt point we must have either $\Gamma_Q = \ell_i \cup \ell \cup \ell'$ where $i = 2$ or 3 and ℓ and ℓ' are Galois conjugate $\mathbb{F}_{q^2}$-lines not defined over K such that $\ell \cdot \ell' = Q$, or Γ_Q is an irreducible cubic curve with a singular point at Q.

Suppose we are in the first case and $\Gamma_Q = \ell_i \cup \ell \cup \ell'$ for $i = 2$ or 3. For any point $R \in \ell_i(K)$ the K-line m joining R and Q is not contained in S so by executing tangent operations on Q we obtain $\ell_i(K) \subset \mathrm{Span}(Q)$. We can then generate $\ell_j(K)$ for $j \neq 1, i$ via secant operations on the points of $\ell_1(K)$ and $\ell_i(K)$ to obtain $\ell_j(K) \subset \mathrm{Span}(\ell_1(K) \cup \ell_i(K))$, which completes the proof in this case.

Otherwise we are in the case where Γ_Q is an irreducible cubic curve with a singular point at Q. In this case the points of $\Gamma_Q(K)$ are generated from Q via tangent operations so $\Gamma_Q(K) \subseteq \mathrm{Span}(Q)$. Let $R = \Pi_Q \cdot \ell_2$. Note that $R \in \Gamma_Q(K)$, therefore $R \in \mathrm{Span}(Q)$. By our choice of Q, R is a non-Eckardt point thus by Lemma 2.4 we have

$$\ell_2(K) \subseteq \mathrm{Span}(R) \subseteq \mathrm{Span}(Q).$$

Note also that

$$Q \in \mathrm{Span}(P) \subseteq \mathrm{Span}(\ell_1(K)),$$

therefore

$$\ell_2(K) \subset \mathrm{Span}(\ell_1(K)).$$

We then apply secant operations to the points of $\ell_1(K)$ and $\ell_2(K)$ to obtain

$$\ell_3(K) \subset \mathrm{Span}(\ell_1(K) \cup \ell_2(K)),$$

which completes the proof. □

From Lemmas 3.3, 2.4, 3.7 and 3.8 we obtain the following result.

Corollary 3.9. *Let K be a field containing at least 8 elements. Let S be a smooth cubic surface defined over K containing at least one K-line, ℓ. Then there is a*

K-line $\ell' \subset S$, possibly equal to ℓ, and a point $P \in \ell'(K)$ such that

$$\bigcup_{Q \in \ell'(K)} \Gamma_Q(K) \subseteq \mathrm{Span}(P).$$

The following lemmas show that for some $P \in S(K)$ there exists a set $T \subset \mathrm{Span}(P)$ such that $|T| > \frac{1}{2}|S(K)| + \frac{q+1}{2}$; this will allow us to complete the proof of Theorem 3.1.

Lemma 3.10. *Let K be a field containing at least 4 elements. Let S be a smooth cubic surface defined over K containing at least one K-line ℓ but no pair of skew K-lines such that the Gauss map on each K-line in S is separable. Let Π be a plane through ℓ such that $\Gamma = \Pi \cdot S$ is of type (3) and $\Gamma = C \cup \ell$. Then there exists a point $P \in C(K)$ such that $\Gamma(K) \subset \mathrm{Span}(P)$.*

Proof. Let E be an Eckardt point in $\ell(K)$ if such a point exists. There are precisely two $\overline{K}$-lines through E in Π that are tangent to C, i.e. there are precisely two points in $C(\overline{K})$ such that E lies in their tangent planes. As there are at most two Eckardt points in $\ell(K)$ there are at most four points in $C(K)$ that generate an Eckardt point in $\ell(K)$ upon performing a tangent operation.

Let $Q \in C(K)$ be neither an Eckardt point nor a point that has an Eckardt point in $\ell(K)$ in its tangent plane. By Lemma 3.5 and Lemma 3.6 we know that none of the points in $C(K)$ are Eckardt points. Since there are at most four points in $C(K)$ that have an Eckardt point in $\ell(K)$ in their tangent planes, there are at least $q-3$ points in $C(K)$ that do not have an Eckardt point in $\ell(K)$ in their tangent planes. So for a finite field $K = \mathbb{F}_q$ there are $q-3$ possibilities for Q, otherwise there are infinitely many possible Q. Since K contains at least 4 elements we know that such a Q exists.

The curve Γ_Q is an absolutely irreducible cubic curve with a singular point at Q. The point $R = \Pi_Q \cdot \ell$ is a K-point in Π_Q and since Q does not lie on a K-line in S by Lemma 3.6 we know that the K-line joining R and Q is not in S. Hence $R \in \Gamma_Q(K) \subseteq \mathrm{Span}(Q)$ as in Figure 3.11.

Note that R is not Eckardt due to our choice of Q. We now apply Lemma 2.4 to obtain $\ell(K) \subseteq \mathrm{Span}(R) \subseteq \mathrm{Span}(Q)$. Secant operations on Q and the points of $\ell(K)$ give

$$C(K) \subset \mathrm{Span}(\ell(K)) \subset \mathrm{Span}(Q),$$

which completes the proof. □

We can now prove the main result of this chapter. Before doing so it will be useful to note the values of $\#\Gamma(K)$ for the cubic curves in S of types (1) to (7),

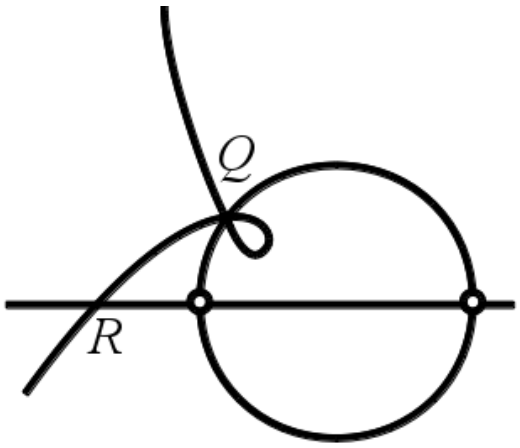

Figure 3.11: We generate $R \in \ell(K)$ from $Q \in C(K)$, where C is of type (3).

which all follow from the fact that lines and absolutely irreducible conics in S are copies of $\mathbb{P}^1_K$ and hence have $q+1$ points. These values are given in Table 3.2 on page 53.

Form of Γ	$\#\Gamma(K)$
(1)	$2q$
(2)	$3q$
(3)	$2q+2$
(4)	$q+2$
(5)	$2q+1$
(6)	$3q+2$
(7)	$q+1$

Table 3.2: Size of $\Gamma(K)$

We restate Theorem 3.1.

Theorem 3.1. *Let $K = \mathbb{F}_q$ be a finite field with $q \geq 8$. Let S be a smooth cubic surface defined over K containing at least one K-rational line. Then there exists a point $P \in S(K)$ such that* $\mathrm{Span}(P) = S(K)$.

Proof of Theorem 3.1. If there is a skew pair of K-lines in S we may invoke Theorem 2.1. We assume that there is no skew pair of K-lines in S.

If S contains a K-line upon which the Gauss map is inseparable the result follows from Lemma 3.3. It remains to show that the result holds when the Gauss map on all K-lines in $S(K)$ is separable. We aim to show that we can can generate

enough points to invoke Theorem 3.4 and hence generate all of $S(K)$.

By Corollary 3.9, there is a K-line $\ell \subset S$ such that $\bigcup_{Q \in \ell(K)} \Gamma_Q(K) \subset \mathrm{Span}(\ell(K))$. Let n be the number of non-parabolic points in $\ell(K)$. Note that n must be even because γ_ℓ has degree 2. In fact, we have

$$\begin{aligned} n &= q && \text{when } \mathrm{char}(K) = 2, \\ n &= q \pm 1 && \text{when } \mathrm{char}(K) \neq 2. \end{aligned}$$

There are precisely $q+1$ distinct K-planes through ℓ. Recall that γ_ℓ maps distinct parabolic points in $\ell(K)$ to distinct K-planes through ℓ and maps distinct pairs of non-parabolic points to distinct K-planes through ℓ. For a parabolic point $P \in \ell(K)$ the tangent plane Π_P is of type (5), (6) or (7) and for a non-parabolic point $Q \in \ell(K)$ the tangent plane Π_Q is of type (1) or (2). Therefore $q+1-n$ of the K-planes through ℓ are the tangent planes of parabolic points in $\ell(K)$ and hence of types (5), (6) and (7), and $\frac{n}{2}$ of the K-planes through ℓ are the tangent planes of non-parabolic points in $\ell(K)$ and hence of types (1) and (2). This leaves $\frac{n}{2}$ K-planes through ℓ remaining and these must be of types (3) and (4).

We will deal with the cases where there exists a K-plane through ℓ of type (3) and does not exist such a plane separately. Suppose that there exists a K-plane through ℓ of type (3) denoted by Π. Let $\Gamma = \Pi \cdot S$ and $\Gamma = C \cup \ell$ where C is an absolutely irreducible conic defined over K. We wish to generate a non-Eckardt point in $\ell(K)$ by a tangent operation on a point in $C(K)$. By Lemma 3.10 we know that there exists $P \in C(K)$ such that $\Gamma(K) = C(K) \cup \ell(K) \subseteq \mathrm{Span}(P)$. By Corollary 3.9 we can also generate $\Gamma_Q(K)$ for all $Q \in \ell(K)$ from the points of $\ell(K)$. Every other point in S does not lie in the tangent plane of a point in $\ell(K)$ so must lie in a plane of type (3) or (4). Let $T = \bigcup_{Q \in \ell(K)} \Gamma_Q(K) \cup C(K) \subseteq \mathrm{Span}(P)$ and $T' = S(K) \backslash T$. We form an inequality on the size of the set T:

$$\begin{aligned} |T| \geq\ & 2q+2 && (\leq \#\Gamma(K)) \\ +\ & 0 && (\leq \#(\Gamma_Q(K) \backslash \ell(K)) \text{ for } Q \in \ell(K) \text{ parabolic}) \\ +\ & \tfrac{n}{2} \cdot (q-1) && (\leq \#(\Gamma_Q(K) \backslash \ell(K))) \text{ for } Q \in \ell(K) \text{ non-parabolic}). \end{aligned}$$

Likewise we have

$$|T'| \leq \left(\frac{n}{2} - 1\right) \cdot (q+1).$$

Therefore

$$|T| \geq \begin{cases} \frac{q^2+2q+5}{2} & \text{if } n = q-1, \\ \frac{q^2+3q+4}{2} & \text{if } n = q, \\ \frac{q^2+4q+3}{2} & \text{if } n = q+1, \end{cases}$$

and

$$|T'| \leq \begin{cases} \frac{q^2-2q-3}{2} & \text{if } n = q-1, \\ \frac{q^2-q-2}{2} & \text{if } n = q, \\ \frac{q^2-1}{2} & \text{if } n = q+1. \end{cases}$$

Notice that this gives us $|T| > |T'| + q + 1$ for all values of n, and that

$$|T| > \frac{1}{2}|S(K)| + \frac{q+1}{2} \iff |T| > |T'| + q + 1.$$

Thus $|T| > \frac{1}{2}|S(K)| + \frac{q+1}{2}$ and we invoke Theorem 3.4 to complete the proof in this case.

It remains to prove the case when there does not exist a K-plane through ℓ of type (3). In this case we must have $\frac{n}{2}$ K-planes through ℓ of type (4). (This case can only occur when $q \leq 11$ due to Proposition 1.19.) Let Π be a K-plane through ℓ of type (4) and let P be the unique K-point in $\Pi \cdot S$ not lying on ℓ. We note that the tangent plane at P, denoted by Π_P, is equal to Π. Any point $R \in \ell(K)$ is in $\Pi_P = \Pi$. By Lemma 1.16 the point P does not lie on any K-line in S so the K-line joining P and R is not in S. Therefore $\ell(K) \subset \mathrm{Span}(P)$. We can then apply Corollary 3.9 to obtain

$$\bigcup_{Q \in \ell(K)} \Gamma_Q(K) \cup \{P\} \subseteq \mathrm{Span}(P).$$

Let $T = \bigcup_{Q \in \ell(K)} \Gamma_Q(K) \cup \{P\}$ and $T' = S(K) \backslash T$. We form an inequality of the size of the set T:

$$\begin{array}{rll} |T| \geq & q+2 & (\leq \#\Gamma_P(K)), \\ + & 0 & (\leq \#(\Gamma_Q(K) \backslash \ell(K)) \text{ for } Q \in \ell(K) \text{ parabolic}), \\ + & \frac{n}{2} \cdot (q-1) & (\leq \#(\Gamma_Q(K) \backslash \ell(K))) \text{ for } Q \in \ell(K) \text{ non-parabolic}). \end{array}$$

The points in T' are in the intersection of S with the remaining K-planes through ℓ of type (4):

$$|T'| = \left(\frac{n}{2} - 1\right).$$

This gives us $|T| > |T'| + q + 1$ for all values of n, which is equivalent to the inequality

$$|T| > \frac{1}{2}|S(K)| + \frac{q+1}{2}.$$

We invoke Theorem 3.4 to complete the proof. □

3.5 Proof of Theorem 3.2

Theorem 3.2 was proved by an exhaustive computer enumeration implemented in `MAGMA` [13] using the programs described in Chapter 2, Section 2.2.

Theorem 3.2. *Let $K = \mathbb{F}_2$. Let S be a smooth cubic surface over K. Suppose S contains a line ℓ defined over K that does not contain any K-rational Eckardt points. Then there exists a point $P \in \ell(K)$ such that* $\mathrm{Span}(P) = S(K)$.

Proof of Theorem 3.2. By a projective change of coordinates we may suppose that the line ℓ is defined by $X = Y = 0$, and that therefore the surface S has the form $XQ_1 + YQ_2$ where $Q_1 \in \mathbb{F}_2[X, Y, Z, W]$ and $Q_2 \in \mathbb{F}_2[Y, Z, W]$ are homogeneous quadratic forms. Our program enumerated all possible Q_1, Q_2, checked the surface for smoothness and whenever ℓ contained no K-rational Eckardt points, it verified that the span of one of its K-points is equal to $S(K)$. This meant the program was enumerated over $2^{16} = 65536$ possible models, as there are 10 degree 2 monomials in X, Y, Z, W, and 6 degree 2 monomials in Y, Z, W. □

Chapter 4

Cubic surfaces containing no rational lines

This chapter concerns Mordell-Weil point generation on cubic surfaces defined over finite fields that do not contain any rational lines. The main result of this chapter is the following theorem.

Theorem 4.1. *Let S be a smooth cubic surface defined over a finite field $K = \mathbb{F}_q$ containing no rational lines. Let $P \in S(K)$ be a non-Eckardt point. Let*

$$n = [(2q+3)/6],$$

where $[x]$ denotes the nearest integer to x. Then

$$\frac{|\operatorname{Span}(P)|}{|S(K)|} \geq \frac{2nq - 3n^2 + 3n}{2(q^2+7q+1)}.$$

Observe that the right-hand side of the inequality tends to $\frac{1}{6}$ as $q \to \infty$.

Proof. Let $P \in S(K)$ be a non-Eckardt point. Consider the set of points

$$\bigcup_{Q \in \Gamma_P(K)} \Gamma_Q(K).$$

Since Γ_P is defined over K, there are no K-lines in S and P is not an Eckardt point, we know that Γ_P is an irreducible cubic defined over K with singular point at P and no other singular points. As in Table 3.1 on page 46 there are three possibilities for Γ_P:

1. Γ_P has a cusp at P and $|\Gamma_P(K)| = q+1$

2. Γ_P has a split node at P and $|\Gamma_P(K)| = q$,

3. Γ_P has a non-split node at P and $|\Gamma_P(K)| = q + 2$.

Let R be any point in $\Gamma_P \backslash \{P\}$. The K-line joining R and P is not contained in S so R is generated from P via a tangent operation. Hence $\Gamma_P(K) \subseteq \mathrm{Span}(P)$. By similarly performing tangent operations on the points of $\Gamma_P(K)$ we obtain

$$\bigcup_{Q \in \Gamma_P(K)} \Gamma_Q(K) \subseteq \mathrm{Span}(P).$$

See Figure 4.1. We know that $q \leq |\Gamma_Q(K)| \leq q + 2$ for $Q \in \Gamma_P(K)$. However, in order to compute $|\mathrm{Span}(P)|$, we need to take into account the points of intersection between the different cubic curves. We use an inclusion-exclusion principle to count the minimum number of points we expect to have in $\left|\bigcup_{Q \in \Gamma_P(K)} \Gamma_Q(K)\right|$. Note that for distinct points Q, $Q' \in S(K)$, the intersection $\Pi_Q \cdot \Pi_{Q'}$ of their tangent planes is a K-line in $\mathbb{P}^3_K$. This line intersects both Γ_Q and $\Gamma_{Q'}$ in three $\overline{K}$-points counting multiplicities.

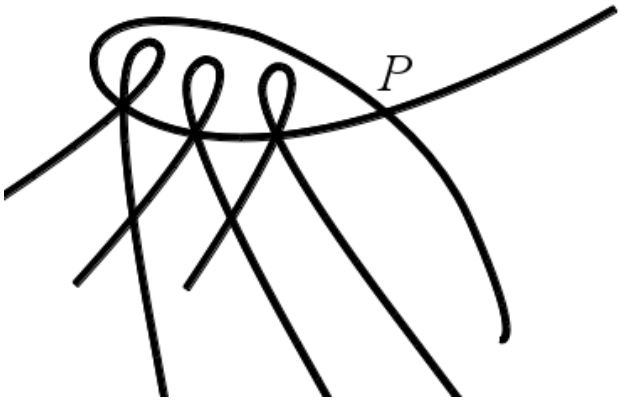

Figure 4.1: Tangent operations on the points of $\Gamma_P(K)$.

We are now equipped to use the inclusion-exclusion principle, namely, for a collection of sets, A_i, we have

$$\left|\bigcup_i A_i\right| = \sum_i |A_i| - \sum_{i \neq j} |A_i \cap A_j| + \sum_{i \neq j, j \neq k, i \neq k} |A_i \cap A_j \cap A_k| - \dots \quad .$$

We want to find a minimum number of points generated from P so we form the

inequality

$$\left|\bigcup_{Q\in\Gamma_P(K)}\Gamma_Q(K)\right| \geq \sum_{Q\in\Gamma_P(K)}|\Gamma_Q(K)| - \sum_{Q,Q'\in\Gamma_P(K),Q\neq Q'}|(\Gamma_Q\cdot\Gamma_{Q'})(K)|.$$

Let N be any non-empty subset of $\Gamma_P(K)$. Then certainly,

$$\left|\bigcup_{Q\in\Gamma_P(K)}\Gamma_Q(K)\right| \geq \sum_{Q\in N}|\Gamma_Q(K)| - \sum_{Q,Q'\in N,Q\neq Q'}|(\Gamma_Q\cdot\Gamma_{Q'})(K)|.$$

At first, it seems that there is nothing to be gained in replacing $\Gamma_P(K)$ by a subset. However by decreasing the number of Γ_Q for $Q \in \Gamma_P$ that we consider we also decrease the number of points of intersection $\Gamma_Q\cdot\Gamma_{Q'}$ for $Q, Q' \in \Gamma_P$. This will prove to be advantageous.

We have

$$|\Gamma_Q(K)| \geq q$$

and

$$|(\Gamma_Q\cdot\Gamma_{Q'})(K)| \leq 3.$$

Let $n = |N|$. Then

$$\begin{aligned}\left|\bigcup_{Q\in\Gamma_P(K)}\Gamma_Q(K)\right| &\geq nq - 3\binom{n}{2}\\ &= nq - \tfrac{3}{2}n^2 + \tfrac{3}{2}n.\end{aligned}$$

This is a quadratic in n with a negative n^2-coefficient and achieves its maximum (as a real function) when

$$n = \frac{2q+3}{6}.$$

However, n is a number of points in the subset N, and must be an integer. We choose

$$n = [(2q+3)/6],$$

where $[x]$ denotes the nearest integer to x. By Theorem 1.22 we know that $|S(K)|$ is at most q^2+7q+1, hence we obtain

$$\frac{|\operatorname{Span}(P)|}{|S(K)|} \geq \frac{2nq-3n^2+3n}{2(q^2+7q+1)}.$$

□

Chapter 5

c-invariants of cubic surfaces containing a K-line

The theory contained in this chapter was originally motivated by the Mordell-Weil Problem for a cubic surface over a finite field $K = \mathbb{F}_q$ and containing a K-line when q is small. Indeed, Chapter 3 could be rewritten in the language of c-invariants as described below. Ultimately it did not produce stronger results than those of Chapter 3, however some other interesting results were obtained using this theory. These include a formulation of the number of points of a cubic surface S over a finite field K containing a K-line ℓ in terms of the conic line bundle structure of S with respect to ℓ, and a result on the nature of some of the lines in S.

5.1 Defining the c-invariants

Let S be a smooth cubic surface defined over a finite field $K = \mathbb{F}_q$ containing at least one K-line, ℓ. As discussed in Chapter 3, there is a pencil of $q+1$ K-planes through ℓ. Every point in $S(K)\backslash\ell(K)$ lies on exactly one of these K-planes. In Chapter 3 we also classified these K-planes by the shape of their intersections with S. Let Π be a K-plane through ℓ, let $\Gamma = \Pi \cdot S$ and let $\Gamma = C \cup \ell$. The classification is as follows.

(1) C is absolutely irreducible and meets ℓ in two distinct K-points. (Figure 3.1 on page 42.)

(2) C decomposes into two K-lines, m and m', and $m \cdot \ell \neq m' \cdot \ell$. (Figure 3.2 on page 42.)

(3) C is absolutely irreducible and meets ℓ in two distinct points that are not K-points, but are defined over $\mathbb{F}_{q^2}$ and are Galois conjugates. (Figure 3.3 on

page 42.)

(4) C decomposes into two Galois conjugate lines m, m', that are defined over $\mathbb{F}_{q^2}$ but not K. We have $m \cdot m'$ is a K-point, $m \cdot \ell \neq m' \cdot \ell$, and $m \cdot \ell$, $m' \cdot \ell$ are defined over $\mathbb{F}_{q^2}$ but are not K-points. (Figure 3.4 on page 42.)

(5) C is absolutely irreducible and ℓ is tangent to C, so meeting C in exactly one K-point. (Figure 3.5 on page 42.)

(6) C decomposes into two K-lines, m and m', and $m \cdot \ell = m' \cdot \ell$, and hence is an Eckardt point in $\ell(K)$. (Figure 3.6 on page 42.)

(7) C decomposes into two Galois conjugate lines m, m', that are defined over $\mathbb{F}_{q^2}$ but not K. We have $m \cdot \ell = m' \cdot \ell$, and hence is an Eckardt point in $\ell(K)$. (Figure 3.7 on page 42.)

We now define the *c-invariants* of a smooth cubic surface S with respect to a K-line, $\ell \subset S$.

c_1 = number of K-planes through ℓ of type (1)
c_2 = number of K-planes through ℓ of type (2)
c_3 = number of K-planes through ℓ of type (3)
c_4 = number of K-planes through ℓ of type (4)
c_5 = number of K-planes through ℓ of type (5)
c_6 = number of K-planes through ℓ of type (6)
c_7 = number of K-planes through ℓ of type (7)

For any cubic surface S we can make a choice of a line $\ell \subset S$ and then every point on the surface is either on ℓ or is on a plane that contains ℓ and hence on a conic in S. This is referred to as S having a *conic line bundle* structure with respect to ℓ. In this chapter we will refer to the K-points of S as having a conic line bundle structure with respect to a K-line $\ell \subset S$. We note that every point in $S(K)$ lies on a K-plane through ℓ.

5.2 c-invariants and $|S(K)|$

Table 3.2 on page 53 shows the number of K-points in $\Gamma = \Pi \cdot S$ for each type of K-plane Π through ℓ. The intersection of all these planes is precisely ℓ itself, which gives us the following theorem on the number of K-points in S.

Theorem 5.1. *Let S be a smooth cubic surface defined over $K = \mathbb{F}_q$ containing a K-line, ℓ, and let $c_1, \ldots, c_7$ be the c-invariants of S with respect to ℓ. Then*

$$c_1 + c_2 = c_3 + c_4$$

and

$$|S(K)| = q + 1 + c_1(q-1) + c_2(2q-1) + c_3(q+1) + c_4 + c_5 q + 2c_6 q.$$

Proof. Let N be the number of parabolic points in $\ell(K)$. Then there are $q+1-N$ non-parabolic points in $\ell(K)$ and note that $q+1-N$ is even. Recall that γ_ℓ maps distinct parabolic points in $\ell(K)$ to distinct K-planes through ℓ and maps distinct pairs of non-parabolic points in $\ell(K)$ to distinct K-planes through ℓ. Therefore N of the $q+1$ K-planes through ℓ are tangent planes to S at parabolic points in $\ell(K)$ and $\frac{q+1-N}{2}$ of the K-planes through ℓ are tangent planes to non-parabolic points in $\ell(K)$. Non-parabolic points in $\ell(K)$ are of type (1) and type (2) only, therefore $c_1 + c_2 = \frac{q+1-N}{2}$. There are $\frac{q+1-N}{2}$ remaining K-planes through ℓ so these must be of types (3) and (4). Therefore $c_3 + c_4 = q + 1 - N$ and hence $c_1 + c_2 = c_3 + c_4$.

The statement

$$|S(K)| = q + 1 + c_1(q-1) + c_2(2q-1) + c_3(q+1) + c_4 + c_5 q + 2c_6 q$$

follows from the fact that

$$S(K) = \bigcup_{\Pi \ K\text{-plane through } \ell} (\Pi \cdot S)(K).$$

□

Proposition 5.2. *Let S be a smooth cubic surface defined over $K = \mathbb{F}_q$ containing a K-line, ℓ, and let $c_1, \ldots, c_7$ be the c-invariants of S with respect to ℓ. Then we have the following relations between the c_i.*

When $\mathrm{char}(K) = 2$ *and γ_ℓ is inseparable,*

$$\begin{aligned} &c_1 = c_2 = c_3 = c_4 = 0, \\ &c_5 + c_6 + c_7 = q + 1, \\ &c_6 + c_7 \leq 5. \end{aligned}$$

When $\mathrm{char}(K) = 2$ *and γ_ℓ is separable,*

$$\begin{aligned} &c_5 + c_6 + c_7 = 1, \\ &c_1 + c_2 = c_3 + c_4 = \tfrac{q}{2}, \\ &c_2 + c_4 + c_6 + c_7 \leq 5. \end{aligned}$$

When $\mathrm{char}(K) \neq 2$ *and there are no parabolic points in* $\ell(K)$*,*

$$\begin{aligned} c_5 = c_6 = c_7 &= 0, \\ c_1 + c_2 = c_3 + c_4 &= \tfrac{q+1}{2}, \\ c_2 + c_4 + c_6 + c_7 &\leq 5. \end{aligned}$$

When $\mathrm{char}(K) \neq 2$ *and there are exactly two parabolic points in* $\ell(K)$*,*

$$\begin{aligned} c_5 + c_6 + c_7 &= 2, \\ c_1 + c_2 = c_3 + c_4 &= \tfrac{q-1}{2}, \\ c_2 + c_4 + c_6 + c_7 &\leq 5. \end{aligned}$$

Proof. Recall that the number of K-planes through ℓ is $q+1$. By Proposition 1.19 ℓ is intersected by exactly ten other $\overline{K}$-lines in S that come in coplanar pairs. Therefore the number of K-planes through ℓ that contain three $\overline{K}$-lines in S (including ℓ itself) is at most 5. These are the planes of type (2), (4), (6) and (7), hence $c_2+c_4+c_6+c_7 \leq 5$ in all cases.

When $\mathrm{char}(K) = 2$ and γ_ℓ is inseparable every point in $\ell(K)$ is parabolic and hence the K-planes through ℓ are precisely the $q+1$ tangent planes of the points of $\ell(K)$. Thus all the K-planes through ℓ are of type (5), (6) and (7), giving $c_5 + c_6 + c_7 = q + 1$ and $c_1 = c_2 = c_3 = c_4 = 0$. Therefore $c_2 + c_4 + c_6 + c_7 = c_6 + c_7$ so $c_6 + c_7 \leq 5$.

When $\mathrm{char}(K) = 2$ and γ_ℓ is separable there is exactly one parabolic point in $\ell(K)$ by Lemma 1.21. Thus there is exactly one K-plane through ℓ of type (5), (6) or (7), so $c_5 + c_6 + c_7 = 1$. There are q remaining K-planes through ℓ and q non-parabolic points in $\ell(K)$. Each non-parabolic point in $\ell(K)$ shares its tangent plane with precisely one other such point. Thus $\frac{q}{2}$ of the remaining q planes are the tangent planes of the non-parabolic points of $\ell(K)$ and hence are of types (1) and (2), thus $c_1 + c_2 = \frac{q}{2}$. The remaining K-planes through ℓ are of types (3) and (4), therefore $c_3 + c_4 = \frac{q}{2}$.

When $\mathrm{char}(K) \neq 2$ and there are no parabolic points in $\ell(K)$ we have no K-planes through ℓ of types (5), (6) or (7), so $c_5 = c_6 = c_7 = 0$. Exactly half of the K-planes through ℓ are the tangent planes of the points of $\ell(K)$ and hence are of types (1) and (2). Therefore $c_1 + c_2 = \frac{q+1}{2}$. The remaining planes are of types (3) and (4) so we have $c_3 + c_4 = \frac{q+1}{2}$.

When $\mathrm{char}(K) \neq 2$ and there are exactly two parabolic points in $\ell(K)$ there is a total of two K-planes of types (5), (6) and (7) through ℓ, so $c_5 + c_6 + c_7 = 2$. There are $q-1$ remaining K-planes through ℓ. Half of these are the tangent planes of the non-parabolic points of $\ell(K)$ and so are of types (1) and (2), and the rest are of types (3) and (4). Hence $c_1 + c_2 = c_3 + c_4 = \frac{q+1}{2}$. □

Notice that the contribution to $S(K)$ from the K-planes through ℓ of types (1) and (2) is

$$c_1(q-1) + c_2(2q-1) \equiv -(c_1 + c_2) \pmod{q},$$

the contribution from K-planes of types (3) and (4) is

$$c_3(q+1) + c_4 \equiv (c_3 + c_4) \pmod{q},$$

and the contribution from K-planes of types (5), (6) and (7) is

$$c_5 q + 2c_6 q \equiv 0 \pmod{q},$$

from which we have the following corollary to Theorem 5.1.

Corollary 5.3. *For S a smooth cubic surface defined over $K = \mathbb{F}_q$,*

$$S(K) \equiv 1 \pmod{q}.$$

This is consistent with Theorem 1.22, which stated that $|S(K)| = q^2 + mq + 1$, where $-2 \le m \le 5$ for $q = 2, 3, 5$ and $-2 \le m \le 7$, $m \ne 6$ otherwise. The next result is also a corollary to Theorem 5.1 and gives an expression for m in terms of the c_i.

Corollary 5.4. *In the notation of Theorem 5.1 and Theorem 1.22*

$$m = 2 - c_1 + c_3 + c_6 - c_7.$$

Proof. By equating the expressions for $|S(K)|$ given in Theorems 5.1 and 1.22 we obtain

$$\begin{aligned} mq &= q + 1 + c_1(q-1) + c_2(2q-1) + c_3(q+1) + c_4 + c_5 q + 2c_6 q - q^2 - 1 \\ &= (1 + c_1 + 2c_2 + c_3 + c_5 + 2c_6 - q)q + (-c_1 - c_2 + c_3 + c_4). \end{aligned}$$

We then use the statement that $c_1 + c_2 = c_3 + c_4$ from Theorem 5.1 and the fact that $\sum_i c_i = q + 1$ to achieve the result as follows.

$$\begin{aligned} m &= 1 + c_1 + 2c_2 + c_3 + c_5 + 2c_6 - q \\ &= 2 + c_1 + c_2 + (c_3 + c_4 - c_1) + c_3 + c_5 + 2c_6 - (q+1) \\ &= 2 + c_2 + 2c_3 + c_4 + c_5 + 2c_6 - (c_1 + c_2 + c_3 + c_4 + c_5 + c_6 + c_7) \\ &= 2 - c_1 + c_3 + c_6 - c_7. \end{aligned}$$

□

5.3 Examples and consequences of Theorem 5.1 and Proposition 5.2

Example 5.5. Consider S a smooth cubic surface defined over $K = \mathbb{F}_5$ containing exactly three K-lines ℓ, ℓ' and ℓ'' that meet at an Eckardt point $E \in S(K)$. We may deduce the following facts about such a surface.

Let c_i for $i = 1, \ldots, 7$ be the c-invariants for S with respect to the K-line ℓ. We know that $c_6 = 1$ because ℓ, ℓ' and ℓ'' meet at E. Therefore $c_5 + c_6 + c_7 \neq 0$ and so $c_5 + c_6 + c_7 = 2$, which implies that $c_5 + c_7 = 1$. It follows that $c_2 = 0$, hence $c_1 = \frac{q-1}{2} = 2$ and $c_3 + c_4 = 2$. From the expression for the number of K-points of a smooth cubic surface defined over a finite field given in Theorem 5.1 we have

$$\begin{aligned} |S(K)| &= q + 1 + c_1(q-1) + c_2(2q-1) + c_3(q+1) + c_4 + c_5 q + 2c_6 q \\ &= 6 + 2 \cdot 4 + 6c_3 + (2 - c_3) + 5c_5 + 2 \cdot 5 \\ &= 26 + 5(c_3 + c_5). \end{aligned}$$

From the relations in Proposition 5.2 we have $c_3 = 0, 1$ or 2 and $c_5 = 0$ or 1. This gives us a complete list of the possible values for $|S(K)|$. These are $|S(K)| = 26$, 31, 36 or 41. This tells us that a smooth cubic surface of this form can attain neither the lower bound nor the upper bound for $|S(K)|$ given by Theorem 1.22, which is 16 or 51 respectively. However, these bounds are sharp for a general cubic surface over a finite field. It was shown by Swinnerton-Dyer in [24] that for every value of m in Theorem 1.22 there exists a cubic surface with the corresponding number of rational points. The other possible values for $|S(K)|$ that are not attained by a cubic surface as stated in this example are 21 and 46.

The number of K-points remains invariant under choice of ℓ. Let c_i' and c_i'' for $i = 1, \ldots, 7$ be the c-invariants for S with respect to ℓ' and ℓ'' respectively. Then we have

$$|S(K)| = 26 + 5(c_3 + c_5) = 26 + 5(c_3' + c_5') = 26 + 5(c_3'' + c_5''),$$

so

$$c_3 + c_5 = c_3' + c_5' = c_3'' + c_5''.$$

Note that, since $c_1 + c_2 = c_3 + c_4$ and likewise $c_1' + c_2' = c_3' + c_4'$ and $c_1'' + c_2'' = c_3'' + c_4''$, we can deduce that $c_4 + c_7 = c_4' + c_7' = c_4'' + c_7''$. This means that the number of $\mathbb{F}_{q^2}$-lines intersecting ℓ is the same as that for ℓ' and ℓ''.

We remark that $|S(K)| = 26$ only when $c_3 = c_5 = c_3' = c_5' = c_3'' = c_5'' = 0$, and $|S(K)| = 41$ only when $c_3 = c_3' = c_3'' = 2$ and $c_5 = c_5' = c_5'' = 1$, from which we can deduce that $c_i = c_i' = c_i''$ for all $i = 1, \ldots, 7$. Geometrically speaking, the sets of

K-rational points on these cubic surfaces have the same conic line bundle structure with respect to each of the three K-lines, ℓ, ℓ' and ℓ'', up to ordering of the conics.

Example 5.6. Consider S a smooth cubic surface defined over $K = \mathbb{F}_4$ and containing three K-lines ℓ, ℓ' and ℓ'' that meet in a Eckardt point E. Suppose that the Gauss map on ℓ, γ_ℓ, is inseparable. Let c_i, c_i' and c_i'' for $i = 1, \ldots, 7$ be the c-invariants for ℓ, ℓ' and ℓ'' respectively. Recall that $c_1 = c_2 = c_3 = c_4 = 0$, $c_6 \geq 1$ and $c_5 + c_6 + c_7 = 5$. Table 5.1 on page 66 gives all the possible values of c_5, c_6, c_7 and the corresponding sizes of $S(K)$.

c_5	c_6	c_7	$\lvert S(K)\rvert$
4	1	0	29
3	2	0	33
3	1	1	25
2	3	0	37
2	2	1	29
2	1	2	21
1	4	0	41
1	3	1	33
1	2	2	25
1	1	3	17
0	5	0	45
0	4	1	37
0	3	2	29
0	2	3	21
0	1	4	13

Table 5.1: Size of $S(K)$ given c_5, c_6 and c_7.

Note that if $\gamma_{\ell'}$ and $\gamma_{\ell''}$ are both also inseparable, then the corresponding tables for size of $|S(K)|$ with respect to c_i' and c_i'' for $i = 1, \ldots, 7$ would be exactly the same. Therefore, for the values of $|S(K)|$ that appear precisely once in Table 5.1 on page 66 the conic line bundle structure for the K-points of S is the same with respect to each of the lines ℓ, ℓ' and ℓ'' up to ordering of the conics.

Let us now suppose that $\gamma_{\ell'}$ is separable. Then we have $c_1' + c_2' = c_3' + c_4' = 2$, $c_5' = c_7' = 0$ and $c_6' = 1$. From which we see that

$$\begin{aligned} |S(K)| &= 5 + 3c_1' + 7c_2' + 5c_3' + c_4' + 4c_5' + 8c_6' \\ &= 29 + 4(c_3' - c_1'). \end{aligned}$$

Table 5.2 gives all the possible values of c_1' and c_3' and the corresponding sizes of $S(K)$.

c_1'	c_3'	$\lvert S(K)\rvert$
0	0	29
0	1	33
0	2	37
1	0	25
1	1	29
1	2	33
2	0	21
2	1	25
2	2	29

Table 5.2: Size of $S(K)$ given c_1' and c_3'.

There are four potential values for $|S(K)|$ that appear in Table 5.1 on page 66 that do not appear in Table 5.2 on page 67. These values are 13, 17, 41 and 45. If a surface as described in this example and with 13, 17, 41 or 45 rational points exists, then the Gauss map must be inseparable on both ℓ' and ℓ'' since $|S(K)|$ is a surface invariant. Furthermore, each of these values appears precisely once in Table 5.2, so the conic line bundle structure of S with respect to ℓ, ℓ' and ℓ'' is the same up to reordering of the conics.

Example 5.7. Consider a smooth cubic surface S defined over $K = \mathbb{F}_4$ that contains a K-line ℓ upon which the Gauss map γ_ℓ is inseparable. Recall that $c_1 = c_2 = c_3 = c_4 = 0$ and $c_5 + c_6 + c_7 = 5$. Table 5.3 on page 68 gives all the possible values of c_5, c_6 and c_7, and the corresponding sizes of $S(K)$.

We see that when $c_1 = c_2 = c_3 = c_4 = c_5 = c_6 = 0$ and $c_7 = 5$ we have $|S(K)| = 5$. However this is inconsistent with the lower bound for the number of rational points on a cubic surface over $\mathbb{F}_4$ given by Theorem 1.22, which is $q^2 - 2q + 1 = 9$. Therefore a cubic surface defined over $K = \mathbb{F}_4$ with only five K-points cannot exist and we see that not all combinations of c-invariants come from valid cubic surfaces.

Theorem 5.8. *Let S be a cubic surface defined over a finite field $K = \mathbb{F}_q$ and containing a K-line, ℓ. Then, of the ten $\overline{K}$-lines in S that intersect ℓ, at most eight can be contained in K-planes through ℓ and defined over $\mathbb{F}_{q^2}$ but not K.*

Proof. We will refer to lines defined over $\mathbb{F}_{q^2}$ but not K as $\mathbb{F}_{q^2}$-lines. First note that the $\overline{K}$-lines intersecting ℓ come in coplanar pairs by Proposition 1.19. If a pair of $\overline{K}$-lines intersecting ℓ lie in a K-plane through ℓ, then the lines are either K-lines or are a Galois conjugate pair of $\mathbb{F}_{q^2}$-lines. Such Galois conjugate pairs are contained in planes of type (4) and (7).

c_5	c_6	c_7	$\lvert S(K)\rvert$
5	0	0	25
4	1	0	29
4	0	1	21
3	2	0	33
3	1	1	25
3	0	2	17
2	3	0	37
2	2	1	29
2	1	2	21
2	0	3	13
1	4	0	41
1	3	1	33
1	2	2	25
1	1	3	17
1	0	4	9
0	5	0	45
0	4	1	37
0	3	2	29
0	2	3	21
0	1	4	13
0	0	5	5

Table 5.3: Some of these values for $|S(K)|$ contradict the Hasse bounds.

Let $c_1, \ldots, c_7$ be the c-invariants of S with respect to ℓ and let m be the surface invariant from Theorem 1.22 given in the equation $|S(K)| = q^2 + mq + 1$. Note that the statement of this theorem is equivalent to saying that $c_4 + c_7 \leq 4$. Let us suppose for a contradiction that $c_4 + c_7 = 5$. Thus we have $c_2 = c_6 = 0$ by Proposition 5.2.

If we are in the case where γ_ℓ is inseparable we have $c_1 = c_2 = c_3 = c_4 = c_6 = 0$ and $c_7 = 5$ by Proposition 5.2. By Corollary 5.4

$$m = 2 - c_1 + c_3 + c_6 - c_7 = 2 - 5 = -3,$$

which contradicts Theorem 1.22.

Otherwise we are in the case where γ_ℓ is separable. Let $N = c_1 + c_2 = c_3 + c_4$, i.e. $N = \frac{q-1}{2}$, $\frac{q}{2}$ or $\frac{q+1}{2}$ depending on the characteristic of K and the number of parabolic points in $\ell(K)$. By Proposition 5.2 we have $c_1 = N$ and $c_3 = N - c_4 = N - (5 - c_7)$. Hence

$$m = 2 - c_1 + c_3 + c_6 - c_7 = 2 - N + (N - 5 + c_7) - c_7 = -3,$$

which once again contradicts Theorem 1.22. Therefore $c_4 + c_7 \neq 5$, so there can be at most eight $\mathbb{F}_{q^2}$-lines in S that intersect ℓ. □

We can now add some relations to those in Proposition 5.2.

Theorem 5.9. *Let S be a smooth cubic surface defined over $K = \mathbb{F}_q$ containing a K-line, ℓ, and let $c_1, \ldots, c_7$ be the c-invariants of S with respect to ℓ. Let m be the surface invariant satisfying $|S(K)| = q^2 + mq + 1$. Then we have the following relations between the c_i and m.*

$$\begin{aligned} & c_5 + c_6 + c_7 = q + 1 - 2N, \\ & c_1 + c_2 = c_3 + c_4 = N, \\ & c_2 + c_4 + c_6 + c_7 \leq 5, \\ & c_4 + c_7 \leq 4 \\ \text{and} \quad & m = 2 - c_1 + c_3 + c_6 - c_7, \end{aligned}$$

where

$$N = \begin{cases} 0 & \text{if } \gamma_\ell \text{ is inseparable} \\ \frac{q-1}{2} & \text{if } \operatorname{char}(K) \neq 2 \text{ and there are two parabolic points in } \ell(K) \\ \frac{q}{2} & \text{if } \operatorname{char}(K) = 2 \text{ and } \gamma_\ell \text{ is separable} \\ \frac{q+1}{2} & \text{if } \operatorname{char}(K) \neq 2 \text{ and there are no parabolic points in } \ell(K). \end{cases}$$

Proof. Consequence of Proposition 5.2, Corollary 5.4 and Theorem 5.8. □

Chapter 6

Equivalence classes of pointed cubic surfaces

In this chapter we prove the following theorem.

Theorem 6.2. *Let S be a smooth cubic surface defined over $K = \mathbb{F}_5$ or $\mathbb{F}_7$ and containing a non-Eckardt point $P \in S(K)$ such that P is a cusp of Γ_P. Then*

$$\mathrm{Span}(P) = S(K).$$

We also lay down the groundwork for proving similar theorems computationally for a given finite field. For this we require a method of enumerating pointed cubic surfaces over $K = \mathbb{F}_q$ up to equivalence. By a *pointed cubic surface* we mean a pair (S, P) where S is a cubic surface and $P \in S(K)$ is a non-singular point. Two pairs (S, P), (S', P') are *equivalent* if there is a linear transformation over K that takes S to S' and P to P'.

In many situations when computing with cubic surfaces it is sufficient to consider isomorphism class representatives rather than all cubic surfaces. The moduli space of cubic surfaces is isomorphic to the weighted projective space $\mathbb{P}(1, 2, 3, 4, 5)$ [8], which is in fact a modern re-writing of the results of Salmon and Clebsch in [17] and [3] respectively. This space is 5-dimensional. Heuristically this would imply that the moduli space of pointed cubic surfaces is 7-dimensional. Testing that two cubic surfaces defined over a field K are isomorphic over K involves testing for equivalence of cubic polynomials in four variables defined over K under an action of $K^* \times \mathrm{GL}(4, K)$; K^* acts by scaling and $\mathrm{GL}(4, K)$ by substitution.

For a pointed cubic surface (S, P) there are several different possibilities for Γ_P. These possibilities are non-isomorphic so in this chapter we aim to find

subgroups of $K^* \times \mathrm{GL}(4,K)$ that preserve the form of Γ_P. Orbits of these subgroups of $K^* \times \mathrm{GL}(4,K)$ are equivalence classes over K of pointed cubic surfaces defined over K.

6.1 Computing equivalence classes of pointed cubic surfaces

Throughout this chapter let $K = \mathbb{F}_q$. In this section we will give a form for the defining polynomial of a general pointed cubic surface (S,P), with $P = (0:0:0:1)$ and $\Pi_P : X = 0$. We will consider the collection of such surfaces denoted by $\mathcal{F}$ and give the subgroup $\mathcal{G}$ of $K^* \times \mathrm{GL}(4,K)$ that preserves $\mathcal{F}$. We will then find subsets of $\mathcal{F}$ that correspond to different possibilities for Γ_P. We will find subgroups of $\mathcal{G}$ that preserve these subsets of $\mathcal{F}$ and give generators.

6.1.1 General pointed cubic surfaces

Lemma 6.1. *Every pointed cubic surface over K is equivalent to a cubic surface in the set*

$$\mathcal{F} := \left\{ XW^2 + Q(X,Y,Z)W + C(X,Y,Z) \;\middle|\; \begin{array}{l} Q \text{ and } C \text{ are homogeneous cubic} \\ \text{polynomials in } X,\ Y \text{ and } Z \end{array} \right\},$$

and this set is preserved by an action of the group

$$\mathcal{G} := \left\{ G = \begin{pmatrix} a_{44}^{-2} & a_{12} & a_{13} & a_{14} \\ 0 & a_{22} & a_{23} & a_{24} \\ 0 & a_{32} & a_{33} & a_{34} \\ 0 & 0 & 0 & a_{44} \end{pmatrix} \middle| G \in \mathrm{GL}(4,K) \right\}$$

on the variables X, Y, Z and W.

Further, any $F \in \mathcal{F}$ is equivalent to a polynomial of the form

$$XW^2 + (aY^2 + bYZ + cZ^2)W + C(X,Y,Z)$$

where $a,b,c \in K$ and C is a homogeneous cubic form.

Proof. Any cubic surface defined over a field K and containing a smooth K-point is equivalent to a cubic surface defined over K that contains the smooth point $P = (0:0:0:1)$ and is such that Π_P is the plane $X = 0$. Therefore we need only consider surfaces in this form.

Let S be a cubic surface defined by the equation $F(X,Y,Z,W) = 0$ where F is a homogeneous cubic polynomial with coefficients in a finite field $K = \mathbb{F}_q$. Suppose that S contains the smooth point $P = (0:0:0:1)$ and Π_P is the plane $X = 0$. Then the equation of the surface can be written as

$$S : F(X,Y,Z,W) = XW^2 + Q(X,Y,Z)W + C(X,Y,Z) = 0,$$

where Q and C are respectively homogeneous quadratic and cubic polynomials with coefficients in K. We define the set $\mathcal{F}$ as follows

$$\mathcal{F} := \left\{ XW^2 + Q(X,Y,Z)W + C(X,Y,Z) \quad \middle| \quad \begin{array}{l} Q \text{ and } C \text{ are homogeneous cubic} \\ \text{polynomials in } X,\ Y \text{ and } Z \end{array} \right\}$$

Note that this fixes the choice of the coefficient of XW^2 as 1. Therefore we need no longer consider the scaling action of K^*, but consider only $\mathrm{GL}(4,K)$. We aim to find the subgroup $\mathcal{G}$ of $\mathrm{GL}(4,K)$ that preserves the set $\mathcal{F}$. We may start with a general invertible matrix

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{pmatrix} \in \mathrm{GL}(4,K),$$

which represents the transformation

$$\begin{aligned} X &\longmapsto a_{11}X + a_{21}Y + a_{31}Z + a_{41}W \\ Y &\longmapsto a_{12}X + a_{22}Y + a_{32}Z + a_{42}W \\ Z &\longmapsto a_{13}X + a_{23}Y + a_{33}Z + a_{43}W \\ W &\longmapsto a_{14}X + a_{24}Y + a_{34}Z + a_{44}W. \end{aligned}$$

Our first condition is that the point P should map to itself.

$$\begin{pmatrix} 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & a_{44} \end{pmatrix}.$$

Therefore $a_{41} = a_{42} = a_{43} = 0$. So we have the transformation

$$\begin{aligned} X &\longmapsto a_{11}X + a_{21}Y + a_{31}Z \\ Y &\longmapsto a_{12}X + a_{22}Y + a_{32}Z \\ Z &\longmapsto a_{13}X + a_{23}Y + a_{33}Z \\ W &\longmapsto a_{14}X + a_{24}Y + a_{34}Z + a_{44}W. \end{aligned}$$

Notice that X, Y and Z map to K-linear forms in X, Y and Z. Thus $Q(X,Y,Z)$ will map to $Q'(X,Y,Z)$ and $C(X,Y,Z)$ will map to $C'(X,Y,Z)$, where Q' and C' are respectively homgeneous quadratic and cubic polynomials with coefficients in K. This will make it easier for us to see which terms of the equation are divisible by W and W^2 after the transformation.

First consider the term XW^2. We want the W^2-term of f to remain as XW^2 after the transformation.

$$\begin{aligned} XW^2 &\longmapsto (a_{11}X + a_{21}Y + a_{31}Z)(a_{14} + a_{24}Y + a_{34} + a_{44})^2 \\ &= (a_{11}X + a_{21}Y + a_{31}Z)a_{44}^2W^2 + \cdots \end{aligned}$$

Thus we require $a_{21} = a_{31} = 0$ and $a_{11}a_{44}^2XW^2 = XW^2$, so $a_{11} = a_{44}^{-2}$. Only matrices of the form

$$\begin{pmatrix} a_{44}^{-2} & a_{12} & a_{13} & a_{14} \\ 0 & a_{22} & a_{23} & a_{24} \\ 0 & a_{32} & a_{33} & a_{34} \\ 0 & 0 & 0 & a_{44} \end{pmatrix}$$

with $a_{44} \neq 0$ preserve pointed surfaces with $P = (0:0:0:1)$ and $\Pi_P : X = 0$. Hence the subgroup $\mathcal{G}$ of $\mathrm{GL}(4,K)$ that preserves the set F is precisely invertible matrices of this form. We now simplify the quadratic $Q(X,Y,Z)$ using the transformations of this form.

$$\begin{aligned} X &\longmapsto a_{44}^{-2}X \\ Y &\longmapsto a_{12}X + a_{22}Y + a_{32}Z \\ Z &\longmapsto a_{13}X + a_{23}Y + a_{33}Z \\ W &\longmapsto a_{14}X + a_{24}Y + a_{34}Z + a_{44}W. \end{aligned}$$

The transformation of F is given by

$$\begin{aligned} & XW^2 + Q(X,Y,Z) + C(X,Y,Z) \\ \longmapsto\ & a_{44}^{-2} X(a_{14}X + a_{24}Y + a_{34}Z + a_{44}W)^2 \\ & + Q'(X,Y,Z)(a_{14}X + a_{24}Y + a_{34}Z + a_{44}W) \\ & + C'(X,Y,Z) \\ =\ & XW^2 \\ & + (2a_{44}^{-1}X(a_{14}X + a_{24}Y + a_{34}Z) + Q'(X,Y,Z))W \\ & + a_{44}^{-2}(a_{14}X + a_{24}Y + a_{34}Z)^2 + C'(X,Y,Z). \end{aligned}$$

The transformed quadratic $Q'(X,Y,Z)$ can be written as

$$Q'(X,Y,Z) = b_{11}X^2 + b_{22}Y^2 + b_{33}Z^2 + b_{12}XY + b_{13}XZ + b_{23}YZ$$

with the $b_{ij} \in K$. The b_{ij} are fixed, but we can choose the a_{kl} provided the determinant of the matrix remains nonzero. We now consider the terms of the transformed F that are divisble by W but not W^2, which are

$$(2a_{44}^{-1}X(a_{14}X + a_{24}Y + a_{34}Z) + Q'(X,Y,Z))W.$$

We wish to simplify the expression. Notice that we can eliminate the terms containing X by our choice of a_{14}, a_{24} and a_{34}, i.e.

$$\begin{aligned} a_{14} &= -2a_{44}b_{11}, \\ a_{24} &= -2a_{44}b_{12}, \\ a_{34} &= -2a_{44}b_{13}. \end{aligned}$$

So every pointed cubic surface over K is equivalent to one of the form

$$S : XW^2 + (b_{22}Y^2 + b_{23}YZ + b_{33}Z^2)W + C(X,Y,Z) = 0.$$

where $C(X,Y,Z)$ is some homogeneous cubic polynomial. □

6.1.2 Cases for the quadratic part of S

For the remainder of Section 6.1 we assume that $\mathrm{char}(K) \neq 2$. We may complete the square to get[1]

$$S : XW^2 + (\alpha Y^2 + \beta Z^2)W + C(X,Y,Z) = 0,$$

[1] If $b_{22} = b_{33} = 0$ then we can employ the identity $YZ = \frac{1}{4}\left((Y+Z)^2 - (Y-Z)^2\right)$.

where C is some homogeneous cubic polynomial in X, Y and Z. This yields the following cases for the defining equation of S

(a) $XW^2 + C(X,Y,Z) = 0$,

(b) $XW^2 + Y^2W + C(X,Y,Z) = 0$,

(c) $XW^2 + \eta Y^2W + C(X,Y,Z) = 0$,

(d) $XW^2 + (Y^2 - Z^2)W + C(X,Y,Z) = 0$,

(e) $XW^2 + (Y^2 - \eta Z^2)W + C(X,Y,Z) = 0$,

(f) $XW^2 + \eta(Y^2 - Z^2)W + C(X,Y,Z) = 0$,

where η is a chosen non-square element of K^*. In fact we can reduce case (c) to case (b) using the following transformation.

$$\begin{aligned} X &\longmapsto X \\ Y &\longmapsto Y \\ Z &\longmapsto Z \\ W &\longmapsto \eta W \end{aligned}$$

When applied to the defining equation of S given in case (c) this transformation yields

$$XW^2 + \eta Y^2W + C(X,Y,Z) \longmapsto \eta^2XW^2 + \eta^2Y^2W + C(X,Y,Z),$$

so the equation of S is

$$\eta^2XW^2 + \eta^2Y^2W + C(X,Y,Z) = 0.$$

We may divide through by η^2 to get

$$XW^2 + Y^2W + C'(X,Y,Z) = 0,$$

which is case (b). Similarly, we can reduce case (f) to case (d). This means we have the following four possible cases.

1. $XW^2 + C(X,Y,Z) = 0$,
2. $XW^2 + Y^2W + C(X,Y,Z) = 0$,
3. $XW^2 + (Y^2 - Z^2)W + C(X,Y,Z) = 0$,

4. $XW^2 + (Y^2 - \eta Z^2)W + C(X, Y, Z) = 0$.

We can now describe these four cases geometrically. Here $P = (0 : 0 : 0 : 1)$ and Γ_P is a cubic curve in the plane with equation $X = 0$.

1. **Eckardt pointed surface.** $\Gamma_P : X = C(0, Y, Z) = 0$. The polynomial $C(0, Y, Z)$ is homogeneous so, over some extension of K, it will factor into three linear components. These correspond to three lines in S all passing through P, so P is an Eckardt point and Γ_P is a special case of a cuspidal cubic. See Figures 1.7, 1.8 and 1.9 on page 10.

2. **Cusp pointed surface.** $\Gamma_P : X = Y^2W + C(0, Y, Z) = 0$. In this case Γ_P is a cubic curve with a cusp at P. Asymptotically we can see that there is a double tangent line at $Y = 0$. This case includes absolutely irreducible curves with a cusp at P as in Figure 1.5 on page 10 and those where $Y^2W + C(0, Y, Z)$ factors into a linear component and a quadratic component over K and the line and conic that these represent have a double intersection at the point P as in Figure 1.6 on page 10.

3. **Split node pointed surface.** $\Gamma_P : X = (Y^2 - Z^2)W + C(0, Y, Z) = 0$. Here Γ_P is a cubic curve with a split node at the point P, so there are two tangent lines at P, namely, $Y + Z = 0$ and $Y - Z = 0$, which are both defined over K. Generally Γ_P is an irreducible plane cubic curve with a node at P as in Figure 1.1 on page 9, but there are also two special cases. The first is where $(Y^2 - Z^2)W + C(0, Y, Z)$ factors over K into a linear component and a quadratic component and hence we have a line and a conic with two distinct intersection points, one of which is P, see Figure 1.2 on page 1.2. The second is where $(Y^2 - Z^2)W + C(0, Y, Z)$ has three linear factors over K and hence we have three lines that intersect pairwise, but not all in the same point as P is not Eckardt, and one of the three points of intersection is P as in Figure 1.3 on page 9.

4. **Non-split node pointed surface.** $\Gamma_P : X = (Y^2 - \eta Z^2)W + C(0, Y, Z) = 0$, where η is a fixed choice of non-square in K. In this case Γ_P is a cubic curve with a non-split node at P so there are two tangent lines at P, namely, $Y + \sqrt{\eta}Z = 0$ and $Y - \sqrt{\eta}Z = 0$, neither of which is defined over K. This case is as illustrated in Figure 1.1 on page 9, but with the tangent lines at P non-rational. There is one special case: Γ_P can split into three lines: one K-line ℓ and two others that are Galois conjugates defined over $K(\sqrt{\eta})$, whose point of intersection is $P \notin \ell$. See Figure 3.4 on page 42.

Every pointed cubic surface over K is equivalent to a pointed cubic surface (S, P) over K with $P = (0 : 0 : 0 : 1)$ that is in one of these four forms. The four forms are non-equivalent, but are not equivalence classes so we now wish to find subgroups of $\mathcal{G} \subset \mathrm{GL}(4, K)$ that preserve equations in each of these forms. Then representatives of the orbits of the group actions of these subgroups will be equivalence class representatives. Such subgroups will be considerably smaller than $\mathrm{GL}(4, K)$ so the orbits of the group actions will take substantially less time to compute.

6.1.3 Eckardt pointed cubic surfaces

We want to find invertible matrices with entries in K that preserve the equation of a pointed cubic surface (S, P) with P an Eckardt point. From Section 6.1.2 we know that the equations for such surfaces have the following form:

$$S : XW^2 + C(X, Y, Z) = 0.$$

From now on we consider the collection of such surfaces:

$$\mathcal{F}_E := \left\{ XW^2 + C(X, Y, Z) \quad \middle| \quad \begin{array}{l} C(X, Y, Z) \text{ is a homogeneous} \\ \text{cubic polynomial in } X, Y \text{ and } Z \end{array} \right\}.$$

Let $\mathcal{G}_E$ be the subgroup of $\mathrm{GL}(4, K)$ preserving $\mathcal{F}_E$. First we will write down explicit generators for $\mathcal{G}_E$, and using this it should be possible, for given $\mathbb{F}_q$, to determine the equivalence classes $\mathcal{G}_E \backslash \mathcal{F}_E$.

We start with the transformation

$$\begin{aligned} X &\longmapsto a_{44}^{-2} X \\ Y &\longmapsto a_{12}X + a_{22}Y + a_{32}Z \\ Z &\longmapsto a_{13}X + a_{23}Y + a_{33}Z \\ W &\longmapsto a_{14}X + a_{24}Y + a_{34}Z + a_{44}W \end{aligned}$$

and apply it to the equation for S:

$$\begin{gathered} XW^2 + C(X, Y, Z) \\ \downarrow \\ a_{44}^{-2} X (a_{14}X + a_{24}Y + a_{34}Z + a_{44}W)^2 + C'(X, Y, Z) \\ = \\ XW^2 + (2a_{44}^{-1}a_{14}X^2 + 2a_{44}^{-1}a_{24}XY + 2a_{44}^{-1}a_{34}XZ)W + C''(X, Y, Z). \end{gathered}$$

For this equation to hold we require that $a_{14} = a_{24} = a_{34} = 0$. Therefore $\mathcal{G}_E$ consists of invertible matrices of the form

$$\begin{pmatrix} a_{44}^{-2} & a_{12} & a_{13} & 0 \\ 0 & a_{22} & a_{23} & 0 \\ 0 & a_{32} & a_{33} & 0 \\ 0 & 0 & 0 & a_{44} \end{pmatrix}.$$

In order to use this subgroup to compute equivalence classes of Eckardt pointed cubic surfaces we find its generators. Let g be a generator of $K^\times$ and write $a_{44} = g^\alpha$. It follows that

$$\begin{pmatrix} g^{-2} & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & g \end{pmatrix}^{-\alpha} \begin{pmatrix} a_{44}^{-2} & a_{12} & a_{13} & 0 \\ 0 & a_{22} & a_{23} & 0 \\ 0 & a_{32} & a_{33} & 0 \\ 0 & 0 & 0 & a_{44} \end{pmatrix} = \begin{pmatrix} 1 & a'_{12} & a'_{13} & 0 \\ 0 & a_{22} & a_{23} & 0 \\ 0 & a_{32} & a_{33} & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

We can then reduce the central minor of the matrix by using the generators of $\mathrm{GL}_2(K)$, which we will call A_1, A_2, $\ldots$ A_k. This gives

$$\begin{pmatrix} 1 & \cdots & 0 \\ \vdots & A_1 & \vdots \\ 0 & \cdots & 1 \end{pmatrix}^{-\alpha_1} \begin{pmatrix} 1 & \cdots & 0 \\ \vdots & A_2 & \vdots \\ 0 & \cdots & 1 \end{pmatrix}^{-\alpha_2} \cdots \begin{pmatrix} 1 & \cdots & 0 \\ \vdots & A_k & \vdots \\ 0 & \cdots & 1 \end{pmatrix}^{-\alpha_k} \begin{pmatrix} 1 & a'_{12} & a'_{13} & 0 \\ 0 & a_{22} & a_{23} & 0 \\ 0 & a_{32} & a_{33} & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & a'_{12} & a'_{13} & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

where

$$A_1^{\alpha_1} A_2^{\alpha_2} \ldots A_k^{\alpha_k} = \begin{pmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{pmatrix}.$$

A further decomposition shows that

$$\begin{pmatrix} 1 & v_1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}^{\beta_1} \begin{pmatrix} 1 & v_2 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}^{\beta_2} \cdots \begin{pmatrix} 1 & v_n & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}^{\beta_n} \begin{pmatrix} 1 & a'_{12} & a'_{13} & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 0 & a'_{13} & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

where $v_1, \ldots, v_n$ is a basis for $K = \mathbb{F}_{p^n} = \mathbb{F}_q$ over $\mathbb{F}_p$ and $\beta_1 v_1 + \cdots + \beta_n v_n = -a'_{12}$. Likewise we can formulate

$$\begin{pmatrix} 1 & 0 & v_1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}^{\gamma_1} \begin{pmatrix} 1 & 0 & v_2 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}^{\gamma_2} \cdots \begin{pmatrix} 1 & 0 & v_n & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}^{\gamma_n} \begin{pmatrix} 1 & 0 & a'_{13} & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

where $\gamma_1 v_1 + \cdots + \gamma_n v_n = -a'_{13}$. Hence the matrices

$$\begin{pmatrix} g^{-2} & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & g \end{pmatrix},$$

$$\begin{pmatrix} 1 & \cdots & 0 \\ \vdots & A_1 & \vdots \\ 0 & \cdots & 1 \end{pmatrix}, \begin{pmatrix} 1 & \cdots & 0 \\ \vdots & A_2 & \vdots \\ 0 & \cdots & 1 \end{pmatrix}, \ldots, \begin{pmatrix} 1 & \cdots & 0 \\ \vdots & A_k & \vdots \\ 0 & \cdots & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & v_1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & v_2 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \ldots, \begin{pmatrix} 1 & v_n & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

and

$$\begin{pmatrix} 1 & 0 & v_1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & v_2 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \ldots, \begin{pmatrix} 1 & 0 & v_n & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

form a set of generators for $\mathcal{G}_E$. The orbits of this subgroup $\mathcal{G}_E$ acting on $\mathcal{F}_E$ are

the equivalence classes of Eckardt pointed cubic surfaces defined over K.

Once equipped with the generators of $\mathcal{G}_E$ we can compute equivalence class representatives of Eckardt pointed cubic surfaces. Below are the details of a program written in `MAGMA` [13] that computes a list of such equivalence class representatives. First note that the equation for an Eckardt pointed cubic surface (S, P) defined over a field K with $P = (0:0:0:1)$ and $\Pi_P : X = 0$ can be written

$$S : XW^2 + aX^3 + L(Y,Z)X^2 + Q(Y,Z)X + C(Y,Z) = 0,$$

where L, Q and C are homogeneous linear, quadratic and cubic polynomials respectively, and $a \in K$. We then need only consider homogeneous cubic polynomials $C(Y,Z)$ that are inequivalent under an action of $\mathrm{GL}(2,K)$.

We begin by defining a finite field K of odd characteristic. For example

```
p:=3 ;
K := GF(p);
```

For the first of our generators for $\mathcal{G}_E$ we require a generator of $K^\times$, denoted g. We will create $\mathcal{G}_E$ as a subgroup of $\mathrm{GL}(4,K)$, which is denoted `G`.

```
g:=PrimitiveElement(K);
G:=GL(4,K);
gens:=[
G![[g^-2,0,0,0],[0,1,0,0],[0,0,1,0],[0,0,0,g]]
];
```

We then make a complete list of all possible homogeneous cubic binomials in Z and Y over K, denoted `bins`. These are all the possibilities for $C(Y,Z)$.

```
P<Y,Z>:=PolynomialRing(K,2);
mons:=[Y^3,Y^2*Z,Y*Z^2,Z^3];
V:=VectorSpace(K,4);
V:=[Eltseq(v) : v in V];
bins:=[ &+[v[i]*mons[i] : i in [1..4]] : v in V];
```

We now perform a group action of $\mathrm{GL}(2,K)$ on the elements of `bins` and take one representative binomial from each of the orbits of this group action. The list of these representatives is `binreps`. This group action is defined similarly to that of $\mathrm{GL}(4,K)$ on homogeneous cubic polynomials in four variables described in Subsection 6.1.1. In order to find orbit representatives we repeat the following two steps until `bins` is empty.

1. Pick a random element of `bins`, denoted `F`, and put it in `binreps`.

2. Remove the orbit of `F` (including `F`) from `bins`.

```
G2:=GL(2,K);
binreps:=[];
print #binreps,#bins;
repeat
F:=Random(bins);
orb:=Orbit(G2,F);
bins:=[ h : h in bins | h in orb eq false];
Append(~binreps,F);
print #binreps,#bins;
until #bins eq 0;
```

The reason we pick a random element of `bins` is so that probabilistically we are more likely to pick binomials with large orbits in `bins` earlier in the process that we would by iterating through the elements of `bins` in the lexicographical order in which they are given by `MAGMA`. This means that the list `bins` should decrease in size in relatively few iterations towards the beginning of the process, which will mean that fewer comparisons between elements in the orbit of a monomial `F` and the elements of `bins` need to be computed. This speeds up the program.

The following code adds these matrices

$$\begin{pmatrix} 1 & \cdots & 0 \\ \vdots & A_1 & \vdots \\ 0 & \cdots & 1 \end{pmatrix}, \begin{pmatrix} 1 & \cdots & 0 \\ \vdots & A_2 & \vdots \\ 0 & \cdots & 1 \end{pmatrix}, \ldots, \begin{pmatrix} 1 & \cdots & 0 \\ \vdots & A_k & \vdots \\ 0 & \cdots & 1 \end{pmatrix}$$

to the list of generators of $\mathcal{G}_E$, where $A_1, \ldots, A_k$ are generators of $\mathrm{GL}(2, K)$.

```
for m in Generators(G2) do
Append(~gens,
G![
[1,0,0,0], [0,m[1,1],m[1,2],0], [0,m[2,1],m[2,2],0], [0,0,0,1]
]);
end for;
```

This code does the same for the matrices

$$\begin{pmatrix} 1 & v_1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & v_2 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \ldots, \begin{pmatrix} 1 & v_n & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

and

$$\begin{pmatrix} 1 & 0 & v_1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & v_2 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \ldots, \begin{pmatrix} 1 & 0 & v_n & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

where $v_1, \ldots, v_n$ are a basis for $K = \mathbb{F}_q$ over $\mathbb{F}_p$ with p prime and $q = p^n$, for some positive integer n. The v_i are denoted `b` in the `MAGMA` code.

```
for b in Basis(K) do
Append(~gens,
G![ [1,b,0,0],[0,1,0,0],[0,0,1,0],[0,0,0,1] ]
);
Append(~gens,
G![ [1,0,b,0],[0,1,0,0],[0,0,1,0],[0,0,0,1] ]
);
end for;
```

We now have a full set of generators for $\mathcal{G}_E$, denoted `H` in the code, so can create it as a subgroup of $\mathrm{GL}(4, K)$.

```
H:=sub< G | gens >;
```

The elements of `binreps` are currently elements of $K[Y, Z]$, and we require `MAGMA` to recognise them as elements of $K[X, Y, Z, W]$, denoted `P` below.

```
P<X,Y,Z,W>:=PolynomialRing(K,4);
binreps:=[ Evaluate(F,[Y,Z])   : F in binreps];
```

An Eckardt pointed cubic surface (S, P) with $P = (0 : 0 : 0 : 1)$ and $\Pi_P : X = 0$ has equation

$$S : XW^3 + aX^3 + X^2L(Y, Z) + XQ(Y, Z) + C(Y, Z) = 0,$$

where L, Q and C are respectively homogeneous linear, quadratic and cubic polynomials in Y and Z, and $a \in K$. The list `binreps` contains all the inequivalent possibilities for $C(Y, Z)$ under an action of $\mathrm{GL}(2, K)$. The list `mons` is all possible

monomials in $aX^3 + X^2L(Y,Z) + XQ(Y,Z)$. We confirm that there are six such monomials, namely, X^3, X^2Y, X^2Z, XY^2, XYZ and XZ^2.

```
mons:=MonomialsOfDegree(P,3);
mons:=[ m : m in mons |
IsDivisibleBy(m,W) eq false and IsDivisibleBy(m,X) eq true
];
assert #mons eq 6;
```

We now create the list `surfaces1`, which is all homogeneous cubic polynomials in X, Y, Z and W of the form $XW^3 + aX^3 + X^2L(Y,Z) + XQ(Y,Z)$.

```
V:=VectorSpace(K,6);
V:=[Eltseq(v) : v in V];
surfaces1:=[ W^2*X+ &+[ v[i]*mons[i] : i in [1..6] ] : v in V ];
```

The list `surfaces` is all homogeneous cubic polynomials in X, Y, Z and W of the form $XW^3+aX^3+X^2L(Y,Z)+XQ(Y,Z)+C(Y,Z)$ with $C(Y,Z)$ inequivalent under an action of $\mathrm{GL}(2,K)$. We can find orbit representatives of the action of $\mathcal{G}_E$ on the elements of `surfaces`; these are stored in the list `reps`. We test for equivalence of the $C(Y,Z)$ first to avoid redundant comparisons between members of the orbit of a polynomial `h` with equivalent forms in `surfaces`.

```
reps:=[];
for f in binreps do
surfaces:=[ g+f : g in surfaces1 ];
print #reps,#surfaces;
repeat
h:=Random(surfaces);
orb:=Orbit(H,h);
Append(~reps,h);
surfaces:=[F : F in surfaces | F in orb eq false   ];
print #reps,#surfaces;
until #surfaces eq 0;
end for;
```

This process terminates when all orbits have been removed from `surfaces`. The list `reps` is a complete list of polynomials representing inequivalent Eckardt pointed cubic surfaces over K under an action of $K^* \times \mathrm{GL}(4,K)$.

6.1.4 Cusp pointed surfaces

We define the set

$$\mathcal{F}_C := \left\{ XW^2 + Y^2W + C(X,Y,Z) \quad \middle| \quad \begin{array}{l} C(X,Y,Z) \text{ is a homogeneous} \\ \text{cubic polynomial in } X,\ Y,\ Z \end{array} \right\},$$

and aim to find the subgroup $\mathcal{G}_C$ of $\mathrm{GL}(4,K)$ that preserves $\mathcal{F}_C$. We shall refer to a pointed cubic surface (S,P) where P is a cusp of Γ_P as cusp pointed surfaces. The set $\mathcal{F}_C$ is a set of cusp pointed cubic surfaces with $P = (0:0:0:1)$ and $\Pi_P : X = 0$. Note that any cusp pointed cubic surface over K is equivalent to a surface in $\mathcal{F}_C$. Let $(S,P) \in \mathcal{F}_C$ and let F be the defining polynomial of S. We apply the following transformation to F.

$$\begin{array}{rcl} X & \longmapsto & a_{44}^{-2}X, \\ Y & \longmapsto & a_{12}X + a_{22}Y + a_{32}Z, \\ Z & \longmapsto & a_{13}X + a_{23}Y + a_{33}Z, \\ W & \longmapsto & a_{14}X + a_{24}Y + a_{34}Z + a_{44}W, \end{array}$$

and we arrive at

$$\begin{array}{rl} & XW^2 \\ + & (2a_{44}^{-1}a_{14} + a_{12}^2a_{44})X^2W \\ + & (2a_{44}^{-1}a_{24} + 2a_{12}a_{22}a_{44})XYW \\ + & (2a_{44}^{-1}a_{34} + 2a_{12}a_{32}a_{44})XZW \\ + & a_{22}^2a_{44}Y^2W + a_{32}^2a_{44}Z^2W \\ + & 2a_{22}a_{32}a_{44}YZW. \end{array}$$

For this to hold we require

$$\begin{array}{rcl} 2a_{44}^{-1}a_{14} + a_{12}^2a_{44} & = & 0, \\ 2a_{44}^{-1}a_{24} + 2a_{12}a_{22}a_{44} & = & 0, \\ 2a_{44}^{-1}a_{34} + 2a_{12}a_{32}a_{44} & = & 0, \\ a_{22}^2a_{44} & = & 1, \\ a_{32}^2a_{44} & = & 0, \\ 2a_{22}a_{32}a_{44} & = & 0. \end{array}$$

The coefficient a_{44} is nonzero because the determinant of the matrix representing the transformation is nonzero. So $a_{32}^2a_{44} = 0$ implies that $a_{32} = 0$. From $a_{22}^2a_{44} = 1$ we deduce that $a_{44} = a_{22}^{-2}$. We find that $a_{34} = 0$ because $a_{32} = 0$ and $2a_{44}^{-1}a_{34}+2a_{12}a_{32}a_{44} = 0$. We also find that $a_{14} = -\frac{1}{2}a_{22}^{-4}a_{12}^2$ and $a_{24} = -a_{22}^{-3}a_{12}$. Hence the matrix of any

transformation that preserves a cusp pointed surface is of the form

$$\begin{pmatrix} a_{22}^4 & a_{12} & a_{13} & -\frac{1}{2}a_{22}^{-4}a_{12}^2 \\ 0 & a_{22} & a_{23} & -a_{22}^{-3}a_{12} \\ 0 & 0 & a_{33} & 0 \\ 0 & 0 & 0 & a_{22}^{-2} \end{pmatrix}.$$

Following a similar process to that used in Section 6.1.3 we find a set of generators for $\mathcal{G}_C$ is as follows.

$$\begin{pmatrix} g^4 & 0 & 0 & 0 \\ 0 & g & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & g^{-2} \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & g & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

$$\begin{pmatrix} 1 & v_i & 0 & -\frac{1}{2}v_i^2 \\ 0 & 1 & 0 & -v_i \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & v_i & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & v_i & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

where g is again a generator for $K^\times$ and v_i, $i \in \{1, \ldots, n\}$ is a vector basis for $K = \mathbb{F}_{p^n}$ over $\mathbb{F}_p$, p prime.

In order to further improve the efficiency of programs that find equivalence classes of cusp pointed cubic surfaces, one could consider subcases of cusp pointed cubic surfaces.

Subcase 1: Γ_P is a general reducible cubic curve over K with a cusp at P. Thus Γ_P is the union of a line ℓ and a conic C, and P is the unique intersection point of ℓ and C.

We have $\ell : X = Y = 0$ since $Y = 0$ is a double tangent line to Γ_P at P in the plane $\Pi_P : X = 0$. The general equation of a cubic curve with a cusp at the point $P = (0:0:0:1)$ and a double tangent line to P at $Y = 0$ is

$$S : XW^2 + Y^2W + C(X, Y, Z) = 0$$

or, more fully,

$$\begin{aligned} S: \quad XW^2 + Y^2W &+ a_1X^3 + a_2X^2Y + a_3X^2Z + a_4XY^2 \\ &+ a_5XYZ + a_6XZ^2 + a_7Y^3 + a_8Y^2Z + a_9YZ^2 + a_{10}Z^3 = 0. \end{aligned}$$

We set $X = 0$ to obtain the equation for Γ_P:

$$\Gamma_P : Y^2W + a_7Y^3 + a_8Y^2Z + a_9YZ^2 + a_{10}Z^3 = 0.$$

In order for Γ_P to split into ℓ and C, we must have Y as a factor of the defining polynomial for Γ_P, therefore $a_{10} = 0$. This reduces the equation to

$$\Gamma_P : Y^2W + a_7Y^3 + a_8Y^2Z + a_9YZ^2 = 0.$$

Since $\mathrm{char}(K) \neq 2$ we may complete the square in Z to further simplify the defining polynomial for Γ_P as follows:

$$\begin{aligned}
& Y^2W + a_7Y^3 + a_8Y^2Z + a_9YZ^2 \\
= \;& Y^2W + a_9Y(Z^2 + \tfrac{a_8}{a_9}YZ + \tfrac{a_7}{a_9}Y^2) \\
= \;& Y^2 + a_9Y((Z + \tfrac{a_8}{2a_9}Y)^2 + (\tfrac{a_7}{a_9} - \tfrac{a_8^2}{4a_9^2})Y^2) \\
= \;& Y^2W + a_9YZ'^2 + a_9(\tfrac{a_7}{a_9} - \tfrac{a_8^2}{4a_9^2})Y^3 \\
= \;& Y^2W + b_1Y^3 + b_2YZ'^2,
\end{aligned}$$

where $Z' = Z + \frac{a_8}{2a_9}Y$, $b_1 = a_9(\frac{a_7}{a_9} - \frac{a_8^2}{4a_9^2})$ and $b_2 = a_9$. Note that $a_9 = b_2 = 0$ implies that Z is a factor, meaning that Γ_P is the union of the lines $Z = 0$ with multiplicity 1 and $Y = 0$ with multiplicity 2. This is a contradiction to the smoothness of S so $a_9 \neq 0$.

The equation of a general reducible cusp pointed cubic surface can be written as follows:

$$\begin{aligned}
S: \quad XW^2 + Y^2W \;&+\; a_1X^3 + a_2X^2Y + a_3X^2(Z' - cY) + a_4XY^2 \\
&+\; a_5XY(Z' - cY) + a_6X(Z' - cY)^2 + b_1Y^3 + b_2YZ^2 \;=\; 0,
\end{aligned}$$

which may be simplified to

$$\begin{aligned}
S: \quad XW^2 + Y^2W \;&+\; c_1X^3 + c_2X^2Y + c_3X^2Z' + c_4XY^2 \\
&+\; c_5XYZ' + c_6XZ'^2 + c_7Y^3 + c_8YZ'^2 \;=\; 0,
\end{aligned}$$

with $c_i \in K$ and $c_8 \neq 0$. We make a further transformation $Z'' = \alpha Z'$ where $a_9 = \alpha^2$ if a_9 is a quadratic residue in K, and $a_9 = \eta\alpha^2$ otherwise, with η our chosen quadratic non-residue (if one exists in K) otherwise. This allows us to reduce our choice of c_8 to 1 or η meaning that we iterate over a total of $2p^7$ equations for cubic surfaces in the reducible cuspidal case.

Subcase 2: Γ_P is an irreducible cuspidal cubic curve. For this case we will assume

that $\mathrm{char}(K) \neq 2, 3$. The equation of the pointed cubic surface is

$$S : XW^2 + Y^2W + C(X, Y, Z) = 0.$$

As before we set $X = 0$ to find the equation for Γ_P:

$$\Gamma_P : Y^2W + a_7Y^3 + a_8Y^2Z + a_9YZ^2 + a_{10}Z^3 = 0.$$

This time Y must not be a factor of the defining polynomial for Γ_P so $a_{10} \neq 0$. Since $\mathrm{char}(K) \neq 3$ we can "complete the cube" in Z to obtain

$$\begin{aligned} Y^2W + a_{10}\left(Z^3 + \frac{a_9}{a_{10}}YZ^2 + \frac{a_8}{a_{10}}Y^2Z + \frac{a_7}{a_{10}}Y^3\right) &= 0 \\ Y^2W + a_{10}\left(\left(Z + \frac{a_9}{3a_{10}}Y\right)^3 + \left(\frac{a_8}{a_{10}} - \frac{a_9^2}{3a_{10}^2}\right)Y^2Z + \left(\frac{a_7}{a_{10}} - \frac{a_9^3}{27a_{10}^3}\right)Y^3\right) &= 0 \\ Y^2W + b_1Y^3 + b_2Y^2Z' + a_{10}Z'^3 &= 0. \end{aligned}$$

In fact, we may choose $a_{10} = 1, \omega, \omega^2$ where ω is a chosen cubic non-residue in K if such exists, otherwise $a_{10} = 1$. This gives us

$$\begin{aligned} S: \quad XW^2 + Y^2W &+ c_1X^3 + c_2X^2Y + c_3X^2Z'' + c_4XY^2 \\ &+ c_5XYZ'' + c_6XZ''^2 + c_7Y^3 + c_8Y^2Z'' + c_9Z''^3 = 0, \end{aligned}$$

with $c_i \in K$, $c_9 = 1, \omega, \omega^2$. This gives $3q^8$ possible equations for a cusp pointed cubic surface (S, P) where Γ_P is irreducible when there exists a cubic non-residue $\omega \in K$, and q^8 equations otherwise.

We use the computer algebra package `MAGMA` [13] to compute equivalence class representatives $\mathcal{G}_C \backslash \mathcal{F}_C$. We start by defining the finite field K, which cannot be of characteristic 2 or 3. For example,

```
p:=7;
K := GF(p);
```

We make a list of generators of $\mathcal{G}_C$, denoted `gens`. We create the matrices

$$\begin{pmatrix} g^4 & 0 & 0 & 0 \\ 0 & g & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & g^{-2} \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & g & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

where g is a generator for K^*.

```
g:=PrimitiveElement(K);
G:=GL(4,K);
gens:=[
G![[g^4,0,0,0],[0,g,0,0],[0,0,1,0],[0,0,0,g^-2]],
G![[1,0,0,0],[0,1,0,0],[0,0,g,0],[0,0,0,1]]
];
```

We then add to `gens` the matrices

$$\begin{pmatrix} 1 & v_i & 0 & -\frac{1}{2}v_i^2 \\ 0 & 1 & 0 & -v_i \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & v_i & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & v_i & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

where v_i, $i \in \{1, \ldots, n\}$ is a vector basis for $K = \mathbb{F}_{p^n}$ over $\mathbb{F}_p$, p prime. In the code the v_i are represented by `b`.

```
for b in Basis(K) do
        Append(~gens,
                Transpose(G![
[1,b,0,-1/2*b^2],[0,1,0,-b],[0,0,1,0],[0,0,0,1]
])
        );
        Append(~gens,
                Transpose(G![
[1,0,b,0],[0,1,0,0],[0,0,1,0],[0,0,0,1]
])
        );
        Append(~gens,
                Transpose(G![
[1,0,0,0],[0,1,b,0],[0,0,1,0],[0,0,0,1]
])
        );
end for;
```

We define $\mathcal{G}_C$, denoted in the code by `H`, as the subgroup of $G \coloneqq \mathrm{GL}(4, K)$ with generators `gens`.

```
H:=sub< G | gens >;
```

We make a list of cubic surface equations in the cuspidal form. Recall that the equation for such a cubic surface is

$$S : XW^2 + Y^2W + C(X, Y, Z) = 0.$$

The list `mons` contains all the monomials in $C(X, Y, Z)$, of which there should be 10.

```
P<X,Y,Z,W>:=PolynomialRing(K,4);
mons:=MonomialsOfDegree(P,3);
mons:=[ m : m in mons | IsDivisibleBy(m,W) eq false];
assert #mons eq 10;
```

The list `surfaces` contains all possible polynomials of the form

$$S : XW^2 + Y^2W + C(X, Y, Z) = 0,$$

i.e. it is a list of the elements of $\mathcal{F}_C$.

```
V:=VectorSpace(K,10);
V:=[Eltseq(v) : v in V];
surfaces:=[
W^2*X+Y^2*W+ &+[ v[i]*mons[i] : i in [1..10] ] : v in V
];
```

We now compute a list of equivalence class representatives of the group action of $\mathcal{G}_C$ on $\mathcal{F}_C$. The list of representatives is denoted `reps` in the code.

```
reps:=[];
repeat
h:=Random(surfaces);
        orb:=Orbit(H,h);
        Append(~reps,h);
        surfaces:=[F : F in surfaces | F in orb eq false ];
        print #reps,#surfaces;
until #surfaces eq 0;
```

The list `reps` is a complete list of inequivalent cusp pointed cubic surfaces over K under an action of $K^* \times \mathrm{GL}(4, K)$.

We use this program to prove the following theorem.

Theorem 6.2. *Let S be a smooth cubic surface defined over $K = \mathbb{F}_5$ or $\mathbb{F}_7$ and containing a non-Eckardt point $P \in S(K)$ such that P is a cusp of Γ_P. Then*

$$\mathrm{Span}(P) = S(K).$$

This implies that any non-Eckardt parabolic K-point on S generates $S(K)$.

Proof. We used the function `isgenerator` given in Section 2.2 on the elements of a list of inequivalent cubic surfaces in the form

$$S : XW^2 + Y^2W + C(X, Y, Z) = 0$$

along with the point $P = (0 : 0 : 0 : 1)$ to find any representatives of $\mathcal{G}_C \backslash \mathcal{F}_C$ for which $\mathrm{Span}(P) \neq S(K)$. We then checked those surfaces for smoothness and found that there were all in fact singular.

For $K = \mathbb{F}_5$, the list of representatives was computed using the code above and the whole process took 37753.180 seconds, which is approximately 11 hours of CPU time.

For $K = \mathbb{F}_7$, we first split the list of surfaces into those where Γ_P is the union of a line and a conic (Subcase 1), and those with Γ_P irreducible (Subcase 2) before performing the same action of $\mathcal{G}_C$. This was done to speed up the process of removing the orbit of a given cubic surface from the initial list. The whole process took 245040.250 seconds, which is approximately 68 hours of CPU time. □

6.1.5 Split and non-split node pointed cubic surfaces

We have two cases given in section 6.1.2 for node pointed cubic surfaces (S, P). When P is a split node, S is defined by

$$S : XW^2 + (Y^2 - Z^2)W + C(X, Y, Z) = 0,$$

when P is a non-split node, S is defined by

$$S : XW^2 + (Y^2 - \eta Z^2)W + C(X, Y, Z) = 0.$$

We have not completed the details for these cases yet, but we expect that this will be possible using the same strategy as Sections 6.1.3 and 6.1.4.

6.2 Calculating the number of equivalence classes

When computing equivalence class representatives of pointed cubic surfaces over K it is useful to know the number of equivalence classes so that one may check that a complete list of equivalence class representatives has been found. In order to calculate this we use the following two theorems.

Theorem 6.3 (Burnside's Lemma)**.** *Let G be a finite group acting on a set X. Then*

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |\operatorname{Fix}_X(g)|$$

where $\operatorname{Fix}_X(g)$ denotes the set of elements in X fixed by g and $|X/G|$ denotes the number of orbits of G in X.

In our applications X will be the set of all homogeneous cubic polynomials in four variables over $K = \mathbb{F}_q$ that yield the equations of cubic surfaces, or the subsets of such polynomials that define the different types of pointed cubic surfaces given in Section 6.1. The group G will be $\mathrm{GL}(4, K)$, with K a finite field, or the subgroup of $\mathrm{GL}(4, K)$ preserving a particular subset of polynomials. The orbit of an element $x \in X$ is all the pointed cubic surfaces to which x is sent by the action of G, therefore the orbits are the equivalence classes that we wish to find.

The following well-known theorem will be useful when computing the number of equivalence classes.

Theorem 6.4. *Let G be a finite group and let X be a finite set. Let $g_1, g_2 \in G$. If g_1 and g_2 are conjugate, i.e. if there exists $h \in G$ such that $g_1 = hg_2h^{-1}$, then*

$$|\operatorname{Fix}_X(g_1)| = |\operatorname{Fix}_X(g_2)|.$$

Proof. Let $a \in \operatorname{Fix}_X(g_1)$. Then $a^{g_1} = a$. Since $g_1 = h^{-1}g_2h$ we have $a = a^{hg_2h^{-1}}$, which implies that $a^h = a^{hg_2}$. Therefore $a^h \in \operatorname{Fix}_X(g_2)$. The reverse argument works in exactly the same way, so the sets $\operatorname{Fix}_X(g_1)$ and $\operatorname{Fix}_X(g_2)$ are in bijection. They are both finite since they are both subsets of X, which is finite. Hence $|\operatorname{Fix}_X(g_1)| = |\operatorname{Fix}_X(g_2)|$. □

This observation makes the computing the number of equivalence classes much faster because we can simply calculate $|\operatorname{Fix}_X(g)|$ for one g in each conjugacy class and then multiply by the size of the conjugacy class, rather than calculating $|\operatorname{Fix}_X(g)|$ for all $g \in G$. There is already a fast method for computing the size and a representative of all the conjugacy classes implemented in `MAGMA`.

What follows is an implementation in MAGMA code for the computation of the number of isomorphism classes over K of cubic surfaces over K. This could be easily modified for pointed cubic surfaces or specific cases of pointed cubic surfaces such as Eckardt pointed cubic surfaces.

Let p be a prime power. We create a polynomial ring for the 16 entries of $g \in G$.

```
K := GF(p);
S<[A]>:= PolynomialRing(K,16);
```

Next, we include the 20 coefficients of our cubic surface.

```
R<[a]> := PolynomialRing(S,20);
```

Then we include the variables X, Y, Z and W of the cubic equation.

```
P<X,Y,Z,W>:=PolynomialRing(R,4);
```

We create our general cubic equation, which we call F, and perform the group action of G upon it to obtain GG.

```
mons:=MonomialsOfDegree(P,3);
F:=&+[ R.i*mons[i]   : i in [1..20]];
x:=&+[ S.(i)*P.i : i in [1..4] ];
y:=&+[ S.(i+4)*P.i : i in [1..4] ];
z:=&+[ S.(i+8)*P.i : i in [1..4] ];
w:=&+[ S.(i+12)*P.i : i in [1..4] ];
GG:=Evaluate(F,[x,y,z,w]);
```

We extract the coefficients and create a 20 by 20 matrix defined over K that describes the group action upon the coefficients of F. This matrix will be created from the list M.

```
cfs:=[MonomialCoefficient(GG,m) : m in mons];
M:=[ [ MonomialCoefficient(c,R.i) : i in [1..20] ]  : c in cfs];
```

We now create the group G (denoted G) and a list of its conjugacy classes.

```
G:=GL(4,K);
C:=ConjugacyClasses(G);
```

Each entry in the list `C` is a triple giving the order, length and a representative of the conjugacy class. We are interested in the second and third of these. The following code calculates

$$\sum_{g \in G} |\mathrm{Fix}_X(g)|.$$

For each conjugacy class c, we take the representative g, which is given by `MAGMA`. We compute the 20 by 20 matrix M_g that represents the action of g on the 20 coefficients of the surface defined by F. Note that $\mathrm{Fix}_X(g)$ is isomorphic to the set of all vectors $\underline{v}$ such that

$$M_g \underline{v} = \underline{v}.$$

It is the kernel of $M_g - I$ where I is the appropriate identity matrix. We take the sum of the orders of these kernels.

```
sum:=0;
for c in C do
        g:=c[3];
        gvec:=Rows(g);
        gvec:=[Eltseq(k) : k in gvec];
        gvec:=&cat(gvec);
        Mg:=
[ [K | Evaluate(M[i][j],gvec) : j in [1..20]] : i in [1..20] ];
        Mg:=Matrix(Mg);
        I:=Parent(Mg)!1;
        sum:=sum+(#Kernel(Mg-I))*c[2];
        print sum;
end for;
```

All that remains is to divide the sum by the order of G.

```
sum/Order(G);
```

Bibliography

[1] H. F. Baker, *Notes on the theory of the cubic surface*, Proc. London Math. Soc. **1** no. 9 (1910) 145–199.

[2] A. Cayley, *On the triple tangent planes of surfaces of the third order*, Cambridge and Dublin Math. J., **4** (1849), 118–138.

[3] A. Clebsch, *Ueber eine Transformation der homogenen Functionen dritter Ordnung mit vier Veränderlichen*, J. für die Reine und Angew. Math. **58** (1861), 109–126.

[4] A. Clebsch, *Die Geometrie auf den Flächen dritter Ordnung*, J. für die Reine und Angew. Math. **65** (1866), 359–380.

[5] H. Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics, **138**, Springer Verlag, 1993.

[6] J. Cooley, *Generators for cubic surfaces with two skew lines over finite fields*, Arch. Math. (Basel) **100** (2013), no. 5, 401–411.

[7] J. Cooley, *Cubic surfaces with one rational line over finite fields*, `arXiv:1312.5905 [math.NT]`, 20 December 2013.

[8] A.-S. Elsenhans, J. Jahnel, *Moduli spaces and the inverse Galois problem for cubic surfaces*, to appear in Transactions of the AMS

[9] K. F. Geiser, *Ueber die Doppeltangenten einer eben Curve vierten Grades*, Math. Annalen **1** (1869) no. 1, 129–138.

[10] R. Hartshorne, *Algebraic Geometry*, Graduate Texts in Mathematics **52**, Springer Verlag, 1977.

[11] J. W. P. Hirshfeld, G. Korchmáros, F. Torres, *The number of points on an algebraic curve over a finite field*, London Math. Soc. Lecture Note Ser., **346**, Cambridge Univ. Press, Cambridge, (2007), 175–200

[12] F. C. Kirwan, *Complex Algebraic Curves*, LMS Student Texts **23**, CUP 1992.

[13] W. Bosma, J. Cannon and C. Playoust, *The Magma Algebra System I: The User Language*, J. Symb. Comp. **24** (1997), 235–265. (See also `http://magma.maths.usyd.edu.au/magma/`)

[14] Yu. I. Manin, *Cubic Forms: Algebra, Geometry, Arithmetic*, North-Holland, 1974 and 1986.

[15] M. Reid, *Chapters on algebraic surfaces*, pages 1–154 of *Complex algebraic varieties*, J. Kollár (Ed.), IAS/Park City lecture notes series (1993 volume), AMS, Providence R.I., 1997.

[16] M. Reid, *Undergraduate Algebraic Geometry*, LMS Student Texts **12**, CUP 1988.

[17] G. Salmon, *A treatise on the analytic geometry of three dimensions*, Fourth edition, Hodges, Figgis, and Co., Dublin 1882.

[18] B. Segre, *A note on arithmetical properties of cubic surfaces*, J. London Math. Soc. **18** (1943), 24–31.

[19] I. R. Shafarevich, *Basic Algebraic Geometry 1*, second edition, Springer-Verlag, 1994.

[20] S. Siksek, *On the number of Mordell-Weil generators for cubic surfaces*, J. Number Theory **132** (2012), 2610–2629.

[21] J. H. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, GTM 106, 2nd ed. 2009.

[22] D. van Stratten and O. Labs, *A Visual Introduction to Cubic Surfaces Using the Computer Software Spicy*, pages 225-238 of *Algebra, Geometry, and Software Systems*, M. Joswig and N. Takayama (Editors), Springer, (2003).

[23] H. P. F. Swinnerton-Dyer, *The zeta function of a cubic surface over a finite field*, Math. Proc. Camb. Phil. Soc. (1967), **63**, 55–71.

[24] H. P. F. Swinnerton-Dyer, *Cubic surfaces over finite fields*, Math. Proc. Camb. Phil. Soc. (2010), **149**, 385–388.

[25] J. F. Voloch, *Surfaces in $\mathbb{P}^3$ over finite fields*, pages 219–226 of *Topics in algebraic and noncommutative geometry (Luminy/Annapolis, MD, 2001)*, Contemp. Math. **324**, Amer. Math. Soc., Providence, RI, 2003.