RATIONAL LINES ON SMOOTH CUBIC SURFACES

STEPHEN MCKEAN

Abstract. This is a largely expository account about lines on smooth cubic surfaces over non-algebraically closed fields. 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. We recall Segre's proof and give an alternate proof of this result. We then show that each of these possible line counts is realized by some smooth cubic surface when the base field is a finitely generated field of characteristic 0, a finite transcendental extension of a characteristic 0 field, or a finite field of characteristic 2 and order at least 4.

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]. Following this theme, 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 $\mathbb{Q}$.*

In an earlier version of this article, we gave what we thought was the first proof of Theorem 1.1. We were later informed by Hirschfeld (via Serre) about [Seg49]. Both Segre's original proof and our proof consist of two parts:

(i) For each $n \in \{0, 1, 2, 3, 5, 7, 9, 15, 27\}$, showing that there is a smooth cubic surface over $\mathbb{Q}$ that contains exactly n lines, and

(ii) For each $n \notin \{0, 1, 2, 3, 5, 7, 9, 15, 27\}$, showing that a smooth cubic surface over $\mathbb{Q}$ cannot contain exactly n lines.

For step (i), we investigate various blow-ups of $\mathbb{P}^2_{\overline{\mathbb{Q}}}$ in Section 3. Segre's proof is essentially Example 3.1 of this paper. We fill out the details of this proof in Lemma 3.2.

We give step (ii) in Sections 4 and 5, culminating in Lemmas 4.17 and 5.10. We do this by studying the intersection graphs of smooth cubic surfaces over $\mathbb{C}$, over $\mathbb{R}$, and over $\mathbb{Q}$. In a few cases, we use ideas of Pannekoek [Pan09] (who builds on the work of Swinnerton-Dyer [SD69]) to study Galois-invariant collections of lines. In addition, we make frequent use of equations for lines on smooth cubic surfaces that we derived in

2020 *Mathematics Subject Classification.* 14N15, 14G25.

joint work with Minahan and Zhang [MMZ20]. We use the aforementioned equations for lines on cubic surfaces to write down some explicit examples in Section 5. Appendix A contains relevant code for these computations.

Segre's step (ii) is both more concise and more general than our approach, so we provide the details and correct a minor error in Section 6. This section culminates in the following theorem of Segre.

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*.*

Remark 1.3. Segre's proof of Theorem 1.2 is geometric. Independently, Serre and Loughran pointed out a quick, modern approach to this theorem – one simply needs to consider all conjugacy classes of subgroups of $W(E_6)$. We include Loughran's Magma implementation of this computation in Appendix C. The work of Elsenhans and Jahnel on the inverse Galois problem for cubic surfaces (see e.g. [EJ15]) gives an alternate proof of Theorem 1.1.

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 $\mathbb{C}$ have 27 lines [Cay49].
- Smooth cubic surfaces over $\mathbb{R}$ have 3, 7, 15, or 27 lines, and each of these counts occurs [Sch58].
- Smooth cubic surfaces over $\mathbb{F}_2$ have 0, 1, 2, 3, 5, 9, or 15 lines, and each of these counts occurs [Dic15].
- Smooth cubic surfaces over $\mathbb{Q}$ have 0, 1, 2, 3, 5, 7, 9, 15, or 27 lines, and each of these counts occurs [Seg49].
- Smooth cubic surfaces over $\mathbb{F}_q$ have 0, 1, 2, 3, 5, 7, 9, 15, or 27 lines when q is odd, and each of these counts occurs [Ros57].
- Smooth cubic surfaces over $\mathbb{F}_{2^d}$ have 0, 1, 2, 3, 5, 7, 9, 15, or 27 lines when $d > 1$, and each of these counts occurs [LT19].

We add to this list by classifying all possible line counts for smooth cubic surfaces over finitely generated fields of characteristic 0 and transcendental extensions of characteristic 0 fields in Section 7. We also give an alternate proof of Loughran and Trepalin's classification of line counts over $\mathbb{F}_{2^d}$.

Theorem 1.4. *Let k be a finitely generated field of characteristic 0 or a finite transcendental extension of a field of characteristic 0. 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, Theorem 1.4 in this generality is new to the literature.

Theorem 1.5. *[LT19] Let $d > 1$ be an integer. There is a smooth cubic surface over $\mathbb{F}_{2^d}$ containing n lines defined over $\mathbb{F}_{2^d}$ for each $n \in \{0, 1, 2, 3, 5, 7, 9, 15, 27\}$.*

We apply similar techniques to prove Theorem 1.4 and Theorem 1.5 when $d > 2$. We classify all possible line counts for smooth cubic surfaces over $\mathbb{F}_4$ by brute force; the relevant code is provided in Appendix B.

Throughout this article, we will only consider smooth cubic surfaces. We may therefore simply refer to smooth cubic surfaces as *cubic surfaces*. We will also use the terms *rational, real,* or *complex cubic surface* to refer to a cubic surface defined over $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$, respectively. In particular, we do not use the term *rational cubic surface* when discussing cubic surfaces that are birational to $\mathbb{P}^2$. Likewise, we will use the terms *rational, real,* or *complex lines* to refer to lines defined over $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$, respectively. When working over an arbitrary field k, we will use the term *rational lines* to refer to lines defined over k.

When a smooth cubic surface contains three skew lines, we say that the cubic surface contains a *skew triple*. When a rational cubic surface does not contain a skew triple, we obtain a constraint on the total number of lines it can contain. This allows us to treat the case of rational cubic surfaces with no skew triples in Section 4. In joint work with Minahan and Zhang [MMZ20], we give explicit equations for all lines on any complex cubic surface in terms of a skew triple. We use these equations to study rational cubic surfaces with a skew triple in Section 5.

1.1. **Acknowledgements.** We thank Kirsten Wickelgren for her help and support. We also thank Ronno Das, Igor Dolgachev, Viatcheslav Kharlamov, Antonio Lerario, Dan Loughran, Jean-Pierre Serre, and Ravi Vakil for helpful correspondence. We are especially indebted to JWP Hirschfeld and Serre for bringing Segre's result [Seg49] to our attention, as well as to Serre for several enlightening discussions.

2. Preliminaries

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

Definition 2.1. [Dol16, Proposition 1.2] Let k be a field, and let $k \subseteq F \subseteq E$ be a tower of fields. We say that a closed subscheme $X \subseteq \mathbb{P}^n_E$ is *defined over* F or *has field of definition* F if the following equivalent conditions are satisfied.

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

(b) There exists a closed subscheme $Y \subseteq \mathbb{P}^n_F$ such that $X = Y \times_F \operatorname{Spec} E$.

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.*

Proposition 2.2. *Let k'/k be a field extension, X a k-scheme, and $X_{k'} = X \times_k \operatorname{Spec} k'$ the base change of X. Then X is smooth over k if and only if $X_{k'}$ is smooth over k'.*

Proof. See [DG67, IV_4, Proposition (17.3.3) (iii) and Corollaire (17.7.3) (ii)]. $\square$

Given a smooth cubic surface S over $\mathbb{Q}$ and an intermediate field $\mathbb{Q} \subseteq k \subseteq \mathbb{C}$, Proposition 2.2 enables us to base change and consider the smooth cubic surface S_k over k. We remark that given a $\mathbb{Q}$-rational line $L \subset S$, the line $L_k \subset S_k$ remains $\mathbb{Q}$-rational. Moreover, if S_k contains a $\mathbb{Q}$-rational line L_k, then S contains L as well. In particular, we can enumerate $\mathbb{Q}$-rational lines on S by base changing to $\mathbb{C}$ or $\overline{\mathbb{Q}}$ and studying the $\mathbb{Q}$-rationality of lines on $S_{\mathbb{C}}$ or $S_{\overline{\mathbb{Q}}}$.

We can 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 2.3. *Let k be a perfect field, and fix an algebraic closure $\overline{k}$ of k. A geometrically reduced closed subscheme $X \subseteq \mathbb{P}^n_{\overline{k}}$ is defined over k if and only if $\sigma \cdot X = X$ for all $\sigma \in \operatorname{Gal}(\overline{k}/k)$.*

Proof. The group $\operatorname{Gal}(\overline{k}/k)$ acts on the defining ideal $\mathcal{I} \subseteq \overline{k}[x_0, \ldots, x_n]$ 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 $\operatorname{Gal}(\overline{k}/k)$-action and hence so is X.

Now suppose X is fixed under $\operatorname{Gal}(\overline{k}/k)$-action. By Hilbert's Basis Theorem, X is defined by a finite set $\{f_1, \ldots, f_r\}$ of polynomials over some finite extension k' of k. Given $f \in \mathcal{I}$ and $\sigma \in \operatorname{Gal}(k'/k)$, 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 $\{e_1, \ldots, e_m\}$ of k', and let $\operatorname{Tr}_{k'/k} : k'[x_0, \ldots, x_n] \to k[x_0, \ldots, x_n]$ be given by taking the Galois trace of each coefficient of a given polynomial. Then $\{\operatorname{Tr}_{k'/k}(e_i f_j)\}_{i,j}$ generates the ideal $\mathcal{I}$. Moreover, since $\operatorname{Tr}_{k'/k}(e_i f_j)^\sigma = \operatorname{Tr}_{k'/k}(e_i f_j)$ for all $\sigma \in \operatorname{Gal}(k'/k)$, it follows that $\operatorname{Tr}_{k'/k}(e_i f_j) \in k[x_0, \ldots, x_n]$. Thus $\mathcal{I}$ is generated by polynomials over k, as desired. $\square$

A cubic surface S defined over k is fixed by $\operatorname{Gal}(\overline{k}/k)$-action, so Galois action preserves the set of 27 lines on $S_{\overline{k}}$. Moreover, Galois action preserves the incidence relations of the 27 lines:

Proposition 2.4. *Let k be a perfect field with $\overline{k}$ a fixed algebraic closure, S be a smooth cubic surface defined over k, and $\sigma \in \operatorname{Gal}(\overline{k}/k)$. Two lines L and L' in $S_{\overline{k}}$ 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 2.5. *Let k be a perfect field with fixed algebraic closure $\overline{k}$, and let S_k be a smooth cubic surface defined over k. If $L_1, L_2, L_3 \subseteq S_{\overline{k}}$ 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, we have $H_{\overline{k}} \cap S_{\overline{k}} = L_1 \cup L_2 \cup L_3$. The varieties L_1, L_2, H, and S are each fixed by all $\mathrm{Gal}(\overline{k}/k)$-actions since they are defined over k. We now act on the configuration $H_{\overline{k}} \cap S_{\overline{k}}$ by each $\sigma \in \mathrm{Gal}(\overline{k}/k)$. Since H and S are defined over k, we have $\sigma \cdot (H_{\overline{k}} \cap S_{\overline{k}}) = H_{\overline{k}} \cap S_{\overline{k}}$. 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 $\sigma \in \mathrm{Gal}(\overline{k}/k)$, so L_3 is defined over k. □

Corollary 2.6. *If a smooth cubic surface S over a perfect field k contains two lines L_1, L_2 that intersect each other, then S contains a third 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, $S_{\overline{k}} \cap H_{\overline{k}}$ consists of L_1, L_2, and a third line L_3. Since L_1 and L_2 are defined over k, Proposition 2.5 implies that L_3 is also defined over k, so S contains L_3. □

Remark 2.7. Propositions 2.3, 2.4, 2.5, and Corollary 2.6 assume that the base field k is perfect so that $\overline{k}/k$ is a separable extension. However, since smooth cubic surfaces are separably split [Coo88], we also apply these results to smooth cubic surfaces even if k is not perfect by working with the separable closure k_s/k rather than $\overline{k}/k$.

3. Blow-ups

Every smooth cubic surface over $\mathbb{C}$ is the blow-up of $\mathbb{P}^2_{\mathbb{C}}$ at six general points. On the other hand, not every smooth cubic surface over $\mathbb{R}$ is the blow-up of $\mathbb{P}^2_{\mathbb{C}}$ at six general points. There are five isotopy classes of smooth cubic surfaces over $\mathbb{R}$:

(i) Real smooth cubic surfaces that contain 27 real lines. These are all a blow-up of $\mathbb{P}^2_{\mathbb{C}}$ at six real points.

(ii) Real smooth cubic surfaces that contain 15 real lines. These are all a blow-up of $\mathbb{P}^2_{\mathbb{C}}$ at four real points and a complex conjugate pair.

(iii) Real smooth cubic surfaces that contain 7 real lines. These are all a blow-up of $\mathbb{P}^2_{\mathbb{C}}$ at two real points and two complex conjugate pairs.

(iv) Real smooth cubic surfaces that contain 3 real lines that are birational to $\mathbb{P}^2_{\mathbb{C}}(\mathbb{R})$. These are all a blow-up of $\mathbb{P}^2_{\mathbb{C}}$ at three pairs of complex conjugate points.

(v) Real smooth cubic surfaces that contain 3 real lines that are not birational to $\mathbb{P}^2_{\mathbb{C}}(\mathbb{R})$.

See e.g. [Seg42, PBT08] for more details. We note that although some real cubic surfaces do not arise as a blow-up of $\mathbb{P}^2_{\mathbb{C}}$, every possible count and configuration of real lines on a cubic surface is realized by a real cubic surface that is the blow-up of $\mathbb{P}^2_{\mathbb{C}}$.

As in the real case, not every smooth cubic surface over $\mathbb{Q}$ is the blow-up of $\mathbb{P}^2_{\overline{\mathbb{Q}}}$ at six general points (see e.g. [KSC04]). However, studying cubic surfaces over $\mathbb{Q}$ that do arise as the blow-up of $\mathbb{P}^2_{\overline{\mathbb{Q}}}$ give us a wealth of examples of rational lines on smooth cubic surfaces. In fact, it will turn out that every possible count and configuration of rational lines on a smooth cubic surface is realized by a rational cubic surface that is the blow-up of $\mathbb{P}^2_{\overline{\mathbb{Q}}}$. We will describe the examples here, and the remainder of this article will obstruct any other cases from occurring.

Let $\{p_1, \ldots, p_6\} \subset \mathbb{P}^2_{\mathbb{C}}$ be a collection of six points that do not lie on a conic, and such that no three lie on a line. Then the blow-up of $\mathbb{P}^2_{\mathbb{C}}$ at $\{p_1, \ldots, p_6\}$ is a smooth cubic surface defined over $\mathbb{C}$. By the Lefschetz principle, we may also conclude that the blow-up of $\mathbb{P}^2_{\overline{\mathbb{Q}}}$ at such a collection of six points is a smooth cubic surface defined over $\overline{\mathbb{Q}}$. We denote the blow-up of $\mathbb{P}^2_{\overline{\mathbb{Q}}}$ at $\{p_1, \ldots, p_6\}$ by $S(p_1, \ldots, p_6)$. The 27 lines on $S(p_1, \ldots, p_6)$ are obtained as follows:

(i) E_i is the exceptional divisor corresponding to p_i;

(ii) C_i is the strict transform of the conic passing through $\{p_1, \ldots, p_6\} - \{p_i\}$;

(iii) L_{ij} is the strict transform of the line passing through p_i and p_j.

The cubic surface $S(p_1, \ldots, p_6)$ is defined over $\mathbb{Q}$ if and only if it is invariant under $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-action. In particular, $S(p_1, \ldots, p_6)$ is defined over $\mathbb{Q}$ if and only if $\{p_1, \ldots, p_6\}$ is invariant under $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-action. Likewise, a line $L \subset S(p_1, \ldots, p_6)$ is defined over $\mathbb{Q}$ if and only if it is invariant under $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-action. In particular:

(i) E_i is defined over $\mathbb{Q}$ if and only if p_i is defined over $\mathbb{Q}$;

(ii) C_i is defined over $\mathbb{Q}$ if and only if $\{p_1, \ldots, p_6\} - \{p_i\}$ is invariant under $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-action;

(iii) L_{ij} is defined over $\mathbb{Q}$ if and only if $\{p_i, p_j\}$ is invariant under $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-action.

Example 3.1. We may now construct various examples by partitioning $\{p_1, \ldots, p_6\}$ into Galois-invariant subsets. In each of these cases, the entire set $\{p_1, \ldots, p_6\}$ is Galois-invariant, so that $S(p_1, \ldots, p_6)$ is defined over $\mathbb{Q}$.

(1) If $p_1, \ldots, p_6$ are all defined over $\mathbb{Q}$, then all 27 lines on $S(p_1, \ldots, p_6)$ are rational. This also forces all 27 lines on $S(p_1, \ldots, p_6)$ to be real.

(2) If $p_1, \ldots, p_4$ are defined over $\mathbb{Q}$ and p_5, p_6 are Galois conjugates, then precisely the lines L_{56} and E_i, C_j, L_{ij} for $1 \leq i, j \leq 4$ are defined over $\mathbb{Q}$. Thus $S(p_1, \ldots, p_6)$ contains 15 rational lines. Moreover, $\{p_1, \ldots, p_6\}$ can contain zero or one complex conjugate pair, so $S(p_1, \ldots, p_6)$ contains 15 or 27 real lines.

(3) If p_1, p_2, p_3 are defined over $\mathbb{Q}$ and p_4, p_5, p_6 are Galois conjugates, then precisely the lines E_i, C_j, L_{ij} for $1 \leq i, j \leq 3$ are defined over $\mathbb{Q}$. Thus $S(p_1, \ldots, p_6)$ contains 9 rational lines. Moreover, $\{p_1, \ldots, p_6\}$ can contain zero or one complex conjugate pair, so $S(p_1, \ldots, p_6)$ contains 15 or 27 real lines.

(4) If p_1, p_2 are defined over $\mathbb{Q}$, and if p_3, p_4 and p_5, p_6 are two pairs of Galois conjugates, then precisely the lines $E_1, E_2, C_1, C_2, L_{12}, L_{34}$, and L_{56} are defined over $\mathbb{Q}$. Thus $S(p_1, \ldots, p_6)$ contains 7 rational lines. Moreover, $\{p_1, \ldots, p_6\}$ can contain zero, one, or two complex conjugate pairs, so $S(p_1, \ldots, p_6)$ contains 7, 15, or 27 real lines.

(5) If p_1, p_2 are defined over $\mathbb{Q}$ and $p_3, \ldots, p_6$ are Galois conjugates, then precisely the lines E_1, E_2, C_1, C_2, and L_{12} are defined over $\mathbb{Q}$. Thus $S(p_1, \ldots, p_6)$ contains 5 rational lines. Moreover, $\{p_1, \ldots, p_6\}$ can contain zero, one, or two complex conjugate pairs, so $S(p_1, \ldots, p_6)$ contains 7, 15, or 27 real lines.

(6) If p_1 is defined over $\mathbb{Q}$, p_2, p_3, p_4 are Galois conjugates, and p_5, p_6 are Galois conjugates, then precisely the lines E_1, C_1, and L_{56} are defined over $\mathbb{Q}$. Thus $S(p_1, \ldots, p_6)$ contains 3 rational lines, and these lines are skew. Moreover, $\{p_1, \ldots, p_6\}$ can contain zero, one, or two complex conjugate pairs, so $S(p_1, \ldots, p_6)$ contains 7, 15, or 27 real lines.

(7) If p_i, p_j is a Galois conjugate pair for $(i, j) = (1, 2)$, $(3, 4)$, and $(5, 6)$, then precisely the lines L_{12}, L_{34}, and L_{56} are defined over $\mathbb{Q}$. Thus $S(p_1, \ldots, p_6)$ contains 3 rational lines, and these lines are not skew. Moreover, $\{p_1, \ldots, p_6\}$ can contain zero, one, two, or three complex conjugate pairs, so $S(p_1, \ldots, p_6)$ contains 3, 7, 15, or 27 real lines.

(8) If p_1 is defined over $\mathbb{Q}$ and $p_2, \ldots, p_6$ are Galois conjugates, then precisely the lines E_1 and C_1 are defined over $\mathbb{Q}$. Thus $S(p_1, \ldots, p_6)$ contains 2 rational lines, and these lines are skew. Moreover, $\{p_1, \ldots, p_6\}$ can contain zero, one, or two complex conjugate pairs, so $S(p_1, \ldots, p_6)$ contains 7, 15, or 27 real lines.

(9) If $p_1, \ldots, p_4$ are Galois conjugates and p_5, p_6 are Galois conjugates, then precisely the line L_{56} is defined over $\mathbb{Q}$. Thus $S(p_1, \ldots, p_6)$ contains 1 rational line. Moreover, $\{p_1, \ldots, p_6\}$ can contain zero, one, two, or three complex conjugate pairs, so $S(p_1, \ldots, p_6)$ contains 3, 7, 15, or 27 real lines.

(10) If p_1, p_2, p_3 are Galois conjugates and p_4, p_5, p_6 are Galois conjugates, then $S(p_1, \ldots, p_6)$ contains no rational lines. Moreover, $\{p_1, \ldots, p_6\}$ can contain zero, one, or two complex conjugate pairs, so $S(p_1, \ldots, p_6)$ contains 7, 15, or 27 real lines.

(11) If $p_1, \ldots, p_6$ are Galois conjugates, then $S(p_1, \ldots, p_6)$ contains no rational lines. Moreover, $\{p_1, \ldots, p_6\}$ can contain zero, one, two, or three complex conjugate pairs, so $S(p_1, \ldots, p_6)$ contains 3, 7, 15, or 27 real lines.

Example 3.1 allows us to prove the following lemma.

Lemma 3.2. *Let n be 0, 1, 2, 3, 5, 7, 9, 15, or 27. Then there is a smooth cubic surface over $\mathbb{Q}$ that contains exactly n rational lines.*

Proof. It suffices to show that every scenario in Example 3.1 occurs for some set of six points in $\mathbb{P}^2_{\overline{\mathbb{Q}}}$, where the six points do not lie a conic and no three of the points lie on a line. We describe an approach (suggested to us by Serre) that allows one to explicitly construct the desired set of six points.

Let $C = \{[1:t:t^3] : t \in \overline{\mathbb{Q}}\}$ be a parameterized cubic in $\mathbb{P}^2_{\overline{\mathbb{Q}}}$. 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 $[1:t_i:t_i^3]$ lie on a line for $i = 1,2,3$ if and only if $t_1+t_2+t_3 = 0$. Likewise, six distinct points $[1:t_i:t_i^3]$ lie on the conic $\mathbb{V}(ax^2+bxy+cy^2+dxz+eyz+fz^2)$ 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 conic for $i = 1,\ldots,6$ if and only if $t_1+\ldots+t_6 = 0$.

Next, note that $[1:s:s^3]$ and $[1:t:t^3]$ are $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-conjugate if and only if s and t are $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-conjugate. In order to construct a set of six general points $\{p_1,\ldots,p_6\}$ with the desired Galois conjugacies, it thus suffices to write down a degree six polynomial $G(t) \in \mathbb{Q}[t]$ satisfying the following properties.

(i) All roots of $G(t)$ are distinct.

(ii) The degree 5 term of $G(t)$ is non-zero.

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

(iv) If $\{p_1,\ldots,p_6\}$ has a minimal Galois-invariant subset of order n, then $G(t)$ has a degree n factor that is irreducible over $\mathbb{Q}$.

Such a polynomial exists for each scenario in Example 3.1. To be thorough, we give an example for each scenario.

(1) $G(t) = t(t+1)(t+2)(t+3)(t+4)(t+5) = t^6+15t^5+85t^4+225t^3+274t^2+120t$.

(2) $G(t) = (t+1)(t+2)(t+3)(t+4)(t^2+1) = t^6+10t^5+36t^4+60t^3+59t^2+50t+24$.

(3) $G(t) = (t+1)(t+2)(t+3)(t^3+t^2+1) = t^6+7t^5+17t^4+18t^3+12t^2+11t+6$.

(4) $G(t) = (t+1)(t+2)(t^2+1)(t^2+2) = t^6+3t^5+5t^4+9t^3+8t^2+6t+4$.

(5) $G(t) = (t+1)(t+2)(t^4+1) = t^6+3t^5+2t^4+t^2+3t+2$.

(6) $G(t) = (t+1)(t^2+1)(t^3+t^2+1) = t^6+2t^5+2t^4+3t^3+2t^2+t+1$.

(7) $G(t) = (t^2+1)(t^2+2)(t^2+t+1) = t^6+t^5+4t^4+3t^3+5t^2+2t+2$.

(8) $G(t) = t(t^5+t^4+t^2+1) = t^6+t^5+t^3+t$.

(9) $G(t) = (t^2+t+1)(t^4+1) = t^6+t^5+t^4+t^2+t+1$.

(10) $G(t) = (t^3+t^2+1)(t^3+2t^2+1) = t^6+3t^5+2t^4+2t^3+3t^2+1$.

(11) $G(t) = t^6+t^5+1$.

We will use this method to construct examples of lines on smooth cubic surfaces over other fields in Section 7. ☐

4. Rational cubic surfaces with no skew triples

In general, a smooth cubic surface over $\mathbb{Q}$ need not contain a skew triple. For example, such a cubic surface might contain no rational lines at all.

Example 4.1. Consider the Fermat cubic $S^a = \mathbb{V}(x_0^3 + ax_1^3 + ax_2^3 + ax_3^3)$, where $a \in \mathbb{Q}$ is not a cube. All 27 lines on $S^a_{\mathbb{C}}$ are of the form $\mathbb{V}(x_0 + cx_i, x_j + \zeta x_k)$, where c is a cube root of a, ζ is a third root of unity, and $i, j, k \in \{1, 2, 3\}$ are pairwise distinct. Since a is not a cube in $\mathbb{Q}$, it follows that $c \notin \mathbb{Q}$ and hence these lines are not defined over $\mathbb{Q}$. We remark that 3 of these lines are defined over $\mathbb{R}$. Compare to Example 3.1 (11).

If a smooth cubic surface S over $\mathbb{Q}$ does not contain a skew triple but does contain a rational line, then we can apply Bézout's theorem to constrain the number of lines that S contains. To do so, we first recall a particular graph associated to a smooth cubic surface and its lines.

Definition 4.2. Let S be a smooth cubic surface over a field k. The *intersection graph* $G(S)$ of S is the graph whose vertices are given by the lines contained in S and whose edges correspond to intersections of lines on S.

Next, we recall a proposition from [MMZ20].

Proposition 4.3. *[MMZ20, Proposition 9.2] Let G be a graph with at least seven vertices such that for any triple of vertices $v_1, v_2, , v_3$, at least two of v_1, v_2, v_3 are connected by an edge. Then G contains two distinct 3-cycles that share an edge.*

Remark 4.4. If a smooth cubic surface S does not contain a skew triple, then the graph $G(S)$ must satisfy the property that for any triple of vertices v_1, v_2, v_3, at least two of v_1, v_2, v_3 are connected by an edge. We say that a graph with this property *has no disjoint triples.*

Corollary 4.5. *If a smooth cubic surface S does not contain a skew triple, then S contains at most six lines.*

Proof. By Bézout's theorem, any plane contains at most three lines contained in S, so the line graph $G(S)$ may not contain any distinct 3-cycles that share an edge. By the contrapositive of Proposition 4.3, it follows that $G(S)$ contains at most six vertices and hence S contains at most six lines. ☐

We can consider all possible configurations of lines on a rational cubic surface S with no skew triples by studying the intersection graph $G(S)$. In particular, if S contains exactly n lines, then $G(S)$ must be a graph of order n with no disjoint triples. Moreover, $G(S)$ may not contain any disjoint 3-cycles that share an edge. By Corollary 2.6, any edge in $G(S)$ must be contained in a 3-cycle. We call any order n graph satisfying these conditions a *permissible* graph. By considering all finite simple graphs of order $1 \leq n \leq 6$, we can classify all permissible graphs of order at most six. It turns out that for each $1 \leq n \leq 6$, there is exactly one permissible graph of order n. For $n = 1$ and $n = 2$, the permissible graph of order n consists of n vertices and no edges. The permissible graphs of order $3 \leq n \leq 6$ are illustrated in Figure 1.

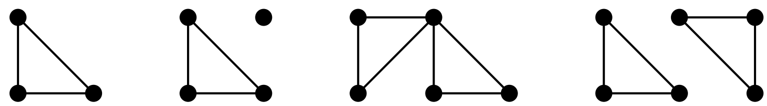

FIGURE 1. Permissible graphs of order $3 \leq n \leq 6$.

Given a rational cubic surface S, we will sometimes compare its intersection graph $G(S)$ with the intersection graph $G(S_{\mathbb{R}})$ of the corresponding real cubic surface. Using the topological classification of real smooth cubic surfaces (due to Schläfli, Klein, and Zeuthen [Sch58, Kle73, Zeu74] and summarized by Segre [Seg42]) we can completely classify the intersection graphs of real cubic surfaces.

Proposition 4.6. *If two smooth cubic surfaces are projectively equivalent, then they have the same intersection graph.*

Proof. Let k be a field, and suppose $S = \mathbb{V}(f), S' = \mathbb{V}(f')$ are smooth cubic surfaces over k that are projectively equivalent. Then there exists $\varphi \in \mathrm{PGL}_3(k)$ such that $S' = \varphi S$, or in other words $f' = f \circ \varphi^{-1}$. Note that a line L is contained in S if and only if $f|_L \equiv 0$. Moreover, φL is also a line, and $f \circ \varphi^{-1}|_{\varphi L} \equiv 0$, so S' contains the line φL. The same line of reasoning shows that if L' is a line in S', then $\varphi^{-1} L'$ is a line in S. We thus see that φ induces a bijection on the lines in S and S', which induces a bijection on the vertices of $G(S)$ and $G(S')$.

It remains to show that two distinct lines $L_1, L_2 \subset S$ intersect if and only if $\varphi L_1, \varphi L_2 \subset S'$ intersect. If $L_1 \cap L_2 = \{p\}$, then both φL_1 and φL_2 contain the point $\{\varphi(p)\}$ and therefore must intersect. Likewise, if $\varphi L_1 \cap \varphi L_2 = \{q\}$, then both L_1 and L_2 contain the point $\{\varphi^{-1}(q)\}$. $\square$

Proposition 4.7. *If two real smooth cubic surfaces in $\mathbb{P}^3_{\mathbb{R}}$ are topologically equivalent, then they are projectively equivalent.*

Proof. By the work of Klein [Kle73], the following equivalence relations for real smooth cubic surfaces in $\mathbb{P}^3_{\mathbb{R}}$ all coincide.

(a) Topological equivalence. Two real smooth cubic surfaces are said to be *topologically equivalent* if there is a homeomorphism between their real points.

(b) Isotopy. Here, the ambient space is $\mathbb{P}^3_{\mathbb{R}}$.

(c) Rigid isotopy. Two real smooth cubic surfaces are said to be *rigidly isotopic* if there exists an isotopy from one to the other that preserves singularity types.

(d) Rough projective equivalence. Two real smooth cubic surfaces are said to be *rough projectively equivalent* if they are projectively equivalent and rigidly isotopic.

For a discussion of this result in modern language, see [DK00, Section 3.5.1]. □

Corollary 4.8. *Any two real smooth cubic surfaces with the same number of lines have the same intersection graph.*

Proof. Segre shows that for $n = 7, 15$, or 27, there is one topological equivalence class of real smooth cubic surfaces containing n lines [Seg42]. These equivalence classes are also projective equivalence classes by Proposition 4.7, so Proposition 4.6 implies that each equivalence class of real smooth cubic surfaces has a fixed intersection graph. There are two topological equivalence classes of real smooth cubic surfaces containing three lines, but [Seg42, III, §31, (iv) and (v)] implies that any cubic surface in either of these equivalence classes have intersection graph K_3, the complete graph of order 3. □

Alternate proof. Corollary 4.8 also follows from [MMZ20, Theorem 9.4] and [Seg42, III, §31, (iv) and (v)]. The latter reference shows that all real smooth cubic surfaces with exactly three lines have the same intersection graph. The former reference shows that for real smooth cubic surfaces containing at least seven lines, the number of lines is determined by the (non)-reality of the roots of a cubic polynomial and a quadratic polynomial. Moreover, these roots determine which lines the real cubic surface contains, and the intersection properties of these lines depend only on the number of lines within the cubic surface. □

Yet another proof. [Seg42, III, §31, (iv) and (v)] shows that all real smooth cubic surfaces with exactly three lines have the same intersection graph. All other real smooth cubic surfaces are the blow-up of $\mathbb{P}^2$ at a set of six general points $\{p_1, \ldots, p_6\} \subset \mathbb{P}^2$ that is invariant under $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$-action. The lines on the resulting cubic surface are as follows.

(i) E_i is the exceptional divisor corresponding to the point p_i. This line is defined over $\mathbb{R}$ if and only if p_i is a real point.

(ii) C_i is the strict transform of the conic through the points $\{p_1, \ldots, p_6\} - \{p_i\}$. This line is defined over $\mathbb{R}$ if and only if $\{p_1, \ldots, p_6\} - \{p_i\}$ is invariant under $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$-action.

(iii) L_{ij} is the strict transform of the line through p_i and p_j. This line is defined over $\mathbb{R}$ if and only if $\{p_i, p_j\}$ is invariant under $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$-action.

If $\{p_1, \ldots, p_6\}$ consists of six real points, four real points and a pair of complex conjugate points, or two real points and two pairs of complex conjugate points, then the resulting real smooth cubic surface has 27, 15, or 7 real lines, respectively. The intersection graph does not depend on the choice of labeling of $\{p_1, \ldots, p_6\}$, which proves the desired result. □

As previously mentioned, the intersection graph of a real smooth cubic surface with 3 lines is the complete graph K_3. The intersection graph of a smooth cubic surface with

27 lines is the complement of the Schläfli graph and has been the subject of extensive study. By considering Examples 5.13 and 5.14, Corollary 4.8 allows us to describe the intersection graphs of real smooth cubic surfaces containing 7 or 15 lines.

Proposition 4.9. *Any real smooth cubic surface S with seven lines has intersection graph F_3, the friendship graph of order 7 (see Figure 2).*

Proof. It in fact suffices to notice that S contains a line that meets the other six lines. Thus $G(S)$ contains S_6, the star graph of order 7. By generalizing the proof of Corollary 2.6 for real smooth cubic surfaces, we note that every edge in the intersection graph must be contained in a 3-cycle. Thus $G(S)$ contains F_3. As previously remarked, any 3-cycle in the intersection graph of a smooth cubic surface corresponds to three coplanar lines. By Bézout's theorem, any hyperplane section of S may contain at most three lines, so the intersection graph $G(S)$ may not contain any distinct 3-cycles that share an edge. There are hence no additional edges in $G(S)$, so $G(S)$ must be equal to F_3. $\square$

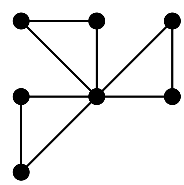

FIGURE 2. Intersection graph of a real smooth cubic surface with 7 lines.

4.1. **Rational cubic surfaces with one line.** Assume that S is a rational cubic surface containing exactly one line L. Suppose $S_{\mathbb{R}}$ contains exactly 3 lines. Then $S_{\mathbb{R}}$ would contain L (considered as a line over $\mathbb{R}$) as well as two real lines L_1, L_2 that are not defined over $\mathbb{Q}$. By modifying the coefficients of the cubic surface in Example 4.1, we can describe some cubic surfaces that match this description.

Example 4.10. Consider the Fermat cubic $S^a = \mathbb{V}(a^4x_0^3 + ax_1^3 + x_2^3 + x_3^3)$, where $a \in \mathbb{Q}$ is not a cube. The smooth cubic surface $S^a_{\mathbb{C}}$ contains the 9 lines $\mathbb{V}(bx_0 + x_1, x_2 + \zeta x_3)$, where b is a cube root of a^3 and ζ is a third root of unity. Precisely one of these 9 lines is defined over $\mathbb{Q}$, namely when $b = a$ and $\zeta = 1$. The other 18 lines on $S^a_{\mathbb{C}}$ are of the form $\mathbb{V}(bx_0 + x_i, cx_1 + x_j)$, where b is a cube root of a^4, c is a cube root of a, and $i \neq j$. Since a is not a cube in $\mathbb{Q}$, it follows that $c \notin \mathbb{Q}$ and hence these lines are not defined over $\mathbb{Q}$. Thus S^a contains exactly one rational line. Compare to Example 3.1 (9).

Remark 4.11. In [MMZ20], the authors note that $S_{\mathbb{R}}$ contains three skew lines if and only if $S_{\mathbb{R}}$ contains 7, 15, or 27 real lines. By [Seg42, III, §31, (iv) and (v)], $S_{\mathbb{R}}$ does not contain three skew lines if and only if $S_{\mathbb{R}}$ contains exactly 3 lines, all of which are pairwise-intersecting.

4.2. **Rational cubic surfaces with two lines.** Assume that S is a rational cubic surface containing exactly two lines L_1, L_2. By Corollary 2.6, we know that L_1 and L_2 do not intersect. If $S_{\mathbb{R}}$ were to contain only three lines, then the rational lines L_1, L_2 in S would necessarily intersect by Remark 4.11. We can thus conclude that $S_{\mathbb{R}}$ contains at least seven lines. By Example 3.1 (8), there is a smooth cubic surface over $\mathbb{Q}$ that contains two rational lines.

Example 4.12. [Pan09, Section 4.3.3] Pannekoek shows that the smooth cubic surface $\mathbb{V}(f)$ contains two rational lines, where

$$\begin{aligned} f = {} & 175959x_0^2x_2 + 518643x_0x_1x_2 - 131841x_0x_2^2 + 19x_0x_2x_3 \\ & + 27x_0^2x_3 + 400653x_0x_1x_3 + 121068x_0x_3^2 + 52326x_1^2x_2 \\ & + 11799x_1x_2^2 + 383211x_1x_2x_3 + 235467x_1^2x_3 + 108243x_1x_3^2. \end{aligned}$$

4.3. **Rational cubic surfaces with three lines.** Let $S_{\mathbb{R}}$ be a real cubic surface that contains exactly three lines. As previously remarked, Segre shows that the lines in $S_{\mathbb{R}}$ are all pairwise-intersecting. To construct a rational cubic surface with exactly three lines, we simply need to construct a real cubic surface containing exactly three lines, all of which are rational.

Example 4.13. Consider the Fermat cubic $S = \mathbb{V}(x_0^3+x_1^3+x_2^3+x_3^3)$. As with the Fermat cubics in Examples 4.1 and 4.10, $S_{\mathbb{R}}$ contains three real lines. Over $\mathbb{R}$, the only lines contained in this surface are $\mathbb{V}(x_0+x_1, x_2+x_3)$, $\mathbb{V}(x_0+x_2, x_1+x_3)$, and $\mathbb{V}(x_0+x_3, x_1+x_2)$. Since all of these lines are defined over $\mathbb{Q}$, it follows that S contains exactly three lines over $\mathbb{Q}$. Compare to Example 3.1 (7).

4.4. **Rational cubic surfaces with four lines.** We will show that there are no rational cubic surfaces containing exactly four lines with no skew triple.

Proposition 4.14. *Let S be a rational smooth cubic surface containing three pairwise-intersecting lines. Every other rational line on S must intersect one of these three lines.*

Proof. Without loss of generality, we may assume that the three pairwise-intersecting lines are E_1, C_6, and L_{16}. Over $\mathbb{C}$, the lines C_i and L_{1i} for $2 \le i \le 6$ intersect E_1, the lines E_j and L_{j6} for $1 \le j \le 5$ intersect C_6, and the lines E_6, C_1, and L_{mn} for $m > 1$ and $n < 6$ intersect L_{16}. This accounts for all 27 lines on $S_{\mathbb{C}}$. If S contains E_1, C_6, L_{16}, and another line L, then $L_{\mathbb{C}}$ intersects $L'_{\mathbb{C}}$, where L' is one of E_1, C_6, or L_{16}. Since L and L' are defined over $\mathbb{Q}$, they must also intersect over $\mathbb{Q}$. □

Corollary 4.15. *A rational smooth cubic surface with no skew triple cannot contain exactly four lines.*

Proof. The permissible graph of order 4 (see Figure 1) implies that any rational cubic surface with no skew triple and exactly four lines must contain three pairwise-intersecting lines. Proposition 4.14 implies that the intersection graph of such a cubic surface must be connected. Since the permissible graph of order 4 is not connected, there is no rational smooth cubic surface with no skew triple that contains exactly four lines. ☐

4.5. **Rational cubic surfaces with five lines.** Assume that S is a rational cubic surface containing exactly five lines with no skew triple. It follows that $S_{\mathbb{R}}$ contains at least seven lines, so $S_{\mathbb{R}}$ contains a skew triple. By Example 3.1 (5), there is a smooth cubic surface over $\mathbb{Q}$ that contains five rational lines.

4.6. **Rational cubic surfaces with six lines.** As in the case of rational cubic surfaces with no skew triples and four lines, Proposition 4.14 implies that there are no rational smooth cubic surface with no skew triples and exactly six lines.

Corollary 4.16. *A rational smooth cubic surface with no skew triple cannot contain exactly six lines.*

Proof. The permissible graph of order 6 (see Figure 1) implies that any rational cubic surface with no skew triple and exactly six lines must contain three pairwise-intersecting lines. Proposition 4.14 implies that the intersection graph of such a cubic surface must be connected. Since the permissible graph of order 6 is not connected, there is no rational smooth cubic surface with no skew triple that contains exactly six lines. ☐

In summary of this section, we have proved the following lemma.

Lemma 4.17. *A smooth cubic surface over $\mathbb{Q}$ with no skew triple must contain 0, 1, 2, 3, or 5 rational lines.*

5. Rational cubic surfaces with a skew triple

If S is a rational smooth cubic surface that contains a skew triple, then we may assume that S contains the lines $E_1 = \mathbb{V}(x_0, x_1)$, $E_2 = \mathbb{V}(x_2, x_3)$, and $E_3 = \mathbb{V}(x_0 - x_2, x_1 - x_3)$ by a projective change of coordinates. In this context, we may apply the results of [MMZ20]. We recall the relevant details here.

Proposition 5.1. *[MMZ20, Proposition 3.1] There is a cubic polynomial $g(t) \in \mathbb{Q}[t]$ with distinct roots t_4, t_5, t_6 such that the lines C_i contained in $S_{\mathbb{C}}$ are defined over $\mathbb{Q}(t_i)$ for $4 \leq i \leq 6$.*

Proof. Since S is defined over $\mathbb{Q}$, we have $S = \mathbb{V}(f)$ for $f \in \mathbb{Q}[x_0, x_1, x_2, x_3]$. This implies that $g(t) \in \mathbb{Q}[t]$. Explicitly, we have the line $C_i = \mathbb{V}(x_0 - t_i x_1, x_2 - t_i x_3)$, so this line is defined over $\mathbb{Q}(t_i)$. ☐

This allows us study the rationality of C_4, C_5, C_6. There are three cases to consider.

(1) If $g(t)$ is irreducible over $\mathbb{Q}$, then t_4, t_5, t_6 are algebraic numbers not contained in $\mathbb{Q}$. In this case, C_4, C_5, C_6 are not rational.

(2) If $g(t)$ has only one rational root, then we may assume without loss of generality that $t_4 \in \mathbb{Q}$ and t_5, t_6 are algebraic numbers not contained in $\mathbb{Q}$. In this case, C_4 is rational and C_5, C_6 are not rational.

(3) If $g(t)$ has at least two rational roots, then all three roots of $g(t)$ are rational and hence C_4, C_5, C_6 are rational.

For $1 \leq i \leq 3$ and $4 \leq j \leq 6$, the lines E_i and C_j intersect. By [MMZ20, Proposition 4.1], $S_{\mathbb{C}}$ also contains the line L_{ij}, and the lines E_i, C_j, L_{ij} are coplanar.

Proposition 5.2. *If C_j is not rational, then L_{ij} is not rational.*

Proof. Since E_i is rational, if L_{ij} were rational, then Proposition 2.5 would imply that C_j is also rational. □

The previous proposition allows us to determine the (non)-rationality of the nine lines L_{ij}. As before, we have the following three cases.

(1) If C_4, C_5, C_6 are not rational, then L_{ij} is not rational for $1 \leq i \leq 3$ and $4 \leq j \leq 6$.

(2) If C_4 is rational and C_5, C_6 are not rational, then L_{i4} is rational and L_{i5}, L_{i6} are not rational for $1 \leq i \leq 3$.

(3) If C_4, C_5, C_6 are rational, then L_{ij} is rational for $1 \leq i \leq 3$ and $4 \leq j \leq 6$.

Proposition 5.3. *[MMZ20, Proposition 5.5] There is a quadratic polynomial $h(s) \in \mathbb{Q}(t_4, t_5)[s]$ with distinct roots s_1, s_2 such that the lines C_3 and L_{12} contained in $S_{\mathbb{C}}$ are defined over $\mathbb{Q}(s_1, t_4)$ and $\mathbb{Q}(s_2, t_4)$, respectively. In particular, we have*

$$\begin{aligned} C_3 &= \mathbb{V}(x_0 + (-s_1c_1 - t_4)x_1, (1 + s_1c_2)x_2 + (s_1c_3 - t_4)x_3), \\ L_{12} &= \mathbb{V}(x_0 + (-s_2c_1 - t_4)x_1, (1 + s_2c_2)x_2 + (s_2c_3 - t_4)x_3), \end{aligned}$$

where $c_1x_1 + c_2x_2 + c_3x_3$ is one of the linear forms defining L_{34}.

This proposition allows us to analyze the rationality of C_3 and L_{12} in terms of the rationality of s_1, s_2, and t_4.

Corollary 5.4. *If t_4 and s_1 (respectively s_2) are rational, then C_3 (respectively L_{12}) is defined over $\mathbb{Q}$.*

Proof. If $t_4, s_i \in \mathbb{Q}$, then $\mathbb{Q}(s_i, t_4) = \mathbb{Q}$. □

Corollary 5.5. *If t_4 is rational and s_1 (respectively s_2) is not rational, then C_3 (respectively L_{12}) is not defined over $\mathbb{Q}$.*

Proof. By a slight modification of [MMZ20, Proposition 5.2], we have that $c_1 \neq 0$. Thus if t_4 is rational and s_i is not rational for $i = 1$ (respectively $i = 2$), then $s_ic_1 + t_4 \in \mathbb{Q}(s_i) \backslash \mathbb{Q}$, so C_3 (respectively L_{12}) is not defined over $\mathbb{Q}$. □

Corollary 5.6. *If t_4 is not rational and s_1 (respectively s_2) is rational, then C_3 (respectively L_{12}) is not defined over $\mathbb{Q}$.*

Proof. If t_4 is not rational, then the cubic polynomial $g(t)$ from Proposition 5.1 is a $\mathbb{Q}$-scalar multiple of the minimal polynomial for t_4 over $\mathbb{Q}$. By [MMZ20, Propositions 3.1 and 4.1], we have $c_1 = at_4^2 + xt_4 + y$ for some $a, x, y \in \mathbb{Q}$ with $a \neq 0$. Thus c_1 is not rational. Moreover, if s_i is rational for $i = 1$ (respectively $i = 2$), then $s_ic_1 + t_4 = (s_ia)t_4^2 + (s_ix + 1)t_4 + s_iy$ is not rational, so C_3 (respectively L_{12}) is not defined over $\mathbb{Q}$. □

It turns out that if one of C_3 and L_{12} is not defined over $\mathbb{Q}$, then the other line is also not defined over $\mathbb{Q}$.

Proposition 5.7. *If C_3 is not defined over $\mathbb{Q}$, then L_{12} is not defined over $\mathbb{Q}$. Likewise, if L_{12} is not defined over $\mathbb{Q}$, then C_3 is not defined over $\mathbb{Q}$.*

Proof. It suffices to prove the statement under the assumption that C_3 is not defined over $\mathbb{Q}$. The other case follows by relabeling s_1 and s_2. Since E_2 is rational and C_3 is not rational, Proposition 2.5 implies that L_{23} is not rational. Since E_3 is rational and L_{23} is not rational, C_2 is not rational. Finally, since E_1 is rational and C_2 is not rational, L_{12} is not rational, as desired. □

When t_4, t_5, t_6 are not rational, our cubic surface has either 3 rational lines or at least 15 real lines.

Lemma 5.8. *If $t_4, t_5, t_6 \notin \mathbb{Q}$, then $S_\mathbb{C}$ has either exactly 3 rational lines or at least 15 real lines.*

Proof. By assumption, the lines E_1, E_2, E_3 are rational, and the lines C_4, C_5, C_6, and L_{ij} for $1 \leq i \leq 3$ and $4 \leq j \leq 6$ are not rational. If C_3 and L_{12} are rational, then Proposition 2.5 implies that C_1, C_2, L_{13}, and L_{23} are rational, and the remaining lines on $S_\mathbb{C}$ are not rational. Thus S contains 9 rational lines. Since all rational lines are also real lines, this implies that $S_\mathbb{R}$ contains at least 15 lines.

If C_3 and L_{12} are not rational, then E_1, E_2, E_3 are rational and C_i, L_{jk} are not rational for $1 \leq i \leq 6$, $1 \leq j \leq 3$ and $4 \leq k \leq 6$, and $(j,k) = (1,2)$, $(1,3)$, or $(2,3)$. The remaining lines are $E_4, E_5, E_6, L_{45}, L_{46}$, and L_{56}. If all of these remaining lines are not rational, then S contains exactly three rational lines. Moreover, these rational lines are skew, so $S_\mathbb{R}$ contains at least 7 lines by Corollary 4.8.

If one of the remaining lines $E_4, E_5, E_6, L_{45}, L_{46}$, and L_{56} is rational, then S contains at least 4 rational lines. Moreover, E_1, E_2, E_3, and any one of the remaining lines are all pairwise skew, so the intersection graph $G(S_\mathbb{Q})$ contains 4 non-adjacent vertices. Since there is no such collection of vertices in the complete graph K_3 or the friendship graph F_3, and since $G(S_\mathbb{Q})$ is a subgraph of $G(S_\mathbb{R})$, it follows that $S_\mathbb{R}$ must contain at least 15 lines. □

We can now consider the following cases.

(a) Both s_1, s_2 are not rational.

(b) One of s_1, s_2 is not rational. Without loss of generality, we may assume in this case that s_1 is not rational and s_2 is rational.

(c) Both s_1, s_2 are rational.

As mentioned by Harris [Har79, p. 719], the remaining ten lines in $S_{\mathbb{C}}$ are residually determined. In particular, L_{ij}, E_i, C_j are coplanar for $i \neq j$, and L_{ij}, L_{mn}, L_{pq} are coplanar for i, j, m, n, p, q all distinct. This allows us to solve for the lines C_1, C_2, E_4, E_5, E_6, L_{13}, L_{23}, L_{45}, L_{46}, and L_{56}.

Remark 5.9. Combining with cases (1), (2), and (3) and applying Proposition 2.5 to the relevant triples of coplanar lines, we can now list all possible line counts for rational cubic surfaces containing a skew triple.

(1) If t_4, t_5, t_6 are not rational, then C_4, C_5, C_6, and L_{ij} are not rational for $1 \leq i \leq 3$ and $4 \leq j \leq 6$.

  (a) If s_2 is not rational, then L_{12} may or may not be rational. If L_{12} is rational, then C_3 is also rational by Proposition 5.7. It follows that C_1, C_2, L_{13}, L_{23} are rational, and $E_4, E_5, E_6, L_{45}, L_{46}, L_{56}$ are not rational. Thus S contains nine lines. While this line count depends on the assumption that L_{12} is rational, Example 3.1 (3) proves that there is in fact a rational cubic surface that contains exactly nine lines.

  (b) If L_{12} is not rational (for example, if s_2 is rational), then C_3 is not rational by Proposition 5.7. Thus C_1, C_2, L_{13}, L_{23} are not rational. The remaining lines to consider are $E_4, E_5, E_6, L_{45}, L_{46}$, and L_{56}. If at least one of these lines is rational, then S contains four skew rational lines. We will show that this forces C_3 or L_{12} to be rational, which is a contradiction.

  Let L be a rational line from the set of $E_4, E_5, E_6, L_{45}, L_{46}$, and L_{56}. Recall that $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-action preserves the incidence properties of the lines on $S_{\mathbb{C}}$. In particular, the set of lines meeting E_1 and E_2 but not E_3 and L is invariant under $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-action, since E_1, E_2, E_3, L are fixed under $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-action as rational lines. If L is E_4, E_5, or E_6, then L_{12} is the unique line meeting E_1 and E_2 but not E_3 or L, so L_{12} is fixed by $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-action. In particular, L_{12} is rational, which contradicts the fact that s_2 is rational. On the other hand, if L is L_{45}, L_{46}, or L_{56}, then C_3 is the unique line meeting E_1 and E_2 but not E_3 or L. In this case, we conclude that C_3 is rational, again obtaining a contradiction. We thus conclude that if s_2 is rational, then S contains exactly three rational lines, and these lines are skew. Compare to Example 3.1 (6).

(2) If t_4 is rational and t_5, t_6 are not rational, then C_4 and L_{i4} are rational and C_5, C_6, L_{i5}, L_{i6} are not rational for $1 \leq i \leq 3$.

(a) If s_1, s_2 are not rational, then C_3, L_{12} are not rational. Thus the remaining lines are not rational. In this case, $S_{\mathbb{C}}$ contains seven rational lines, so the rational cubic surface S contains seven lines. Compare to Example 3.1 (4).

(b) If s_1 is not rational and s_2 is rational, then C_3 is not rational and L_{12} is rational. By Proposition 5.7, this scenario cannot occur.

(c) If s_1, s_2 are rational, then C_3, L_{12} are rational. Thus $C_1, C_2, E_4, L_{13}, L_{23}, L_{56}$ are rational and E_5, E_6, L_{45}, L_{46} are not rational. In this case, $S_{\mathbb{C}}$ contains fifteen rational lines, so the rational cubic surface S contains fifteen lines. Compare to Example 3.1 (2).

(3) If t_4, t_5, t_6 are rational, then C_j and L_{ij} are rational for $1 \leq i \leq 3$ and $4 \leq j \leq 6$.

(a) If s_1, s_2 are not rational, then C_3, L_{12} are not rational. Thus the remaining lines are not rational. In this case, $S_{\mathbb{C}}$ contains fifteen rational lines, so the rational cubic surface S contains fifteen lines. Compare to Example 3.1 (2).

(b) If s_1 is not rational and s_2 is rational, then C_3 is not rational and L_{12} is rational. By Proposition 5.7, this scenario cannot occur.

(c) If s_1, s_2 are rational, then C_3, L_{12} are rational. Thus the remaining lines are rational, so all twenty-seven lines on $S_{\mathbb{C}}$ are rational. In this case, the rational cubic surface S contains twenty-seven lines. Compare to Example 3.1 (1).

In summary, we have proved the following lemma.

Lemma 5.10. *A smooth cubic surface over $\mathbb{Q}$ that contains a skew triple must contain 3, 7, 9, 15, or 27 lines.*

We have also proved Theorem 1.1.

Proof of Theorem 1.1. By Lemma 4.17 and Lemma 5.10, a smooth cubic surface over $\mathbb{Q}$ can only have 0, 1, 2, 3, 5, 7, 9, 15, or 27 rational lines. By Lemma 3.2, each of these line counts is realized by a smooth cubic surface over $\mathbb{Q}$. □

Remark 5.11. There are ten distinct intersection graphs for rational cubic surfaces that occur as blow-ups of $\mathbb{P}^2$ (see Example 3.1). Our work in Sections 4 and 5 shows that no other intersection graphs occur. For example, any rational cubic surface that is not a blow-up of $\mathbb{P}^2$ has the intersection graph of a rational cubic surface that is a blow-up of $\mathbb{P}^2$.

5.1. **Examples.** We conclude this section by giving examples of smooth cubic surfaces over $\mathbb{Q}$ that satisfy the various situations considered in Remark 5.9. We remark that the formulas for $h(s)$ depend on our choice of labels t_4, t_5, t_6 of the roots of $g(t)$. However, the overall count of lines on our cubic surface with a prescribed field of definition does not depend on this choice.

Example 5.12. Let $f = x_0^2x_2 - x_0x_2^2 + 2x_0^2x_3 - 2x_0x_1x_2 + x_1^2x_2 - x_0x_1x_3 + 2x_1^2x_3 - 2x_1x_3^2$. The rational cubic surface $S = \mathbb{V}(f)$ has $g(t) = t^3+2$, so $t_4, t_5, t_6 \notin \mathbb{Q}$. Setting $t_4 = -\sqrt[3]{2}$, $t_5 = \frac{\sqrt[3]{2}(1-i\sqrt{3})}{2}$, and $t_6 = \frac{\sqrt[3]{2}(1+i\sqrt{3})}{2}$, the roots of $h(s)$ are

$$\frac{8i\sqrt{3}(4\sqrt[3]{2}+1) \pm \sqrt{1152i\sqrt{3} - 1152} - 96\sqrt[3]{2} - 24}{32i\sqrt{3}(\sqrt[3]{4} + 2\sqrt[3]{2} + 1) - 96\sqrt[3]{4} - 192\sqrt[3]{2} - 96}.$$

We have $c_1 = \sqrt[3]{4} + 2\sqrt[3]{2} + 1$, and hence $s_ic_1 + t_4 \notin \mathbb{R}$, where s_i is a root of $h(s)$. By [MMZ20, Proposition 5.5], the lines C_3 and L_{12} of $S_{\mathbb{C}}$ are not real. Since L_{12} is not rational, Remark 5.9 (1b) implies that S contains exactly three rational lines. These are $E_1 = \mathbb{V}(x_0, x_1)$, $E_2 = \mathbb{V}(x_2, x_3)$, and $E_3 = \mathbb{V}(x_0 - x_2, x_1 - x_3)$.

We note that $s_2 \notin \mathbb{Q}$, which was the initial assumption in Remark 5.9 (1a). This shows that, in contrast to [MMZ20, Theorem 9.4] for real cubic surfaces, the (non)-rationality of the roots of $g(t)$ and $h(s)$ do not always determine the number of lines on a rational cubic surface with a skew triple.

Example 5.13. Let $f = x_0^2x_2 - x_0x_2^2 + 2x_0^2x_3 - 2x_0x_1x_2 + x_1^2x_2 - x_0x_1x_3 + x_1^2x_3 - x_1x_3^2$. The rational cubic surface $S = \mathbb{V}(f)$ has $g(t) = t^3+1$. Setting $t_4 = -1, t_5 = \frac{1+i\sqrt{3}}{2}, t_6 = \frac{1-i\sqrt{3}}{2}$, we have $h(s) = -\frac{i\sqrt{3}+3}{2}(16s^2 - 11s + 2)$. Thus S contains seven lines by Remark 5.9 (2a).

Example 5.14. Let $f = x_0^2x_2 - x_0z_2^2 + x_0^2x_3 - x_0x_1x_2 + x_1^2x_2 - 2x_0x_1x_3 + x_1x_2^2 - x_0x_2x_3 - x_0x_3^2 + 2x_1x_2x_3$. The rational cubic surface $S = \mathbb{V}(f)$ has $g(t) = t^3 - t$. Setting $t_4 = 0, t_5 = 1, t_6 = -1$, we have $h(s) = s^2 - 2s + 3$. Thus S contains fifteen lines by Remark 5.9 (3a).

Example 5.15. Let $f = x_0^2x_2 - x_0x_2^2 + x_0^2x_3 - x_0x_1x_2 + \frac{17}{39}x_1x_2^2 - \frac{17}{39}x_0x_2x_3 + 2x_1^2x_2 - 3x_0x_1x_3 + \frac{12}{13}x_0x_3^2 + \frac{1}{13}x_1x_2x_3$. The rational cubic surface $S = \mathbb{V}(f)$ has $g(t) = t^3 - t$. Setting $t_4 = 0, t_5 = 1, t_6 = -1$, we have $h(s) = \frac{1}{72}(28s^2 + 108s - 81)$. Thus S contains twenty-seven lines by Remark 5.9 (3c).

6. Segre's proof

We now explain the details of Segre's proof of Theorem 1.2 [Seg49]. The general philosophy is to pass to the algebraic closure, work geometrically, and keep track of the field of definition of each line. First, we modify Proposition 4.14 to hold for arbitrary fields.

Lemma 6.1. *Let X be a smooth cubic surface over a field k. Given three pairwise-intersecting lines L_1, L_2, L_3 on X, any other line on X must meet one of L_1, L_2, L_3.*

Proof. As in the case of Proposition 4.14, we may assume that L_1, L_2, L_3 are given by a particular triple of coplanar lines. We then consider the intersection graph of $X_{\overline{k}}$, which will be the same as the intersection graph of a smooth cubic surface over $\mathbb{C}$. $\square$

Proof of Theorem 1.2. Let X be a smooth cubic surface over a field k. Segre's proof consists of the following three geometric facts about lines on smooth cubic surfaces.

(i) If X contains two k-rational lines L_1 and L_2 that intersect each other, then X contains a third k-rational line that intersects L_1 and L_2. If k is perfect, this is proved in Corollary 2.6. Remark 2.7 implies that this approach still works if k is not perfect.

(ii) Given four pairwise skew lines $L_1, \ldots, L_4 \subset \mathbb{P}^3_k$, there are two (not necessarily k-rational) lines $L, L' \subset \mathbb{P}^3_k$ meeting $L_1, \ldots, L_4$. If X contains four pairwise skew k-rational lines $L_1, \ldots, L_4$, then the lines L, L' meeting $L_1, \ldots, L_4$ also belong to X. Moreover, there is a unique double six of X such that L and L' belong to different sextuples. The 15 lines of X not belonging to this double six are all defined over k, and the lines of the double six are either all defined over k or all not defined over k.

To see this, we first explain why L, L' are contained in X. Any three skew lines, in particular L_1, L_2, L_3, lie in a ruling of a quadric surface $Q \subset \mathbb{P}^3_k$. By Bézout's theorem, the intersection $X \cap Q$ consists of six lines (three of which are L_1, L_2, L_3) over $\overline{k}$. The other three lines, say M_1, M_2, M_3, in $X \cap Q$ belong to the ruling of Q not containing L_1, L_2, L_3. This implies that each L_i meets each M_j for $1 \leq i, j \leq 3$. Let N_{ij} be the line in X meeting L_i and M_j for $1 \leq i, j \leq 3$. If L_4 meets two of the six lines in $X \cap Q$, then these two lines must be L and L'. Suppose that L_4 meets at most one of the six lines in $X \cap Q$. Over $\overline{k}$, every line on X meets 10 other lines, so there are at least 9 lines meeting L_4 that are not contained in Q. By Lemma 6.1, each M_{ij} must meet L_4. But there are several other coplanar triples on X that do not contain N_{ij} for $1 \leq i, j \leq 3$, so L_4 meets more than 10 lines. By contradiction, we conclude that L_4 must meet two of M_1, M_2, M_3.

By the above discussion, we can solve for L and L' by intersecting L_4 with Q. Since $L_1, \ldots, L_4$ are defined over k, the quadric Q is also defined over k (as are its two rulings). Solving for $L_4 \cap Q$ consists of solving a quadratic equation over k. The lines L, L' can then be recovered from the points $L_4 \cap Q$ and the appropriate ruling on Q. Since the solutions to a quadratic equation in any characteristic have the same field of definition, the lines L, L' will have the same field of definition.

Suppose L, L' are defined over k. By (i), each pair L, L_i and L', L_i determines another line (denoted P_i and P'_i, respectively) on X defined over k, so X contains at least 14 lines over k. By Lemma 6.1, every line on X over $\overline{k}$ meets one of the Λ_i. It follows that each of P_2, P_3, P_4 must meet one of L', L_1, P'_1. Each of these intersections gives us another k-rational line by (i), so X contains at least 17 lines over k. We repeat this process for each coplanar triple of lines on X, which forces the remaining 10 lines on X to be defined over k.

Now suppose that L, L' are not defined over k. Over $\overline{k}$, we may label the lines on X by $E_i, C_j, L_{ij} = L_{ji}$ for $1 \leq i, j \leq 6$. These lines satisfy the following intersection properties.

- E_i meets C_j if and only if $i \neq j$.
- E_i does not meet E_j, and C_i does not meet C_j, for $i \neq j$.

- E_i and C_i meet L_{mn} if and only if $i = m$ or $i = n$.
- L_{ij} meets L_{mn} if and only if $\{i, j\} = \{m, n\}$.

Without loss of generality, we may assume that $L_i = E_i$ for $1 \leq i \leq 3$, $L_4 = E_6$, $L = C_4$, and $C_5 = L'$. If L_{12} is defined over k, then repeatedly applying (i) shows that X contains exactly 15 lines defined over k, with the 12 non-rational lines on X forming a double six. If k is perfect, then we may modify Remark 5.9 (1b) to show that L_{12} must be defined over k. Remark 2.7 implies that this approach still works if k is not perfect.

(iii) A *Steiner system* is a collection of nine lines $\{L_i^j\}_{1\leq i,j\leq 3}$ on a smooth cubic surface such that 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. If X contains two triples L_1, L_2, L_3 and L_1', L_2', L_3' of k-rational coplanar lines, then X also contains three k-rational lines L_1'', L_2'', L_3'' such that $\{L_i, L_i', L_i''\}_{1\leq i\leq 3}$ form a Steiner system.

Lemma 6.1 implies that each L_i must intersect one of L_1', L_2', L_3'. Moreover, L_i and L_j may not intersect the same line from L_1', L_2', L_3', or else X would contain a quadruple of coplanar lines, contradicting Bézout's theorem. By relabeling, we may assume that L_i intersects L_i' for $i = 1, 2, 3$. Since L_i and L_i' are intersecting k-rational lines, X also contains the residual k-rational line L_i'' meeting L_i and L_i' by (i). The set $\{L_i, L_i', L_i''\}_{1\leq i\leq 3}$ gives the desired Steiner system.

We now use the observations to obstruct various configurations of k-rational lines. A cubic surface X over k may contain 0 lines, 1 line, or 2 skew lines. Given two intersecting lines on X, (i) implies that X in fact contains 3 coplanar lines. We may thus assume that our configuration of lines never contains a pair of intersecting lines that do not belong to a triple of coplanar lines. It follows that if X contains 3 lines, then these lines are either skew or coplanar.

By Lemma 6.1, if X contains 3 coplanar lines, then the intersection graph of X over k is connected. If X contains 4 lines, then these are either skew, or three are coplanar and the fourth intersects one of these lines. In the latter case, (i) forces X to contain a fifth line, and the intersection graph of X is as in Figure 1. If X contains 4 skew lines, then (ii) implies that X contains either 15 or 27 rational lines. If X contains exactly 5 lines, then X may not contain 4 skew lines by (ii). It follows by (i) that X must contain a triple of coplanar lines, so the intersection graph of X must be connected. The only possible intersection graph of this form is given in Figure 1.

If X contains at least 6 lines, then (i) and (ii) again imply that the intersection graph of X is connected and that every line of X belongs to a coplanar triple. Moreover, any line on X must meet a line of each coplanar triple on X. Bézout's theorem prohibits the intersection graph of X from having triangles that share an edge. For $n \in \{7, 9, 15, 27\}$, there is precisely one graph of order n satisfying these criteria. (The case of $n = 9$ is given by (iii), where the lines on X form a Steiner system.) On the other hand, if $6 \leq n \leq 26$ and $n \notin \{7, 9, 15\}$, there are no graphs of order n satisfying these criteria and hence no smooth cubic surfaces over k containing exactly n lines defined over k. $\square$

While this proof works in any characteristic, 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, 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 rational 15 points and 35 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 agree.

Proposition 6.2. *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 $|k| < \infty$, then $L \cong \mathbb{P}^1_k$ contains $|k| + 1 > 3$ points defined over k. If $|k|$ is infinite, then $L \cong \mathbb{P}^1_k$ contains infinitely many k-rational points. In either case, the intersection $L \cap X$ contains more than 3 points. Since $\deg(L) \cdot \deg(X) = 3$, Bézout's theorem implies that L must be contained in X. $\square$

Proposition 6.2 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 $\mathbb{F}_2$.

7. Counting lines over other fields

In Lemma 3.2, we used blow-ups to show that each possible line count is indeed realized by some smooth cubic surface over $\mathbb{Q}$. We will use the same approach to classify line counts for smooth cubic surfaces over other fields.

7.1. **Characteristic 0.**

In characteristic 0, the task at hand is to find irreducible polynomials satisfying the various conditions listed in Lemma 3.2.

Lemma 7.1. *Let k be a finite algebraic extension of $\mathbb{Q}$. There is a smooth cubic surface over k with exactly n lines for each $n \in \{0, 1, 2, 3, 5, 7, 9, 15, 27\}$.*

Proof. As discussed in the proof of Lemma 3.2, it suffices to construct, for each n, a sextic polynomial $G(t)$ satisfying various properties. Since $\mathbb{Q} \subset k$, it suffices to find appropriate replacements for the non-linear factors of the polynomials given in the proof of Lemma 3.2. Let $\mathcal{O}$ be the ring of integers of k, and let $\mathfrak{p} \neq \mathfrak{q} \subset \mathcal{O}$ be distinct non-zero prime ideals. Take $0 \neq p \in \mathfrak{p}$ and $0 \neq q \in \mathfrak{q}$.

- Replace t^2+1 with t^2+p.
- Replace t^2+2 with t^2+q.
- Replace t^2+t+1 with t^2+t+p.
- Replace t^3+t^2+1 with t^3+pt^2+p.
- Replace t^3+2t^2+1 with $t^3+p^2t^2+p$.
- Replace t^4+1 with t^4+p.
- Replace $t^5+t^4+t^2+1$ with t^5+pt^4+p.
- Replace t^6+t^5+1 with t^6+pt^5+p.

By the Eisenstein criterion for $\mathcal{O}$ at $\mathfrak{p}$ (or $\mathfrak{q}$), these polynomials are irreducible over $\mathcal{O}$. By localizing and working over $\mathcal{O}_\mathfrak{p}$ (or $\mathcal{O}_\mathfrak{q}$) and then passing to the fraction field $\mathrm{Frac}(\mathcal{O}_\mathfrak{p}) = \mathrm{Frac}(\mathcal{O}_\mathfrak{q}) = k$, it follows that these polynomials are also irreducible over k. One can check that the resulting sextic polynomials have all distinct roots, no three roots that sum to zero, a non-zero degree 5 term, and irreducible factors of the desired degrees. □

These same ideas work for fields that are finite transcendental extensions of a characteristic 0 field.

Lemma 7.2. *Let k be a field of characteristic 0. Let z be transcendental over k. There is a smooth cubic surface over $k(z)$ with exactly n lines for each $n \in \{0,1,2,3,5,7,9,15,27\}$.*

Proof. Since $\operatorname{char} k = 0$, we have $\mathbb{Q} \subset k(z)$. It therefore suffices to find appropriate replacements for the non-linear factors of the polynomials given in the proof of Lemma 3.2.

- Replace t^2+1 with t^2+z.
- Replace t^2+2 with t^2+z+1.
- Replace t^2+t+1 with t^2+t+z.
- Replace t^3+t^2+1 with t^3+zt^2+z.
- Replace t^3+2t^2+1 with $t^3+z^2t^2+z$.
- Replace t^4+1 with t^4+z.
- Replace $t^5+t^4+t^2+1$ with t^5+zt^4+z.
- Replace t^6+t^5+1 with t^6+zt^5+z.

The roots of the above polynomials are not contained in $k(z)$, so it suffices to check that the degree 4, 5, and 6 polynomials are irreducible. Since (z) is a prime ideal in $k[z]$, Eisenstein's criterion for $k[z]$ and Gauss's lemma imply that that these polynomials are irreducible over $k(z)$. As with Lemma 7.1, one can check that the resulting sextic polynomials satisfy the desired properties. □

Together, Lemmas 7.1 and 7.2 prove Theorem 1.4. Indeed, if a finitely generated field of characteristic zero is not an algebraic extension of $\mathbb{Q}$, then it must be a finite transcendental extension $F(z_1,\ldots,z_n)$ of some field F of characteristic 0. The result follows from Lemma 7.2 by setting $k := F(z_1,\ldots,z_{n-1})$ and $z := z_n$.

7.2. **Characteristic 2.** Since finite fields are perfect, we can still use this blow-up technique to find cubic surfaces with various line counts. Cubic surfaces over $\mathbb{F}_2$ were addressed by Dickson [Dic15], while cubic surfaces over finite fields of odd characteristic were treated by Rosati [Ros57]. We apply the blow-up technique to finite fields of characteristic 2 and order at least 8.

Proposition 7.3. *There is a smooth cubic surface over $\mathbb{F}_8$ with 27 lines.*

Proof. Any set of six elements in $\mathbb{F}_8$ contains a subset of three elements that sum to zero, so we cannot apply the blow-up technique to prove this proposition. However, the smooth cubic surface defined by $f = x_0^2x_3 + x_1^2x_2 + x_0x_3^2 + x_1x_2^2 + x_1x_2x_3$ has 27 lines over $\mathbb{F}_8$ [Bet18]. We remark that any smooth cubic surface with 27 lines must contain a Cremona–Richmond configuration of 15 lines. Over $\mathbb{F}_8$, such configurations contain 105 rational points, so a smooth cubic surface over $\mathbb{F}_8$ with 27 lines must contain more than 105 rational points. This observation can be used to simplify the search for cubic surfaces over $\mathbb{F}_8$ with 27 lines. □

Proposition 7.4. *Let $d \geq 4$. There is a smooth cubic surface over $\mathbb{F}_{2^d}$ with exactly 27 lines.*

Proof. Let a be a primitive element for $\mathbb{F}_{2^d}$ over $\mathbb{F}_2$. If $d \geq 5$, then $1, a, a^2, a^3, a^4$ are linearly independent over $\mathbb{F}_2$, so no subset of these numbers sums to 0. We may thus take $G(t) = t(t-1)(t-a)(t-a^2)(t-a^3)(t-a^4)$ as the desired sextic polynomial.

For $d = 4$, we have that $x^4 + x + 1$ is irreducible over $\mathbb{F}_2$. Letting our primitive element a be a root of $x^4 + x + 1$, no three elements from $\{0, 1, a, a^2, a^2 + a + 1, a^3\}$ sum to 0. Moreover, $0 + 1 + a + a^2 + (a^2 + a + 1) + a^3 = a^3 \neq 0$. We may thus take $G(t) = t(t-1)(t-a)(t-a^2)(t-a^2-a-1)(t-a^3)$ as the desired sextic polynomial. □

For our next step, we need various irreducible polynomials over $\mathbb{F}_{2^d}$ for $d \geq 3$. We give some of these now.

Proposition 7.5. *Let $d \geq 3$. There exist distinct, non-zero elements $b_1, b_2, b_3, b_4 \in \mathbb{F}_{2^d}$ such that $t^2 + t + b_i$ are irreducible over $\mathbb{F}_{2^d}$.*

Proof. First, note that $\phi : \mathbb{F}_{2^d} \to \mathbb{F}_{2^d}$ defined by $\phi(x) = x^2 + x$ is an additive group homomorphism. Moreover, $1 \in \ker\phi$, so ϕ is not surjective. In particular, there exist $2^d - |\operatorname{im}\phi| = 2^d - \frac{2^d}{|\ker\phi|} \geq 2^{d-1}$ elements in $\mathbb{F}_{2^d}$ that are not of the form $x^2 + x$. Let b_1, b_2, b_3, b_4 be four such elements. Then $t^2 + t + b_i$ have no roots in $\mathbb{F}_{2^d}$ and are hence irreducible. We also remark that for $i \neq j \in \{1, 2, 3\}$, the four roots of $t^2 + t + b_i$ and $t^2 + t + b_j$ sum to $1 + 1 = 0$, so no three of these roots sum to 0. □

Proposition 7.6. *Let $d \geq 3$. Let a be a primitive element for $\mathbb{F}_{2^d}$ over $\mathbb{F}_2$. There exist non-zero elements $c_1, c_2 \in \mathbb{F}_{2^d}$ such that $t^3 + t^2 + c_1$ and $t^3 + at^2 + c_2$ are irreducible over $\mathbb{F}_{2^d}$.*

Proof. Let $\psi_y : \mathbb{F}_{2^d} \to \mathbb{F}_{2^d}$ be the map of finite sets defined by $\psi_y(x) = x^3 + yx^2$. While ψ_1 and ψ_a are not group homomorphisms, we have that $\psi_1(0) = \psi_1(1) = 0$ and $\psi_a(0) = \psi_a(a) = 0$. By the pigeonhole principle, there exist $c_1, c_2 \in \mathbb{F}_{2^d}$ such that $c_1 \notin \psi_1(\mathbb{F}_{2^d})$ and $c_2 \notin \psi_a(\mathbb{F}_{2^d})$. Thus $t^3 + t^2 + c_1$ and $t^3 + at^2 + c_2$ have no roots in $\mathbb{F}_{2^d}$, so these polynomials are irreducible over $\mathbb{F}_{2^d}$. □

Proposition 7.7. *Let $d \geq 3$. Let b_i be as in Proposition 7.5. There exists $\gamma \in \mathbb{F}_{2^d}$ such that $t^4 + (b_i + 1)t^2 + b_i t + \gamma b_i^2$ is irreducible over $\mathbb{F}_{2^d}$ for $1 \leq i \leq 4$.*

Proof. Let $\mathrm{Tr} : \mathbb{F}_{2^d} \to \mathbb{F}_2$ be the field trace, which is a group homomorphism. The kernel of Tr has cardinality 2^{d-1}, so we may pick an element $\gamma \in \mathbb{F}_{2^d} \setminus \ker \mathrm{Tr}$. Then $\mathrm{Tr}(\gamma) = 1$.

We now refer to [LW72] to prove the result. The quartic polynomial $t^4+(b_i+1)t^2+b_it+\gamma b_i^2$ yields the cubic polynomial $g(t) = t^3 + (b_i + 1)t + b_i = (t^2 + t + b_i)(t + 1)$, whose only $\mathbb{F}_{2^d}$-rational root is 1. Moreover, $\mathrm{Tr}(\frac{\gamma b_i^2 \cdot 1}{b_i^2}) = \mathrm{Tr}(\gamma) = 1$, so [LW72, Theorem (e)] implies that $t^4 + (b_i + 1)t^2 + b_i t + \gamma b_i^2$ is irreducible over $\mathbb{F}_{2^d}$. We remark that no three roots of this quartic polynomial sum to 0, or else the fourth root would be $0 \in \mathbb{F}_{2^d}$, contradicting the irreducibility of the quartic. □

Proposition 7.8. *Let $d \geq 3$. Let a be a primitive element for $\mathbb{F}_{2^d}$ over $\mathbb{F}_2$. Let γ be as in Proposition 7.7. There exist distinct, non-zero elements $b_5, b_6, b_7, b_8 \in \mathbb{F}_{2^d}$ such that $t^4 + (a^2 + b_j)t^2 + ab_j t + \gamma b_j^2$ are irreducible over $\mathbb{F}_{2^d}$.*

Proof. Modifying the proof of Proposition 7.5, there exist $b_5, b_6, b_7, b_8 \in \mathbb{F}_{2^d}$ such that $t^2 + at + b_j$ is irreducible over $\mathbb{F}_{2^d}$ for $5 \leq j \leq 8$. In the context of [LW72], the quartic polynomial $t^4 + (a^2 + b_j)t^2 + ab_j t + \gamma b_j^2$ yields the cubic polynomial $g(t) = t^3 + (a^2 + b_j)t + ab_j = (t^2 + at + b_j)(t + a)$, whose only $\mathbb{F}_{2^d}$-rational root is a. Moreover, $\mathrm{Tr}(\frac{\gamma b_j^2 \cdot a^2}{(ab_j)^2}) = 1$, so [LW72, Theorem (e)] implies that $t^4 + (a^2 + b_j)t^2 + ab_j t + \gamma b_j^2$ is irreducible over $\mathbb{F}_{2^d}$. As described in the proof of Proposition 7.7, no three roots of $t^4 + (a^2 + b_j)t^2 + ab_j t + \gamma b_j^2$ sum to 0. □

In order to construct suitable quintic and sextic polynomials, we give a brief interlude on counting irreducible polynomials over finite fields.

Lemma 7.9. *Let p be a prime number. Let $n \geq 1$ be a positive integer. If $f(t)$ is a monic irreducible polynomial over $\mathbb{F}_{p^n}$, then $f(t - a)$ is an irreducible polynomial over $\mathbb{F}_{p^n}$ for any $a \in \mathbb{F}_{p^n}$.*

Proof. If $f(t)$ is an irreducible polynomial of degree d over $\mathbb{F}_{p^n}$, then f is the minimal polynomial of some $\alpha \in \mathbb{F}_{p^{dn}}$. By construction, $\alpha + a$ is a root of $f(t - a)$, so it remains to show that $f(t - a)$ is defined and irreducible over $\mathbb{F}_{p^n}$.

The roots of $f(t)$ are $\alpha, \alpha^{p^n}, \ldots, \alpha^{p^{(d-1)n}}$, so $f(t)$ splits over $\mathbb{F}_{p^{dn}}$ as

$$f(t) = (t-\alpha)(t-\alpha^{p^n})\cdots(t-\alpha^{p^{(d-1)n}}).$$

Thus $f(t-a)$ splits over $\mathbb{F}_{p^{dn}}$ as

$$f(t-a) = (t-\alpha-a)(t-\alpha^{p^n}-a)\cdots(t-\alpha^{p^{(d-1)n}}-a).$$

Since $a \in \mathbb{F}_{p^n}$, we have that $a^{p^n} = a$. Setting $f(t-a) =: g(t) = \sum_{i=0}^d g_i t^i$, we have $g(t)^{p^n} = g(t^{p^n})$. In particular, $g_i^{p^n} = g_i$, so $g_i \in \mathbb{F}_{p^n}$ for all i. Thus $f(t-a) \in \mathbb{F}_{p^n}[t]$.

To show that $f(t-a)$ is irreducible over $\mathbb{F}_{p^n}$, it suffices to show that the degree of $\alpha+a$ is at least d. Suppose that the degree of $\alpha+a$ were $e < d$. Then $\alpha + a \in \mathbb{F}_{p^{en}}$, so $(\alpha+a)^{p^{en}} = \alpha + a$. Expanding this out, we have $(\alpha+a)^{p^{en}} = \alpha^{p^{en}} + a^{p^{en}} = \alpha^{p^{en}} + a$, which implies that $\alpha^{p^{en}} = \alpha$. But this means that $\alpha \in \mathbb{F}_{p^{en}}$, which contradicts our assumption that the degree of α is $d > e$. □

Corollary 7.10. *Let p be a prime number. Let $n \geq 1$ be a positive integer. Let d be a positive integer that is coprime to p. Let*

$$N_d(p^n) = \left\{ f(t) = t^d + \sum_{i=0}^{d-1} a_i t^i \in \mathbb{F}_{p^n}[t] : f \text{ is irreducible} \right\},$$

$$N_d(p^n, a) = \left\{ f(t) = t^d + \sum_{i=0}^{d-1} a_i t^i \in N_d(p^n) : a_{d-1} = a \in \mathbb{F}_{p^n} \right\}.$$

Then $|N_d(p^n, a)| = \frac{|N_d(p^n)|}{p^n}$ for all $a \in \mathbb{F}_{p^n}$.

Proof. Let $0 \neq r \in \mathbb{F}_p \subseteq \mathbb{F}_{p^n}$ be the image of $d \mod p$. Given $f(t) = t^d + \sum_{i=0}^{d-1} a_i t^i$ with roots $\alpha, \alpha^{p^n}, \ldots, \alpha^{p^{(d-1)n}}$, Lemma 7.9 implies that $f(t - \frac{a-a_{d-1}}{r})$ is irreducible over $\mathbb{F}_{p^n}$ for all $a \in \mathbb{F}_{p^n}$. The sum of the roots of $f(t)$ is given by $\alpha + \alpha^{p^n} + \ldots + \alpha^{p^{(d-1)n}} = -a_{d-1}$. The sum of the roots of $f(t - \frac{a-a_{d-1}}{r}) = \sum_{i=0}^d c_i t^i$ is given by

$$\begin{aligned} -c_{d-1} &= (\alpha - \tfrac{a-a_{d-1}}{r}) + (\alpha^{p^n} - \tfrac{a-a_{d-1}}{r}) + \ldots + (\alpha^{p^{(d-1)n}} - \tfrac{a-a_{d-1}}{r}) \\ &= -a_{d-1} - d(\tfrac{a-a_{d-1}}{r}) \\ &= -a. \end{aligned}$$

That is, $f(t - \frac{a-a_{d-1}}{r}) \in N_d(p^n, a)$. Over a finite field, two irreducible polynomials are distinct if and only if their sets of roots are disjoint, so $\{f(t - \frac{a-a_{d-1}}{r}) : a \in \mathbb{F}_{p^n}\} = \{f(t-a) : a \in \mathbb{F}_{p^n}\}$ has order p^n for any $f \in N_d(p^n)$. Finally, if $f \in N_d(p^n)$ and $g \in N_d(p^n) \backslash \{f(t-a) : a \in \mathbb{F}_{p^n}\}$, then $\{f(t-a) : a \in \mathbb{F}_{p^n}\} \cap \{g(t-a) : a \in \mathbb{F}_{p^n}\} = \emptyset$. Indeed, otherwise we would have $f(t-a) = g(t-b)$ for some $a, b \in \mathbb{F}_{p^n}$, which would imply that $g(t) = f(t-a+b)$. It follows that for any $a, b \in \mathbb{F}_{p^n}$, we have $|N_d(p^n, a)| = |N_d(p^n, b)|$. Since

$$N_d(p^n) = \bigsqcup_{a \in \mathbb{F}_{p^n}} N_d(p^n, a),$$

we have $|N_d(p^n)| = p^n |N_d(p^n, a)|$ for all $a \in \mathbb{F}_{p^n}$, as desired. □

The value $|N_d(p^n)|$ is the count of irreducible monic polynomials of fixed degree over a finite field, which is classically known. Corollary 7.10 allows us to count such polynomials with a specified second-to-leading term.

Proposition 7.11. *Let $d \geq 1$. There exist $e_1, \dots, e_4 \in \mathbb{F}_{2^d}$ such that $t^5 + t^4 + e_1t^3 + e_2t^2 + e_3t + e_4$ is irreducible over $\mathbb{F}_{2^d}$ with no three roots summing to 0.*

Proof. We first remark that an irreducible polynomial over $\mathbb{F}_{2^d}$ of the form $t^5 + t^4 + e_1t^3 + e_2t^2 + e_3t + e_4$ cannot have three roots that sum to 0 if $e_2 \neq 1$ or if $e_2 = 1$ and $e_1 + e_3 + e_4 \neq 1$. Indeed, if this quintic polynomial were to have three roots that summed to 0, then it would factor as $(t^3+E_1t+E_2)(t^2+t+E_3)$ for some E_1, E_2, E_3 in an extension of $\mathbb{F}_{2^d}$. Comparing coefficients, we find that

$$\begin{aligned} E_2 &= E_1 + e_2, \\ E_3 &= E_1 + e_1, \\ 0 &= E_1^2 + (e_1 + 1)E_1 + e_2 + e_3, \\ 0 &= E_1^2 + (e_1 + e_2)E_1 + e_1e_2 + e_4. \end{aligned}$$

If $e_2 \neq 1$, then summing the last two equations together gives us $E_1 = \frac{e_1e_2+e_2+e_3+e_4}{e_2+1}$, which would imply that $t^5 + t^4 + e_1t^3 + e_2t^2 + e_3t + e_4$ is reducible over $\mathbb{F}_{2^d}$, which contradicts our irreducibility assumption. If $e_2 = 1$, then summing the last two equations together gives us $e_1 + e_3 + e_4 = 1$, which contradicts our assumption that $e_1 + e_3 + e_4 \neq 1$ when $e_2 = 1$.

By Corollary 7.10, there are $\frac{2^{5d}-2^d}{2^d \cdot 5} = \frac{2^{4d}-1}{5}$ irreducible polynomials over $\mathbb{F}_{2^d}$ of the form $t^5+t^4+e_1t^3+e_2t^2+e_3t+e_4$. On the other hand, there are $2^{3d}(2^d-1)$ polynomials of the form $t^5 + t^4 + e_1t^3 + e_2t^2 + e_3t + e_4$ with $e_2 \neq 1$ and $2^{2d}(2^d - 1)$ polynomials of the form $t^5+t^4+e_1t^3+t^2+e_3t+e_4$ with $e_1+e_3+e_4 \neq 1$. Since $2^{3d}(2^d-1)+2^{2d}(2^d-1) > \frac{2^{4d}-1}{5}$ for $d > 0$, we conclude that there must be a polynomial of desired form that is irreducible over $\mathbb{F}_{2^d}$. □

Proposition 7.12. *Let $d \geq 2$. There exist $f_0, f_1 \in \mathbb{F}_{2^d}$ such that $t^6 + t^5 + f_1t^4 + f_0t^3 + f_1t^2 + t + 1$ is irreducible over $\mathbb{F}_{2^d}$.*

Proof. By [Mey90, Theorem 6], it suffices to find $f_0 \in \mathbb{F}_{2^d}^\times$ and $f_1 \in \mathbb{F}_{2^d}$ such that $\mathrm{Tr}(\frac{f_1}{f_0}) = 1$ and $t^3 + t^2 + f_1t + f_0$ is irreducible over $\mathbb{F}_{2^d}$. Let

$$N_3(2^d, 1) = \{(a, b) \in \mathbb{F}_{2^d} \times \mathbb{F}_{2^d}^\times : t^3 + t^2 + at + b \text{ is irreducible over } \mathbb{F}_{2^d}\}.$$

Corollary 7.10 implies that $|N_3(2^d, 1)| = \frac{2^{3d}-2^d}{2^d \cdot 3} = \frac{2^{2d}-1}{3}$. It follows that there exists $f_0 \in \mathbb{F}_{2^d}^\times$ such that $X = \{a \in \mathbb{F}_{2^d} : t^3 + t^2 + at + f_0 \text{ is irreducible}\}$ has order at least $\frac{1}{2^d-1} \cdot \frac{2^{2d}-1}{3} = \frac{2^d+1}{3}$. The set $Y = \{a \in \mathbb{F}_{2^d} : \mathrm{Tr}(\frac{a}{f_0}) = 1\}$ has order 2^{d-1}. Since $2^{d-1} > \frac{2^d+1}{3}$ for $d > 1$, it follows that $X \cap Y \neq \emptyset$. Any choice of $f_1 \in X \cap Y$ gives us f_0, f_1 satisfying the desired properties.

We remark that no three roots of $t^6+t^5+f_1t^4+f_0t^3+f_1t^2+t+1$ sum to 0. Indeed, otherwise this sextic would factor as $(t^3+F_1t+F_2)(t^3+t^2+F_3t+F_4)$ for some $F_1,\ldots,F_4$ in an extension of $\mathbb{F}_{2^d}$. This would imply that

$$\begin{aligned}
F_1 &= f_1+F_3,\\
F_2 &= f_0+f_1+F_3,\\
F_4 &= (f_0+f_1+F_3)^{-1},\\
0 &= f_1F_3^2+(f_0^2+f_1^2+f_0+f_1+1)F_3.
\end{aligned}$$

Thus $F_3=0$ or $F_3=\frac{f_0^2+f_1^2+f_0+f_1+1}{f_1}$, so $F_3\in\mathbb{F}_{2^d}$. But then $t^3+F_1t+F_2$ and $t^3+t^2+F_3t+F_4$ would be defined over $\mathbb{F}_{2^d}$, contradicting the irreducibility of $t^6+t^5+f_1t^4+f_0t^3+f_1t^2+t+1$. □

Lemma 7.13. *Let $d\geq 2$. There is a smooth cubic surface over $\mathbb{F}_{2^d}$ with exactly n lines for each $n\in\{0,1,2,3,5,7,9,15,27\}$.*

Proof. The case of 27 lines was addressed in Propositions 7.3 and 7.4. For each of the remaining 10 cases, we give a sextic polynomial satisfying the necessary criteria. As has been our convention, we let a be a primitive element for $\mathbb{F}_{2^d}$ over $\mathbb{F}_2$. Any other notation that appears is introduced in Propositions 7.5 through 7.12. We start numbering at (2) to stay consistent with the format of the proof of Lemma 3.2.

We remark that irreducible polynomials over finite fields cannot have repeated roots, so no two roots of an irreducible polynomial over $\mathbb{F}_{2^d}$ may sum to 0. Similarly, two distinct monic irreducible polynomials over a finite field cannot have any common roots. It follows that for each of the following sextic polynomials $G(t)$, no two roots of $G(t)$ sum to 0.

(2) $G(t)=t(t+a)(t+a^2)(t+a^2+1)(t^2+t+b_1)$. The degree 5 term of $G(t)$ is $a\neq 0$. The only way for three roots of $G(t)$ to sum to zero is if two $\mathbb{F}_{2^d}$-rational roots of $G(t)$ sum to one of the roots of t^2+t+b_1. But such a sum would be $\mathbb{F}_{2^d}$-rational, while the roots of t^2+t+b_1 are not defined over $\mathbb{F}_{2^d}$.

(3) $G(t)=t(t+a)(t+a^2)(t^3+t^2+c_1)$. The degree 5 term of $G(t)$ is $a^2+a+1\neq 0$. The three roots of $t^3+t^2+c_1$ sum to 1, so no two of these roots can sum to an element of $\mathbb{F}_{2^d}$. It follows that no three roots of $G(t)$ sum to 0.

(4) $G(t)=t(t+a)(t^2+t+b_1)(t^2+t+b_2)$. The degree 5 term of $G(t)$ is $a\neq 0$. It remains to show that a root r_1 of t^2+t+b_1 and a root r_2 of t^2+t+b_2 cannot sum to a. If $r_1+r_2=a$, then replace the factor t^2+t+b_2 with t^2+t+b_3. Then given any root r_1 of t^2+t+b_1 and r_3 of t^2+t+b_3, the above argument implies that $r_1+r_3\neq 0$. Moreover, if $r_1+r_3=a$, then $r_2=r_3$ and hence the minimal polynomials of r_2 and r_3 must be equal. But $b_2\neq b_3$, so this cannot happen.

(5) $G(t)=t(t+1)(t^4+(a^2+b_j)t^2+ab_jt+\gamma b_j^2)$. The degree 5 term of $G(t)$ is $1\neq 0$. It remains to show that no two roots of the quartic sum to 1. Two roots of $t^4+(a^2+b_j)t^2+ab_jt+\gamma b_j^2$ sum to 1 if and only if this quartic polynomial factors

as $(t+r)(t+r+1)(t+s)(t+s')$ over some extension of $\mathbb{F}_{2^d}$. This would imply that $a^2+b_j = r(r+1)+s(s+1)+1$ and $ab_j = r(r+1)+s(s+1)$. Solving for b_j, we find that $b_j = a+1$. Since b_5, b_6, b_7, b_8 are distinct, at least three of these are not equal to $a+1$. We may thus choose $b_j \neq a+1$.

(6) $G(t) = (t+a)(t^2+t+b_1)(t^3+t^2+c_1)$. The degree 5 term of $G(t)$ is $a \neq 0$. We need to show that a root of the quadratic factor and a root of the cubic factor cannot sum to a, and that a root of the quadratic factor and two roots of the cubic factor cannot sum to 0. Note that if two roots r_1, r_2 of $t^3+t^2+c_1$ and a root r_3 of t^2+t+b_1 sum to 0, then $r_1+r_2 = r_3$. This implies that $1+r_3$ is a root of $t^3+t^2+c_1$, and this irreducible cubic must be the minimal polynomial of $1+r_3$. But $1+r_3$ is a root of t^2+t+b_1, so we obtain a contradiction.

Similarly, if a root r_1 of $t^3+t^2+c_1$ and a root r_2 of t^2+t+b_1 sum to a, then the minimal polynomial of $r_1 = r_2+a$ is a cubic. On the other hand, r_2+a is a root of $t^2+t+b_1+a^2+a$, so the minimal polynomial of r_1 must be a quadratic. We again obtain a contradiction.

(7) $G(t) = (t^2+t+b_1)(t^2+t+b_2)(t^2+t+b_3)$. The degree 5 term of $G(t)$ is $1 \neq 0$. It remains to show that if r_i is a root of t^2+t+b_i for $i = 1,2,3$, then $r_1+r_2+r_3 \neq 0$. If $r_1+r_2+r_3 = 0$, then $r_1 = r_2+r_3$ and hence $(r_2+r_3)^2+(r_2+r_3)+b_1 = 0$. This implies that $b_1 = b_2+b_3$. Since $b_4 \neq b_1$, we may simply replace the factor t^2+t+b_1 with t^2+t+b_4 in this case.

(8) $G(t) = t(t^5+t^4+e_1t^3+e_2t^2+e_3t+e_4)$. The degree 5 term of $G(t)$ is $1 \neq 0$. We showed in Proposition 7.11 that no three roots of the quintic factor of $G(t)$ sum to 0.

(9) $G(t) = (t^2+t+b_m)(t^4+(b_1+1)t^2+b_1t+\gamma b_1^2)$. The degree 5 term of $G(t)$ is $1 \neq 0$. It suffices to show that no two roots of $t^4+(b_1+1)t^2+b_1t+\gamma b_1^2$ sum to equal a root of t^2+t+b_m for an appropriate choice of $m \in \{1,2,3,4\}$. Let r_i, r_i' be the roots of t^2+t+b_i. Since $b_i \neq b_j$, it follows that $r_i \neq r_j$ and $r_i \neq r_j'$ for any $i \neq j$. Let $s_1, \ldots, s_4$ be the roots of $t^4+(b_1+1)t^2+b_1t+\gamma b_1^2$. There are $\binom{4}{2}$ sums of the form s_i+s_j for $1 \leq i < j \leq 4$. Since $s_1+s_2+s_3+s_4 = 0$, we have $s_i+s_j = s_k+s_\ell$ for $\{i,j,k,\ell\} = \{1,2,3,4\}$. In particular, there are only three distinct sums of pairs of roots of $t^4+(b_1+1)t^2+b_1t+\gamma b_1^2$, so these sums of pairs of roots cannot be equal to r_m or r_m' for at least one choice of m.

(10) $G(t) = (t^3+t^2+c_1)(t^3+at^2+c_2)$. The degree 5 term of $G(t)$ is $a+1 \neq 0$. It remains to show that two roots of $t^3+t^2+c_1$ do not sum to a root of $t^3+at^2+c_2$, and that two roots of $t^3+at^2+c_2$ do not sum to a root of $t^3+t^2+c_1$. Let r_1, r_2, r_3 be the roots of $t^3+t^2+c_1$, and let s be a root of $t^3+at^2+c_2$. If $r_1+r_2 = s$, then $s+r_3 = 1$ and hence $1+r_3$ is a root of $t^3+at^2+c_2$. But this implies that $r_3^3+(a+1)r_3^2+r_3+c_2+a+1 = 0$, so r_3 is a root of $t^3+(a+1)t^2+t+c_2+a+1$. On the other hand, the minimal polynomial of r_3 is $t^3+t^2+c_1$, so we conclude by contradiction that no two roots of t^3+t+c_1 sum to equal a root of $t^3+at^2+c_2$. A similar argument can be used to show that no two roots of the latter cubic polynomial sum to equal a root of the former cubic polynomial.

(11) $G(t)=t^6+t^5+f_1t^4+f_0t^3+f_1t^2+t+1$. As shown in Proposition 7.12, no three roots of $G(t)$ sum to 0.

As in Lemma 3.2, we obtain smooth cubic surfaces with the desired line counts over $\mathbb{F}_{2^d}$ by blowing up at points corresponding to the roots of these polynomials. □

To finish classifying all lines counts for smooth cubic surfaces over finite fields of characteristic 2, we can apply Proposition 6.2 and perform a search. With enough computing power, this search can even be made exhaustive. However, we will settle for an example of a smooth cubic surface satisfying each line count.

Lemma 7.14. *There is a smooth cubic surface over $\mathbb{F}_4$ with exactly n lines for each $n\in\{0,1,2,3,5,7,9,15,27\}$.*

Proof. Let a be a primitive element for $\mathbb{F}_4$ over $\mathbb{F}_2$. The following equations define smooth cubic surfaces, and we give the number of lines they contain.

- 0 lines: $f=x_0^3+x_1^3+x_0^2x_2+x_2^3+x_3^3$.
- 1 line: $f=x_0^3+ax_0x_1^2+x_1^3+ax_0^2x_2+x_2^3+ax_0^2x_3+ax_0x_1x_3+x_3^3$.
- 2 lines: $f=x_0^3+ax_0x_1^2+x_1^3+ax_0x_1x_2+x_2^3+ax_0^2x_3+ax_0x_1x_3+x_3^3$.
- 3 lines: $f=x_0^3+x_0^2x_1+x_1^3+x_0^2x_2+x_2^3+x_3^3$.
- 5 lines: $f=x_0^3+ax_0^2x_1+ax_0x_1^2+x_1^3+ax_0x_1x_2+x_2^3+ax_0x_1x_3+x_3^3$.
- 7 lines: $f=x_0^2x_1+x_0x_1^2+x_0^2x_2+x_2^3+x_0^2x_3+x_3^3$.
- 9 lines: $f=x_0^3+x_1^3+ax_2^3+ax_3^3$.
- 15 lines:
$$\begin{aligned} f=\ & ax_0^3+x_0^2x_1+x_0x_1^2+ax_1^3+x_0^2x_2+x_0x_1x_2+x_1^2x_2\\ &+x_0x_2^2+x_1x_2^2+ax_2^3+x_0^2x_3+x_0x_1x_3+x_1^2x_3+x_0x_2x_3\\ &+x_1x_2x_3+x_2^2x_3+x_0x_3^2+x_1x_3^2+x_2x_3^2+ax_3^3.\end{aligned}$$
- 27 lines: $f=x_0^3+x_1^3+x_2^3+x_3^3$.

The code used to find these cubic surfaces is given in Appendix B. We remark that this code should be modified in practice – as written, the search runs through 4^{20} cases. We found the above lines by searching through various combinations of simpler coefficient combinations. □

Remark 7.15. There has been extensive work on the subject of lines on cubic surfaces over finite fields, especially on classifying cubic surfaces with 27 lines over a finite field. See e.g. [Hir67a, Hir67b, BHK18, BK19].

Remark 7.16. Given a field k, one can ask about the distributions of line configurations for smooth cubic surfaces over k. Since the line count determines the intersection graph over any field (except in the case of $n = 3$, where there are two distinct intersection graphs), it suffices to understand the distributions of line counts for such smooth cubic surfaces. In the case of $n = 3$, one also needs to understand the proportion of cubic surfaces with 3 lines that contain a skew triple. 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 $\mathbb{Q}$.

Appendix A. Cubic surfaces with a skew triple

In this appendix, we include some Sage code that we use to study smooth cubic surfaces over $\mathbb{Q}$ with a skew triple. In [MMZ20], we assume that our cubic surface contains the skew triple $E_1 = \mathbb{V}(x_0, x_1)$, $E_2 = \mathbb{V}(x_2, x_3)$, and $E_3 = \mathbb{V}(x_0 - x_2, x_1 - x_3)$ to simplify calculations. We make this assumption here as well. Cubic surfaces containing this particular skew triple are of the form $\mathbb{V}\left(\sum_{i+j+k+\ell=3} \alpha_{i,j,k,\ell} x_0^i x_1^j x_2^k x_3^\ell\right)$ with

$$\begin{aligned}
\alpha_{3,0,0,0} = \alpha_{0,3,0,0} = \alpha_{0,0,3,0} = \alpha_{0,0,0,3} = 0,\\
\alpha_{2,1,0,0} = \alpha_{1,2,0,0} = \alpha_{0,0,2,1} = \alpha_{0,0,1,2} = 0,\\
\alpha_{0,2,0,1} + \alpha_{0,1,0,2} = \alpha_{2,0,1,0} + \alpha_{1,0,2,0} = 0,\\
\alpha_{0,2,1,0} + \alpha_{1,0,0,2} + \alpha_{1,1,0,1} + \alpha_{0,1,1,1} = 0,\\
\alpha_{0,1,2,0} + \alpha_{2,0,0,1} + \alpha_{1,0,1,1} + \alpha_{1,1,1,0} = 0.
\end{aligned}$$

Given $\alpha_{i,j,k,\ell}$ that satisfy the above relations, we first check if the resulting cubic surface is smooth.

```
P3 = ProjectiveSpace(3, QQ, 'x');
P3.inject_variables();
var('a0201 a0102 a2010 a1020 a0210 a1002
     a1101 a0111 a0120 a2001 a1011 a1110');
f = a0201*x1^2*x3+a0102*x1*x3^2+a2010*x0^2*x2
   +a1020*x0*x2^2+a0210*x1^2*x2+a1002*x0*x3^2
   +a1101*x0*x1*x3+a0111*x1*x2*x3+a0120*x1*x2^2
   +a2001*x0^2*x3+a1011*x0*x2*x3+a1110*x0*x1*x2;
f = f.substitute(
   {a0201:α_{0,2,0,1}, a0102:α_{0,1,0,2}, a2010:α_{2,0,1,0}, a1020:α_{1,0,2,0},
    a0210:α_{0,2,1,0}, a1002:α_{1,0,0,2}, a1101:α_{1,1,0,1}, a0111:α_{0,1,1,1},
    a0120:α_{0,1,2,0}, a2001:α_{2,0,0,1}, a1011:α_{1,0,1,1}, a1110:α_{1,1,1,0}});
P3.subscheme(f).is_smooth()
```

If the resulting cubic surface is smooth, we can compute t_4, t_5, t_6.

```
var('a0201 a0102 a2010 a1020 a0210 a1002
     a1101 a0111 a0120 a2001 a1011 a1110');
R.<t> = QQbar[];
g = a2010*t^3+(a2001+a1110)*t^2+(a0210+a1101)*t+a0201;
g = g.substitute(
```

```
    {a0201:$\alpha_{0,2,0,1}$, a0102:$\alpha_{0,1,0,2}$, a2010:$\alpha_{2,0,1,0}$, a1020:$\alpha_{1,0,2,0}$,
     a0210:$\alpha_{0,2,1,0}$, a1002:$\alpha_{1,0,0,2}$, a1101:$\alpha_{1,1,0,1}$, a0111:$\alpha_{0,1,1,1}$,
     a0120:$\alpha_{0,1,2,0}$, a2001:$\alpha_{2,0,0,1}$, a1011:$\alpha_{1,0,1,1}$, a1110:$\alpha_{1,1,1,0}$});
g.roots()
```

We label the roots of $g(t)$ as t_4, t_5, t_6. Permuting the labels for these roots only permutes the names of the remaining 24 lines on our smooth cubic surface. In this paper, our convention has been to pick t_4 to be rational if $g(t)$ has a rational root. Finally, we can compute s_1, s_2.

```
var('a0201 a0102 a2010 a1020 a0210 a1002
     a1101 a0111 a0120 a2001 a1011 a1110');
var('t4 t5 t6');
R.<t> = QQbar[];
l3 = vector([a2010*t^2+a1110*t+a0210,
             a2010*t+a0120+a1110,
             a2001*t-a1002]);
l34 = l3.substitute(t=t4);
l35 = l3.substitute(t=t5);
c1 = l34[0]; c2 = l34[1]; c3 = l34[2];
d1 = l35[0]; d2 = l35[1]; d3 = l35[2];
u1 = (t4-t5)/c1;
u2 = -(c3+c2*t5)/(c3+c2*t4);
u3 = (t4-t5)/(c3+c2*t4);
v2 = (c1/d1)*(d2*c3-d3*c2)/(c3+c2*t4);
v3 = -(c1/d1)*(d2*t4+d3)/(c3+c2*t4);
h = v2*t^2+(u1*v2-u2+v3)*t+(u1*v3-u3);
h = h.substitute(
    {a0201:$\alpha_{0,2,0,1}$, a0102:$\alpha_{0,1,0,2}$, a2010:$\alpha_{2,0,1,0}$, a1020:$\alpha_{1,0,2,0}$,
     a0210:$\alpha_{0,2,1,0}$, a1002:$\alpha_{1,0,0,2}$, a1101:$\alpha_{1,1,0,1}$, a0111:$\alpha_{0,1,1,1}$,
     a0120:$\alpha_{0,1,2,0}$, a2001:$\alpha_{2,0,0,1}$, a1011:$\alpha_{1,0,1,1}$, a1110:$\alpha_{1,1,1,0}$,
     t4:$t_4$, t5:$t_5$, t6:$t_6$});
h.roots()
```

Appendix B. Cubic surfaces over $\mathbb{F}_4$

In this appendix, we include some Sage code that we use to classify all lines counts for smooth cubic surfaces over $\mathbb{F}_4$.

```
from itertools import product, combinations;
k = GF(4,'a');
P3 = ProjectiveSpace(3, k, 'x');
P3.inject_variables();
points = [P3(1,0,0,0)];
for p in enumerate(k):
```

```
        points.append(P3(p[1],1,0,0));
    for A in product(enumerate(k),repeat=2):
        p = [i[1] for i in A];
        points.append(P3(p[0],p[1],1,0));
    for A in product(enumerate(k),repeat=3):
        p = [i[1] for i in A];
        points.append(P3(p[0],p[1],p[2],1));
    lines = [];
    for p,q in combinations(points,2):
        y = set(P3.line_through(p,q).rational_points());
        if not y in lines:
            lines.append(y);
    counts = [];
    for L in product(enumerate(k),repeat=20):
        v = [i[1] for i in L];
        if v != [0]*20:
            f = v[0]*x0^3+v[1]*x1^3+v[2]*x2^3+v[3]*x3^3
               +v[4]*x0^2*x1+v[5]*x0^2*x2+v[6]*x0^2*x3
               +v[7]*x0*x1^2+v[8]*x0*x1*x2+v[9]*x0*x1*x3
               +v[10]*x0*x2^2+v[11]*x0*x2*x3+v[12]*x0*x3^2
               +v[13]*x1^2*x2+v[14]*x1^2*x3+v[15]*x1*x2^2
               +v[16]*x1*x2*x3+v[17]*x1*x3^2+v[18]*x2^2*x3
               +v[19]*x2*x3^2;
            if P3.subscheme(f).is_smooth():
                kpoints = set(P3.subscheme(f).rational_points());
                S = 0;
                for j in lines:
                    if j.issubset(kpoints): S+=1;
                if not S in counts:
                    counts.append(S);
                    print(f, " has ", S, " lines")
    counts.sort();
    counts
```

In practice, this code should be modified to reduce its run time. As is, the code runs through 4^{20} cases. We found the desired examples by considering various simpler combinations of coefficients. For example, one can replace:

```
    for L in product(enumerate(k),repeat=20):
        v = [i[1] for i in L];
```

with:

```
    r = r;
```

```
j = j;
for L in product(enumerate(k),repeat=r):
    v = [1]*j + [i[1] for i in L] + [1]*(20-r-j);
```

With this change, the code will check 4^r cases. By picking an integer r small enough (we used $r = 6$ for our computations), one can obtain the desired examples in a reasonable amount of time. The integer j shifts the varying coefficients within v, while `[1]*j` denotes that the first j entries will all be 1. Of course, one could choose any element of $\mathbb{F}_4$ to fill these repeated slots.

Appendix C. Subgroups of $W(E_6)$

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 $W(E_6)$. 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;
```

References

[Bet18] Anton Betten. Classifying cubic surfaces over finite fields using orbiter. In James H. Davenport, Manuel Kauers, George Labahn, and Josef Urban, editors, *Mathematical Software – ICMS 2018*, pages 55–61, Cham, 2018. Springer International Publishing.

[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.

[DK00] A. I. Degtyarev and V. M. Kharlamov. Topological properties of real algebraic varieties: Rokhlin's way. *Uspekhi Mat. Nauk*, 55(4(334)):129–212, 2000.

[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.

[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.

[Kle73] Felix Klein. Ueber Flächen dritter Ordnung. *Math. Ann.*, 6(4):551–581, 1873.

[KSC04] János Kollár, Karen E. Smith, and Alessio Corti. *Cubic surfaces*, pages 35–59. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 2004.

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

[LW72] Philip A. Leonard and Kenneth S. Williams. Quartics over $\mathrm{GF}(2^n)$. *Proc. Amer. Math. Soc.*, 36:347–350, 1972.

[Mey90] Helmut Meyn. On the construction of irreducible self-reciprocal polynomials over finite fields. *Appl. Algebra Engrg. Comm. Comput.*, 1(1):43–53, 1990.

[MMZ20] Stephen McKean, Daniel Minahan, and Tianyi Zhang. All lines on a smooth cubic surface in terms of three skew lines, 2020.

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

[PBT08] Irene Polo-Blanco and Jaap Top. Explicit real cubic surfaces. *Canad. Math. Bull.*, 51(1):125–133, 2008.

[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.

[Ros57] Luigi Antonio Rosati. L'equazione delle 27 rette della superficie cubica generale in un corpo finito. I. *Boll. Un. Mat. Ital. (3)*, 12:612–626, 1957.

[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.

[SD69] H. P. F. Swinnerton-Dyer. Applications of algebraic geometry to number theory. In *1969 Number Theory Institute (Proc. Sympos. Pure Math., Vol. XX, State Univ. New York, Stony Brook, N.Y., 1969)*, pages 1–52, 1969.

[Seg42] Beniamino Segre. *The Non-singular Cubic Surfaces.* Oxford University Press, Oxford, 1942.

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

[Zeu74] H. G. Zeuthen. Etudes des propriétés de situation des surfaces cubiques. *Math. Ann.*, 8(1):1–30, 1874.