RATIONAL LINES ON SMOOTH CUBIC SURFACES

STEPHEN MCKEAN

Abstract. We prove that the enumerative geometry of lines on smooth cubic surfaces is governed by the arithmetic of the base field. In 1949, Segre proved that the number of lines on a smooth cubic surface over any field is 0, 1, 2, 3, 5, 7, 9, 15, or 27. Over a given field, each of these line counts may or may not be realized by some cubic surface. We give a necessary criterion for each of these line counts in terms of the Galois theory of the base field. Over fields with at least 22 elements, we show that these necessary criteria are also sufficient. As examples, we use these criteria to classify line counts over finitely generated fields, finite transcendental extensions of arbitrary fields, finite fields of order at least 22, real closed fields, and the field of constructible numbers.

1. Introduction

In 1849, Cayley and Salmon proved that every smooth cubic surface over $\mathbb{C}$ contains exactly 27 complex lines [Cay49]. By 1858, Schläfli had proved that every smooth cubic surface over $\mathbb{R}$ contains exactly 3, 7, 15, or 27 real lines [Sch58], with each of these counts occurring for some real cubic surface. Following this theme, B. Segre classified all possible rational line counts for smooth cubic surfaces over $\mathbb{Q}$ in 1949 [Seg49].

Theorem 1.1 (Segre)**.** *Every smooth cubic surface over $\mathbb{Q}$ contains 0, 1, 2, 3, 5, 7, 9, 15, or 27 lines defined over $\mathbb{Q}$. Moreover, each of these counts is realized by some smooth cubic surface over $\mathbb{Q}$.*

B. Segre further showed in *loc. cit.* that the line counts in Theorem 1.1 are the only possible line counts for smooth cubic surfaces over any field:

Theorem 1.2 (Segre)**.** *The number of lines on a smooth cubic surface over any field must be $0, 1, 2, 3, 5, 7, 9, 15,$ or 27.*

In light of Theorem 1.2, one can try to classify all which line counts actually occur for smooth cubic surfaces over a given field. These line counts will be a subset of $\{0, 1, 2, 3, 5, 7, 9, 15, 27\}$. For example, all line counts have been classified for smooth cubic surfaces over the following fields.

- Smooth cubic surfaces over $\mathbb{C}$ can only have 27 lines [Cay49].
- Smooth cubic surfaces over $\mathbb{R}$ can only have 3, 7, 15, or 27 lines, and each of these counts occurs [Sch58].

1991 *Mathematics Subject Classification.* 14N15, 14G25.

- Smooth cubic surfaces over $\mathbb{Q}$ can have 0, 1, 2, 3, 5, 7, 9, 15, or 27 lines, and each of these counts occurs [Seg49].
- Smooth cubic surfaces over $\mathbb{F}_2$ and $\mathbb{F}_3$ can only have 0, 1, 2, 3, 5, 9, or 15 lines, and each of these counts occurs [Dic15, LT19].
- Smooth cubic surfaces over $\mathbb{F}_5$ can only have 0, 1, 2, 3, 5, 7, 9, or 15 lines, and each of these counts occurs [LT19].
- Smooth cubic surfaces over $\mathbb{F}_q$ can have 0, 1, 2, 3, 5, 7, 9, 15, or 27 lines when $q > 5$ is odd or $q = 2^d$ with $d > 1$, and each of these counts occurs [LT19].

We clarify these results by providing, for each $n \in \{0, 1, 2, 3, 5, 7, 9, 15, 27\}$, a necessary and sufficient criterion for the occurrence of the line count n over any given field k (assuming $|k| \geq 22$). These criteria depend only on the Galois theory of k, so our main theorem can be summarized by saying that arithmetic governs the enumerative geometry of lines on cubic surfaces.

Theorem 1.3. *Let k be a field with $|k| \geq 22$. There is a smooth cubic surface over k whose 27 lines are all defined over k. Moreover, there is a smooth cubic surface over k containing n lines defined over k if and only if k admits a separable field extension of the degrees listed in Table 1.*

TABLE 1. Line counts and degrees of extensions

n	*degree(s)*
15	*2*
9	*3*
7	*2*
5	*4*

n	*degree(s)*
3	*2*
2	*5*
1	*2 and 4*
0	*3 or 6*

Remark 1.4. Even more can be said about cubic surfaces with 3 lines. Such triples of lines are either skew or coplanar and pairwise intersecting. There is a smooth cubic surface over k with 3 skew lines if and only if k admits separable extensions of degrees 2 and 3, and there is a smooth cubic surface over k with 3 coplanar lines if and only if k admits a separable extension of degree 2.

Remark 1.5. Theorem 1.3 is only true if $|k| > 5$, as the fields $\mathbb{F}_2$, $\mathbb{F}_3$, and $\mathbb{F}_5$ admit separable field extensions of arbitrary degree but do not admit all possible line counts for smooth cubic surfaces. While $\mathbb{F}_q$ does not contradict Theorem 1.3 unless $q = 2, 3, 5$, our methods do not account for this. In Theorem 4.1, we prove (under the assumption that $|k| \geq 22$) that k admitting separable extensions of the degrees listed in Table 1 is sufficient to realize the respective line counts. We prove Theorem 4.1 by blowing up

Galois-invariant sets of points in the plane, and the cardinality assumption allows us to ensure that these sets of points can be arranged in general position.

1.1. **Application: classifying line counts.** As an application of Theorem 1.3, we classify all possible line counts for smooth cubic surfaces over various fields. We begin with finitely generated fields and finite transcendental extensions of arbitrary fields.

Corollary 1.6. *Let k be a finitely generated field (with $|k| \geq 22$) or a finite transcendental extension of an arbitrary field. There is a smooth cubic surface over k containing n lines defined over k for each $n \in \{0, 1, 2, 3, 5, 7, 9, 15, 27\}$.*

As far as we are aware, Corollary 1.6 in this generality is new to the literature. We also give an alternate proof of Loughran and Trepalin's classification of line counts over finite fields of order at least 22 [LT19].

Corollary 1.7 (Loughran–Trepalin)**.** *Let $q \geq 22$ be a prime power. There is a smooth cubic surface over $\mathbb{F}_q$ containing n lines defined over $\mathbb{F}_q$ for each $n \in \{0, 1, 2, 3, 5, 7, 9, 15, 27\}$.*

Corollaries 1.6 and 1.7 both involve fields that admit separable extensions of arbitrary degree, so Theorem 1.3 states that all possible line counts indeed occur over these fields. The exceptional case is when separable field extensions of certain degrees are obstructed, so that not all line counts occur. We give two examples of such fields. We start with real closed fields, whose only non-trivial finite extensions are of degree 2.

Corollary 1.8. *Let k be a real closed field. Any smooth cubic surface over k has 3, 7, 15, or 27 lines, and each of these counts occurs.*

Arithmetically, real closed fields are indistinguishable from $\mathbb{R}$, so Corollary 1.8 is just a reincarnation of Schläfli's classical count of lines on real cubic surfaces. A more interesting field to consider is the field $\mathbb{F}_\measuredangle$ of complex constructible numbers. This is a quadratically closed field, so Theorem 1.3 implies that the line counts 1, 3, 7, and 15 cannot happen over $\mathbb{F}_\measuredangle$.

Corollary 1.9. *Any smooth cubic surface over the field of complex constructible numbers has 0, 2, 5, 9, or 27 lines, and each of these counts occurs.*

In general, one can manufacture a field to get certain line counts. For example, if a field k has no separable extensions of degree $2 \leq d \leq 6$, then every smooth cubic surface over k has exactly 27 lines. This can be viewed as an arithmetic version of Cayley and Salmon's fundamental result. If k has no separable extensions of degree $2 \leq d \leq 5$ but does have a separable degree 6 extension, then we get all or nothing — every cubic surface over k has either 0 or 27 lines. In Appendix B, we use Theorem 1.3 to give a complete list of all possible sets of line counts over fields of sufficient cardinality.

1.2. **Application: inverse Galois problem for cubic surfaces.** B. Segre's proof of Theorem 1.2 is geometric. A modern approach to this theorem comes from the inverse Galois problem for cubic surfaces. An integer n can be a line count for some smooth cubic surface over some field only if there is a subgroup conjugacy class of the Weyl group $W(\mathrm{E}_6)$ whose action on the Schläfli graph has n fixed points. There are 25 conjugacy classes to consider, and each of the counts given in Theorem 1.2 occurs for at least one of these conjugacy classes. We include Loughran's Magma implementation of this computation in Appendix A. See also [BFL19, Table 7.1] for a list of the conjugacy classes and their corresponding line counts.

Because we can deduce all occuring line counts over a given field k by solving the inverse Galois problem for cubic surfaces over k, this inverse Galois problem is stronger than just classifying all line counts over k. The inverse Galois problem for cubic surfaces was solved over $\mathbb{Q}$ by Elsenhans and Jahnel [EJ15] (which thus gives an alternate proof of Theorem 1.1) and over finite fields by Loughran and Trepalin [LT19] (see also [BFL19]).

Loughran and Trepalin show that fewer conjugacy classes occur for cubic surfaces over $\mathbb{F}_2$ than over $\mathbb{F}_3$ [LT19, Theorem 1.1], even though the sets of line counts over these two fields agree. In particular, the inverse Galois problem is *strictly* stronger than classifying line counts. However, we can actually solve the inverse Galois problem for cubic surfaces over some fields by obstructing certain line counts. The only line counts coming from more than one conjugacy class are 0, 1, and 3, so if the only possible line counts over k are a subset of $\{2, 5, 7, 9, 15, 27\}$, then we have solved the inverse Galois problem for cubic surfaces over k. We give an example of such a solution in the following corollary of Theorem 1.3. We refer to [BFL19, Table 7.1] for a list of subgroup conjugacy classes of $W(\mathrm{E}_6)$.

Corollary 1.10. *Let k be a field of order at least 22. The conjugacy class C_1 occurs for smooth cubic surfaces over k. Now assume that k does not admit separable extensions of degree 2, 3, or 6. Then no other classes occur over k except possibly C_{15} and C_{18}. The class C_{15} (respectively, C_{18}) occurs over k if and only if k admits a separable extension of degree 5 (respectively, degree 4).*

Theorem 1.3 implies that some line counts cannot be divorced over any field of sufficient cardinality. For example, the line counts 3, 7, and 15 all arise from quadratic extensions of k, so these three counts all occur over k if and only if any one of them occurs over k. It follows that some conjugacy classes likewise cannot be divorced over any field of sufficient cardinality. In Appendix B, we solve the inverse Galois problem for smooth cubic surfaces over any field (of cardinality at least 22) for the subset of conjugacy classes that are completely determined by their corresponding line count.

Note that the only line counts coming from more than one conjugacy class are also the only line counts that involve more than one field extension in Theorem 1.3: cubic surfaces with 0 lines come from separable extensions of degrees 3 or 6, cubic surfaces with 1 line come from separable extensions of degrees 2 and 4, and cubic surfaces with 3 skew lines come from separable extensions of degrees 2 and 3. However, since cubic surfaces with 3 coplanar lines require only degree 2 separable extensions, we ask the following question:

Question 1.11. Is there a unique conjugacy class of subgroups of $W(\mathrm{E}_6)$ corresponding to smooth cubic surfaces with 3 coplanar lines?

An affirmative answer to Question 1.11 would imply that the only conjugacy classes that cannot be immediately realized or obstructed by Theorem 1.3 correspond to the line counts that require or permit more than one type of field extension. In other words, Question 1.11 would imply that difficult conjugacy classes correspond to arithmetically complicated line counts.

1.3. **Open question: counting lines on a given cubic surface.** While Theorem 1.3 completes the classification of line counts for smooth cubic surfaces over any field, one can still ask about the number of rational lines on a given cubic surface. Ideally, we would like to be able to determine this number directly from the defining polynomial of the given cubic surface.

In joint work with Minahan and Zhang [MMZ21, Theorem 1.1], we prove that the number of real lines on a smooth cubic surface X over $\mathbb{R}$ can be determined from the defining polynomial of X and the defining equations of 3 skew real lines on X. It seems reasonable that one could generalize this result to hold over other subcomplex fields.

The reason behind requiring the data of 3 skew lines is Galois-theoretic: the Galois group of solving for the 27 lines on a cubic surface is not solvable [Jor57], so there is no equation in radicals for the defining equations of these 27 lines. In contrast, the Galois group of solving for the 27 lines on a cubic surface with 3 skew lines is solvable [Har79], so there is a formula in radicals for the 27 lines in terms of the cubic surface and the given 3 skew lines. Even without the data of 3 skew lines, there is an algebraic function solving for the 27 lines on X in terms of its defining polynomial, so one could hope that the count of rational lines on X can also be read from its defining polynomial.

Question 1.12. Let k be a field. Given a homogeneous polynomial $F \in k[x_0, \dots, x_3]$ of degree 3 whose associated cubic surface $\mathbb{V}(F) \subset \mathbb{P}^3$ is smooth, can the number of k-rational lines on $\mathbb{V}(F)$ be determined from the coefficients of F?

1.4. **Methods and related work.** Studying rational lines on cubic surfaces via blow ups is a classical technique. See [LT19, BFL19] and the references therein for some recent applications of this approach. When blowing up collections of closed points to get smooth cubic surfaces, one technical requirement is that the points lie in general position. One can derive algebraic criteria for this by requiring the points to lie on the cusp $\mathbb{V}(y^3 - x^2z) \subset \mathbb{P}^2_k$ (see Section 4.1). We learned this trick from a private communication from J.-P. Serre, but the same idea appears in [PSS20].

Building on an earlier version of this article, El Manssour–El Maazouz–Kaya–Rose use the method described in Section 4.1 to show that all line counts occur for smooth cubic surfaces over p-adic fields [MMKR22].

While we focus on the (non)-existence of line counts for cubic surfaces over various fields, one can go further by investigating the distributions of these line counts or even

classifying all cubic surfaces with a given line count. These distributions are known over finite fields due to the work of Das [Das20]. One can apply the methods of [PV04, Proposition 3.4] to understand these distributions over $\mathbb{Q}$. There has been extensive work on the subject of classifying cubic surfaces and their lines over finite fields, especially on classifying cubic surfaces with 27 lines over a finite field. See e.g. [Hir67a, Hir67b, BHK18, BK19].

1.5. **Outline and conventions.** We begin with an overview of some useful classical results in Section 2. We then give B. Segre's original geometric proof of Theorem 1.2 (with some details added and a minor error corrected) in Section 3. We prove that the criteria in Theorem 1.3 are sufficient in Section 4 and necessary in Section 5, which together yield Theorem 1.3. Finally, we apply Theorem 1.3 in Section 6 to classify line counts over various fields. In Appendix A, we give Loughran's code that gives a modern proof of Theorem 1.2. In Appendix B, we compile a table listing all possible sets of line counts, along with the conjugacy classes of subgroups of $W(\mathrm{E}_6)$ that are guaranteed or obstructed by each of these sets of line counts.

Throughout this article, we will only consider smooth cubic surfaces. When working over a field k, we will use the term *rational lines* to refer to lines defined over k (see Definition 2.1). Whenever we write $Y \subseteq X$ or $Y \subset X$ for schemes X, Y, we mean that Y is a closed subscheme of X.

Remark 1.13. In an earlier version of this article, we used the results of [MMZ21] to give what we thought was the first proof of Theorem 1.1. We were later informed by J.W.P. Hirschfeld (via J.-P. Serre) about [Seg49]. Our original proof of the existence part of Theorem 1.1 has been omitted (to improve the narrative flow of this article) but can be found in [McK21, Sections 4 and 5].

Acknowledgements. We thank Kirsten Wickelgren for her advice and support, as well as Alex Betts, Ronno Das, Igor Dolgachev, Enis Kaya, Viatcheslav Kharlamov, Aaron Landesman, Antonio Lerario, Dan Loughran, Jean-Pierre Serre, and Ravi Vakil for their helpful correspondence. We also thank the anonymous referee whose thorough feedback encouraged us to rewrite this article. We are especially indebted to J.W.P. Hirschfeld and J.-P. Serre for bringing Segre's result [Seg49] to our attention, as well as to J.-P. Serre for several enlightening discussions. We thank the anonymous referee whose thorough feedback inspired us to strengthen our results and rewrite this article. The author received support from an NSF MSPRF grant (DMS-2202825) and Kirsten Wickelgren's NSF CAREER grant (DMS-1552730).

2. Preliminaries

We state a few classical results that we will use throughout this article.

Definition 2.1. Let K/k be a field extension. We say that a closed subscheme $X \subseteq \mathbb{P}^n_K$ is *defined over* k or *has field of definition* k if the following equivalent conditions are satisfied (see e.g. [Dol16, Proposition 1.2]).

(a) The defining ideal of X is generated by homogeneous polynomials in $k[x_0, \ldots, x_n]$.

(b) There exists a closed subscheme $Y \subseteq \mathbb{P}^n_k$ such that $X = Y \times_{\operatorname{Spec} k} \operatorname{Spec} K$.

Any closed subscheme of projective space has a minimal field of definition by [DG67, IV_2, Corollaire (4.8.11)]. If a scheme X has field of definition k, we may also say that X is *k-rational*. Definition 2.1 (b) immediately implies that field of definition is preserved under base change.

Proposition 2.2. *Let $k \subseteq K \subseteq K'$ be a tower of fields. Let $X \subseteq \mathbb{P}^n_K$ be a closed subscheme. If X is defined over k, then the base change $X_{K'} = X \times_{\operatorname{Spec} K} \operatorname{Spec} K'$ is defined over k.*

Proof. By assumption, there exists a closed subscheme $Y \subseteq \mathbb{P}^n_k$ such that $X = Y \times_{\operatorname{Spec} k} \operatorname{Spec} K$. Thus

$$\begin{aligned} X_{K'} &= (Y \times_{\operatorname{Spec} k} \operatorname{Spec} K) \times_{\operatorname{Spec} K} \operatorname{Spec} K' \\ &= Y \times_{\operatorname{Spec} k} \operatorname{Spec} K', \end{aligned}$$

as desired. □

Since closed immersions are stable under base change [Sta18, Lemma 01JY], Proposition 2.2 states that k-rational subschemes get sent to k-rational subschemes under base change. The converse is also true.

Proposition 2.3. *Let $k \subseteq K \subseteq K'$ be a tower of fields. Let $X, Y \subseteq \mathbb{P}^n_K$. Suppose that $Y_{K'} \subseteq X_{K'}$ and that $X_{K'}, Y_{K'}$ are both defined over k. Then $Y \subseteq X$, and X, Y are both defined over k.*

Proof of Proposition 2.3. Field extensions are fpqc and closed immersions satisfy fpqc descent [DG67, IV_2, Proposition (2.7.1) (xii)], so the assumption that $Y_{K'} \subseteq X_{K'}$ implies that $Y \subseteq X$.

We now show that X is defined over k. The proof that Y is defined over k follows the same argument. Let $\mathcal{I}$ and $\mathcal{J}$ be the defining ideals of X and $X_{K'}$, respectively, so that $\mathcal{I} = \mathcal{J} \cap K[x_0, \ldots, x_n]$. Under Definition 2.1 (a), the assumption that $X_{K'}$ is defined over k means that there are homogeneous polynomials $f_1, \ldots, f_m \in k[x_0, \ldots, x_n]$ such that $\mathcal{J} = (f_1, \ldots, f_m) \cdot K'[x_0, \ldots, x_m]$. Since $k[x_0, \ldots, x_n] \subseteq K[x_0, \ldots, x_n]$, it follows that $\mathcal{J} \cap K[x_0, \ldots, x_n]$ is again generated by $f_1, \ldots, f_m$. In particular, $\mathcal{I}$ is generated by homogeneous polynomials in $k[x_0, \ldots, x_n]$, so X is defined over k. □

For any field extension K/k, a cubic surface over k is smooth if and only if its base change to K is smooth (see e.g. [DG67, IV_4, Proposition (17.3.3) (iii) and Corollaire (17.7.3) (ii)]). Together with Propositions 2.2 and 2.3, this means that we can enumerate k-rational lines on X by base changing to a field K over which all 27 lines on X are defined and studying the k-rationality of lines on X_K. Since smooth cubic surfaces are

separably split [Coo88], all lines on a smooth cubic surface over a field k are defined over the separable closure k^s (within any chosen algebraic closure of k).

We have thus reduced the study of rational lines on X to the study of k-rational lines on X_{k^s}. We will study the field of definition of lines on cubic surfaces by acting on the relevant varieties by the absolute Galois group. This was done classically for lines on cubic surfaces over $\mathbb{R}$, as well as by Pannekoek [Pan09] for studying Galois orbits of lines on cubic surfaces over number fields.

Proposition 2.4. *Let k be a field, and fix a separable closure k^s of k. A geometrically reduced closed subscheme $X \subseteq \mathbb{P}^n_{k^s}$ is defined over k if and only if $\sigma \cdot X = X$ for all $\sigma \in \mathrm{Gal}(k^s/k)$.*

Proof. The group $\mathrm{Gal}(k^s/k)$ acts on the defining ideal $\mathcal{I} \subseteq k^s[x_0, \dots, x_n]$ of X by acting on the coefficients of each $f \in \mathcal{I}$. If X is defined over k, then the coefficients of any generating set of $\mathcal{I}$ are fixed under $\mathrm{Gal}(k^s/k)$-action and hence so is X.

Now suppose X is fixed under $\mathrm{Gal}(k^s/k)$-action. By Hilbert's Basis Theorem, X is defined by a finite set $\{f_1, \dots, f_r\}$ of polynomials over some finite extension $k' \subseteq k^s$ of k. Given $f \in \mathcal{I}$ and $\sigma \in \mathrm{Gal}(k'/k)$, denote the image of f under σ-action by f^σ. Since $\sigma \cdot X = X$, we have that $f^\sigma(p) = 0$ for all $p \in X$. In particular, $f^\sigma \in \mathcal{I}$ for all $f \in \mathcal{I}$. The desired result follows from [HRC12, Lemma 1 (b)]. We describe the relevant ideas here. Fix a k-basis $\{e_1, \dots, e_m\}$ of k', and let $\mathrm{Tr}_{k'/k} : k'[x_0, \dots, x_n] \to k[x_0, \dots, x_n]$ be given by taking the Galois trace of each coefficient of a given polynomial. Then $\{\mathrm{Tr}_{k'/k}(e_i f_j)\}_{i,j}$ generates the ideal $\mathcal{I}$. Moreover, since $\mathrm{Tr}_{k'/k}(e_i f_j)^\sigma = \mathrm{Tr}_{k'/k}(e_i f_j)$ for all $\sigma \in \mathrm{Gal}(k'/k)$, it follows that $\mathrm{Tr}_{k'/k}(e_i f_j) \in k[x_0, \dots, x_n]$. Thus $\mathcal{I}$ is generated by polynomials over k, as desired. □

A cubic surface X defined over k is fixed by $\mathrm{Gal}(k^s/k)$-action, so Galois action preserves the set of 27 lines on X_{k^s}. Moreover, Galois action preserves the incidence relations of the 27 lines:

Proposition 2.5. *Let k be a field with k^s a fixed separable closure, X be a smooth cubic surface defined over k, and $\sigma \in \mathrm{Gal}(k^s/k)$. Two lines L and L' in X_{k^s} intersect if and only if $\sigma \cdot L$ and $\sigma \cdot L'$ intersect.*

Proof. The σ-action is defined pointwise. In particular, if L and L' intersect in the point p, then $\sigma \cdot L$ and $\sigma \cdot L'$ intersect in the point $\sigma \cdot p$. Conversely, if $\sigma \cdot L$ and $\sigma \cdot L'$ intersect in the point q, then L and L' intersect in the point $\sigma^{-1} \cdot q$. □

Proposition 2.6. *Let k be a field with fixed separable closure k^s, and let X be a smooth cubic surface defined over k. If $L_1, L_2, L_3 \subseteq X_{k^s}$ are three coplanar lines, and if L_1 and L_2 are defined over k, then L_3 is also defined over k.*

Proof. Since L_1 and L_2 are defined over k, the plane $H \subset \mathbb{P}^3_k$ that contains them is also defined over k. By Bézout's theorem (and the fact that all lines on X are defined over

k^s [Coo88]), we have $H_{k^s} \cap X_{k^s} = L_1 \cup L_2 \cup L_3$. The varieties L_1, L_2, H, and X are each fixed by all $\mathrm{Gal}(k^s/k)$-actions since they are defined over k. We now act on the configuration $H_{k^s} \cap X_{k^s}$ by each $\sigma \in \mathrm{Gal}(k^s/k)$. Since H and X are defined over k, we have $\sigma \cdot (H_{k^s} \cap X_{k^s}) = H_{k^s} \cap X_{k^s}$. That is, $L_1 \cup L_2 \cup L_3 = (\sigma \cdot L_1) \cup (\sigma \cdot L_2) \cup (\sigma \cdot L_3)$. Since L_1 and L_2 are defined over k, we have $\sigma \cdot L_1 = L_1$ and $\sigma \cdot L_2 = L_2$, so $L_1 \cup L_2 \cup L_3 = L_1 \cup L_2 \cup (\sigma \cdot L_3)$. It follows that $L_3 = \sigma \cdot L_3$ for all $\sigma \in \mathrm{Gal}(k^s/k)$, so L_3 is defined over k. □

Corollary 2.7. *If a smooth cubic surface X over a field k contains two rational lines L_1, L_2 that intersect each other, then X contains a third rational line L_3 that intersects L_1 and L_2.*

Proof. Let H be the plane containing L_1 and L_2. By Bézout's theorem and [Coo88], $X_{k^s} \cap H_{k^s}$ consists of (the base changes of) L_1, L_2, and a third line L_3. Since L_1 and L_2 are defined over k, Proposition 2.6 implies that L_3 is also defined over k. Thus each of these three lines on X_{k^s} are the base change of a k-rational line on X, and their intersection data are preserved by Proposition 2.5. □

It is a classical result that every smooth cubic surface is the blow-up of $\mathbb{P}^2$ at 6 general points — provided that one works over an algebraically closed field. In general, a smooth cubic surface need not be birational to $\mathbb{P}^2$. For example, Schläfli proved that there are smooth cubic surfaces over $\mathbb{R}$ whose $\mathbb{R}$-points are homeomorphic to $\mathbb{RP}^2 \sqcup S^2$, where S^2 is a 2-sphere (for a modern treatment, see e.g. [Kol97, Section 5]). So while a smooth cubic surface X over an arbitrary field k need not be rational, X is *geometrically* rational: we can view $X_{\overline{k}}$ as the blow-up of $\mathbb{P}^2_{\overline{k}}$ at 6 points. We will exploit this perspective in Section 5. However, we cannot use Galois descent to pass from $X_{\overline{k}}$ back to X if k is not perfect. To resolve this issue, we need to show that X is in fact *separably* rational.

Lemma 2.8. *Let k be a field, and let k^s be the separable closure of k in some algebraic closure $\overline{k}$. If X is a smooth cubic surface over k, then X_{k^s} is the blow-up of $\mathbb{P}^2_{k^s}$ at 6 points.*

Proof. The proof follows a classical argument. We assume that $k = k^s$ (to simplify notation), so that all 27 lines on X are k-rational [Coo88]. Since X contains at least four rational lines, Bézout's theorem implies that X contains two skew rational lines (otherwise all four lines would be coplanar, contradicting the fact that X is cubic). We can also show that each line on X meets 5 pairs of intersecting lines on X, with each pair of lines disjoint from the others [Sha13, Chapter IV.2.5, p. 256].

Let $L \subset X$ be a line, and let $\{L_i, L_i'\}_{i=1}^5$ be the set of pairs of lines meeting L (with $L_i \cap L_i' \neq \varnothing$ and $(L_i \cup L_i') \cap (L_j \cup L_j') = \varnothing$ for $i \neq j$). If $\Lambda \subset X$ is a line that does not meet L, then Λ meets at most one of L_i, L_i' for each i (otherwise L and Λ would be coplanar and hence not disjoint). In fact, Λ meets precisely one of L_i, L_i' for each i. To see this, let H_i be the plane such that $X \cap H_i = L \cup L_i \cup L_i'$. Since $\Lambda \subset X$, the intersection $H_i \cap \Lambda$ consists of a single point that must lie on X. Thus $H_i \cap \Lambda \subset X \cap H_i = L \cup L_i \cup L_i'$. Since

$L \cap \Lambda = \varnothing$ by assumption, we are done and can conclude that there are exactly 5 lines in X meeting any skew pair of lines.

Given two skew lines $L_1, L_2 \subset X$, we construct mutually inverse rational maps $\phi : X \dashrightarrow L_1 \times L_2$ and $\psi : L_1 \times L_2 \dashrightarrow X$ as follows. For each $x \in X \backslash (L_1 \cup L_2)$, let $L_x \subset \mathbb{P}^3$ be the unique line through x and meeting L_1 and L_2. Define $\phi(x) = (L_1 \cap L_x, L_2 \cap L_x)$. For each $(\ell_1, \ell_2) \in L_1 \times L_2$, let $\overline{\ell_1 \ell_2}$ be the line through ℓ_1 and ℓ_2. If $\overline{\ell_1 \ell_2}$ is not contained in X, then Bézout's theorem implies that $X \cap \overline{\ell_1 \ell_2}$ consists of three distinct points: $L_1 \cap \overline{\ell_1 \ell_2}$, $L_2 \cap \overline{\ell_1 \ell_2}$, and a third point, which we denote $\psi(\ell_1, \ell_2)$. Thus X is birational to $L_1 \times L_2 \cong \mathbb{P}^1_k \times \mathbb{P}^1_k$.

We next extend $\phi : X \dashrightarrow \mathbb{P}^1_k \times \mathbb{P}^1_k$ to a morphism. If $x \in X \backslash L_i$, let H_i be the unique plane in $\mathbb{P}^3_k$ containing $L_i \cup x$ for $i = 1, 2$. If $x \in L_i$, let $H_i = T_x X$. Setting $\phi(x) = (H_2 \cap L_1, H_1 \cap L_2)$, one can check that $\phi : X \to \mathbb{P}^1_k \times \mathbb{P}^1_k$ is now a well-defined morphism. The inverse of ϕ is not well-defined precisely where ψ is not well-defined, namely whenever $\overline{\ell_1 \ell_2} \subset X$. These are lines in X that meet the two skew lines L_1 and L_2, and there are 5 such lines. One then checks that $\phi : X \to \mathbb{P}^1_k \times \mathbb{P}^1_k$ is a blow-up at these 5 points. Since $\mathbb{P}^1_k \times \mathbb{P}^1_k$ is the blow-up of $\mathbb{P}^2_k$ at 1 point, it follows that X is the blow-up of $\mathbb{P}^2_k$ at 6 points. □

3. The list of possible line counts

We now give B. Segre's proof of Theorem 1.2. The general idea is to pass to the separable closure, work geometrically, and keep track of the field of definition of each line. As mentioned in Section 1.2, Theorem 1.2 can be proved by a computation on the Weyl group $W(\mathrm{E}_6)$ (see Appendix A for a Magma implementation of this computation, provided to us by Loughran). However, we find Segre's geometric proof interesting and worth expositing. We will add various details omitted from Segre's original account, streamline some of the arguments, and correct Segre's erroneous $\operatorname{char} k \neq 2$ assumption.

The proof utilizes a few geometric facts, which we list for the reader's convenience. These facts are classical, although we keep track of the field of definition of the lines involved when necessary. We will omit any proofs that do not require us to keep track of fields of definition. The first fact is that every line L on a smooth cubic surface meets exactly one line in each triple of coplanar lines (to which L does not belong).

Lemma 3.1. *Let X be a smooth cubic surface. Given three pairwise-intersecting lines L_1, L_2, L_3 on X, any other line on X meets exactly one of L_1, L_2, L_3.*

In Lemma 3.7, we will show that if a smooth cubic surface X contains four skew k-rational lines, then X contains either 15 or 27 k-rational lines. Two key ingredients are: each triple of skew lines on X meets a unique triple of skew lines on X, and each quadruple of skew lines on X meets a unique pair of skew lines on X.

Proposition 3.2. *Let X be a smooth cubic surface. Given three skew lines $L_1, L_2, L_3 \subset X$, there is a unique triple $M_1, M_2, M_3 \subset X$ of skew lines that each meet L_i.*

Proposition 3.3. *Let X be a smooth cubic surface. Given four skew lines $L_1, \dots, L_4 \subset X$, there is a unique pair $L, L' \subset X$ of skew lines meeting each L_i.*

We will also need the facts that each pair of skew lines on X belongs to a unique double six that splits the pair, and that the intersection graph of the 15 lines in the complement of any double six is given by Figure 3I.

Definition 3.4. A *double six* is a collection $\{L_i, L_i'\}_{i=1}^6$ of twelve lines such that $L_1, \dots, L_6$ are skew, $L_1', \dots, L_6'$ are skew, L_i and L_i' are skew, and L_i and L_j' are not skew for $i \neq j$. The two subsets $\{L_i\}$ and $\{L_i'\}$ are called *sextuples*.

Proposition 3.5. *Let X be a smooth cubic surface. Given two skew lines $L, L' \subset X$, there is a unique double six of lines on X with L and L' belonging to different sextuples.*

Lemma 3.6. *Let X be a smooth cubic surface. The intersection graph of the lines in the complement of any double six on X is the graph given in Figure 3I.*

Proof. The incidence pattern of the lines in the complement of a double six, together with the tritangent planes to which they belong, form the Cremona–Richmond configuration CR [Sch58]. Since the Cremona–Richmond configuration is self-dual, we can take the vertices of CR to represent the 15 lines on X and the lines of CR to represent the tritangent planes to which these lines on X belong. Each such tritangent plane corresponds to a 3-cycle in G since coplanar lines on X are pairwise-intersecting. It follows that we can obtain G by "projectivizing" CR: we turn each line on CR into a 3-cycle by joining the vertices on each end with a new edge. This is the graph given in Figure 3I. □

We can now show that if a smooth cubic surface X contains four skew k-rational lines, then X contains either 15 or 27 k-rational lines.

Lemma 3.7. *Let X be a smooth cubic surface over a field k with four skew k-rational lines $L_1, \dots, L_4 \subset X$. Let $L, L' \subset X$ be the (not necessarily k-rational) lines meeting each L_i. Let D be the double six of X such that L and L' belong to different sextuples. The 15 lines of X not belonging to D are all defined over k, and the lines belonging to D are either all defined over k or all not defined over k.*

Proof. We will first show that L, L' are either both k-rational or both not k-rational. Three skew lines in $\mathbb{P}^3_k$ determine a unique quadric surface. Let Q be the quadric determined by L_1, L_2, L_3. Let M_1, M_2, M_3 be the triple of skew lines meeting L_1, L_2, L_3 as given by Proposition 3.2. Bézout's theorem and the fact that each M_i meets each L_1, L_2, L_3 implies that M_1, M_2, M_3 are also contained in Q. Since L and L' meet L_1, L_2, L_3, we deduce that $L, L' \in \{M_1, M_2, M_3\}$. Because the set $\{L_1, L_2, L_3\}$ is Galois-fixed, the quadric Q and both of its rulings are all defined over k. To solve for L, L', we first compute the intersection $Q \cap L_4 = \{p_1, p_2\}$. We then take the ruling R of Q that does not contain L_1, L_2, L_3 and find the lines $R_1, R_2 \in R$ that pass through p_1, p_2, respectively. Algebraically, this corresponds to solving a quadratic equation over k. Since

the roots of a quadratic equation over k have the same field of definition, L and L' are either both k-rational or both not k-rational.

Fix a separable closure k^s of k, and let $G_k = \mathrm{Gal}(k^s/k)$. Let Λ be such that $\{L, L', \Lambda\} = \{M_1, M_2, M_3\}$. While L, L' need not be k-rational, the line Λ is k-rational. Indeed, L_4 and Q are defined over k, so the intersection $L_4 \cap Q$ is fixed under G_k-action. Both rulings of Q are also defined over k, so the set of lines through $L_4 \cap Q$ in either of these rulings is fixed under G_k. Thus $\{L, L'\}$ is G_k-fixed. Since X is also defined over k, the intersection $X \cap Q = \{L_1, L_2, L_3, L, L', \Lambda\}$ is G_k-fixed. Since L_1, L_2, L_3 are all k-rational and $\{L, L'\}$ is G_k-fixed, it follows that Λ is also G_k-fixed and is hence k-rational by Proposition 2.4.

Since L and L' belong to different sextuples in D, any line in D must be skew to exactly one of L and L'. In particular, the lines $L_1, \ldots, L_4$ do not belong to D. Since Λ is in a different ruling of Q than L_1, L_2, L_3, the rational lines Λ and L_i intersect and hence determine a new k-rational line $N_i \subset X$ for $1 \leq i \leq 3$. Note that each N_i cannot meet L or L', or else we would have two distinct triples of coplanar lines that both contain L_i and N_i. In particular, $N_i \notin D$ for each i.

The line L_4 does not meet L_1, L_2, L_3, or Λ, so Lemma 3.1 implies that L_4 meets each N_i for $1 \leq i \leq 3$. We thus obtain new k-rational lines P_1, P_2, P_3, with P_i meeting L_4 and N_i. As with each N_i, the fact that L_4 meets L and L' implies that P_i cannot meet L or L', so $P_i \notin D$. We have thus found 11 k-rational lines in the complement of D.

We now fill out the rest of the intersection graph of the complement of D. Each P_i must be adjacent to the 3-cycle $\{\Lambda, L_j, N_j\}$ for $i \neq j$. In order to avoid creating two distinct 3-cycles that share an edge, P_i cannot intersect Λ or N_j. We thus get a k-rational line $A_{i,j}$ meeting P_i and L_j. Since $A_{i,j}$ meets L_j and L_j meets L, L', it follows as before that $A_{i,j} \notin D$. Moreover, working within the graph in Figure 3I shows that $A_{i,j} = A_{j,i}$, so we have found 14 k-rational lines in the complement of D. The final line in the complement of D is residual to N_ℓ and $A_{i,j}$ (where $\{i, j, \ell\} = \{1, 2, 3\}$), so the final line in D is k-rational as well.

Let S and S' be the sextuples in D to which L and L' respectively belong. Since L and L' are disjoint, L intersects each line in $S' - \{L'\}$. Let $\Lambda \in S' - \{L'\}$ be such a line. There is a third line $R \subset X$ that intersects both L and Λ. Since R intersects L, we have $R \notin S$. Since R intersects $\Lambda \in S'$, we have $R \notin S'$. Thus R is not contained in the double six D, so R is k-rational by the previous paragraph. If L is k-rational, then Corollary 2.7 implies that Λ is also k-rational. Similarly, if L is not k-rational, then we deduce that Λ cannot be k-rational by the contraposition of Corollary 2.7. Repeating this argument for all lines in $S' - \{L'\}$, as well as the symmetric argument for all lines in $S - \{L\}$, we find that X contains exactly 15 k-rational if L, L' are not k-rational or 27 k-rational lines if L, L' are k-rational. □

The final fact we will use is that if a smooth cubic surface X contains two triples of coplanar k-rational lines, then X contains a *Steiner system* of k-rational lines.

Definition 3.8. A set $\{L_i^j\}_{i,j=1}^3$ of nine lines on a smooth cubic surface is called a *Steiner system* if L_i^1, L_i^2, L_i^3 are coplanar for all i and L_1^j, L_2^j, L_3^j are coplanar for all j.

Lemma 3.9. *Let X be a smooth cubic surface over a field k. Let L_1^1, L_2^1, L_3^1 and L_1^2, L_2^2, L_3^2 be two distinct triples of k-rational coplanar lines on X. Then there exist k-rational lines $L_1^3, L_2^3, L_3^3 \subset X$ such that $\{L_i^j\}_{i,j=1}^3$ form a Steiner system.*

Proof. Lines on X intersect if and only if they are coplanar. Thus Lemma 3.1 implies that for each $1 \leq i \leq 3$, the line L_i^1 meets L_j^2 for precisely one of $1 \leq j \leq 3$. Symmetrically, the line L_i^2 meets L_j^1 for precisely one of $1 \leq j \leq 3$. Thus the lines L_i^1 and L_j^2 can be paired off into three couples of intersecting lines. Relabel the lines L_j^2 so that $L_i^1 \cap L_i^2 \neq \varnothing$ for each i. Since all of the lines at hand are k-rational, each of these pairs gives rise to another k-rational line by Corollary 2.7. Denote the new k-rational line coming from L_i^1 and L_i^2 by L_i^3. Then $\{L_i^j\}_{i,j=1}^3$ is the desired Steiner system. □

We are almost ready to prove Theorem 1.2. We will phrase our argument in terms of the *intersection graph* G of X. The vertices of G correspond to k-rational lines on X, and two vertices of G are adjacent if the corresponding lines on X intersect. We will reinterpret some of the above geometric facts in terms of the intersection graph, after which we will prove Theorem 1.2.

Lemma 3.10. *Let X be a smooth cubic surface over a field k, and let G be its intersection graph. Then:*

(i) Every edge of G belongs to a 3-cycle.

(ii) No two 3-cycles in G share an edge.

(iii) If G contains a 3-cycle, then G is connected.

(iv) If G contains two 3-cycles that do not share any vertices, then G contains a Steiner system.

(v) If G contains four non-adjacent vertices, then G is either the graph given in Figure 31 or the complement of the Schläfli graph.

Proof. An edge in G corresponds to two intersecting k-rational lines, and a 3-cycle in G corresponds to three pairwise-intersecting (equivalently, coplanar) k-rational lines. Thus Corollary 2.7 implies (i).

If G were to contain two 3-cycles that shared an edge, then the four vertices in this configuration would correspond to four coplanar lines on X. Letting H be the plane containing these four lines, we would have four lines in $X \cap H$. But Bézout's theorem implies that $X \cap H$ contains at most $\deg X \cdot \deg H = 3$ lines, so we deduce (ii) by contradiction.

Lemma 3.1 implies that if G contains a 3-cycle, then every vertex in G is adjacent to one of the vertices in the 3-cycle. This in turn implies that G is connected, giving us (iii).

Item (iv) is just a restatement of Lemma 3.9. Item (v) follows from Lemmas 3.6 and 3.7. Indeed, four non-adjacent vertices in G correspond to four skew lines on X. The k-rational lines on X then either belong to the complement of a double six (whose intersection graph is given in Figure 3I), or all 27 lines on X are k-rational (whose intersection graph is the complement of the Schläfli graph [Sch58, Tod32]). □

Proof of Theorem 1.2. The method of proof is to list all graphs satisfying the criteria given in Lemma 3.10. Let G be the intersection graph of a smooth cubic surface over a field k. There are no obstructions to G being the empty graph (Figure 3A), a single vertex (Figure 3B), or two disjoint vertices (Figure 3C). If G contains an edge between two vertices, then G contains a 3-cycle by Lemma 3.10 (i). There are no obstructions to G consisting of three vertices with no edges (Figure 3D) or a 3-cycle (Figure 3E).

If G contains at least four vertices, then every vertex of G must belong to a 3-cycle. Indeed, if G contains an edge and therefore a 3-cycle by Lemma 3.10 (i), then G is connected by Lemma 3.10 (iii). It follows that every vertex of G has an incident edge and therefore belongs to a 3-cycle. If G contains four disjoint vertices, then G contains an edge by Lemma 3.10 (v) and hence every vertex of G belongs to a 3-cycle.

It follows that if G contains at least four vertices, then we must obtain G by taking a 3-cycle C, adjoining additional 3-cycles to C (with each additional 3-cycle meeting C at precisely one of its vertices), and then adding any edges necessary to satisfy the constraints listed in Lemma 3.10. One consequence is that if G contains at least four vertices, then G must contain an odd number of vertices, since we begin with a 3-cycle but only add two new vertices for each additional 3-cycle.

There is only one way to construct a graph with five vertices in this manner (Figure 3F). To obtain a graph with seven vertices, we take two adjoined 3-cycles and adjoin a third 3-cycle. If these three 3-cycles do not share a common vertex, then we have a chain of 3-cycles (see Figure 1). Each vertex on one end of this chain must be adjacent to the 3-cycle on the other end, so we need to add edges accordingly (one example illustrated in cyan). We must add more edges to G until every edge belongs to a 3-cycle, but this will then force G to contain two 3-cycles that share an edge (one example illustrated in red). This contradicts Lemma 3.10 (ii), so we conclude that all three 3-cycles must be joined at a common vertex (Figure 3G).

If G has nine vertices, then we attach three 3-cycles T_1, T_2, T_3 to a fourth 3-cycle C. If two of T_1, T_2, T_3 are attached to C at the same vertex, then there are four non-adjacent vertices in G (see Figure 2). We must therefore add edges until no set of four vertices are mutually non-adjacent, but any choice of such edges will conflict with Lemma 3.10 (ii). We therefore conclude that each T_i must be adjoined to C at a different vertex of C. We must then add edges until G satisfies Lemma 3.10. This process results in the intersection graph of the Steiner system (Figure 3H).

To conclude, we will show that if G has more than nine vertices, then G contains four non-adjacent vertices. If G has more than nine vertices, then G is obtained by attaching at least four 3-cycles to a central 3-cycle. By the pigeonhole principle, G will contain one

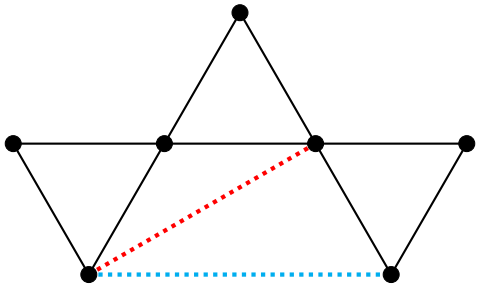
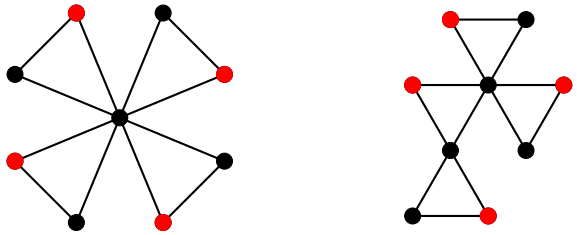


FIGURE 1. Impermissible graph of seven lines

of the graphs in Figure 2 as a subgraph. If no four vertices of G are non-adjacent, we will need to add edges to G, but we have already seen that this will force G to conflict with Lemma 3.10 (ii). We thus conclude that G contains four non-adjacent vertices, so G has 15 or 27 vertices by Lemma 3.10 (v). □



(A) All T_i sharing a vertex (B) Two T_i sharing a vertex

FIGURE 2. Impermissible graphs of nine lines

Remark 3.11. The results of Section 5 give another proof of Theorem 1.2. Given a smooth cubic surface X over a field k with separable closure k^s, all of the k-rational lines on X descend from k-rational lines on X_{k^s} by Proposition 2.4. Since X_{k^s} arises from blowing up $\mathbb{P}^2_{k^s}$ at 6 points (see Lemma 2.8), the configuration and number of k-rational lines on X can be deduced from the $\mathrm{Gal}(k^s/k)$-invariant subsets of the 6 points in $\mathbb{P}^2_{k^s}$.

3.1. **Characteristic 2.** While his proof works in any characteristic, B. Segre incorrectly states that Theorem 1.2 fails in characteristic 2. He then proceeds to describe three smooth cubic surfaces over $\mathbb{F}_2$ that contain 35, 13, and 6 lines. These line counts contradict the classification of smooth cubic surfaces over $\mathbb{F}_2$ given by Dickson [Dic15]. In private communication, J.-P. Serre pointed out to us that Segre's lines are defined set-wise rather than algebraically. That is, Segre implicitly defines a line L to be contained in a smooth cubic surface X if every rational point of L is contained in X. Since $\mathbb{P}^3_{\mathbb{F}_2}$ contains 15 rational points and 35 rational lines, Segre calculates the lines in his examples by checking which of these 15 points are contained in his cubic surfaces.

Over fields of cardinality at least 3, the set-theoretic and algebraic definitions of line containment for cubic surfaces agree.

Proposition 3.12. *Let k be a field of cardinality at least 3. Let X be a cubic surface defined over k. Let L be a line defined over k. Then L is contained in X if and only if every k-rational point of L is contained in X.*

Proof. If $L \subset X$, then every point of L is contained in X. Thus all k-rational points of L are contained in X. Conversely, suppose all k-rational points of L are contained in X. Since L is defined over k, this line is isomorphic to $\mathbb{P}^1_k$. If $|k| > 2$, then $L \cong \mathbb{P}^1_k$ contains $|k| + 1 > 3$ points defined over k. Since $\deg L \cdot \deg X = 3$, Bézout's theorem implies that L must be contained in X. □

Proposition 3.12 fails over $\mathbb{F}_2$. Indeed, $\mathbb{P}^1_{\mathbb{F}_2}$ only contains three $\mathbb{F}_2$-rational points, so a cubic surface X may intersect a line L in three $\mathbb{F}_2$-points without containing any points of L not defined over $\mathbb{F}_2$. This accounts for the discrepancy between Segre's claim and Dickson's theorem [Dic15] about lines on cubic surfaces over $\mathbb{F}_2$.

4. Sufficient criteria for line counts

In this section, we prove that the arithmetic criteria in Theorem 1.3 are sufficient to obtain the corresponding line counts over a given field.

Theorem 4.1. *Let k be a field with $|k| \geq 22$. There is a smooth cubic surface over k whose 27 lines are all defined over k. Moreover, there is a smooth cubic surface over k containing n lines defined over k if k admits a separable field extension of the degrees listed in Table 1.*

We prove Theorem 4.1 by blowing up $\mathbb{P}^2_k$ at appropriate sets of points. The various line counts arise from the arithmetic configurations of the sets at which we blow up. This technique is classical and appears extensively in the study of lines on real cubic surfaces. As we will see in Section 4.1, most of the work goes into showing that the relevant sets of points can be arranged in general position over k.

Setup 4.2. There is a well-known method for constructing the 27 lines on a smooth cubic surface via blow-ups. If X is the smooth cubic surface obtained by blowing up $\mathbb{P}^2_k$ at the six geometric points $p_1, \ldots, p_6$, then we get the following lines on X:

- E_i, the exceptional divisor above p_i, for $1 \leq i \leq 6$.
- C_i, the strict transform of the unique conic through $\{p_1, \ldots, p_6\} - \{p_i\}$, for $1 \leq i \leq 6$.
- L_{ij}, the strict transform of the unique line through p_i and p_j, for $1 \leq i < j \leq 6$.

We also deduce that only pairs among these lines that intersect are E_i and C_j for $i \neq j$, E_n and L_{ij} for $n = i, j$, C_n and L_{ij} for $n = i, j$, and L_{ij} and L_{mn} for $\{i, j\} \cap \{m, n\} = \varnothing$.

Since all lines on X are defined over a separable closure k^s of k [Coo88], we may take $p_1, \ldots, p_6$ to be k^s-rational. We can now check whether X and any of its line are defined over k using Proposition 2.4. The surface X is defined over k if and only if the set $\{p_1, \ldots, p_6\}$ is $\mathrm{Gal}(k^s/k)$-fixed. Moreover:

- E_i is k-rational if and only if p_i is k-rational.
- C_i is k-rational if and only if the set $\{p_1, \ldots, p_6\} - \{p_i\}$ is $\mathrm{Gal}(k^s/k)$-fixed.
- L_{ij} is k-rational if and only if the set $\{p_i, p_j\}$ is $\mathrm{Gal}(k^s/k)$-fixed.

Each possible line count (and configuration) for smooth cubic surfaces arises from partitioning $\{p_1, \ldots, p_6\}$ into Galois orbits.

(1_6) If $p_1, \ldots, p_6$ are all k-rational, then all 27 lines on X are k-rational.

($1_4, 2_1$) If $p_1, \ldots, p_4$ are k-rational and $\{p_5, p_6\}$ is a Galois orbit, then L_{56} and E_i, C_j, L_{ij} for $1 \leq i, j \leq 4$ are the only k-rational lines on X. Thus X has 15 k-rational lines.

($1_3, 3_1$) If p_1, p_2, p_3 are k-rational and $\{p_4, p_5, p_6\}$ is a Galois orbit, then E_i, C_j, L_{ij} for $1 \leq i, j \leq 3$ are the only k-rational lines on X. Thus X has 9 k-rational lines.

($1_2, 2_2$) If p_1, p_2 are k-rational, $\{p_3, p_4\}$ is a Galois orbit, and $\{p_5, p_6\}$ is a Galois orbit, then $E_1, E_2, C_1, C_2, L_{12}, L_{34}$, and L_{56} are the only k-rational lines on X. Thus X has 7 k-rational lines.

($1_2, 4_1$) If p_1, p_2 are k-rational and $\{p_3, \ldots, p_6\}$ is a Galois orbit, then E_1, E_2, C_1, C_2, and L_{12} are the only k-rational lines on X. Thus X has 5 k-rational lines.

($1_1, 2_1, 3_1$) If p_1 is k-rational, $\{p_2, p_3\}$ is a Galois orbit, and $\{p_4, p_5, p_6\}$ is a Galois orbit, then E_1, C_1, and L_{23} are the only k-rational lines on X. Thus X contains 3 skew k-rational lines.

(2_3) If $\{p_i, p_j\}$ is a Galois orbit for $(i, j) = (1, 2)$, $(3, 4)$, and $(5, 6)$, then L_{12}, L_{34}, and L_{56} are the only k-rational lines on X. Thus X contains 3 k-rational lines that are pairwise intersecting.

($1_1, 5_1$) If p_1 is k-rational and $\{p_2, \ldots, p_6\}$ is a Galois orbit, then E_1 and C_1 are the only k-rational lines on X. Thus X contains 2 k-rational lines.

($2_1, 4_1$) If $\{p_1, p_2\}$ and $\{p_3, \ldots, p_6\}$ are each Galois orbits, then L_{12} is the only k-rational line on X. Thus X contains 1 k-rational line.

(3_2) If $\{p_1, p_2, p_3\}$ and $\{p_4, p_5, p_6\}$ are each Galois orbits, then X has no k-rational lines.

(6_1) If $\{p_1, \ldots, p_6\}$ is a Galois orbit, then X has no k-rational lines.

4.1. **Blowing up on the cusp.** In order to obtain a smooth cubic surface by blowing up $\mathbb{P}^2_k$ at one of the sets described in Setup 4.2, we need to ensure that the points at which we are blowing up lie in general position. (Over $\overline{k}$, our collection of points splits into six points. These six points are said to lie in *general position* if no three are contained in a line and all six are not contained in a conic.)

If we require our six points to lie on the cusp $C = \mathbb{V}(y^3 - x^2 z)$, the parameterization $C = \{[1 : t : t^3]\}$ gives us an algebraic method for checking whether the points lie in

general position. Three distinct points $[1 : t_i : t_i^3]$ lie on the line $\mathbb{V}(ax + by + cz)$ if and only if each t_i is a root of $F(t) = a + bt + ct^3$. The sum of these roots is a scalar multiple of the coefficient of the degree 2 term of $F(t)$, so the points $[1 : t_i : t_i^3]$ lie on a shared line if and only if $t_1 + t_2 + t_3 = 0$. Similarly, six distinct points $[1 : t_i : t_i^3]$ lie on the conic $\mathbb{V}(ax^2 + bxy + cy^2 + xz + eyz + fz^2)$ if and only if each t_i is a root of $G(t) = a + bt + ct^2 + dt^3 + et^4 + ft^6$. The sum of these roots is a scalar multiple of the coefficient of the degree 5 term of $G(t)$, so $[1 : t_i : t_i^3]$ lie on a shared conic if and only if $t_1 + \ldots + t_6 = 0$.

In order to find six points on the cusp that lie in general position in $\mathbb{P}^2_k$, it therefore suffices to construct a degree 6 monic polynomial $G(t)$ such that:

(i) $G(t)$ has no repeated roots.

(ii) No three roots of $G(t)$ sum to zero.

(iii) The degree 5 coefficient of $G(t)$ is not zero.

In Section 4.2, we will prove Theorem 4.1 by constructing various degree 6 monic polynomials that satisfy the above criteria.

4.2. **Proof of Theorem 4.1.** We are now ready to prove Theorem 4.1. We treat each Galois partition of $\{p_1, \ldots, p_6\}$ (see Setup 4.2) in a separate lemma. We remark that the cardinality assumptions on k in each of these lemmas need not be optimal — for example, Lemma 4.4 requires $|k| \geq 13$ in order to find 6 k-rational points in general position on the cusp. If one does not restrict to the cusp, then there are collections of 6 k-rational points in $\mathbb{P}^2_k$ in general position. However, we will be content to restrict our search to points on the cusp. We also remark that the proofs in this section are fairly computational. This is intentional — in case some reader wishes to construct a smooth cubic surface over a given field with a desired line count, these proofs outline how to find an explicit set of points at which to blow up.

Throughout this section, all irreducible polynomials that we work with are assumed to be separable. We will make frequent use of the following lemma, which allows us to furnish monic, separable, irreducible polynomials with a prescribed penultimate coefficient.

Lemma 4.3. *Let k be a field. Pick $a \in k$. Assume that k admits a finite separable extension of degree $n \geq 2$. If $\operatorname{char} k = n = 2$, we assume that $a \neq 0$. Then there is a monic, separable, irreducible polynomial $f(t) \in k[t]$ of degree n whose degree $n - 1$ coefficient is a.*

Proof. When k is a finite field, this is a special case of the Hansen–Mullen conjecture, which was proved by Wan [Wan97] and Ham–Mullen [HM98]. We may thus assume that k is an infinite field, although we will not need this assumption in most cases. In general, the assumption that k admits a finite separable extension of degree n implies that there is a monic, separable, irreducible polynomial $m(t) \in k[t]$ of degree n. The goal is to use $m(t)$ to find another monic, separable, irreducible polynomial $f(t)$ with the prescribed coefficient in degree $n - 1$.

To begin, assume that $\operatorname{char} k = 0$ or that $\operatorname{char} k$ does not divide n.

(i) If the degree $n-1$ coefficient of $m(t)$ is $c \neq 0$ and the prescribed coefficient is $a \neq 0$, then set $f(t) := (a^{-1}c)^{-n} \cdot m(a^{-1}ct)$. The separability and irreducibility of $f(t)$ follow from that of $m(t)$, and the degree $n-1$ coefficient of $f(t)$ is $(a^{-1}c)^{-n} \cdot c(a^{-1}c)^{n-1} = a$, as desired.

(ii) If $c = 0$ and $a \neq 0$, then set $g(t) := m(t+1)$ (which is again separable and irreducible). By the binomial theorem, the degree $n-1$ coefficient of $g(t)$ is $\binom{n}{1} = n$ (or $n \mod \operatorname{char} k$ in positive characteristic), which is non-zero since we have assumed that $\operatorname{char} k = 0$ or $\operatorname{char} k \nmid n$. We can then set $f(t) = (a^{-1}n)^{-n} \cdot g(a^{-1}nt)$ as in (i).

(iii) If $c \neq 0$ and $a = 0$, then set $f(t) := m(t - \frac{c}{n})$. Since $-c$ is the sum of the roots of $m(t)$, the sum of the roots of $f(t)$ is $-c + n \cdot \frac{c}{n} = 0$, which is the desired degree $n-1$ coefficient.

(iv) If $a = c = 0$, then we simply take $f(t) := m(t)$.

Now suppose that $\operatorname{char} k = p$ and $n = pq$ for some integer $q > 0$. In characteristic p, an irreducible polynomial $m(t) \in k[t]$ is separable if and only if it is not of the form $m(t) = h(t^p)$ for some polynomial $h(t) \in k[t]$. Let $m(t) \in k[t]$ be a monic, separable, irreducible polynomial of degree n. Then there exists $1 \leq d \leq n$ with $p \nmid d$ such that the degree d term of $m(t)$ is non-zero. Let c be the degree d coefficient of $m(t)$.

(v) If $d = n-1$ and the prescribed coefficient is $a \neq 0$, then set $f(t) := (a^{-1}c)^{-n} \cdot m(a^{-1}ct)$ as in (i).

(vi) If $d = 1$ and $a \neq 0$, then the scaled reciprocal polynomial $m^*(t) := m(0)^{-1}t^n \cdot m(t^{-1})$ is again separable and irreducible with degree $n-1$ coefficient $m(0)^{-1}c \neq 0$. We then set $f(t) := (a^{-1}m(0)^{-1}c)^{-n} \cdot m^*(a^{-1}m(0)^{-1}ct)$.

(vii) If the degree 1 and $n-1$ terms of $m(t)$ are zero and $a \neq 0$, then consider $g_x(t) := m(t+x)$. The degree 1 term of $g_x(t)$ is $c_x := \sum_{i=2}^{n-2} i m_i x^{i-1}$, where m_i is the degree i coefficient of $m(t)$. Since c_x is a degree $n-2$ polynomial in x, our assumption that $|k| = \infty > n-2$ implies that there exists $\alpha \in k$ such that $c_\alpha \neq 0$. It follows that the scaled reciprocal polynomial $g_\alpha^*(t)$ is a monic, separable, irreducible polynomial with degree $n-1$ coefficient $m(\alpha)^{-1}c_\alpha \neq 0$, so we can set $f(t) := (a^{-1}m(\alpha)^{-1}c_\alpha)^{-n} \cdot g_\alpha^*(a^{-1}m(\alpha)^{-1}c_\alpha t)$.

(viii) If $c \neq 0$ and $a = 0$, then let α be a root of $m(t)$. It suffices to find $\beta \in k(\alpha)$ with trace zero such that β is not contained in any proper subextension of $k(\alpha)/k$. Once we have done so, it will follow that $k(\beta) = k(\alpha)$ is separable over k, and hence the minimal polynomial of β will be a monic, separable, irreducible polynomial of degree n. By picking β with trace zero, the trace of its minimal polynomial (i.e. the degree $n-1$ coefficient) will be zero as well.

The trace defines a k-linear map $\operatorname{tr} : k(\alpha) \to k$, so $\ker(\operatorname{tr})$ is a k-vector space of dimension $n-1$. Since $k(\alpha)/k$ is a separable extension, there are only finitely many subextensions $k \subset L \subset k(\alpha)$. Moreover, since $[k(\alpha) : k] = [k(\alpha) : L] \cdot [L : k]$, each

subextension L is a vector subspace of $k(\alpha)$ of dimension at most $n/2$. It suffices to choose $\beta \in \ker(\mathrm{tr}) - \bigcup_{k \subset L \subset k(\alpha)} L$. If $n > 2$, then a finite union of at most $n/2$-dimensional subspaces cannot cover an $(n-1)$-dimensional subspace. Paired with the assumption that k is infinite, it follows that $\ker(\mathrm{tr}) - \bigcup_{k \subset L \subset k(\alpha)} L$ is non-empty if $n > 2$. The $n = 2$ case is already solved by case (iii) and our assumption that $a \neq 0$ if $\mathrm{char}\, k = n = 2$.

(ix) If $a = c = 0$, then we take $f(t) := m(t)$ as in case (iv). □

Lemma 4.4. *Let k be a field with $|k| \geq 13$. Then there is a smooth cubic surface over k with 27 k-rational lines.*

Proof. It suffices to find 6 k-rational points on the cusp C that are in general position. If $\mathrm{char}\, k$ is 0 or at least 13, then $G(t) = \prod_{i=0}^{5}(t+i)$ satisfies the desired criteria. Otherwise, write $\mathrm{char}\, k = p$.

- If p is 5, 7, or 11, then there exists $\alpha \in k - \mathbb{F}_p$, and $G(t) = t(t+1)(t+2)(t+\alpha)(t+\alpha+1)(t+\alpha+2)$ satisfies the desired criteria.
- If $p = 3$, then there exist $\alpha, \beta \in k - \mathbb{F}_3$ such that $\{1, \alpha, \beta\}$ are $\mathbb{F}_3$-linearly independent. Indeed, if k is a finite extension of $\mathbb{F}_3$, then $|k| \geq 27$ and hence $\dim_{\mathbb{F}_3} k \geq 3$. If k is an infinite extension of $\mathbb{F}_3$, then take $\alpha \in k$ to be transcendental over $\mathbb{F}_3$ and set $\beta = \alpha^2$. In either case, $G(t) = t(t+1)(t+\alpha)(t+\alpha+1)(t+\beta)(t+\beta+1)$ satisfies the desired criteria.
- If $p = 2$, then there exist $\alpha, \beta, \gamma \in k - \mathbb{F}_2$ such that $\{1, \alpha, \beta, \gamma\}$ are $\mathbb{F}_2$-linearly independent. Indeed, if k is a finite extension of $\mathbb{F}_2$, then $|k| \geq 16$ and hence $\dim_{\mathbb{F}_2} k \geq 4$. If k is an infinite extension of $\mathbb{F}_2$, then take α to be transcendental over $\mathbb{F}_2$ and set $\beta = \alpha^2$ and $\gamma = \alpha^3$. In either case, $G(t) = t(t+1)(t+\alpha)(t+\beta)(t+\gamma)(t+\alpha+\beta+\gamma)$ satisfies the desired criteria. □

Lemma 4.5. *Let k be a field with $|k| \geq 7$. Assume that k admits a separable degree 2 extension. Then there is a smooth cubic surface over k with 15 k-rational lines.*

Proof. Let $m(t) = t^2 + at + b \in k[t]$ be a separable irreducible polynomial. It suffices to pick four distinct elements $r_1, r_2, r_3, r_4 \in k$ such that $\sum_{i=1}^{4} r_i \neq a$ and $\sum_{i \neq j} r_i \neq 0$ for $1 \leq j \leq 4$ (since the roots of $m(t)$ are not defined over k and are thus not equal to $-r_i - r_j$). Once we have done so, $G(t) = m(t) \cdot \prod_{i=1}^{4}(t - r_i)$ will satisfy the desired criteria.

Pick distinct $r_1, r_2 \in k$. We then need to choose $r_3 \in k - \{r_1, r_2\}$ such that $r_3 \neq -r_1 - r_2$, so we may freely pick $r_3 \in k - \{r_1, r_2, -r_1 - r_2\}$. Finally, we need to choose $r_4 \in k - \{r_1, r_2, r_3, -r_1 - r_2, -r_1 - r_3, -r_2 - r_3\}$. Since we have assumed $|k| \geq 7$, such an r_4 exists, and we are done. □

Lemma 4.6. *Let k be a field with $|k| \geq 5$. Assume that k admits a separable degree 3 extension. Then there is a smooth cubic surface over k with 9 k-rational lines.*

Proof. By Lemma 4.3, there is a separable irreducible polynomial $m(t) = t^3+at^2+bt+c \in k[t]$ with $a \neq 0$. Since $a \neq 0$, the three roots of $m(t)$ do not sum to zero. Since $m(t)$ is irreducible of degree 3, no two roots of $m(t)$ sum to an element of k (or else the third root would belong to k and $m(t)$ would not be irreducible). It thus suffices to find distinct $r_1, r_2, r_3 \in k$ such that $r_1 + r_2 + r_3 \neq 0$ and $r_1 + r_2 + r_3 \neq a$. Once we have done so, $G(t) = m(t) \cdot \prod_{i=1}^{3}(t - r_i)$ will satisfy the desired criteria.

Pick distinct $r_1, r_2 \in k$. We may then freely pick $r_3 \in k - \{r_1, r_2, -r_1 - r_2, a - r_1 - r_2\}$. Since we have assumed $|k| \geq 5$, such an r_3 exists. □

Lemma 4.7. *Let k be a field with $|k| \geq 4$. Assume that k admits a separable degree 2 extension. Then there is a smooth cubic surface over k with 7 k-rational lines.*

Proof. Let $m(t) = t^2 + at + b \in k[t]$ be a separable irreducible polynomial with $a \neq 0$ (which exists by Lemma 4.3). First suppose $\operatorname{char} k \neq 2$, so that $a \neq -a$. Then $n(t) := m(-t) = t^2 - at + b$ also does not have any k-rational roots, so $n(t)$ is also separable and irreducible over k. Pick $r \in k - \{\pm a, 0\}$, which is possible since $|k| \geq 4$. Then $G(t) = t(t - r) \cdot m(t) \cdot n(t)$ satisfies the desired criteria. Indeed, the degree 5 term is $a - a - r + 0 = -r$ is non-zero, and the sum of one (respectively, two) rational roots of $G(t)$ with two (respectively, one) non-rational roots of $G(t)$ cannot be zero (since $r \neq \pm a$). Finally, all four roots of $m(t)$ and $n(t)$ sum to zero, so no three of these roots can sum to zero (or else the fourth root would be $0 \in k$, a contradiction).

If $\operatorname{char} k = 2$, then pick $a \in k - \mathbb{F}_2$ (which we may do since $|k| \geq 4$). By Lemma 4.3, there exists b such that $m(t) = t^2 + at + b$ is separable and irreducible. Take $n(t) := m(t+1) = t^2 + at + a + b + 1$ as our second irreducible polynomial, and note that $m(t) \neq n(t)$ since $a \neq 1$. Then $G(t) = t(t + 1) \cdot m(t) \cdot n(t)$ satisfies the desired criteria. Indeed, the degree 5 term is $1 \neq 0$, sums of three roots involving one or two rational roots cannot be zero, and the sum of all four non-rational roots is $a + a = 0$, so any three of these roots cannot sum to zero. □

Lemma 4.8. *Let k be a field with $|k| \geq 8$. Assume that k admits a separable degree 4 extension. Then there is a smooth cubic surface over k with 5 k-rational lines.*

Proof. Let $m(t) = t^4 + at^2 + bt + c \in k[t]$ be a separable irreducible polynomial, which exists by Lemma 4.3. Since the sum of the roots of $m(t)$ is zero, no three roots of $m(t)$ can sum to zero. Let $s_1, \ldots, s_6$ be the $\binom{4}{2}$ sums of pairs of roots of $m(t)$. We want to pick $r \in k^\times$ such that $r \neq s_i$ for each i. There are at most six elements to avoid (in the case that each $s_i \in k$ and all are distinct). We thus pick $r \in k - \{0, s_1, \ldots, s_6\}$. Since $|k| \geq 8$, such an r exists. Now $G(t) = t(t - r) \cdot m(t)$ satisfies the desired criteria, since the sum of all roots is $-r \neq 0$ and any sum of three roots involving 0 or r cannot be zero. □

Lemma 4.9. *Let k be a field with $|k| \geq 3$. Assume that k admits separable extensions of degree 2 and 3. Then there is a smooth cubic surface over k with 3 k-rational lines that are skew.*

Proof. Pick $a \in k - \{0, -1\}$. By Lemma 4.3, there are separable irreducible polynomials $m(t) = t^3 + at^2 + bt + c \in k[t]$ and $n(t) = t^2 + t + d \in k[t]$. Since $a \neq 0$, the three roots of $m(t)$ do not sum to zero. Note that no three of the five roots of $m(t)$ and $n(t)$ sum to zero. Indeed, the roots of $n(t)$ sum to -1, and no root of $m(t)$ can be an element of k. If two roots of $m(t)$ and one root of $n(t)$ sum to zero, then the remaining roots r_m, r_n of $m(t), n(t)$, respectively, sum to $-a - 1$. But this would imply that $r_m = -r_n - a - 1$ is a root of the irreducible polynomial $n(-t - a - 1) \in k[t]$, which in turn implies that $n(-t - a - 1)$ must be an irreducible factor of $m(t)$. Since $m(t)$ is irreducible, such a factor does not exist.

We conclude by noting that $G(t) = t \cdot m(t) \cdot n(t)$ satisfies the desired criteria, since the degree 5 term is $a + 1 \neq 0$ and no three roots sum to zero. □

Lemma 4.10. *Let k be a field with $|k| \geq 5$. Assume that k admits a separable extension of degree 2. Then there is a smooth cubic surface over k with 3 k-rational lines that are coplanar.*

Proof. First assume $\operatorname{char} k = 2$. Pick a separable irreducible polynomial $m(t) = t^2 + t + a \in k[t]$ (which exists due to Lemma 4.3). Now pick distinct $\alpha, \beta \in k - \{0, 1\}$ such that $\alpha \neq \beta + 1$ (which exist since $|k| \geq 5$), and set $n(t) = m(t + \alpha) = t^2 + t + a + \alpha^2 + \alpha$ and $p(t) = m(t+\beta) = t^2+t+a+\beta^2+\beta$. Since $\alpha, \beta \neq 0, 1$, we have $\alpha^2+\alpha \neq 0$ and $\beta^2+\beta \neq 0$. Since $\alpha \neq \beta$ and $\alpha \neq \beta+1$, we have that (α, β) is not a solution to $(x+y)(x+y+1) = 0$ and hence $\alpha^2 + \alpha \neq \beta^2 + \beta$. In particular, the polynomials $m(t), n(t)$, and $p(t)$ are all distinct, so their six collective roots must also be distinct. Moreover, the sum of the four roots of any two of $m(t), n(t), p(t)$ is zero, so no three of these roots can sum to zero. The sum of all six roots is 1, so it remains to check that the sum of three roots, one from each of $m(t), n(t), p(t)$, cannot be zero. Then $G(t) = m(t) \cdot n(t) \cdot p(t)$ will satisfy the desired criteria.

Let μ_1, μ_2 be the roots of $m(t)$. The roots of $n(t)$ are $\mu_1 + \alpha, \mu_2 + \alpha$, and the roots of $p(t)$ are $\mu_1 + \beta, \mu_2 + \beta$. The sum of three roots, one from each of $m(t), n(t), p(t)$, is therefore either $3\mu_i + \alpha + \beta = \mu_i + \alpha + \beta$ for $i \in \{1, 2\}$ or $2\mu_i + \mu_j + \alpha + \beta = \mu_j + \alpha + \beta$ for $\{i, j\} = \{1, 2\}$. Since $\alpha, \beta \in k$ and $\mu_i, \mu_j \notin k$, these sums are non-zero.

Now assume $\operatorname{char} k \neq 2$. If $\operatorname{char} k \neq 3$, let $a = 2$. If $\operatorname{char} k = 3$, pick $a \in k - \mathbb{F}_3$. Then there is a separable irreducible polynomial $m(t) = t^2 + at + b \in k[t]$. Pick $\gamma \in k - \{0, \pm 1, -\frac{a}{2} - 1\}$, and set $n(t) = m(t + 1)$ and $p(t) = m(t + \gamma)$. Since $\gamma \neq 0, 1$, the polynomials $m(t), n(t), p(t)$ are distinct. The sum of the four roots of any two of $m(t), n(t), p(t)$ is k-rational, so no three of these roots can sum to zero (or else the fourth root would be rational). The sum of all six roots is $-a - 2 - 2\gamma \neq 0$ (by our choice of γ), so it remains to check that the sum of three roots, one from each of $m(t), n(t), p(t)$, cannot be zero. Then $G(t) = m(t) \cdot n(t) \cdot p(t)$ will satisfy the desired criteria.

Let μ_1, μ_2 be the roots of $m(t)$. The roots of $n(t)$ are $\mu_1 - 1, \mu_2 - 1$, and the roots of $p(t)$ are $\mu_1 - \gamma, \mu_2 - \gamma$. The sum of three roots, one from each of $m(t), n(t), p(t)$, is either $3\mu_i - 1 - \gamma$ or $2\mu_i + \mu_j - 1 - \gamma = \mu_i - a - 1 - \gamma$. We have assumed that $\gamma \neq -1$, so

$3\mu_i - 1 - \gamma$ is not zero even in characteristic 3. Since $1, a, \gamma \in k$ and $\mu_1, \mu_2 \notin k$, it follows that neither of these sums can be zero. □

Lemma 4.11. *Let k be a field. Assume that k admits a separable extension of degree 5. Then there is a smooth cubic surface over k with 2 k-rational lines.*

Proof. Pick a separable irreducible polynomial $m(t) = t^5 + at^3 + bt^2 + ct + d$. We will set $G(t) = (t+1) \cdot m(t)$. If three roots of $m(t)$ sum to 0, then so do the remaining two roots of $m(t)$. If two roots of $m(t)$ sum to 1, then the roots of $G(t)$ will sum to 0. It thus suffices to show that no two roots of $m(t)$ can sum to 0 or 1.

In characteristic 2, two roots of $m(t)$ summing to zero implies that $m(t)$ has a repeated root, which contradicts our assumption that $m(t)$ is separable. If $\operatorname{char} k \neq 2$ and r is a root of $m(t)$, then $0 = m(r) + m(-r) = 2br^2 + 2d$. If $b \neq 0$, then the minimal polynomial of r has degree less than 5, contradicting the irreducibility of $m(t)$. Otherwise, we have $2d = 0$, which implies that 0 is a root of $m(t)$ and again contradicts the irreducibility of $m(t)$. If two roots of $m(t)$ sum to 1, then there is a root r such that $m(r) = m(1-r) = 0$. Thus r is a root of

$$\begin{aligned} m(t) + m(1-t) = 5t^4 - 10t^3 + (10 + 3a + 2b)t^2 \\ - (5 + 3a + 2b + c)t + 1 + a + b + c + 2d. \end{aligned}$$

If $\operatorname{char} k \neq 5$, then $m(t) + m(1-t)$ is a non-zero polynomial of degree strictly less than 5. This again contradicts the irreducibility of $m(t)$. If $\operatorname{char} k = 5$, then $m(t) + m(1-t)$ is identically zero only if $b = -\frac{3a}{2} = a$, $c = 0$, and $d = -\frac{1+a+b+c}{2} = \frac{2+a}{4} = 3 + 4a$. If $m(t) + m(1-t)$ is identically zero, then take $G(t) = (t+1) \cdot m(t+1)$. Since $m(t+1) = t^5 + at^3 + 4at^2 + a + 4$, we follow the previous arguments to find that no two roots of $m(t+1)$ sum to 0 or 1, as desired. □

Lemma 4.12. *Let k be a field with $|k| \geq 8$. Assume that k admits separable extensions of degree 2 and 4. Then there is a smooth cubic surface over k with 1 k-rational line.*

Proof. Pick $a \in k^\times$. Let $m(t) = t^2 + at + b$ and $n(t) = t^4 + ct^2 + dt + e$ be separable irreducible polynomials. Since all four roots of $n(t)$ sum to zero, no three of these roots can sum to zero. All six roots of $m(t)$ and $n(t)$ sum to $-a \neq 0$. Moreover, the two roots of $m(t)$ sum to $-a \in k$, so no root of $n(t)$ can yield zero when summed with the roots of $m(t)$. It remains to show that a root of $m(t)$ and two roots of $n(t)$ cannot sum to zero. We then set $G(t) = m(t) \cdot n(t)$.

Let $\nu_1, \ldots, \nu_4$ be the roots of $n(t)$. We want to guarantee that each of the roots of $m(t)$ are not of the form $-(\nu_i + \nu_j)$ for some i, j. If the splitting field of $m(t)$ is not a subfield of $k(\nu_1)$, then we are done. Otherwise, let $r_{i,j} \in k$ be the trace of $-(\nu_i + \nu_j)$, so that the minimal polynomial of $-(\nu_i + \nu_j)$ has penultimate coefficient $-r_{i,j}$. If we pick $a \in k^\times - \bigcup_{1 \leq i < j \leq 6} \{-r_{i,j}\}$ (which is possible since $|k| \geq 8$), then a root of $m(t)$ and two roots of $n(t)$ cannot sum to zero. □

Lemma 4.13. *Let k be a field with $|k| \geq 4$. Assume that k admits a separable extension of degree 3. Then there is a smooth cubic surface over k with no k-rational lines.*

Proof. First assume $\operatorname{char} k$ is not 2 or 3. Pick separable irreducible polynomials $m(t) = t^3 + 2t^2 + at + b$ and $n(t) = t^3 + t^2 + ct + d$. By design, the three roots of $m(t)$ and $n(t)$, respectively, do not sum to zero, and all six roots sum to $-3 \neq 0$. It remains to show that one root of $m(t)$ and two roots of $n(t)$ do not sum to zero (with the same argument holding for two roots of $m(t)$ and one root of $n(t)$). Once we have done so, $G(t) = m(t) \cdot n(t)$ will satisfy the desired criteria.

Let μ_1, μ_2, μ_3 and ν_1, ν_2, ν_3 be the roots of $m(t)$ and $n(t)$, respectively. Assume $\mu_1 + \nu_1 + \nu_2 = 0$. Then $\nu_3 = \mu_1 + \sum_{i=1}^3 \nu_i = \mu_1 + 1$. The minimal polynomial of $\mu_1 + 1$ is $m(t-1)$, so this implies that $m(t-1) = n(t)$. But the degree 2 coefficient of $m(t-1)$ is $2-3 = -1$, and the degree 2 coefficient of $n(t)$ is 1. These are not equal when $\operatorname{char} k \neq 2$.

Now assume $\operatorname{char} k = p$ is 2 or 3. Since $|k| \geq 4$, we may pick $\alpha \in k - \mathbb{F}_p$. Pick separable irreducible polynomials $m(t) = t^3 + \alpha t^2 + at + b$ and $n(t) = t^3 + t^2 + ct + d$. Again, the three roots of each of these polynomials do not sum to zero, and their six roots sum to $-\alpha - 1 \neq 0$. Using the same notation as before, if $\mu_1 + \nu_1 + \nu_2 = 0$, then $\nu_3 = \mu_1 + 1$. The minimal polynomial of $\mu_1 + 1$ is $m(t-1) = n(t)$, but the respective degree 2 coefficients are then $\alpha - 3$ and 1. Since $\alpha \in k - \mathbb{F}_p$, it follows that $\alpha - 3 \neq 1$. □

Lemma 4.14. *Let k be a field with $|k| \geq 22$. Assume that k admits a separable extension of degree 6. Then there is a smooth cubic surface over k with no k-rational lines.*

Proof. First, assume that $\operatorname{char} k \neq 3$. Let $m(t) = t^6 + t^5 + a_4 t^4 + \ldots + a_0 \in k[t]$ be a separable irreducible polynomial with roots $r_1, \ldots, r_6$. If no three of the roots of $m(t)$ sum to zero, then we set $G(t) = m(t)$. Otherwise, consider $m(t - \alpha)$ for some $\alpha \in k^\times$, whose roots are given by $r_1 + \alpha, \ldots, r_6 + \alpha$. If $r_1 + r_2 + r_3 = 0$, then $(r_1 + \alpha) + (r_2 + \alpha) + (r_3 + \alpha) = 3\alpha \neq 0$. However, it may happen that some other roots satisfy $r_i + r_j + r_\ell + 3\alpha = 0$. If this happens, we take $\beta \in k - \{0, \alpha\}$ and investigate $m(t - \beta)$. There are $\binom{6}{3} = 20$ sums of triples of roots to consider, so it appears that $|k| \geq 21$ suffices for our purposes. In fact, there is one more case to avoid: since $\sum_{i=1}^6 r_i = -1$, we have $\sum_{i=1}^6 (r_i + \frac{1}{6}) = 0$. By assuming $|k| \geq 22$, we guarantee that there exists $\alpha \in k - \{-\frac{1}{6}\}$ such that $m(t - \alpha)$ is separable and irreducible, has no three roots summing to zero, and has all six roots not summing to zero. We then set $G(t) = m(t - \alpha)$.

Now assume $\operatorname{char} k = 3$. Since $|k| \geq 22$, we have $|k| \geq 27$ in characteristic 3. Let $m(t) = t^6 + a_5 t^5 + \ldots + a_0 \in k[t]$ be a separable irreducible polynomial with $a_5 \neq 0$. As before, let $r_1, \ldots, r_6$ be the roots of $m(t)$. If no three roots of $m(t)$ sum to zero, then we are done. Otherwise, we will work with the scaled reciprocal of $m(t)$ (possibly after shifting). If $a_1 \neq 0$, let $m^*(t) := a_0^{-1} t^6 \cdot m(t^{-1})$ be the scaled reciprocal of $m(t)$. If $a_1 = 0$, then note that the degree 1 coefficient of $m(t - \alpha)$ is $2a_5\alpha^4 - a_4\alpha^3 - 2a_2\alpha = \alpha(2a_5\alpha^3 - a_4\alpha^2 - 2a_2)$. The sum of any three roots of $m(t - \alpha)$ is of the form $(r_i + \alpha) + (r_j + \alpha) + (r_\ell + \alpha) = r_i + r_j + r_\ell$ (since we are in characteristic 3). By choosing $\alpha \in k^\times$ not a root of $2a_5 t^3 - a_4 t^2 - 2a_2$,

we may assume that the linear term of $m(t)$ is non-zero, so that the degree 5 coefficient of $m^*(t)$ is non-zero.

The roots of $m^*(t)$ are $r_1^{-1}, \ldots, r_6^{-1}$. The assumption that $r_1 + r_2 + r_3 = 0$ implies that $r_1 = -r_2 - r_3$, so

$$\begin{aligned}(r_1r_2r_3)(r_1^{-1} + r_2^{-1} + r_3^{-1}) &= r_1r_2 + r_1r_3 + r_2r_3 \\ &= -(r_2 + r_3)^2 + r_2r_3 \\ &= -(r_2^2 + r_2r_3 + r_3^2) \\ &= -(r_2 - r_3)^2.\end{aligned}$$

Since $r_2 \neq r_3$ by the separability of $m(t)$, we deduce that $r_1^{-1} + r_2^{-1} + r_3^{-1} \neq 0$. If $r_i^{-1} + r_j^{-1} + r_\ell^{-1} = 0$ for some i, j, ℓ, then consider the reciprocal polynomial of $m(t - \alpha)$. The sum of any three roots is of the form

$$\begin{aligned}\frac{1}{r_i + \alpha} + \frac{1}{r_j + \alpha} + \frac{1}{r_\ell + \alpha} &= \frac{r_ir_j + r_ir_\ell + r_jr_\ell + 2\alpha(r_i + r_j + r_\ell) + 3\alpha}{(r_i + \alpha)(r_j + \alpha)(r_\ell + \alpha)} \\ &= \frac{r_ir_j + r_ir_\ell + r_jr_\ell + 2\alpha(r_i + r_j + r_\ell)}{(r_i + \alpha)(r_j + \alpha)(r_\ell + \alpha)} \\ &= \frac{r_ir_j + r_ir_\ell + r_jr_\ell - \alpha(r_i + r_j + r_\ell)}{(r_i + \alpha)(r_j + \alpha)(r_\ell + \alpha)}.\end{aligned}$$

As we have seen, if $r_i + r_j + r_\ell = 0$, then $r_ir_j + r_ir_\ell + r_jr_\ell \neq 0$, and the converse holds as well. It remains to ensure that $r_ir_j + r_ir_\ell + r_jr_\ell \neq \alpha(r_i + r_j + r_\ell)$ when $r_i + r_j + r_\ell \neq 0$. There are $\binom{6}{3} = 20$ sums of triples to consider. Because $|k| > 24$, we can pick $\alpha \in k^\times - \{\rho : 2a_5\rho^3 + a_4\rho^2 + 2a_2 = 0\}$ such that $r_ir_j + r_ir_\ell + r_jr_\ell \neq \alpha(r_i + r_j + r_\ell)$ for all i, j, ℓ. Let $G(t)$ be the scaled reciprocal of $m(t - \alpha)$. Our choice of α ensures that the degree 5 coefficient of $G(t)$ is non-zero and that no three roots of $G(t)$ sum to zero, as desired. □

5. Necessary criteria for line counts

We now prove that the arithmetic criteria in Theorem 1.3 are necessary for the corresponding line counts to occur. Note that our cardinality restriction on k is not necessary for Theorem 5.1.

Theorem 5.1. *Let k be a field. If there is a smooth cubic surface over k containing n lines defined over k, then k admits a separable field extension of the degrees listed in Table 1.*

Proof. The key is Lemma 2.8. Since X is a smooth cubic surface over k, its base change X_{k^s} to a separable closure k^s of k is a blow-up of $\mathbb{P}^2_{k^s}$. By Propositions 2.2 and 2.3, the k-rational lines on X are in bijection with the k-rational lines on X_{k^s}. We can now use Setup 4.2 to deduce the desired result. If $S \subseteq \{p_1, \ldots, p_6\}$ is a Galois orbit, then S corresponds to a closed point $x \in \mathbb{P}^2_k$ of degree $|S|$. In particular, k must admit an extension of degree $|S|$, namely $k(x)/k$. Moreover, since $k(x)$ splits in k^s, we see that $k(x) \subseteq k^s$ and hence the extension $k(x)/k$ is separable.

To see that Galois orbits of k^s-rational points correspond to closed points, recall that closed points correspond to $\mathrm{Aut}(\overline{k}/k)$-orbits of $\overline{k}$-rational points [Poo17, Proposition 2.4.6] (where $\overline{k}$ is a chosen algebraic closure of k containing k^s). If $\overline{k} = k^s$, then there is nothing more to show. Otherwise, any finite extension of k^s is purely inseparable, so the minimal polynomial over k^s of any element $a \in \overline{k} - k^s$ is of the form $(x-a)^{\mathrm{char}\, k^d}$ for some d. This implies that a is fixed under $\mathrm{Aut}(k^s(a)/k^s)$. Thus $\mathrm{Aut}(L/k^s)$ is trivial for any finite extension L/k^s, so $\mathrm{Aut}(\overline{k}/k^s)$ is trivial as well. □

6. Line counts over specific fields

Using Theorem 1.3, we can understand the set of line counts for smooth cubic surfaces over a given field by looking at the field's Galois theory. For example, since finite fields admit finite (separable) extensions of arbitrary degree, every line count must be realized over finite fields of cardinality at least 22 (reproving Corollary 1.7). Since the only non-trivial finite extensions of real closed fields are of degree 2, we immediately deduce Corollary 1.8.

In order to prove Corollary 1.6, it suffices to show that finitely generated fields and finite transcendental extensions of arbitrary fields each admit separable extensions of arbitrary degrees.

Lemma 6.1. *Let k be a finitely generated field or a finite transcendental extension of another field. Then for each integer $n > 0$, there exists a finite separable extension k' of k with $[k' : k] = n$.*

Proof. If k is a finitely generated field, then let k_0 be its prime field (i.e. $\mathbb{Q}$ if $\mathrm{char}\, k = 0$ and $\mathbb{F}_p$ if $\mathrm{char}\, k = p$). If k/k_0 is finite, then k is a number field in characteristic 0 or of the form $\mathbb{F}_q$ in positive characteristic. In the latter case, take $k' = \mathbb{F}_{q^n}$. In the former case, let $\mathcal{O}$ be the ring of integers of k, and let $u \in \mathcal{O}$ be an irreducible non-zero non-unit (such as the uniformizer of a prime ideal). Then there is no element $s \in \mathcal{O}$ such that $s^2 = u$, so $m(t) = t^n + ut + u$ is irreducible in $k[t]$ by Eisenstein's criterion and Gauss's lemma. It thus suffices to set k' to be the splitting field of $m(t)$.

Now suppose k/k_0 is not finite. Since k is finitely generated, there exist generators $z_1, \ldots, z_m$ such that $k = k_0(z_1, \ldots, z_m)$. Since k/k_0 is not finite, at least one of $z_1, \ldots, z_m$ is transcendental over k_0. By reordering if necessary, we may assume that z_m is transcendental over $k_0(z_1, \ldots, z_{m-1})$. Let $F = k_0(z_1, \ldots, z_{m-1})$. Consider $R = F[z_m]$, which is a UFD (since it is a polynomial ring over a field) whose fraction field is k. The assumption that z_m is transcendental over F implies that R is not a field, so we can pick a non-zero non-unit $g \in R$. Let u be an irreducible factor of g. Then $m(t) = t^n + ut + u$ is irreducible over R by Eisenstein's criterion and hence irreducible over k by Gauss's lemma. Moreover, $m'(t)$ is not identically zero, so $m(t)$ is separable. The splitting field k' of $m(t)$ is thus a degree n separable extension of k.

Finally, if k is a finite transcendental extension of some field k_0, then there exist transcendental elements $z_1, \ldots, z_m$ such that $k = k_0(z_1, \ldots, z_m)$. We may thus repeat the arguments of the previous paragraph to obtain the desired extension k'/k. □

In order to prove Corollary 1.9, it suffices to show that the field $\mathbb{F}_\measuredangle$ of complex constructible numbers is quadratically closed but admits finite separable extensions of any other degree.

Lemma 6.2. *Let $\mathbb{F}_\measuredangle$ be the field of complex constructible numbers. Then $\mathbb{F}_\measuredangle$ admits a finite separable extension of degree $n > 0$ if and only if $n \neq 2$.*

Proof. Since $\operatorname{char} \mathbb{F}_\measuredangle = 0$, any extension of $\mathbb{F}_\measuredangle$ is separable. By definition, $\mathbb{F}_\measuredangle$ is the quadratic closure of $\mathbb{Q}$, so there are no degree 2 extensions of $\mathbb{F}_\measuredangle$. If $\alpha \notin \mathbb{Q}$ is an algebraic number of odd degree n, then $[\mathbb{F}_\measuredangle(\alpha) : \mathbb{F}_\measuredangle] = n$ as well. To see that even degree extensions (besides 2) also occur, it suffices to find an algebraic number $\alpha \notin \mathbb{Q}$ of even degree n such that $\mathbb{Q}(\alpha)/\mathbb{Q}$ does not have any degree 2 subextensions. In other words, it suffices to find α such that $\operatorname{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$ does not have any index 2 subgroups. For this purpose, we can take α such that $\operatorname{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q}) \cong A_n$. Since all alternating groups occur as Galois groups over $\mathbb{Q}$, we are done. □

Appendix A. Subgroups of $W(\mathrm{E}_6)$

The following Magma code, provided to us by Dan Loughran, classifies all possible line counts on a smooth cubic surface over any field by considering all conjugacy classes of subgroups of $W(\mathrm{E}_6)$. This provides a modern proof of Theorem 1.2. This code is a variant of the freely available code accompanying [JL15, BFL19].

```
R_e6 := RootDatum("E6");
Cox_e6 := CoxeterGroup(R_e6);
we6 := StandardActionGroup(Cox_e6);
list:=SubgroupClasses(we6);

number_of_lines := function(G);
temp:=0;
for O in Orbits(G) do
 if #O eq 1 then
  temp:=temp+1;
 end if;
end for;
return temp;
end function;

for rec in list do
G := rec`subgroup;
print Order(G),number_of_lines(G);
end for;
```

Appendix B. Sets of line counts

We now give a list of all possible sets of line counts for smooth cubic surfaces over a field of cardinality at least 22 as determined by Theorem 1.3. There are two configurations for 3 lines, which we distinguish in the following list. The notation $3^{\triangle}$ refers to 3 coplanar and pairwise intersecting lines, and the notation $3^{\equiv}$ refers to 3 skew lines.

For each set of line counts, we also include a list of conjugacy classes of subgroups of $W(\mathrm{E}_6)$ that are uniquely determined (or obstructed) by their corresponding line count (or lack thereof). In the notation of [BFL19, Table 7.1], the conjugacy classes $C_1, C_2, C_6, C_{15}, C_{16}$, and C_{18} correspond uniquely to the line counts 27, 7, 9, 15, 2, and 5, respectively. In the "Conjugacy classes" column, we list which of these conjugacy classes are guaranteed to exist over k due to the existence of the corresponding line counts. If one of these classes is not listed under "Conjugacy classes", then it does not occur over k. An affirmative answer to Question 1.11 would allow us to add or obstruct the conjugacy class of $3^{\triangle}$ in Table 2. The remaining conjugacy classes do not correspond one-to-one with their respective line counts, so our methods do not provide any information about which of these classes exist over k (beyond the obstructions discussed in Section 1.2).

The second column ("Missing extensions") gives the set(s) of degree(s) of separable extensions that k should not have in order to obtain the given set of line counts. If an integer $2 \leq n \leq 6$ is not listed in the set of missing extensions, then it is assumed that k admits a separable extension of degree n. For example, the set of line counts $\{0, 9, 27\}$ occurs when k does not admit separable extensions of degrees 2, 4, 5, 6 but does admit a separable extension of degree 3. This same set of line counts also occurs when k does not admit separable extensions of degrees 2, 4, 5 but does admit separable extensions of degrees 3 and 6. The parenthetical 6 in $2, 4, 5, (6)$ under "Missing extensions" for the set of counts $0, 9, 27$ refers to the fact that this same set of counts occurs regardless of whether k admits a separable degree 6 extension or not.

References

[BFL19] Barinder Banwait, Francesc Fité, and Daniel Loughran. Del Pezzo surfaces over finite fields and their Frobenius traces. *Math. Proc. Cambridge Philos. Soc.*, 167(1):35–60, 2019.

[BHK18] Anton Betten, James W. P. Hirschfeld, and Fatma Karaoglu. Classification of cubic surfaces with twenty-seven lines over the finite field of order thirteen. *Eur. J. Math.*, 4(1):37–50, 2018.

[BK19] Anton Betten and Fatma Karaoglu. Cubic surfaces over small finite fields. *Des. Codes Cryptogr.*, 87(4):931–953, 2019.

[Cay49] Arthur Cayley. On the triple tangent planes of surfaces of the third order. *Cambridge and Dublin Math. J.*, (4):118–138, 1849.

[Coo88] Kevin R. Coombes. Every rational surface is separably split. *Comment. Math. Helv.*, 63(2):305–311, 1988.

[Das20] Ronno Das. Arithmetic statistics on cubic surfaces. *Res. Math. Sci.*, 7(3):Paper No. 23, 12, 2020.

[DG67] Jean Dieudonné and Alexander Grothendieck. Éléments de géométrie algébrique. *Inst. Hautes Études Sci. Publ. Math.*, 4, 8, 11, 17, 20, 24, 28, 32, 1961–1967.

[Dic15] L. E. Dickson. Projective classification of cubic surfaces modulo 2. *Ann. of Math. (2)*, 16(1-4):139–157, 1914/15.

[Dol16] Paolo Dolce. Fields of definition and Belyi type theorems for curves and surfaces. *New York J. Math.*, 22:823–851, 2016.

[EJ15] Andreas-Stephan Elsenhans and Jörg Jahnel. Moduli spaces and the inverse Galois problem for cubic surfaces. *Trans. Amer. Math. Soc.*, 367(11):7837–7861, 2015.

[Har79] Joe Harris. Galois groups of enumerative problems. *Duke Math. J.*, 46(4):685–724, 12 1979.

[Hir67a] J. W. P. Hirschfeld. Classical configurations over finite fields. I. The double- six and the cubic surface with 27 lines. *Rend. Mat. e Appl. (5)*, 26:115–152, 1967.

[Hir67b] J. W. P. Hirschfeld. Classical configurations over finite fields. II. Grace's extension of the double-six. *Rend. Mat. e Appl. (5)*, 26:349–374, 1967.

[HM98] Kie H. Ham and Gary L. Mullen. Distribution of irreducible polynomials of small degrees over finite fields. *Math. Comp.*, 67(221):337–341, 1998.

[HRC12] Rubén A. Hidalgo and Sebastián Reyes-Carocca. Weil's Galois descent theorem from a computational point of view, 2012.

[JL15] Jörg Jahnel and Daniel Loughran. The Hasse principle for lines on del Pezzo surfaces. *Int. Math. Res. Not. IMRN*, (23):12877–12919, 2015.

[Jor57] Camille Jordan. *Traité des substitutions et des équations algébriques*. Librairie Scientifique et Technique A. Blanchard, Paris, 1957. Nouveau tirage.

[Kol97] János Kollár. Real algebraic surfaces. arXiv:alg-geom/9712003, 1997.

[LT19] Daniel Loughran and Andrey Trepalin. Inverse Galois problem for del Pezzo surfaces over finite fields, 2019.

[McK21] Stephen McKean. Rational lines on smooth cubic surfaces. arXiv:2101.08217v2, 2021.

[MMKR22] Rida Ait El Manssour, Yassine El Maazouz, Enis Kaya, and Kemal Rose. Lines on p-adic and real cubic surfaces. arXiv:2202.03489, 2022.

[MMZ21] Stephen McKean, Daniel Minahan, and Tianyi Zhang. All lines on a smooth cubic surface in terms of three skew lines. *New York J. Math.*, 27:1305–1327, 2021.

[Pan09] René Pannekoek. On the parameterization over $\mathbb{Q}$ of cubic surfaces. Master's thesis, Rijksuniversiteit Groningen, May 2009.

[Poo17] Bjorn Poonen. *Rational points on varieties*, volume 186 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2017.

[PSS20] Marta Panizzut, Emre Sertöz, and Bernd Sturmfels. An octonomial model for cubic surfaces. *Matematiche (Catania)*, 75(2):517–536, 2020.

[PV04] Bjorn Poonen and José Felipe Voloch. Random Diophantine equations. In *Arithmetic of higher-dimensional algebraic varieties (Palo Alto, CA, 2002)*, volume 226 of *Progr. Math.*, pages 175–184. Birkhäuser Boston, Boston, MA, 2004. With appendices by Jean-Louis Colliot-Thélène and Nicholas M. Katz.

[Sch58] Ludwig Schläfli. An attempt to determine the twenty-seven lines upon a surface of the third order, and to divide such surfaces into species in reference to the reality of the lines upon the surface. *Quart. J. Pure Appl. Math.*, (2):110–120, 1858.

[Seg49] Beniamino Segre. Le rette delle superficie cubiche nei corpi commutativi. *Boll. Un. Mat. Ital. (3)*, 4:223–228, 1949.

[Sha13] Igor R. Shafarevich. *Basic algebraic geometry. 1*. Springer, Heidelberg, third edition, 2013. Varieties in projective space.

[Sta18] The Stacks Project Authors. *Stacks Project*. `https://stacks.math.columbia.edu`, 2018.

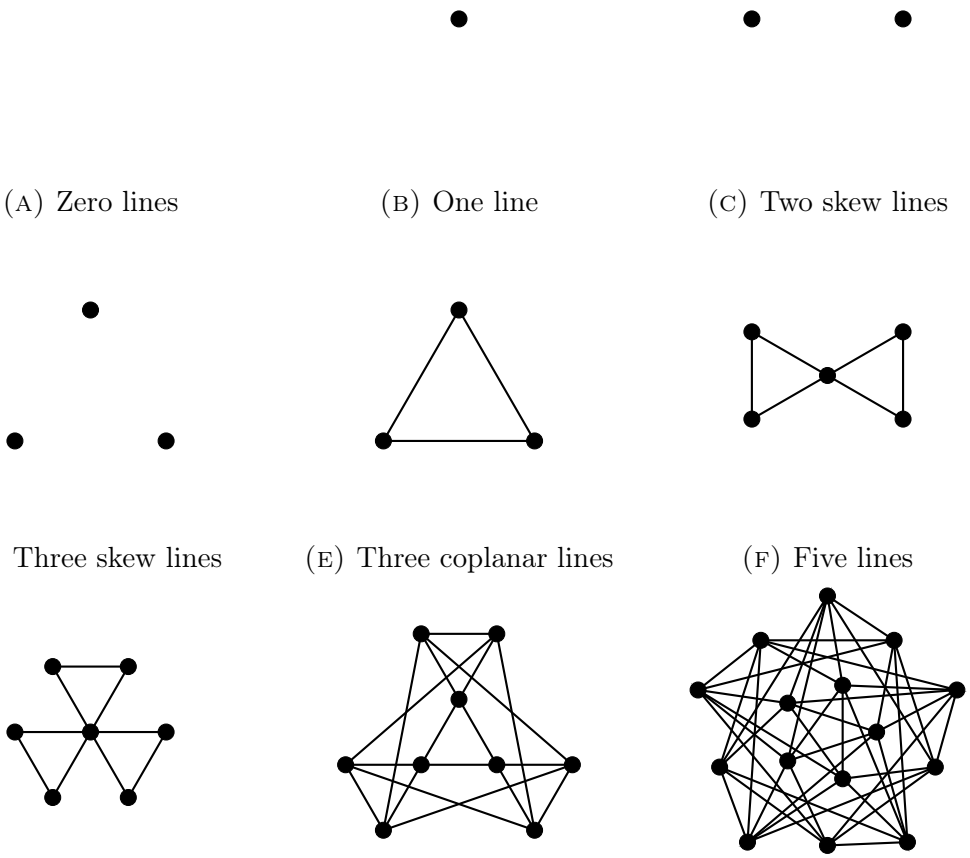
[Tod32] J. A. Todd. Polytopes associated with the general cubic surface. *J. London Math. Soc.*, 7(3):200–205, 1932.

[Wan97] Daqing Wan. Generators and irreducible polynomials over finite fields. *Math. Comp.*, 66(219):1195–1212, 1997.

Department of Mathematics, Harvard University

Email address: `smckean@math.harvard.edu`

URL: `shmckean.github.io`



(A) Zero lines (B) One line (C) Two skew lines

(D) Three skew lines (E) Three coplanar lines (F) Five lines

(G) Seven lines (H) Nine lines (I) Fifteen lines

FIGURE 3. Intersection graphs

TABLE 2. Sets of line counts

Set of counts	Missing extensions	Conjugacy classes
27	$2,3,4,5,6$	C_1
$0,27$	$2,3,4,5$	C_1
$2,27$	$2,3,4,6$	C_1, C_{15}
$5,27$	$2,3,5,6$	C_1, C_{18}
$0,2,27$	$2,3,4$	C_1, C_{15}
$0,5,27$	$2,3,5$	C_1, C_{18}
$0,9,27$	$2,4,5,(6)$	C_1, C_6
$2,5,27$	$2,3,6$	C_1, C_{15}, C_{18}
$0,2,5,27$	$2,3$	C_1, C_{15}, C_{18}
$0,2,9,27$	$2,4,(6)$	C_1, C_6, C_{15}
$0,5,9,27$	$2,5,(6)$	C_1, C_6, C_{18}
$3^{\triangle},7,15,27$	$3,4,5,6$	C_1, C_2, C_{16}
$0,2,5,9,27$	$2,(6)$	C_1, C_6, C_{15}, C_{18}
$0,3^{\triangle},7,15,27$	$3,4,5$	C_1, C_2, C_{16}
$2,3^{\triangle},7,15,27$	$3,4,6$	C_1, C_2, C_{15}, C_{16}
$0,2,3^{\triangle},7,15,27$	$3,4$	C_1, C_2, C_{15}, C_{16}
$1,3^{\triangle},5,7,15,27$	$3,5,6$	C_1, C_2, C_{16}, C_{18}
$0,1,3^{\triangle},5,7,15,27$	$3,5$	C_1, C_2, C_{16}, C_{18}
$0,3^{\triangle},3^{\equiv},7,9,15,27$	$4,5,(6)$	C_1, C_2, C_6, C_{16}
$1,2,3^{\triangle},5,7,15,27$	$3,6$	$C_1, C_2, C_{15}, C_{16}, C_{18}$
$0,1,2,3^{\triangle},5,7,15,27$	3	$C_1, C_2, C_{15}, C_{16}, C_{18}$
$0,2,3^{\triangle},3^{\equiv},7,9,15,27$	$4,(6)$	$C_1, C_2, C_6, C_{15}, C_{16}$
$0,1,3^{\triangle},3^{\equiv},5,7,9,15,27$	$5,(6)$	$C_1, C_2, C_6, C_{16}, C_{18}$
$0,1,2,3^{\triangle},3^{\equiv},5,7,9,15,27$	(6)	$C_1, C_2, C_6, C_{15}, C_{16}, C_{18}$