L'Enseignement Mathématique (2) 65 (2019), 303–376 DOI 10.4171/LEM/65-3/4-2

Resolvent degree, Hilbert's 13th Problem and geometry

Benson Farb and Jesse Wolfson

Abstract. We develop the theory of resolvent degree, introduced by Brauer [Brau2] in order to study the complexity of formulas for roots of polynomials and to give a precise formulation of Hilbert's 13th Problem. We extend the context of this theory to enumerative problems in algebraic geometry, and consider it as an intrinsic invariant of a finite group. As one application of this point of view, we prove that Hilbert's 13th Problem, and his Sextic and Octic Conjectures, are equivalent to various enumerative geometry problems, for example problems of finding lines on a smooth cubic surface or bitangents on a smooth planar quartic.

Mathematics Subject Classification (2010). Primary: 14H30; Secondary: 12E05, 12F10, 14N10, 14G27.

Keywords. Algebraic function, enumerative problems, resolvent degree, Hilbert's 13th Problem.

Contents

1. Introduction

In a never-cited 1975 paper [Brau2], Brauer introduced for a field extension L/K an integer-valued invariant $\mathrm{RD}(L/K)$ that we call *resolvent degree*. Applying RD to function fields gives an invariant $\mathrm{RD}(Y \dashrightarrow X)$ of rational covers[1] (e.g., finite branched covers) of complex algebraic varieties. The resolvent degree $\mathrm{RD}(\widetilde{\mathcal{P}}_n \to \mathcal{P}_n)$ of the root cover of the universal family $\mathcal{P}_n$ of degree n polynomials has the interpretation:

$\mathrm{RD}(\widetilde{\mathcal{P}}_n \to \mathcal{P}_n) =$ the least d for which there exists a formula in algebraic functions of at most d variables for the roots of a polynomial in terms of its coefficients.

While the formal definition seems to have waited until Brauer, the study of "reduction of parameters" for polynomials was initiated by Tschirnhaus [Tsch] in 1683. It was developed and refined by Hamilton, Sylvester, Klein, Hilbert, Segre and others. As we explain below, RD allows one to go beyond the solvable/unsolvable dichotomy provided by Galois theory; in particular, it was introduced by Brauer to give a precise formulation of Hilbert's 13th Problem (see below).

In this paper we pick up where Brauer left off. We extend the scope of RD from polynomials to classical enumerative problems, placing Hilbert's 13th Problem in a broader context and restoring the geometric perspective pioneered by Klein in his study of quintic equations [Kle2]. One use of resolvent degree is that it gives a uniform framework for stating and relating disparate classical results. As an example, we prove (Theorem 8.1) an equivalence of Hilbert's Sextic Conjecture to seven other problems, for example relating it to finding lines on cubic surfaces and finding fixed points for hyperelliptic involutions on genus 2 curves. We prove similar theorems for Hilbert's 13th problem (Theorem 8.3), and Hilbert's Octic Conjecture (Theorem 8.4).

In [Wol], this viewpoint is used to extend a beautiful but little-known trick of Hilbert (who used the existence of lines on a smooth cubic surface to give an upper bound on $\mathrm{RD}(\widetilde{\mathcal{P}}_9 \to \mathcal{P}_9)$) to improve the upper bounds on $\mathrm{RD}(\widetilde{\mathcal{P}}_n \to \mathcal{P}_n)$ given by Hamilton, Sylvester, B. Segre, Brauer and others.

1.1. Resolvent degree. We start with a problem central to classical (and modern) mathematics.

[1] See Definition 1.2 below.

Problem 1.1. Find and understand formulas for the roots of a polynomial

$$P(z) = z^n + a_1 z^{n-1} + \cdots + a_n \tag{1.1}$$

in terms of the coefficients $a_1, \ldots, a_n$.

It is well known that if $n \geq 5$ then no formula exists using only radicals and arithmetic operations in the coefficients a_i.[2] Less known is Bring's 1786 theorem [Bri] that any quintic can be reduced via radicals to a quintic of the form $Q(z) = z^5 + az + 1$ (see [CHM] for a contemporary translation). In 1836, Hamilton [Ham] extended Bring's results to higher degrees, showing, for example, that any sextic can be reduced via radicals to $Q(z) = z^6 + az^2 + bz + 1$, making it a 2-parameter (a and b) problem. He also proved that any degree 7 polynomial can be reduced via radicals to one of the form

$$Q(z) = z^7 + az^3 + bz^2 + cz + 1, \tag{1.2}$$

and that any degree 8 polynomial can be reduced via radicals to one of the form $Q(z) = z^8 + az^4 + bz^3 + cz^2 + dz + 1$. Hilbert conjectured explicitly that one cannot do better: solving a sextic (resp. septic, resp. octic) is fundamentally a 2-parameter (resp. 3-parameter, resp. 4-parameter) problem. Of course we need to know the exact rules of the game here; that is, we need to give a precise definition of what it means to reduce a problem to r parameters. Surprisingly, a precise definition was only written down in 1975, by Brauer [Brau2], and a year later by Arnol'd–Shimura [AS], apparently unaware of Brauer's paper. For motivation, let's look at an example.

Let $\mathcal{P}_n \cong \mathbb{C}^n$ be the space of monic, degree n complex polynomials, and let $\widetilde{\mathcal{P}}_n$ be the *root cover* of $\mathcal{P}_n$:

$$\widetilde{\mathcal{P}}_n := \{(P, \lambda) : P(\lambda) = 0\} \subset \mathcal{P}_n \times \mathbb{C}.$$

The map $(P, \lambda) \mapsto P$ gives an n-sheeted branched cover $\widetilde{\mathcal{P}}_n \to \mathcal{P}_n$, with branch locus precisely the subset of $\mathcal{P}_n$ consisting of polynomials with a repeated root, given by the zero-set of the *discriminant* $\Delta_n(a_1, \ldots, a_n)$, a polynomial in the coefficients a_i.

Recall that a rational map $f : X \dashrightarrow Y$ between irreducible varieties is *dominant* if the image of f is Zariski dense in Y; it is *generically finite* if the generic fiber is finite. For such a map there are Zariski opens $U \subseteq X, V \subseteq Y$ so that the restriction $f : U \to V$ is a finite cover.

[2] This was claimed by Ruffini in 1799; a complete proof was given by Abel in 1824.

Definition 1.2 (Rational cover). Let X and Y be irreducible varieties.[3] A *rational cover* $f : X \dashrightarrow Y$ is a generically finite dominant rational map.

With this definition in hand, "solving an arbitrary degree n polynomial by radicals" means precisely that there is a sequence of rational covers

$$X_r \dashrightarrow \cdots \dashrightarrow X_0 = \mathcal{P}_n$$

such that $X_r \dashrightarrow \mathcal{P}_n$ factors through a rational cover $X_r \dashrightarrow \widetilde{\mathcal{P}}_n$, and where each $X_{i+1} \dashrightarrow X_i$ is birationally a pullback

$$\begin{tikzcd} X_{i+1} \arrow[r, dashed] \arrow[d, dashed] & \mathbb{P}^1 \arrow[d] & z \arrow[d, mapsto] \\ X_i \arrow[r, dashed] & \mathbb{P}^1 & z^{d_i} \end{tikzcd}$$

The fact that each cover $X_{i+1} \dashrightarrow X_i$ is a pullback from $\mathbb{P}^1$ reflects the fact that it is specified by $\dim_{\mathbb{C}} \mathbb{P}^1 = 1$ parameter, namely taking a d_i-th root, and so "solving by radicals" is a process involving only 1 parameter at a time. The final map $X_r \dashrightarrow \widetilde{\mathcal{P}}_n$ is crucial. For example, for Cardano's solution in radicals of the cubic, this map has degree 2, reflecting the fact that Cardano's formula actually produces 6 solutions (with multiplicity), not just 3. While such towers of radicals exist only for $n \leq 4$, Bring's reduction of quintics mentioned above gives for $n = 5$ a tower with each $X_{i+1} \dashrightarrow X_i$ either a radical, or the pullback of the "Bring curve" $\mathcal{C} \to \mathbb{P}^1$ (see [Gre] for a beautiful treatment of this genus 4 curve); in particular we see that solving a general quintic is also a 1-parameter problem. More precisely, we have the following.

Definition 1.3 (Resolvent degree). Let k be a field of characteristic 0 and let $Y \dashrightarrow X$ be a rational cover of k-varieties. The *essential dimension* $\mathrm{ed}_k(Y \dashrightarrow X)$ is the minimal d so that $Y \dashrightarrow X$ is the "rational pullback" of a rational cover of d-dimensional varieties: there exists a rational cover $\widetilde{W} \dashrightarrow W$ with $\dim(W) = d$, a Zariski open $U \subseteq X$, and a morphism $f : U \to W$ such that $f^*\widetilde{W} \cong Y|_U$.

The *resolvent degree* $\mathrm{RD}_k(Y \dashrightarrow X)$ is the minimal d for which there exists a tower of rational covers

$$X_r \dashrightarrow X_{r-1} \dashrightarrow \cdots \dashrightarrow X_1 \dashrightarrow X_0 = X \tag{1.3}$$

with $\mathrm{ed}_k(X_i \dashrightarrow X_{i-1}) \leq d$ for all i and with a dominant map of X-schemes $X_r \dashrightarrow Y$.

[3] See Convention 2.2 for the case of reducible varieties.

Definition 1.3 is equivalent to Brauer's original, purely field-theoretic definition; see §2.1 below. One can easily check [4] that $\mathrm{RD}(\widetilde{\mathcal{P}}_n \to \mathcal{P}_n)$ is the minimal number of parameters to which one can reduce a general degree n polynomial in order to find a formula for the roots. In this language, the results mentioned above on reduction of parameters can be restated succinctly as:

$$\mathrm{RD}(\widetilde{\mathcal{P}}_n \to \mathcal{P}_n) = 1 \quad \forall n \leq 5, \quad \text{and} \quad \mathrm{RD}(\widetilde{\mathcal{P}}_n \to \mathcal{P}_n) \leq n-4 \quad \forall n > 5.$$

Remark 1.4. The theory of essential dimension has been developed by Buhler–Reichstein, Merkurjev and others into a beautiful and widely applicable theory; see Reichstein's 2010 ICM paper [Rei] for a survey. This disallowing of so-called "accessory irrationalities" captures more of the arithmetic of the function field of the base, whereas RD captures more of the intrinsic complexity of the branched cover. For the problems we are considering, forcing a solution in a single step does not give the correct measure. For example, there are finite covers $\widetilde{X} \to X$ that are solvable (hence $\mathrm{RD}(\widetilde{X} \to X) = 1$) but with $\mathrm{ed}(\widetilde{X} \to X)$ as large as one wants; and for example $\mathrm{ed}(\widetilde{\mathcal{P}}_4 \to \mathcal{P}_4) = \mathrm{ed}(\widetilde{\mathcal{P}}_5 \to \mathcal{P}_5) = 2$, even though (as mentioned above) it was known by 1786 that these problems reduce to 1 parameter.

1.2. Hilbert's problems. As already noted by Brauer [Brau2], Hilbert's conjecture (explicitly asked by Hilbert in [Hil1, p.424] and [Hil2, p.247]) that Hamilton's reduction of parameters for the general polynomial of degree $6, 7$, or 8 is optimal, can now be stated precisely, as can the problem for all degrees. Both Klein and Hilbert worked on this general problem for decades (see [Kle3, Hil1, Hil2]).

Problem 1.5 (Klein, Hilbert, Brauer). Compute $\mathrm{RD}(\widetilde{\mathcal{P}}_n \to \mathcal{P}_n)$. In particular:

Hilbert's Sextic Conjecture ([Hil2], p. 247):	$\mathrm{RD}(\widetilde{\mathcal{P}}_6 \to \mathcal{P}_6) = 2.$
Hilbert's 13th Problem ([Hil1], p. 424):	$\mathrm{RD}(\widetilde{\mathcal{P}}_7 \to \mathcal{P}_7) = 3.$
Hilbert's Octic Conjecture ([Hil2], p. 247):	$\mathrm{RD}(\widetilde{\mathcal{P}}_8 \to \mathcal{P}_8) = 4.$

Amazingly, no progress has been made on any of these three conjectures since Hilbert stated them. In 1957, Arnol'd and Kolmogorov proved (see [Arn]) that there is no local topological obstruction to reducing the number of variables; however, as Arnol'd and many others have noted, the global problem remains open. A lot of work has been done on finding upper bounds on $\mathrm{RD}(\widetilde{\mathcal{P}}_n \to \mathcal{P}_n)$. This includes (in other language) theorems of Tschirnhaus (1683), Bring (1786), Hamilton (1836), Sylvester (1887), Klein (1888), Hilbert (1927), and Segre (1945).

The best general upper bound on $\mathrm{RD}(\widetilde{\mathcal{P}}_n \to \mathcal{P}_n)$, prior to the present, was given by Brauer [Brau2]. He proved for $n \geq 4$ that $\mathrm{RD}(\widetilde{\mathcal{P}}_n \to \mathcal{P}_n) \leq n-r$ once

[4] This is somewhat more clear via Brauer's definition.

$n \geq (r-1)! + 1$. Brauer's method was to systematize the classical method of Tschirnhaus transformations. In [Wol], the point of view developed here is used to give a significant improvement on Brauer's bound. One of the key ideas is to expand the context of resolvent degree.

1.3. Expanding the context. Since Hilbert, resolvent degree has been considered primarily for root covers of polynomials. However, as Klein first realized [Kle3], RD is much more widely applicable. After all, many algebraic problems can be reformulated in terms of a rational cover $(P, s) \mapsto P$ from the space $\widetilde{X}$ of pairs (P, s) of input parameters P and solutions s to the space X of parameters P, and

$$\mathrm{RD}(\widetilde{X} \dashrightarrow X) = \text{minimal number of parameters of any algebraic formula for } s \text{ in the coefficients of } P.$$

As Klein himself realized [Kle1], this general setup includes not only roots of polynomials $\widetilde{\mathcal{P}}_n \to \mathcal{P}_n$ (see §7), but also a second fundamental source of examples, namely incidence varieties (see §6).

Incidence varieties. Problems in enumerative geometry are typically set up with the following data:

(1) a pair of moduli spaces $\mathcal{M}, \mathcal{C}$ of algebraic varieties;

(2) a subvariety $\widetilde{\mathcal{M}} \subseteq \mathcal{M} \times \mathcal{C}$, called an *incidence variety*, consisting of pairs (M, C) satisfying a given incidence relation; and

(3) a rational cover $\pi : \widetilde{\mathcal{M}} \dashrightarrow \mathcal{M}$ defined by $\pi(M, C) := M$.

We restrict to characteristic 0 throughout this paper. By the definition of a rational cover, for each component $\mathcal{M}_0$ of $\mathcal{M}$ there exists $n \geq 1$ so that π is an n-sheeted covering space over some Zariski open $U \subseteq \mathcal{M}_0$. In particular for each $M \in U$ there is a set $\pi^{-1}(M) = \{C_1, \ldots, C_n\}$ of n varieties in $\mathcal{C}$, satisfying the given incidence relation, varying in an algebraic way with M. Here are some examples.

Examples 1.6. Let $\mathcal{H}_{d,n}$ denote the moduli space of smooth, degree d hypersurfaces in $\mathbb{P}^n$.

(1) 27 lines on a smooth cubic surface:

$$\mathcal{H}_{3,3}(1) := \big\{(S, L) : S \text{ a smooth cubic surface, } L \subset S \text{ a line}\big\}$$

and $\pi : \mathcal{H}_{3,3}(1) \to \mathcal{H}_{3,3}$ is a 27-sheeted cover. See §4 for precise definitions.

(2) 28 bitangents on a smooth planar quartic:

$$\mathcal{H}_{4,2}(1) := \big\{(C, L) : C \subset \mathbb{P}^2 \text{ a smooth quartic}, \\ L \subset \mathbb{P}^2 \text{ a line tangent to } C \text{ at 2 points}\big\}$$

and $\pi : \mathcal{H}_{4,2}(1) \to \mathcal{H}_{4,2}$ is a 28-sheeted cover. See §5 for precise definitions.

(3) 3264 conics tangent to 5 given conics: Let W be the linear system of conics in $\mathbb{P}^2$ and $W_0 \subset W$ the Zariski open consisting of smooth conics. Then we can define

$$Y := \big\{(C_1, \ldots, C_5, C) : \ C \text{ is tangent to each } C_i\big\} \in W^5 \times W_0$$

and $\pi : Y \to W^5$ is a 3264-sheeted dominant map.

A first goal of enumerative problems is to find such $\widetilde{\mathcal{M}} \dashrightarrow \mathcal{M}$ and then to compute the degree n. One then wants to find points in $\pi^{-1}(M)$ in terms of the data needed to specify M. "Find" can have several meanings.

Example 1.7 (Finding a line on a cubic surface). Cayley–Salmon proved in 1856 that a smooth cubic surface has 27 lines. How hard is it to find such a line? all 27 lines given one of them? Let $\mathcal{H}_{3,3}(r)$ (resp. $\mathcal{H}_{3,3}^{\text{skew}}(r)$) denote the moduli space of $(r+1)$-tuples $(S; L_1, \ldots, L_r)$ where $S \in \mathcal{H}_{3,3}$ and $\{L_i\}$ are lines (resp. disjoint lines) in S; see §4 for precise definitions. Harris [Har] proved:[5]

- The monodromy group of the 27-sheeted cover $\mathcal{H}_{3,3}(1) \to \mathcal{H}_{3,3}$ is the Weyl group $W(E_6)$; in particular it is not solvable. Harris [Har, p. 718] deduces that "there does not exist a formula for the 27 lines of a general cubic surface."
- The monodromy group of $\mathcal{H}_{3,3}(27) \to \mathcal{H}_{3,3}^{\text{skew}}(r)$ is solvable for $r = 3$ but not for $r < 3$. Thus there is a formula in radicals for the 27 lines, given 3 disjoint ones, but no fewer.

The question remains: how hard is it to find a line on a smooth cubic surface? or 27 lines given 1? We just saw examples where a formula in radicals does not exist, and indeed this is typical for enumerative problems; this is the main theme of [Har]. But, in contrast to Harris's conclusion, algebraic formulas not-in-radicals do exist, and indeed have been an object of study since the 17th century. Resolvent degree allows us to move beyond the solvable/unsolvable dichotomy to give a quantitative measure of the possible complexity of such formulas. In particular it allows us to ask: what is $\mathrm{RD}(\mathcal{H}_{3,3}(r) \to \mathcal{H}_{3,3}(s))$? Here is a simple but illustrative example.

[5] The first statement was known to Camille Jordan.

Example 1.8. $\mathrm{RD}\big(\mathcal{H}_{3,3}(27) \to \mathcal{H}_{3,3}(1)\big) \leq \mathrm{RD}(\widetilde{\mathcal{P}}_5 \to \mathcal{P}_5) = 1$.

Example 1.8 follows from a beautiful classical trick: given a line L on a smooth cubic surface S, each plane in the pencil containing L intersects S in L union a conic, and this conic degenerates into a union of two lines at the roots of the discriminant Δ_L of this pencil of conics. Δ_L is a one-variable polynomial of degree 5, which by Bring [Bri] has $\mathrm{RD} = 1$. One then gets 5 pairs of distinct lines on S, and gets the other 16 via radicals, by Harris's theorem.

Conjecture 1.9 (The line-finding conjecture).

$$\mathrm{RD}\big(\mathcal{H}_{3,3}(27) \to \mathcal{H}_{3,3}\big) = \mathrm{RD}\big(\mathcal{H}_{3,3}(1) \to \mathcal{H}_{3,3}\big) = 3.$$

The upper bound of 3 comes from work of Klein and Burkhardt [Kle3, Bur]. We give a concise proof in Theorem 4.3 below.

In §6 we will see how theorems from classical geometry can be used to relate the resolvent degrees of different problems. For example, we use the result described in Figure 1 to prove the following.

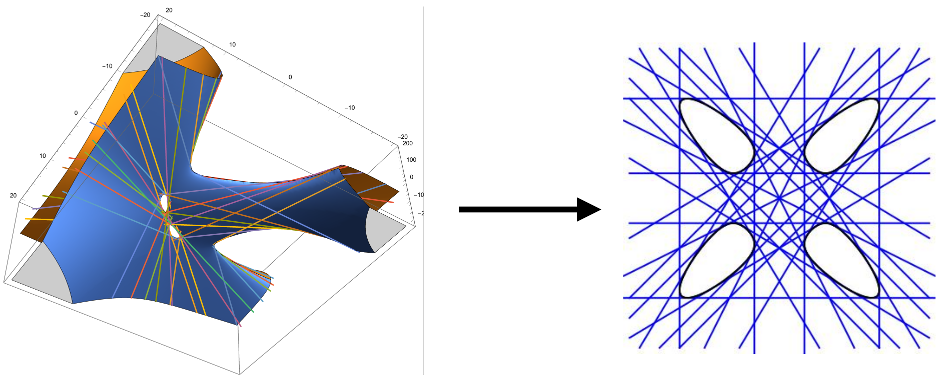


Figure 1

The projection $\pi : \mathrm{Bl}_p(S) \to \mathbb{P}^2$ of the blowup at a point p of a smooth cubic surface S is a 2-sheeted branched cover, branched over a smooth plane quartic C. The branching locus in S is the inner rim of each of the four holes in S, two of which go off to infinity in the left-hand picture. The image $\pi(C)$ of each of the 27 lines in S is a bitangent of C. Here we see (the real points of) a branched cover given by projection to the plane of the paper. The left part of the figure is taken from [SS]; the right from [PSV].

Theorem 1.10. *Any minimal algebraic formula for the 27 lines on a smooth cubic surface (in terms of its coefficients) has the same number of parameters as any minimal algebraic formula for the 28 bitangents on a plane quartic curve, given one of them:*

$$\mathrm{RD}\big(\mathcal{H}_{3,3}(27) \to \mathcal{H}_{3,3}\big) = \mathrm{RD}\big(\mathcal{H}_{4,2}(28) \to \mathcal{H}_{4,2}(1)\big).$$

We discuss in depth lines on smooth cubic surfaces and bitangents on smooth plane quartics in §4 and §5, respectively. We focus on these examples because of their richness and their close relationship to Hilbert's problems (see below). In §6 we discuss RD of some other enumerative problems. It is our hope that others will work out the resolvent degree story for these problems (and many more).

Remark 1.11 (Explicit formulas). Part of the usefulness of the Galois criterion for solvability in radicals is that one can prove it without finding such a formula explicitly. Similarly, one can give an upper bound for the resolvent degree of a problem without finding an explicit formula. At the same time, the answers given by non-explicit methods can sometimes help indicate where to look for explicit formulas.

1.4. The scope of Hilbert's problems. As with many of Hilbert's problems, the 13th Problem and the Sextic and Octic Conjectures are meant to indicate a fundamental phenomenon whose understanding should have implications far beyond the original problem. Hilbert was clearly interested in, and worked on (see, e.g., [Hil1, Hil2]), the general problem of determining $\mathrm{RD}(\widetilde{\mathcal{P}}_n \to \mathcal{P}_n)$, the cases $n = 6$, $n = 7$, and $n = 8$ being the first open cases. In §8 we prove the equivalence of the Sextic Conjecture with seven other statements, the equivalence of Hilbert's 13th Problem with four other statements, and the equivalence of the Octic Conjecture with six other statements.

The point is both to exhibit how rich these problems are, and also to recast them in ways that may be more amenable to solution. As a sample, here is an abridged version of Theorem 8.1 below; for definitions see §8.

Theorem 1.12 (The geometry in Hilbert's Sextic Conjecture). *The following statements are equivalent:*

(1) *Hilbert's Sextic Conjecture is true:* $\mathrm{RD}(\widetilde{\mathcal{P}}_6 \to \mathcal{P}_6) = 2$.
(2) $\mathrm{RD} = 2$ *for the problem of finding the 27 lines on a cubic, given a "double six" set of lines (unordered) (see §4.1 and Figure 2):*

$$\mathrm{RD}\big(\mathcal{H}_{3,3}(27) \to \mathcal{H}_{3,3}(6,6)\big) = 2.$$

In fact, the resolvent degrees of the above problems coincide.

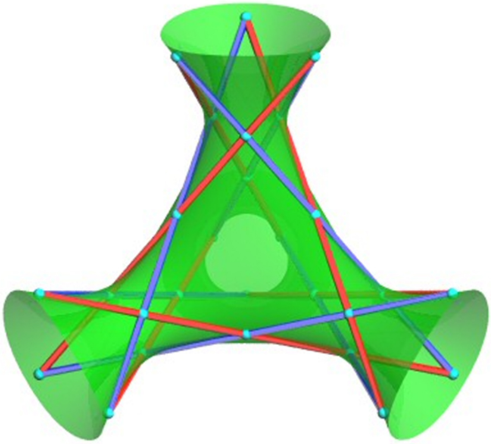


Figure 2
A double-six of lines on (the real points of) a smooth cubic surface. The intersection pattern is given in (4.3), with the a_i colored blue and b_j colored red (see the ebook version for a full color image). One can ask for a formula for the other 15 lines on a smooth cubic given a double-six. The resolvent degree of this problem is 2 if and only if Hilbert's Sextic Conjecture is true. Figure taken from `www.mathcurve.com/surfaces.gb/clebsch/doublesix.shtml`.

For further equivalences, as well as for problems about G-varieties with $G = W(E_6), S_7, S_8$ or $W(E_7)$, see §8.

Our approach to proving Theorem 1.12 (and the versions for other G) is to define RD as an intrinsic invariant of a finite group, in this case S_6 and $S_2 \times S_6$ respectively. We do this in §3. We then show that each of the specific covers in the theorem realizes the resolvent degree of their Galois group. Finally, we show that if a group contains as subgroups all the simple factors in its Jordan-holder decomposition, then its resolvent degree is the maximum of these simple factors (Theorem 3.3). From a classical perspective, a G-variety X gives an algebraic function expressing X in terms of coordinates on X/G. The proof of Theorem 1.12 proceeds by showing that $\mathrm{RD}(G) = \mathrm{RD}(X \to X/G)$ when X is a "*versal*" G-variety, for an appropriate notion of "versal", and then to prove the versality of the varieties listed above. What "versality" means, in this context, is that, up to accessory irrationalities, all G-varieties are birationally pullbacks of any versal one. See §3.2 for details. We give a similar treatment for Hilbert's 13th Problem and S_7, Hilbert's Octic Conjecture and S_8, as well as for various $W(E_6)$ and $W(E_7)$-varieties. For a more detailed treatment of versality in connection with modular functions, see [FKW].

1.5. Lower bounds. Theorems on resolvent degree to date have exclusively concerned providing upper bounds. As Dixmier concludes in his 1993 paper [Di] (using '$s(n)$' for $\mathrm{RD}(\widetilde{\mathcal{P}}_n \to \mathcal{P}_n)$):

> *Terminons sur une note dramatique, qui prouve notre incroyable ignorance. Bien que cela paraisse improbable, il n'est pas exclu que* $s(n) = 1$ *pour tout* n *! ... Toute minoration de* $s(n)$ *serait un progrès sérieux. En particulier, il serait temps de savoir si* $s(6) = 1$ *ou* $s(6) = 2$*."*[6]

In fact, we still cannot solve the following problem, implicit in Klein, Hilbert and Brauer, and stated more explicitly by Arnol'd-Shimura [AS].

Problem 1.13 (Arnol'd-Shimura). Prove that there exists $\widetilde{X} \dashrightarrow X$ with

$$\mathrm{RD}(\widetilde{X} \dashrightarrow X) > 1.$$

In fact, we believe that the following stronger statement should hold.

Conjecture 1.14. $\mathrm{RD}(\widetilde{\mathcal{P}}_n \to \mathcal{P}_n) \to \infty$ *as* $n \to \infty$.

Along with Hilbert's Sextic and Octic Conjectures and Hilbert's 13th Problem, these are clearly among the most important conjectures about resolvent degree. While we make no definite progress in this paper toward solving these problems, we hope that with renewed attention to them, and to the broader framework of resolvent degree, future progress may be more forthcoming.

1.6. Historical Remarks. The concept of resolvent degree originates with the classical problem of solving polynomials. It emerged in the 17th century with the work [Tsch] of Tschirnhaus.[7] In 1786, Bring [Bri] proved $\mathrm{RD} = 1$ for the problem of solving the quintic, and in 1836 Hamilton [Ham] gave a general sequence of upper bounds on $\mathrm{RD}(\widetilde{\mathcal{P}}_n \to \mathcal{P}_n)$ for increasing n. Hamilton's work was picked up by Sylvester and his student Hammond [Syl, SH1, SH2], by Klein [Kle3, Kle2], and by Hilbert [Hil1, Hil2]. Sixty-four years after Hamilton's work, Hilbert brought to the fore the fundamental issue: no *lower* bounds for $\mathrm{RD}(\widetilde{\mathcal{P}}_n \to \mathcal{P}_n)$ had ever been shown. Hilbert's Sextic Conjecture, Hilbert's 13th Problem [8], and Hilbert's Octic Conjecture pose the challenge of proving that $\mathrm{RD}(\widetilde{\mathcal{P}}_6 \to \mathcal{P}_6) = 2$, $\mathrm{RD}(\widetilde{\mathcal{P}}_7 \to \mathcal{P}_7) = 3$, and $\mathrm{RD}(\widetilde{\mathcal{P}}_8 \to \mathcal{P}_8) = 4$ respectively.

[6] In English: "Let's end on a dramatic note, which proves our incredible ignorance. Although this seems unlikely, it is not excluded that $s(n) = 1$ for all n ! ... Any lower bound for $s(n)$ would be serious progress. In particular, it's time that we know whether $s(6) = 1$ or $s(6) = 2$."

[7] See [KK] for a discussion of Tschirnhaus' work and the relevant correspondence with Leibniz.

[8] We will state what is sometimes called the "algebraic version" of this problem. Hilbert's original phrasing of the problem leaves room for various interpretations.

Resolvent degree was first defined explicitly in 1975 by Brauer [Brau2] in order to make precise Hilbert's 13th Problem. Brauer also gave new upper bounds on $\mathrm{RD}(\widetilde{\mathcal{P}}_n \to \mathcal{P}_n)$ for all n; see §7 below. A year later Arnol'd-Shimura [AS], apparently unaware of Brauer's paper, gave an equivalent definition of RD, also in order to make precise Hilbert's 13th. The definition of RD seems to have lain dormant until the paper [Di] of Dixmier, who helped publicize the concept of resolvent degree. This concept was also discussed in passing by Buhler–Reichstein [BR2] and Chernousov–Gille–Reichstein [CGR]. The present paper is the first to cite [Brau2]. The problem of finding any extension L/K with $\mathrm{RD}(L/K) > 1$ remains open.

2. The resolvent degree of a rational cover

In this section we study the basics of resolvent degree RD. After giving the definition of RD of a rational cover, we establish some basic properties of RD, we prove that our definition is equivalent to Brauer's original definition in [Brau2] of the resolvent degree of a finite field extension, and we prove a number of technical foundational results that are useful for computations. More specifically, we relate RD of an extension to that of its Galois closure, and we prove a crucial result on "accessory irrationalities", a classical concept studied by Kronecker, Klein and others, that is a key feature of RD.

2.1. Definitions of resolvent degree. For expositional reasons, we state the results in this paper in the language of k-varieties. For the reader who prefers to work with schemes, we will signal when a result or proof does not trivially extend to this case.

Convention 2.1.

(1) *Unless otherwise specified, throughout this paper we take the base field k to be an arbitrary field of characteristic 0.*

(2) *By a k**-variety** we mean a reduced, possibly reducible k-scheme of finite type.*

(3) *When the ground field k is clear we will generally omit the subscript k and simply write* $\mathrm{RD}(-)$.

(4) *A solid arrow $X \to Y$ denotes a regular map of varieties; a dashed arrow $X \dashrightarrow Y$ denotes a rational map of varieties.*

(5) *Given a rational cover $\widetilde{X} \dashrightarrow X$, we will refer to a tower* (1.3) *as in Definition* 1.3 *as a "tower solving $\widetilde{X} \dashrightarrow X$ in d variables", or as a "tower solving $\widetilde{X}$" for short.*

(6) *We say that* $f\colon X \dashrightarrow Y$ *is a "rational pullback" of* $g\colon W \dashrightarrow Z$ *if there exist dense opens* $U' \subset X$, $U \subset Y$, $V' \subset W$, $V \subset Z$ *and a pullback square of regular maps*

$$\begin{tikzcd} U' \arrow[r] \arrow[d, "f|_U"'] & V' \arrow[d, "g|_V"] \\ U \arrow[r] & V \end{tikzcd}$$

(7) *The "domain" of a rational map* $f\colon X \dashrightarrow Y$ *is the largest* $U \subset X$ *for which* $f|_U$ *is a regular. map. The "image" of* f *is defined to be* $f(U)$.

Convention 2.2 (Rational cover of a reducible variety). *Let* $\widetilde{X}$ *and* X *be a (possibly reducible) varieties. By a* ***rational cover*** $\widetilde{X} \dashrightarrow X$ *we mean a rational map* $\widetilde{X} \dashrightarrow X$ *with which restricts on each irreducible component* $\widetilde{X}_i \subset \widetilde{X}$ *to a dominant rational map* $\widetilde{X}_i \dashrightarrow X_j$ *for some irreducible component* $X_j \subset X$*; some Zariski open of each* X_j *lies in the image of some* $\widetilde{X}_i$*; and for each* j *the generic fiber of* $\widetilde{X}$ *over* X_j *is finite. In particular, we want to avoid pathologies such as* $X \coprod \{x\} \to X$ *(where* $\dim(X) > 0$ *and* $x \in X(k)$*).*

Recall that we defined in Definition 1.3 the resolvent degree of a rational cover. We can also define it in terms of field extensions.

Definition 2.3 (Resolvent Degree of a field extension). Let $K \hookrightarrow L$ be a finite extension of fields over k. The *resolvent degree* $\mathrm{RD}_k(L/K)$ is the minimal d for which there exists a finite sequence of finite extensions

$$K = L_0 \hookrightarrow L_1 \hookrightarrow \cdots \hookrightarrow L_r$$

with $L \hookrightarrow L_r$ (as extensions of K) and for all $i = 1, \dots, r$,

$$L_i = L_{i-1} \otimes_{F_i} \tilde{F}_i$$

where $F_i \hookrightarrow L_{i-1}$ is a subfield with $\mathrm{tr.deg}_k(F_i) \le d$ and where $F_i \hookrightarrow \tilde{F}_i$ is a finite extension. Here $\mathrm{tr.deg}_k(F_i)$ denotes the transcendence degree of F_i over k.

The definition of resolvent degree in terms of rational covers and in terms of field extensions are equivalent.

Proposition 2.4 (Equivalence of definitions). *If* $\widetilde{X} \dashrightarrow X$ *is a rational cover of irreducible* k*-varieties then*

$$\mathrm{RD}(\widetilde{X} \dashrightarrow X) = \mathrm{RD}(k(\widetilde{X})/k(X)).$$

We defer the proof until we have assembled basic properties of RD (as defined in Definition 1.3) in the next section.

Comparison with essential dimension. Essential dimension has its origins in work of Hermite [He], Kronecker [Kro], Joubert [Jou] and Klein [Kle2]. The theory was revived, and definitions made explicit, around twenty years ago by Buhler–Reichstein in [BR1]. It has been studied intensively ever since. See [Rei] and [Mer2] for recent surveys.

A central feature of the theory of essential dimension are the invariants $\mathrm{ed}_k(-;p)$. These measure the *prime-to-p essential dimension*; that is, any auxiliary tower of covers of degree prime to p is allowed before one finds a dominant map to a variety of minimal dimension. One could define the analogous invariant $\mathrm{RD}_k(-;p)$ by saying that in the tower giving a solution, one allows arbitrary prime-to-p covers, but for covers whose degree is divisible by p, only those of $\mathrm{ed}_k(-) \leq d$. Field theoretically, this amounts to working over the prime-to-p closure of the function field of the base; that is, base-changing to *Spec* of the fixed field of a p-Sylow of the absolute Galois group of $k(X)$. Since p-groups and pro-p groups are solvable, we immediately see that $\mathrm{RD}_k(-;p) \equiv 1$ for all k and all p. This is in strong contrast to the case of essential dimension, and shows that the study of resolvent degree is a strictly "Type 2" problem in the dichotomy of [Rei, §5].

2.2. Basic properties. In this section we establish some of the basic properties of RD.

Lemma 2.5 (Easy upper bounds). *Let $\widetilde{X} \dashrightarrow X$ be a rational cover of k-varieties.*

(1) $\mathrm{RD}(\widetilde{X} \dashrightarrow X) \leq \mathrm{ed}(\widetilde{X} \dashrightarrow X) \leq \dim(X)$.

(2) *Let $k \hookrightarrow k'$ be any field extension. Then*

$$\mathrm{RD}_{k'}(\widetilde{X} \times_k k' \dashrightarrow X \times_k k') \leq \mathrm{RD}_k(\widetilde{X} \dashrightarrow X).$$

(3) *Let $Y \dashrightarrow X$ be any dominant rational map of k-varieties. Then*

$$\mathrm{RD}(\widetilde{X} \times_X Y \dashrightarrow Y) \leq \mathrm{RD}(\widetilde{X} \dashrightarrow X).$$

(4) *If the rational map $\widetilde{X} \dashrightarrow X$ is birational over k to $\widetilde{Y} \dashrightarrow Y$; that is, if*

$$\begin{tikzcd} \widetilde{X} \arrow[r, dashed, "\simeq"] \arrow[d, dashed] & \widetilde{Y} \arrow[d, dashed] \\ X \arrow[r, dashed, "\simeq"] & Y \end{tikzcd}$$

for some birational horizontal maps, then

$$\mathrm{RD}(\widetilde{X} \dashrightarrow X) = \mathrm{RD}(\widetilde{Y} \dashrightarrow Y).$$

Proof. The first statement is immediate from the definitions. The second, third and fourth statements follow from base change: e.g., given a tower solving $\widetilde{X} \dashrightarrow X$ over k, by base change we obtain an analogous tower over k' solving $\widetilde{X} \times_k k' \dashrightarrow X \times_k k'$. This shows that any upper bound for towers over k immediately gives one over k' as well. The argument for the third and fourth is analogous. $\square$

Many natural branched covers are reducible; indeed such covers arise in Cardano's solution to the cubic; these components are responsible for so-called "parasitic roots" in the solution. The following lemma allows us to reduce the study of RD to irreducible components.

Lemma 2.6 (Irreducible components). *Let $\widetilde{X} \dashrightarrow X$ be a rational cover. Let $\{X_i \subset X\}$ be the set of irreducible components of X, and let $\{\widetilde{X}_{i,j} \subset \widetilde{X}|_{X_i}\}$ be the set of irreducible components of $\widetilde{X}|_{X_i} \dashrightarrow X_i$. Then*

$$\mathrm{RD}(\widetilde{X} \dashrightarrow X) = \max_{i,j}\{\mathrm{RD}(\widetilde{X}_{i,j} \dashrightarrow X_i)\}.$$

Proof. From the definition of resolvent degree, if $X = \coprod_i X_i$, then

$$\mathrm{RD}(\widetilde{X} \dashrightarrow X) = \max_i\{\mathrm{RD}(\widetilde{X}|_{X_i} \dashrightarrow X_i)\}.$$

Let $X = \bigcup X_i$, and let $X^\sigma = \bigcup_{i \neq j} X_i \cap X_j$ be the set of points contained in more than one irreducible component. Then $X - X^\sigma$ is a disjoint union of irreducible components, and $X - X^\sigma$ is birationally equivalent to X. Because resolvent degree is a birational invariant (Lemma 2.5), it suffices to assume that X is irreducible, and that $\widetilde{X} = \coprod_i \widetilde{X}_i$.

The inequality

$$\mathrm{RD}(\widetilde{X} \dashrightarrow X) \leq \max_i\{\mathrm{RD}(\widetilde{X}_i \dashrightarrow X)\}$$

is clear. Indeed, given a tower solving $\widetilde{X}_i \dashrightarrow X$ for each i, we construct a tower solving $\widetilde{X} \dashrightarrow X$ as follows, first if r is the length of the longest tower solving one of the $\widetilde{X}_i \dashrightarrow X$, we extend all the other towers (for $j \neq i$) to towers of length r by adding identity maps after the final stage. Next, we form a tower over X whose ℓ^{th} stage is the disjoint union of the ℓ^{th} stages of the towers for the $\widetilde{X}_i$s. By construction, each stage of this tower is pulled back from something of dimension at most $\max_i\{\mathrm{RD}(\widetilde{X}_i \dashrightarrow X)\}$. It remains to show that

$$\mathrm{RD}(\widetilde{X} \dashrightarrow X) \geq \mathrm{RD}(\widetilde{X}_i \dashrightarrow X)$$

for any i. This follows from a standard argument in covering space theory (equivalently the étale fundamental group). Without loss of generality, take $i = 1$.

A simple induction reduces us to the case where $\widetilde{X}$ is the disjoint union of two irreducible components. Write $\widetilde{X} = \widetilde{X}_1 \coprod \widetilde{X}_2$. Shrinking X as necessary, we can further assume that X and $\widetilde{X}$ are regular (since, here and throughout this paper, we work in characteristic 0). Suppose now that we have a tower of rational covers

$$Y_r \dashrightarrow \cdots \dashrightarrow Y_0 = X$$

solving $\widetilde{X} \dashrightarrow X$ in functions of at most d variables. Let $U_i \subset Y_i$ be smooth dense opens such that we have a tower of regular étale maps

$$U_r \to \cdots \to U_0 \subset X,$$

a dominant regular map $p\colon U_r \to \widetilde{X}$, and for each i, a pullback diagram

$$\begin{tikzcd} U_i \arrow[r] \arrow[d] & \tilde{Z}_i \arrow[d] \\ U_{i-1} \arrow[r] & Z_i \end{tikzcd}$$

where $\dim Z_i \leq d$. Let $U_{r,i}$ be the union of irreducible components mapping dominantly onto $\widetilde{X}_i$. Let s be the greatest integer for which U_s is irreducible (note that by assumption, $U_0 \subset X$ is irreducible). We induct on $r - s$. For the base, $r - s = 1$, we have a pullback diagram

$$\begin{tikzcd} U_r \arrow[r] \arrow[d] & \tilde{Z}_r \arrow[d] \\ U_{r-1} \arrow[r] & Z_r \end{tikzcd}$$

where U_{r-1} is irreducible, and without loss of generality Z_r is too. If the branched cover $\tilde{Z}_r$ can be partitioned as $\tilde{Z}_{r,i}$ with $U_{r,i} \cong U_{r-1} \times_{Z_r} \tilde{Z}_{r,i}$, then, by replacing U_r with $U_{r,1}$, we obtain a tower solving $\widetilde{X}_1$ in the same number of variables as the tower solving $\widetilde{X}$. Suppose therefore that $\tilde{Z}_r$ is connected. Therefore, the connected generically étale map $\tilde{Z}_r \to Z_r$ splits when pulled back along $U_{r-1} \to Z_r$. Equivalently, fixing a geometric point $\Omega \to U_{r-1} \to Z_r$, the image

$$\pi_1^{et}(U_{r-1}, \Omega) \to \pi_1^{et}(Z_r, \Omega) \to \mathrm{Perm}(\tilde{Z}_r|_\Omega)$$

lies in a subgroup of the form $\mathrm{Perm}(A_1) \times \mathrm{Perm}(A_2) \subset \mathrm{Perm}(\tilde{Z}_r|_\Omega)$. Let $H \subset \pi_1^{et}(Z_r, \Omega)$ be the pre-image of $\mathrm{Perm}(A_1) \times \mathrm{Perm}(A_2)$, and let

$$\tilde{Z}_H \to Z_r$$

denote the corresponding étale map. Because $\pi_1^{et}(U_{r-1}, \Omega)$ factors through the inclusion $H \subset \pi_1^{et}(Z_r, \Omega)$, the map $U_{r-1} \to Z_r$ factors through $\tilde{Z}_H$. By construction, the pullback $\tilde{Z}_r \times_{Z_r} \tilde{Z}_H$ splits as

$$(\tilde{Z}_r \times_{Z_r} \tilde{Z}_H)_1 \coprod (\tilde{Z}_r \times_{Z_r} \tilde{Z}_H)_2$$

with $(\tilde{Z}_r \times_{Z_r} \tilde{Z}_H)_i \times_{Z_H} U_{r-1} \cong U_{r,i}$. Because $\dim(Z_H) = \dim(Z_r)$, we have reduced to the case where the cover $\tilde{Z}_r \to Z_r$ is disconnected, and thus have exhibited a tower solving $\widetilde{X}_1 \to X$ with the same bounds as the tower solving $\widetilde{X} \to X$. This completes the base of the induction. The inductive step follows from the same construction. If $r - s > 1$, then applying the above construction in sequence, we obtain a tower

$$U_r' \to \cdots U_{s+1}' \to U_s' = U_s \to \cdots \to U_0 \subset X$$

solving $\widetilde{X}_1 \to X$, which agrees with the tower solving $\widetilde{X} \to X$ for $i \leq s$, and in which $U_i' \to U_{i-1}'$ for $i > s$ is pulled back from a variety of the same dimension which $U_i \to U_{i-1}$ is. We conclude that $\mathrm{RD}(\widetilde{X} \dashrightarrow X) \geq \mathrm{RD}(\widetilde{X}_1 \dashrightarrow X)$. $\square$

Proof of Proposition 2.4. The inequality $\mathrm{RD}(\widetilde{X} \dashrightarrow X) \geq \mathrm{RD}(k(\widetilde{X})/k(X))$ follows from pulling back any tower solving $\widetilde{X} \dashrightarrow X$ along the map $Spec(k(X)) \to X$, and then applying Lemma 2.6.

For the reverse inequality, let

$$k(X) = L_0 \hookrightarrow L_1 \hookrightarrow \cdots \hookrightarrow L_r$$

be any tower solving $k(\widetilde{X})/k(X)$. For each i, pick varieties Y_i, Z_i and $\tilde{Z}_i$ such that $k(Y_i) = L_i$, $k(Z_i) = F_i$ and $k(\tilde{Z}_i) = \tilde{F}_i$ respectively. Then we obtain a tower of rational covers

$$Y_r \dashrightarrow \cdots \dashrightarrow Y_1 \dashrightarrow Y_0 = X$$

such that $Y_r \dashrightarrow X$ factors through a rational cover $Y_r \dashrightarrow \widetilde{X} \dashrightarrow X$, and such that each Y_i sits in a birational pullback diagram

$$\begin{tikzcd} Y_i \arrow[r, dashed] \arrow[d, dashed] & \tilde{Z}_i \arrow[d, dashed] \\ Y_{i-1} \arrow[r, dashed] & Z_i \end{tikzcd}$$

Because $\dim(Z_i) = \operatorname{tr.deg}(F_i)$, the upper bound on $\mathrm{RD}(k(\widetilde{X})/k(X))$ provided by the tower over $k(X)$ carries over to give an identical upper bound on $\mathrm{RD}(\widetilde{X} \dashrightarrow X)$. Taking the minimum over all such towers gives

$$\mathrm{RD}(\widetilde{X} \dashrightarrow X) \leq \mathrm{RD}\big(k(\widetilde{X})/k(X)\big)$$

as desired. $\square$

Lemma 2.7 (RD of a composition). *Let $Z \dashrightarrow Y \dashrightarrow X$ be a pair of rational covers of k-varieties. Then*

$$\mathrm{RD}(Z \dashrightarrow X) = \max\big\{\mathrm{RD}(Z \dashrightarrow Y), \mathrm{RD}(Y \dashrightarrow X)\big\}.$$

Proof. The definition immediately implies that $\mathrm{RD}(Z \dashrightarrow X) \leq \max\{\mathrm{RD}(Z \dashrightarrow Y), \mathrm{RD}(Y \dashrightarrow X)\}$ and $\mathrm{RD}(Z \dashrightarrow X) \geq \mathrm{RD}(Y \dashrightarrow X)$. To see that $\mathrm{RD}(Z \dashrightarrow X) \geq \mathrm{RD}(Z \dashrightarrow Y)$, note that

$$\mathrm{RD}(Z \dashrightarrow X) \geq \mathrm{RD}(Z \times_X Y \dashrightarrow Y)$$

and, because $Z \dashrightarrow Y$ embeds as a collection of components of $Z \times_X Y \dashrightarrow Y$, Lemma 2.6 implies

$$\mathrm{RD}(Z \times_X Y \dashrightarrow Y) \geq \mathrm{RD}(Z \dashrightarrow Y).$$

□

Definition 2.8. A rational cover $\widetilde{X} \dashrightarrow X$ is *generically n-to-1* if $n = [k(X_i) : \mathcal{O}(\widetilde{X}|_{Spec(k(X_i))})]$ for each irreducible component $X_i \subset X$.

While the resolvent degree $\mathrm{RD}(\widetilde{\mathcal{P}}_n \to \mathcal{P}_n)$ of the root cover of the space of degree n polynomials is a specific example, it is universal in the following sense.

Lemma 2.9 (Universality of $\widetilde{\mathcal{P}}_n \to \mathcal{P}_n$). *Let $\widetilde{X} \dashrightarrow X$ be a generically n-to-1 rational cover. Then*

$$\mathrm{RD}(\widetilde{X} \dashrightarrow X) \leq \mathrm{RD}(\widetilde{\mathcal{P}}_n \to \mathcal{P}_n).$$

Proof. By the Theorem of the Primitive Element (using that we are in characteristic 0), there exists $\alpha \in k(\widetilde{X})$ such that

$$k(\widetilde{X}) \cong k(X)(\alpha) \cong k(X)[z]/p_\alpha(z)$$

where

$$p_\alpha(z) = z^n + a_1 z^{n-1} + \cdots + a_n$$

is a minimal polynomial for α. Let $U \subset X$ denote the largest Zariski open for which all the coefficients $a_i \in k(X)$ are regular functions. The polynomial p_α determines a map

$$\begin{aligned} U &\to^{p_\alpha} \mathcal{P}_n \\ u &\mapsto \big(a_1(u), \ldots, a_n(u)\big) \end{aligned}$$

and this map determines a pullback square

$$\begin{tikzcd} \widetilde{X}|_U \arrow[r] \arrow[d] & \widetilde{\mathcal{P}}_n \arrow[d] \\ U \arrow[r, "p_\alpha"] & \mathcal{P}_n \end{tikzcd}$$

Therefore, by Lemma 2.5,

$$\mathrm{RD}(\widetilde{X} \dashrightarrow X) = \mathrm{RD}(\widetilde{X}|_U \to U) \leq \mathrm{RD}(\widetilde{\mathcal{P}}_n \to \mathcal{P}_n). \qquad \square$$

This universal property will show up in many of the examples and computations below.

2.3. Galois closures and resolvent degree. In this subsection we will relate the resolvent degree of L/K with the resolvent degree of various related extensions, for example the Galois closure of L over K. This often will allow us in practice to reduce to the case of Galois covers.

Definition 2.10 (Galois theory terminology for rational covers). Let $\widetilde{X} \dashrightarrow X$ be a rational cover of k-varieties.

(1) If $\widetilde{X}$ is irreducible, then the map $\widetilde{X} \dashrightarrow X$ is *Galois* if the associated extension of function fields $k(X) \hookrightarrow k(\widetilde{X})$ is Galois. We write $\mathrm{Gal}(\widetilde{X} \dashrightarrow X)$ for the Galois group of the associated extension of function fields.

(2) If $\widetilde{X}$ is irreducible, we say that a map $\widetilde{X}' \dashrightarrow X$ is a *Galois closure* of $\widetilde{X} \dashrightarrow X$ if it factors as $\widetilde{X}' \dashrightarrow \widetilde{X} \dashrightarrow X$ and if $k(X) \hookrightarrow k(\widetilde{X}')$ is a Galois closure of $k(X) \hookrightarrow k(\widetilde{X})$.

(3) Given $Z \dashrightarrow Y \dashrightarrow X$ irreducible, with $Z \dashrightarrow X$ Galois, the *Galois closure* of $Y \dashrightarrow X$ in $Z \dashrightarrow X$ is any integral model of the Galois closure of $k(X) \hookrightarrow k(Y)$ in $k(Z)$.

(4) If $\widetilde{X}$ is reducible, we say $\widetilde{X} \dashrightarrow X$ is *Galois* if the restriction of the map to each irreducible component of $\widetilde{X}$ is Galois. Similarly, we say $\widetilde{X}' \dashrightarrow X$ is a *Galois closure* of $\widetilde{X} \dashrightarrow X$ if there is a bijection between the set of irreducible components of $\widetilde{X}'$ and of $\widetilde{X}$ such that the restriction of the map $\widetilde{X}' \dashrightarrow X$ realizes each component of $\widetilde{X}'$ as a Galois closure of the corresponding component of $\widetilde{X}$. Given $Z \dashrightarrow Y \dashrightarrow X$ with Z Galois, a *Galois closure* of Y in $Z \dashrightarrow X$ is union of Galois closures of the components of Y.

The following lemma will allow us to pass to Galois closures when computing RD. The analogous lemma for ed is Lemma 2.3 of [BR1].

Lemma 2.11 (RD is preserved under Galois closure). *Let $\widetilde{X} \dashrightarrow X$ be a rational cover of k-varieties. Let $\widetilde{X}' \dashrightarrow X$ be a Galois closure of $\widetilde{X}$. Then*

$$\mathrm{RD}(\widetilde{X} \dashrightarrow X) = \mathrm{RD}(\widetilde{X}' \dashrightarrow X).$$

Proof. By Lemma 2.6, it suffices to prove this in the case where $\widetilde{X}$ is irreducible. For this, we induct on the degree of the map $\widetilde{X} \dashrightarrow X$. For the base case, $n = 2$, every quadratic extension (in characteristic 0) is already Galois, so the lemma holds trivially.

For the induction step, assume the lemma holds for all rational covers of k-varieties of degree less than n.

Let $\widetilde{X} \dashrightarrow X$ be a rational cover of degree n. Consider the composition

$$\widetilde{X} \times_X \widetilde{X} \dashrightarrow \widetilde{X} \dashrightarrow X$$

The fiber product $\widetilde{X} \times_X \widetilde{X}$ splits as $\widetilde{X} \coprod \widetilde{X}_1$ (at the level of function fields, this follows from the Primitive Element Theorem), where $\widetilde{X} \to \widetilde{X}$ is the identity, and $\widetilde{X}_1 \dashrightarrow \widetilde{X}$ is a rational cover of degree $n-1$. By the inductive hypothesis,

$$\mathrm{RD}(\widetilde{X}'_1 \dashrightarrow \widetilde{X}) = \mathrm{RD}(\widetilde{X}_1 \dashrightarrow \widetilde{X})$$

for any Galois closure $\widetilde{X}'_1 \dashrightarrow \widetilde{X}$ of $\widetilde{X}_1 \dashrightarrow \widetilde{X}$. By Lemma 2.6,

$$\mathrm{RD}(\widetilde{X}_1 \dashrightarrow \widetilde{X}) \leq \mathrm{RD}(\widetilde{X} \dashrightarrow X).$$

Therefore, by Lemma 2.7,

$$\mathrm{RD}(\widetilde{X}'_1 \dashrightarrow X) = \max\{\mathrm{RD}(\widetilde{X}_1 \dashrightarrow \widetilde{X}), \mathrm{RD}(\widetilde{X} \dashrightarrow X)\} = \mathrm{RD}(\widetilde{X} \dashrightarrow X).$$

But, by construction, we see that $\widetilde{X}'_1 \dashrightarrow X$ is a Galois closure of $\widetilde{X} \dashrightarrow X$, and this completes the induction step. □

2.4. Accessory irrationalities. We now give two results about resolvent degree of field extensions; we defer stating the corresponding results for rational covers of k-varieties to below. We adopt this presentation to make use of constructions such as compositum and intersection of subfields which are easier to state in the setting of field extensions than for covering spaces, where they correspond to greatest lower bounds and least upper bounds in a lattice of covering spaces.

The following allows one to pass to towers of Galois covers when analyzing RD.

Lemma 2.12 (Improving towers). *Let $K \hookrightarrow L$ be a finite extension of k-fields. Then without loss of generality, in any tower realizing* $\mathrm{RD}(L/K)$*, we can assume that the extension at each stage is Galois. More precisely, for any $d > 0$ (e.g., $d = \mathrm{RD}(L/K)$), let*

$$K = K_0 \hookrightarrow K_1 \hookrightarrow \cdots \hookrightarrow K_r$$

be any sequence of extensions with $L \hookrightarrow K_r$ *(as fields over* K*) and such that* $\mathrm{ed}(K_i/K_{i-1}) \leq d$ *for all* i*. Then there exists a diagram of sequences of extensions*

(2.1)
$$\begin{tikzcd}
K \arrow[r, hook] \arrow[d, equal] & K_1 \arrow[r, hook] \arrow[d, hook] & K_2 \arrow[r, hook] \arrow[d, hook] & \cdots \arrow[r, hook] & K_r \arrow[d, hook] \\
K \arrow[r, hook] \arrow[d, equal] & K_1' \arrow[r, hook] \arrow[d, equal] & K_2' \arrow[r, hook] \arrow[d, hook] & \cdots \arrow[r, hook] & K_r' \arrow[d, hook] \\
K \arrow[r, hook] & \tilde{K}_1 \arrow[r, hook] & \tilde{K}_2 \arrow[r, hook] & \cdots \arrow[r, hook] & \tilde{K}_r
\end{tikzcd}$$

such that for all i*,*

(1) K_i' *is Galois over* K_{i-1}'*,*

(2) $\tilde{K}_i$ *is a Galois closure of* K_i *over* K*,*

(3) $\mathrm{ed}(K_i'/K_{i-1}') \leq d$ *for all* i*, and*

(4) $\mathrm{RD}(\tilde{K}_i/K) = \mathrm{RD}(K_i/K) \leq d$ *for all* i*.*

Proof. Because we work in characteristic 0, all extensions are separable. Therefore, for the bottom row of (2.1), define $\tilde{K}_r$ to be a Galois closure of K_r over K, and for $i < r$, let $\tilde{K}_i$ denote the Galois closure over K of K_i in $\tilde{K}_r$. Lemma 2.11 implies that

$$\mathrm{RD}(\tilde{K}_i/K) \leq \mathrm{RD}(K_i/K) \leq d.$$

To construct the middle row, we prove by induction that for any $1 \leq j \leq r$ there exists a diagram of sequences of extensions of the form (2.1) in which $\mathrm{ed}(K_i'/K_{i-1}') \leq \mathrm{ed}(K_i/K_{i-1})$ for all i, and in which K_i' is Galois over K_{i-1}' for $i \leq j$. For the base case $j = 1$, let $K_1' = \tilde{K}_1$. This is Galois over K_0. For the induction step, suppose that we have defined K_j' for $j \leq i$. Define K_{i+1}' to be the Galois closure (in $\tilde{K}_r$) of the compositum (in $\tilde{K}_r$) of K_{i+1} with K_i' over K_i. Then the definition of essential dimension and [BR1, Lemma 2.3] imply that

$$\mathrm{ed}(K_{i+1}'/K_i') \leq \mathrm{ed}(K_{i+1}/K_i)$$

as required to complete the induction step. □

The following proposition is quite useful when analyzing the resolvent degree of G-covers (and their subcovers) for G simple. In particular, it shows that a general solution can always be put into a reduced form where the monodromy of the original rational cover occurs precisely at the last stage.

Proposition 2.13 (Accessory irrationalities). *Let G be a finite simple group. Let $K \hookrightarrow L$ be a Galois extension of k-fields with* $\mathrm{Gal}(L/K) = G$. *Fix $d \geq 0$. Let*

$$K = K_0 \hookrightarrow K_1 \hookrightarrow \cdots \hookrightarrow K_r \tag{2.2}$$

be a sequence of extensions such that

(1) $\mathrm{ed}(K_i/K_{i-1}) \leq d$ *for all i, and*

(2) $L \hookrightarrow K_r$ *as fields over K.*

Then, there exists $s < r$ and a modified tower

$$K = K_0 \hookrightarrow K_1 \hookrightarrow \cdots \hookrightarrow K_s \hookrightarrow K_s'$$

such that

(1) *K_s' is a subfield of the Galois closure of K_{s+1} over K_s,*

(2) $\mathrm{ed}(K_s'/K_s) \leq \mathrm{ed}(K_{s+1}/K_s) \leq d$,

(3) *$L \hookrightarrow K_s'$ as K-fields, and under this embedding, $K_s \otimes_K L \to^{\cong} K_s'$.*

Proof. Define s to be the maximum i such that the absolute Galois group of K_i surjects onto G, i.e.

$$s := \max\{i \mid \mathrm{Gal}(\overline{K}/K_i) \twoheadrightarrow G\}.$$

Let $\tilde{K}_{s+1}$ denote the Galois closure of K_{s+1} over K_s. Then

$$\mathrm{Gal}(\overline{K}/\tilde{K}_{s+1}) \trianglelefteq \mathrm{Gal}(\overline{K}/K_s)$$

and, by Lemma 2.11

$$\mathrm{ed}(\tilde{K}_{s+1}/K_s) = \mathrm{ed}(K_{s+1}/K_s).$$

Because $\mathrm{Gal}(\overline{K}/K_s) \twoheadrightarrow G$ is a surjection, it must take $\mathrm{Gal}(\overline{K}/\tilde{K}_{s+1})$ to a normal subgroup of G. By the definition of s, $\mathrm{Gal}(\overline{K}/\tilde{K}_{s+1}) \subset \mathrm{Gal}(\overline{K}/K_{s+1})$ does not surject onto G. Therefore, because G is simple, $\mathrm{Gal}(\overline{K}/\tilde{K}_{s+1})$ must be in the kernel of the map to G. This implies that L is contained in $\tilde{K}_{s+1}$, because

$$L = \overline{K}^{\mathrm{Gal}(\overline{K}/L)} = \overline{K}^{\ker(\mathrm{Gal}(\overline{K}/K) \to G)} \subset \overline{K}^{\mathrm{Gal}(\overline{K}/\tilde{K}_{s+1})} = \tilde{K}_{s+1}.$$

Therefore, we have $L \hookrightarrow \tilde{K}_{s+1}$ but L is not contained in K_s. Define

$$N := \ker\big(\mathrm{Gal}(\tilde{K}_{s+1}/K_s) \twoheadrightarrow G\big).$$

Define

$$K_{s'} := (\tilde{K}_{s+1})^N.$$

Observe that $\mathrm{ed}(K_{s'}/K_s) \leq \mathrm{ed}(K_{s+1}/K_s) = \mathrm{ed}(\tilde{K}_{s+1}/K_s)$, because if $\tilde{K}_{s+1} = K_s \otimes_F \tilde{F}$, then $K_{s'} := K_s \otimes_F \tilde{F}^N$. Finally, because $\mathrm{Gal}(\overline{K}/K_s)$ surjects onto $G = \mathrm{Gal}(L/K)$, we conclude that

$$K_{s'} = K_s \otimes_K L. \qquad \square$$

Corollary 2.14. *Let G be a finite simple group. Let L/K be any finite extension of k-fields for which the Galois closure has Galois group G. Then* $\mathrm{RD}(L/K)$ *equals the minimal d for which there exists a tower*

$$K = K_0 \hookrightarrow K_1 \hookrightarrow \cdots \hookrightarrow K_{r-1} \hookrightarrow K_r$$

for which

(1) $\mathrm{ed}(K_i/K_{i-1}) \le d$, *and*

(2) $K_r \cong K_{r-1} \otimes_K L$.

Proof. For any tower solving the Galois closure $\tilde{L}$ of L over K, we can apply Proposition 2.13. Let $H \subset G$ be the subgroup such that $L = \tilde{L}^H$. Applying Proposition 2.13 and Lemma 2.11, $\mathrm{RD}(L/K)$ is the minimal d for which there exists a tower

$$K = K_0 \hookrightarrow K_1 \hookrightarrow \cdots \hookrightarrow K_{r-1} \hookrightarrow K_r$$

for which

(1) $\mathrm{ed}(K_i/K_{i-1}) \le d$, and

(2) $K_r \cong K_{r-1} \otimes_K \tilde{L}$.

Replacing K_r by $K_r^H \cong K_{r-1} \otimes_K L$, we obtain a tower of the desired form. □

Remark 2.15. An *accessory irrationality* to a rational cover $\tilde{X} \dashrightarrow X$ is any rational cover $E \dashrightarrow X$ which does not factor through $\tilde{X}$. If $\mathrm{RD}(L/K) \neq \mathrm{ed}(L/K)$, then accessory irrationalities are intrinsic features of any solution of L/K in $d < \mathrm{ed}(L/K)$ variables. The notion of accessory irrationality first appeared in work of Kronecker and received intensive study in Klein's lectures on the icosahedron [Kle2] (see also the appendix to [DM]). In particular, Klein proved that

$$\mathrm{ed}(\widetilde{\mathcal{P}}_5 \to \mathcal{P}_5) = 2 \neq \mathrm{RD}(\widetilde{\mathcal{P}}_5 \to \mathcal{P}_5) = 1$$

and thus that accessory irrationalities are an inescapable feature of solutions of the quintic in one variable.

Question 2.16. Let $K \hookrightarrow L$ be a finite extension of k-fields. Among towers solving L/K in the minimal number of variables, can we always find one in which the stages of the tower have monotone increasing essential dimension?

The geometric statement of Lemma 2.12 is the following.

Corollary 2.17 (Improving towers, geometric version). *Let* $\widetilde{X} \dashrightarrow X$ *be a rational cover. Then without loss of generality, in any tower solving* $\widetilde{X} \dashrightarrow X$ *in* d *variables, we can assume that the map at each stage is Galois. More precisely, for any* $d > 0$ *(e.g.,* $d = \mathrm{RD}(\widetilde{X} \dashrightarrow X)$*), let*

$$Y_r \dashrightarrow \cdots \dashrightarrow Y_1 \dashrightarrow Y_0 = X$$

be a tower of rational covers with $Y_r \dashrightarrow X$ *factoring through* $\widetilde{X}$ *and such that for all* i*,* $Y_i \dashrightarrow Y_{i-1}$ *is pulled back from a rational cover of varieties of dimension at most* d*. Then there exists a diagram of sequences of rational covers*

$$\begin{tikzcd} \tilde{Y}_r \arrow[r, dashed] \arrow[d, dashed] & \cdots \arrow[r, dashed] & \tilde{Y}_2 \arrow[r, dashed] \arrow[d] & \tilde{Y}_1 \arrow[r, dashed] \arrow[d, equal] & X \arrow[d, equal] \\ Y'_r \arrow[r, dashed] \arrow[d, dashed] & \cdots \arrow[r, dashed] & Y'_2 \arrow[r, dashed] \arrow[d, dashed] & Y'_1 \arrow[r, dashed] \arrow[d, dashed] & X \arrow[d, equal] \\ Y_r \arrow[r, dashed] & \cdots \arrow[r, dashed] & Y_2 \arrow[r, dashed] & Y_1 \arrow[r, dashed] & X \end{tikzcd} \tag{2.3}$$

such that for all i*,*

(1) $Y'_i \dashrightarrow Y'_{i-1}$ *is Galois,*

(2) $\tilde{Y}_i \dashrightarrow X$ *is a Galois closure of* $Y_i \dashrightarrow X$*,*

(3) $\mathrm{ed}(Y'_i \dashrightarrow Y'_{i-1}) \leq d$*, and*

(4) $\mathrm{RD}(\tilde{Y}_i \dashrightarrow X) = \mathrm{RD}(Y_i \dashrightarrow X) \leq d$*.*

The geometric statement of Proposition 2.13 is the following.

Corollary 2.18 (Geometric accessory irrationalities). *Let* G *be a finite simple group. Let* $\widetilde{X} \dashrightarrow X$ *be a rational cover for which the Galois closure has Galois group* G*. Then* $\mathrm{RD}(\widetilde{X} \dashrightarrow X)$ *equals the minimal* d *for which there exists a tower*

$$Y_r \dashrightarrow \cdots \dashrightarrow Y_1 \dashrightarrow Y_0 = X$$

for which

(1) $Y_r \cong Y_{r-1} \times_X \widetilde{X}$*, and*

(2) *for each* i*,* $Y_{i+1} \dashrightarrow Y_i$ *is pulled back from a map of varieties of dimension at most* d*, i.e. there is a rational pullback square with* $\dim_k(Z_i) \leq d$

$$\begin{tikzcd} Y_{i+1} \arrow[r, dashed] \arrow[d, dashed] & \widetilde{Z}_i \arrow[d, dashed] \\ Y_i \arrow[r, dashed] & Z_i \end{tikzcd}$$

3. The resolvent degree of a finite group

In this section we define the resolvent degree $\mathrm{RD}(G)$ of a finite group G. This intrinsic invariant of G gives a uniform upper bound on the complexity of all G-covers of all varieties. Just as with the theory of essential dimension from which it was inspired, $\mathrm{RD}(G)$ will be quite useful.

3.1. Definition and basic properties. Throughout this section we fix a ground field k of characteristic 0. We will consider finite groups G with G-actions by automorphisms on varieties X, so that X/G is a variety. We say that a G-variety X is *primitive* if G acts transitively on the set of irreducible components of X. We say that X is *faithful* if the representation $G \to Aut(X)$ is injective.

Definition 3.1 (Resolvent degree of a finite group). Let G be a finite group. The *resolvent degree* $\mathrm{RD}(G)$ of G is defined to be

$$\mathrm{RD}(G) := \sup\{\mathrm{RD}(X \to X/G) : X \text{ is a primitive, faithful } G\text{-variety over } k\}.$$

While $\mathrm{RD}(G)$ gives a universal upper bound on any $\mathrm{RD}(X \to X/G)$, it does not in general provide any lower bound on any particular G-cover; see below. On the other hand we will prove that $\mathrm{RD}(G) = \mathrm{RD}(V \to V/G)$ for any faithful linear G-variety V, and more generally for any "versal" G-variety. Replacing RD by ed in Definition 3.1 gives the definition of Buhler–Reichstein [BR1] for the essential dimension of a finite group. Indeed, the two invariants of G-varieties compare as follows.

Lemma 3.2. *Let G be any finite group. Then*

$$\mathrm{RD}(G) \le \mathrm{ed}(G) < \infty.$$

Proof. For any rational cover $X \dashrightarrow Y$ we have by definition $\mathrm{RD}(X \dashrightarrow Y) \le \mathrm{ed}(X \dashrightarrow Y)$. In particular, if X is any faithful G-variety then

$$\begin{aligned} \mathrm{RD}(X \to X/G) &\le \mathrm{ed}(X \to X/G) \\ &\le \mathrm{ed}(\mathbb{A}^G \to \mathbb{A}^G/G) \qquad \text{(by Theorem 3.1 of [BR1])} \\ &= \mathrm{ed}(G) < \infty \end{aligned}$$

where $\mathbb{A}^G$ denotes the regular representation of G viewed as a faithful linear G-variety. □

Theorem 3.3. *Let G be a finite group, and let $\{G_i\}_{i=1}^n$ denote the set of simple factors in its Jordan–Hölder decomposition. Then*

$$\mathrm{RD}(G) \le \max_{1 \le i \le n} \{\mathrm{RD}(G_i)\}.$$

Moreover, if $G_i \hookrightarrow G$ *for all* i, *then*

$$\mathrm{RD}(G) = \max_{1\le i\le n}\{\mathrm{RD}(G_i)\}.$$

The analogue of Theorem 3.3 for essential dimension is false, even in simple examples: take $G_1 = G_2 = \mathbb{Z}/2\mathbb{Z}$ and $G = G_1 \times G_2$. Note too that $\mathrm{ed}(G/H)$ can be much larger than $\mathrm{ed}(G)$ for normal subgroups $H \lhd G$; see Theorem 1.5 of [MR]. We do not know if the hypothesis in Theorem 3.3 that $G_i \subseteq G$ for all i is necessary.

Proof. If $G_i \hookrightarrow G$ for all i, then by Lemma 3.13 below, $\mathrm{RD}(G) \geq \max_i\{\mathrm{RD}(G_i)\}$. To show the opposite inequality in general, we induct on the number of simple factors (with multiplicity). For the base of the induction $n = 1$, there is nothing to show. Assume therefore that we have shown it for $n-1$. Let

$$0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_n = G$$

be a composition series for G with $H_i/H_{i-1} = G_i$. Let X be a primitive faithful G-variety.

The map $X \to X/G$ factors as

$$X \to X/H_{n-1} \to X/G.$$

If X is not primitive as an H_{n-1}-variety, then the set of H_{n-1}-orbits on the set of irreducible components of X partitions X into a union of primitive H_{n-1}-varieties. Moreover, because the G-action is primitive and $H_{n-1} \trianglelefteq G$, the union of the H_{n-1}-quotients is a primitive $G_n = G/H_{n-1}$-variety. Lemma 2.6 implies that

$$\mathrm{RD}(X \to X/H_{n-1}) = \max_j\{\mathrm{RD}(X_j \to X_j/H_{n-1})\}$$

where the maximum is taken over the set of primitive H_{n-1}-varieties in the above partition of X. In particular,

$$\mathrm{RD}(H_{n-1}) \geq \mathrm{RD}(X \to X/H_{n-1}).$$

Therefore

$$\begin{aligned} \max\{\mathrm{RD}(G_n), \mathrm{RD}(H_{n-1})\} &\geq \max\{\mathrm{RD}(X \to X/H_{n-1}), \mathrm{RD}(X/H_{n-1} \to X/G)\} \\ \text{(by Lemma 2.7)} \qquad &= \mathrm{RD}(X \to X/G) \end{aligned}$$

Passing to the supremum and invoking the induction hypothesis, we obtain the desired inequality

$$\max_{1\le i\le n}\{\mathrm{RD}(G_i)\} \geq \mathrm{RD}(G). \qquad \square$$

As a simple application of Theorem 3.3, we have the following.

Corollary 3.4. *Let G be an "almost solvable" group, i.e. a group whose simple factors are cyclic or A_5. Then* $\mathrm{RD}(G) = 1$.

Proof. By Theorem 3.3,

$$\mathrm{RD}(G) \leq \max\big\{\{\mathrm{RD}(\mathbb{Z}/n\mathbb{Z})\}_{n\in\mathbb{N}}, \mathrm{RD}(A_5)\big\}.$$

Because G is nontrivial, there exists a faithful, geometrically connected G-variety X of dimension ≥ 1. Because X is geometrically connected, there is no faithful G-equivariant rational map $X \dashrightarrow Z$ for Z any faithful 0-dimensional G-variety. We conclude that $\mathrm{RD}(G) \geq 1$.

By Bring's bound and item 1 of Corollary 3.17 1 below,

$$1 = \mathrm{RD}(\widetilde{\mathcal{P}}_5 \to \mathcal{P}_5) = \mathrm{RD}(S_5) = \mathrm{RD}(A_5)$$

where the last equality follows from Theorem 3.3. The result now follows from the equality

$$\mathrm{RD}(\mathbb{Z}/n\mathbb{Z}) = 1 \quad \text{for all } n \geq 2$$

which follows from the classical fact that any characteristic 0 field extension with solvable Galois group is solvable in radicals. □

Corollary 3.4 follows from the primary cases of simple groups where RD is currently known exactly (i.e., cyclic groups and A_5).[9] In general, we have at best upper bounds, e.g., $\mathrm{RD}(A_6) \leq 2$ and $\mathrm{RD}(A_7) \leq 3$. Theorem 3.3 indicates the importance of computing the resolvent degree of finite groups.

Problem 3.5 ($\mathrm{RD}(G)$ for G finite simple). Compute the resolvent degree of all finite simple groups G.

3.2. Versal G-varieties. It is useful to have a model (not always unique) G-variety to which all other G-varieties can be compared. Such varieties, called "versal G-varieties", play a crucial role in the theory of essential dimension. After recalling the definition (cf. [DR1]) and some variations that arise naturally when studying resolvent degree, we give some examples.

Definition 3.6 (Versal G-variety). A faithful G-variety X is *versal* if for every G-invariant Zariski open $U \subset X$ and every faithful G-variety Y, there exists a G-equivariant rational map $Y \dashrightarrow U$.

[9] Klein also proved that $\mathrm{RD}(\mathrm{PSL}_2(\mathbb{F}_7) = 1)$. See [FKW, Proposition 4.2.4] for a contemporary treatment.

Our interest in versality comes from the following.

Proposition 3.7. *Let X be a versal G-variety. Then*

(1) $\mathrm{ed}(X \to X/G) = \mathrm{ed}(G)$.

(2) $\mathrm{RD}(X \to X/G) = \mathrm{RD}(G)$.

Proof. The proof for essential dimension is standard; we recall it here as we will use it. Let X be a versal G-variety. Recall that $\mathrm{ed}(G) = \sup\{\mathrm{ed}(Y \to Y/G)\}$ where the supremum is over all faithful G-varieties Y. Let $U \subset X$ be a dense G-invariant Zariski open which admits a G-equivariant dominant map $U \to Z$ to a faithful G-variety Z with $\dim(Z) = \mathrm{ed}(X \to X/G)$. By the definition of versality, there exists a G-equivariant rational map $Y \dashrightarrow U$. Composing with $U \to Z$, we obtain a G-equivariant rational dominant map $Y \dashrightarrow Z$, which implies

$$\mathrm{ed}(Y \to Y/G) \leq \dim(Z) = \mathrm{ed}(X \to X/G).$$

Therefore $\mathrm{ed}(X \to X/G) = \mathrm{ed}(G)$.

We now prove the statement for resolvent degree. By definition, $\mathrm{RD}(X \to X/G) \leq \mathrm{RD}(G)$. It remains to prove that $\mathrm{RD}(X \to X/G) \geq \mathrm{RD}(Y \to Y/G)$ for any faithful G-variety Y. Let

$$\begin{tikzcd} & & & X \arrow[d] \\ X_r \arrow[rrru, dashed] \arrow[r, dashed] & \cdots \arrow[r, dashed] & X_1 \arrow[r, dashed] & X/G \end{tikzcd}$$

be a solution of $X \to X/G$. Let $\bar{U} \subset \mathrm{Image}(X_r \dashrightarrow X/G)$ be a Zariski open, and let $U \subset X$ be its pre-image under the map $X \to X/G$. By the definition of versality, there exists a G-equivariant map

$$V \to U$$

for some dense Zariski open $V \subset Y$. Since both G-varieties are faithful, this determines a pullback diagram

$$\begin{tikzcd} V \arrow[r] \arrow[d] & U \arrow[d] \\ V/G \arrow[r] & U/G \end{tikzcd}$$

and we can pull back the above solution of $X \to X/G$ to $V \to V/G$. Since every solution in d-variables of $X \to X/G$ gives rise to a solution in d-variables of $V \to V/G$, and since $V \to V/G$ is birational to $Y \to Y/G$, we conclude, from the definition, that $\mathrm{RD}(X \to X/G) \geq \mathrm{RD}(Y \to Y/G))$. $\square$

The notion of versal is stronger than we strictly need for resolvent degree.

Definition 3.8 (Solvably-versal, RD-versal). Let G be a finite group. A faithful G-variety X is:

(1) *solvably-versal* if, for every G-invariant Zariski open $U \subset X$ and any faithful G-variety Y, there exists a rational cover

$$\widetilde{Y} \dashrightarrow Y/G$$

with $k(Y/G) \hookrightarrow k(\widetilde{Y})$ a solvable extension, and a G-equivariant rational map

$$\widetilde{Y} \times_{Y/G} Y \dashrightarrow U;$$

(2) RD-*versal* if, for every G-invariant Zariski open $U \subset X$ and any faithful G-variety Y, there exists a rational cover

$$\widetilde{Y} \dashrightarrow Y/G$$

with $\mathrm{RD}(\widetilde{Y} \dashrightarrow Y/G) \leq \mathrm{RD}(X \to X/G)$ and a G-equivariant rational map

$$\widetilde{Y} \times_{Y/G} Y \dashrightarrow U.$$

Note that solvably-versal implies RD-versal; we do not know if the converse is true or not.

Example 3.9 (Klein). Klein [Kle2] proved a "Normalformsatz" for the group A_5, showing that perhaps after passing to an intermediate degree 2 cover, every A_5-cover is pulled back from the canonical A_5-cover of $\mathbb{P}^1 \to \mathbb{P}^1/A_5 \cong \mathbb{P}^1$. In our language, this shows that $\mathbb{P}^1$ with its standard A_5 action is solvably versal.

RD-versal G-varieties realize the resolvent degree of G.

Proposition 3.10. *Let G be a finite group, and let X be an* RD*-versal G-variety. Then*

$$\mathrm{RD}(X \to X/G) = \mathrm{RD}(G).$$

Proof. The proof is similar to that of Proposition 3.7. It suffices to show that $\mathrm{RD}(X \to X/G) \geq \mathrm{RD}(Y \to Y/G)$ for any faithful G-variety Y. Let

$$\begin{tikzcd}
 & & & X \arrow[d] \\
X_r \arrow[rrru, dashed] \arrow[r, dashed] & \cdots \arrow[r, dashed] & X_1 \arrow[r, dashed] & X/G
\end{tikzcd}$$

be a solution of $X \to X/G$. Let $\bar{U} \subset \mathrm{Image}(X_r \dashrightarrow X/G)$ be a Zariski open, and let $U \subset X$ be its pre-image under the map $X \to X/G$. By the definition of RD-versality, there exists a rational cover

$$\widetilde{Y} \dashrightarrow Y/G$$

with $\mathrm{RD}(\widetilde{Y} \dashrightarrow Y/G) \leq \mathrm{RD}(X \to X/G)$ and with a G-equivariant map

$$V \to U$$

for some dense Zariski open $V \subset \widetilde{Y} \times_{Y/G} Y$. Since both G-varieties are faithful, this determines a pullback diagram

$$\begin{tikzcd} V \arrow[r] \arrow[d] & U \arrow[d] \\ V/G \arrow[r] & U/G \end{tikzcd}$$

and we can pullback the above solution of $X \to X/G$ to $V \to V/G$. Since every solution in d-variables of $X \to X/G$ gives rise to a solution in d-variables of $V \to V/G$, and since $V \to V/G$ is birational to $\widetilde{Y} \times_{Y/G} Y \dashrightarrow \widetilde{Y}$, we conclude, from the definition, that $\mathrm{RD}(X \to X/G) \geq \mathrm{RD}(\widetilde{Y} \times_{Y/G} Y \dashrightarrow \widetilde{Y})$. By Lemma 2.7,

$$\begin{aligned} \mathrm{RD}(\widetilde{Y} \times_{Y/G} Y \dashrightarrow Y/G) &= \max\{\mathrm{RD}(\widetilde{Y} \times_{Y/G} Y \dashrightarrow \widetilde{Y}), \mathrm{RD}(\widetilde{Y} \dashrightarrow Y/G)\} \\ &\leq \mathrm{RD}(X \to X/G). \end{aligned}$$

□

3.3. Criteria for versality. In this section we give some basic properties of versality, as well as criteria for detecting it. To start, a G-*compression* (i.e., G-equivariant dominant rational map) of a versal G-variety is versal.

Lemma 3.11 (Compressions of versal are versal). *Let X be a faithful G-variety, and let Y be a versal G-variety. If there exists a G-equivariant dominant rational map $f : Y \dashrightarrow X$, then X is versal.*

Proof. Let $U \subset X$ be a G-invariant Zariski open, and let Z be any faithful G-variety. Then $f^{-1}(U) \subset Y$ is a G-invariant Zariski open, and by the definition of versality, there exists a G-equivariant rational map $Z \dashrightarrow f^{-1}(U)$. Composing with f, we obtain a G-equivariant rational map $Z \dashrightarrow U$ as desired. □

Versal G-varieties are also versal for subgroups.

Lemma 3.12 (Versality descends). *Let G be a finite group. If X is a versal G-variety, then X is also a versal H-variety for any subgroup $H \subseteq G$.*

Proof. By the definition of versal, we must show that for every H-invariant Zariski open $U \subset X$ and every faithful H-variety Y, there exists an H-equivariant rational map $Y \dashrightarrow U$. Given U, let $U' \subseteq U$ be the maximal G-invariant Zariski open contained in U (i.e., $U' = \bigcap_{g \in G} g \cdot U$). Consider the G-variety

$$G \times_H Y := G \times Y / \sim$$

where $\sim$ is the equivalence relation given by $(g, hy) \sim (gh, y)$, and the G-action given by

$$g' \cdot [(g, y)] := [(g'g, y)].$$

It is straightforward to check that because Y is a faithful H-variety, the variety $G \times_H Y$ is a faithful G-variety. Because X is versal, there exists a G-equivariant rational map

$$G \times_H Y \dashrightarrow U' \tag{3.1}$$

One can check explicitly that the map

$$\begin{aligned} Y &\to G \times_H Y \\ y &\mapsto [(e, y)] \end{aligned}$$

is H-equivariant. Composing this with (3.1), we obtain an H-equivariant rational map

$$Y \dashrightarrow U' \subset U$$

as required. $\square$

Lemma 3.12 has the following consequence.

Lemma 3.13. *Let $H \subset G$ be a subgroup. Then* $\mathrm{RD}(H) \leq \mathrm{RD}(G)$.

Proof. Let X be a versal G-variety. Then X is a versal H-variety by Lemma 3.12. By Proposition 3.7 and Lemma 2.7,

$$\begin{aligned} \mathrm{RD}(G) &= \mathrm{RD}(X \to X/G) \\ &= \max\{\mathrm{RD}(X \to X/H), \mathrm{RD}(X/H \to X/G)\} \\ &= \max\{\mathrm{RD}(H), \mathrm{RD}(X/H \to X/G)\} \\ &\geq \mathrm{RD}(H). \end{aligned}$$

$\square$

There exist criteria to check whether a given G-variety is versal.

Lemma 3.14 (Versality criterion). *Let X be a faithful G-variety. Suppose both of the following statements hold.*

(1) *For every faithful, closed G-invariant subvariety $Z_1 \subset X$, and any closed (not necessarily faithful) G-invariant subvariety $Z_2 \subsetneq X$, there exists a G-equivariant rational map $\alpha \colon X \dashrightarrow X$ such that Z_1 is not contained in the indeterminacy locus of α and such that $\alpha(Z_1) \not\subseteq Z_2$.*

(2) *For any faithful G-variety Y, there exists a G-equivariant rational map $Y \dashrightarrow X$.*

Then X is versal.

Proof. Let $U \subset X$ be a G-invariant Zariski open. Denote by $Z_2 := X - U$. Let Y be a faithful G-variety. By Assumption 2, there exists a G-equivariant rational map $f \colon Y \dashrightarrow X$. Let $Z_1 := \overline{f(Y)}$. By Assumption 1, there exists a G-equivariant rational map $\alpha \colon X \dashrightarrow X$ such that the restriction of α to Z_1 is defined, and such that $\alpha(Z_1) \not\subseteq Z_2$. Then $\alpha \circ f$ restricts to a G-equivariant rational map $Y \dashrightarrow U$ as desired. □

Example 3.15. Let $\mathbb{A}^G$ denote the regular representation of G. Then $\mathbb{A}^G$ is a versal G-variety. Indeed, Lemma 3.1(b) of [BR1] shows that $\mathbb{A}^G$ satisfies Assumption 1 of Lemma 3.14, while Lemma 3.4 of [BR1] shows that $\mathbb{A}^G$ satisfies Assumption 2.

3.4. Examples of versal G-varieties. In this section we use the tools from §3.3 to give examples of versal G-varieties. We begin with a result essentially proven by Buhler–Reichstein in [BR1]; we include a proof for completeness.

Proposition 3.16 (Linear varieties are versal). *Let G be a finite group. Let V be any faithful linear G-variety. Then V is versal.*

Proof. Because $\mathbb{A}^G$ is versal, it suffices to prove that for any proper G-invariant closed subvariety $Z \subset V$, there exists a G-equivariant map $f \colon \mathbb{A}^G \to V$ such that $f(\mathbb{A}^G) \not\subseteq Z$. Let $v \in V - Z$ be any point such that $|G \cdot v| = |G|$. Define

$$\begin{aligned} f_v \colon \mathbb{A}^G &\to V \\ \sum_{g \in G} c_g g &\mapsto \sum_{g \in G} c_g (g \cdot v). \end{aligned}$$

Then f_v is a G-equivariant linear embedding, and $f(\mathbb{A}^G) \not\subseteq Z$ as claimed. □

We highlight a specific instance of the above: while Hilbert asked about the resolvent degree of the permutation representation $\mathbb{C}^7$ of S_7, Proposition 3.16 implies that that one can equivalently consider any faithful representation of S_7. This gives an equivalent rephrasing of Hilbert's 13th problem, one for each faithful S_n-representation.

Corollary 3.17. *The following statements are true.*

(1) *Let* $n \geq 1$. *Let* V *be any faithful representation of* $S_n, n \geq 2$. *Then*

$$\mathrm{RD}(S_n) = \mathrm{RD}(V \to V/S_n) = \mathrm{RD}(\widetilde{\mathcal{P}}_n \to \mathcal{P}_n).$$

In particular, $\mathrm{RD}(\widetilde{\mathcal{P}}_n \to \mathcal{P}_n) \leq \mathrm{RD}(\widetilde{\mathcal{P}}_{n+1} \to \mathcal{P}_{n+1})$.

(2) (**Universality of** $\mathrm{RD}(S_n)$) *Let* $\widetilde{X} \dashrightarrow X$ *be a generically* n*-to-*1 *rational cover. Then*

$$\mathrm{RD}(\widetilde{X} \dashrightarrow X) \leq \mathrm{RD}(S_n).$$

Proof. Proposition 3.16 gives the first equality of item 1, and shows that $\mathrm{RD}(V \to V/S_n) = \mathrm{RD}(W \to W/S_n)$ for any two faithful representations V and W. In particular, we can take $W = \mathbb{A}^n$ to be the standard permutation representation. Since $\mathbb{A}^n \to \mathbb{A}^n/S_n$ is the normalization of the branched cover $\widetilde{\mathcal{P}}_n \to \mathcal{P}_n$, the second equality of Item 1 follows from Lemma 2.11. Item 2 now follows from Lemma 2.9. $\square$

Another equivalent restatement of the problem of computing $\mathrm{RD}(\widetilde{\mathcal{P}}_n \to \mathcal{P}_n)$ comes from the following. Denote by $\mathcal{M}_{0,n}$ the moduli of n distinct ordered points in $\mathbb{P}^1$. More generally, let $\mathcal{C}_n(\mathbb{P}^m) := ((\mathbb{P}^m)^{\times n} - \Delta)/\operatorname{PGL}_{m+1}$, where $\Delta \subset (\mathbb{P}^m)^{\times n}$ denotes the "fat diagonal", i.e., the locus of n-tuples in which at least two points coincide.

Corollary 3.18. *For* $n \geq 5$, *the moduli of marked, genus 0 curves* $\mathcal{M}_{0,n}$ *is a versal* S_n*-variety. In particular,*

$$\mathrm{RD}(S_n) = \mathrm{RD}(\mathcal{M}_{0,n} \to \mathcal{M}_{0,n}/S_n).$$

More generally, $\mathcal{C}_n(\mathbb{P}^m)$ *is a versal* S_n*-variety for all* $n \geq \max\{5, m+3\}$.

Proof. There exists a dominant S_n-equivariant rational map $\mathbb{A}^n \dashrightarrow \mathcal{M}_{0,n}$. More generally, consider the m-fold direct sum $(\mathbb{A}^n)^m$ of the permutation representation of S_n. This admits a dominant S_n-equivariant rational map $(\mathbb{A}^n)^m \dashrightarrow ((\mathbb{P}^m)^{\times n} - \Delta)/\operatorname{PGL}_{m+1} =: \mathcal{C}_n(\mathbb{P}^m)$. The corollary now follows from Lemma 3.11 and Proposition 3.16 once we verify that the S_n-action on $\mathcal{C}_n(\mathrm{P}^m)$ is faithful, but this follows from the assumptions that $n \geq \max\{5, m+3\}$. $\square$

4. Lines on smooth cubic surfaces

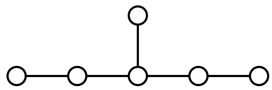
Since the problem of finding lines on smooth cubic surfaces connects with so many other problems, we devote an entire section to it. We also look at this one example in depth because it demonstrates how resolvent degree can be an organizing principle that gives a single framework for many classical results.

4.1. The moduli space of smooth cubic surfaces, and its covers. Let $\mathcal{H}_{3,3}$ denote the moduli space of smooth cubic surfaces. This is a 4-dimensional quasi-projective variety, the quotient of a hypersurface complement $(\mathbb{P}^{19} - \Sigma)$ by the action of PGL_4 induced from its action on $\mathbb{P}^3$. Let $Gr(2,4)$ denote the Grassmannian of projective lines in $\mathbb{P}^3$. Let

$$\mathcal{H}_{3,3}(1) := \big\{(S, L) \in (\mathbb{P}^{19} - \Sigma) \times Gr(2,4) : L \subset S\big\}/\,\mathrm{PGL}_4$$

be the moduli space of smooth cubic surfaces S equipped with a line; here PGL_4 acts diagonally. Cayley and Salmon proved that the projection $\pi : \mathcal{H}_{3,3}(1) \to \mathcal{H}_{3,3}$ given by $\pi(S, L) := S$ is a 27-sheeted covering, and so its monodromy is a subgroup of S_{27}. However, the monodromy must preserve the intersection pattern of the 27 lines. Camille Jordan proved (see, e.g., [Dol] or [Har] for a modern treatment) that the monodromy group of $\pi : \mathcal{H}_{3,3}(1) \to \mathcal{H}_{3,3}$ is isomorphic to the Weyl group $W(E_6)$. Recall that this is the reflection group given by the Dynkin diagram:

E_6



Here each vertex represents (reflection in the hyperplane perpendicular to) a root, and $W(E_6)$ has presentation with a generator s_α for each vertex of the diagram, with relations given by:

- $s_\alpha^2 = 1$ for all α.
- $(s_\alpha s_\beta)^2 = 1$ if α and β are not connected by an edge.
- $(s_\alpha s_\beta)^3 = 1$ if α and β are connected by an edge.

$W(E_6)$ is a group of order 51840; it contains the unique finite simple group of order 25920 as an index 2 subgroup; we denote this group by $W(E_6)^+$. Let $\mathcal{H}_{3,3}(27)$ denote the Galois closure of $\pi : \mathcal{H}_{3,3}(1) \to \mathcal{H}_{3,3}$; this is the (connected) Galois cover of $\mathcal{H}_{3,3}$ with deck group $W(E_6)$, corresponding to the kernel of the monodromy representation $\pi_1(\mathcal{H}_{3,3}) \twoheadrightarrow W(E_6)$. We use the notation $\mathcal{H}_{3,3}(27)$ since this cover corresponds to the moduli space of 28-tuples $(S; L_1, \ldots, L_{27})$ of smooth cubic surfaces equipped with 27 lines with a choice of labelling of the intersection graph of the set of 27 lines.

Let

$$\mathcal{H}^{\text{skew}}_{3,3}(r) := \big\{(S; L_1, \dots, L_r) \in (\mathbb{P}^{19} - \Sigma) \times Gr(2,4)^r : \\ L_i \subset S,\ L_i \cap L_j = \varnothing\ \forall i \neq j\big\}/\operatorname{PGL}_4 . \tag{4.1}$$

denote the moduli space of smooth cubic surfaces S with a choice of $r \leq 6$ skew (i.e., disjoint) lines on S. We remark that $\mathcal{H}^{\text{skew}}_{3,3}(6)$ is connected; this follows for example from the fact that it is isomorphic to the moduli of 6 generic points in $\mathbb{P}^2$ (cf. Section 4.4 below). There is a cover $\mathcal{H}^{\text{skew}}_{3,3}(r) \to \mathcal{H}_{3,3}$ given by $(S; L_1, \dots, L_r) \mapsto S$. This projection gives a (typically non-Galois) finite covering map $\mathcal{H}^{\text{skew}}_{3,3}(r) \to \mathcal{H}_{3,3}$.

The action of $W(E_6)$ on $\mathcal{H}_{3,3}(27)$ is free on a Zariski open. $W(E_6) \cong Aut(\operatorname{Pic}(S))$, and for any class $[L_0]$ of a line we have:

$$\operatorname{Stab}([L_0]) \cong W(D_5) \cong (\mathbb{Z}/2\mathbb{Z})^4 \rtimes S_5$$

where the S_5 action on $(\mathbb{Z}/2\mathbb{Z})^4$ is given by the standard 4-dimensional irreducible permutation representation of S_5. The action of S_5 on a marking is given by permuting the divisor classes of the 5 lines $L_1, \dots, L_5$ disjoint from L_0. Further, $W(D_5)$ is generated by this S_5 together with a Cremona transformation. Since the monodromy $W(E_6)$ acts transitively on the set of lines of any basepoint cubic, this implies that

$$\mathcal{H}_{3,3}(1) = \mathcal{H}_{3,3}(27)/W(D_5). \tag{4.2}$$

We will see throughout this paper how many classical problems about smooth cubic surfaces can be rephrased as understanding various (branched) covers of $\mathcal{H}_{3,3}$; for problems about lines the covers are intermediate between $\mathcal{H}_{3,3}(27) \to \mathcal{H}_{3,3}$. For now we give one example.

Schäfli's double sixes. One of the more well-studied types of configurations of lines on a smooth cubic surface S is the so-called (*Schläfli*) *double six*: it consists of two pairs $\{a_i\}$ and $\{b_j\}$ of 6 disjoint lines on S with intersection pattern given (in Schläfli's original notation):

$$\left\{\begin{matrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ b_1 & b_2 & b_3 & b_4 & b_5 & b_6 \end{matrix}\right\} \tag{4.3}$$

where any line does not meet any of the lines in the same row or column, but does meet the other 5 lines. See Figure 2 on Page 312.

The group $W(E_6)$ acts transitively on the set of 6-tuples of disjoint lines on S, with stabilizer the symmetric group S_6. There are thus $[W(E_6) : S_6] = 51840/720 = 72$ choices of such 6-tuples. Each such 6-tuple determines a unique double-six, and since any double-six contains 2 such 6-tuples, there are $72/2 = 36$ double-sixes. Denote the moduli of smooth cubic surfaces equipped with a double-six by

$$\mathcal{H}_{3,3}(6,6) := \{(S,D) : S \in \mathcal{H}_{3,3} \text{ and } D \text{ is a double-six in } S\}.$$

The stabilizer of a double-six is the maximal subgroup $S_6 \times \mathbb{Z}/2\mathbb{Z} \subset W(E_6)$ (cf. [Dol, Proposition 9.4, Theorem 9.5.2]). We can thus make the identification

$$\mathcal{H}_{3,3}(27)/(S_6 \times \mathbb{Z}/2\mathbb{Z}) = \mathcal{H}_{3,3}^{\text{skew}}(6)/(S_6 \times \mathbb{Z}/2\mathbb{Z}) = \mathcal{H}_{3,3}(6,6) \tag{4.4}$$

where the first equality comes from (4.6) below.

4.2. Finding 27 lines from a given line. In this section we consider the following problem: given a single line on a smooth cubic surface, how hard is it to find more lines? We will prove that given one line, the problem of finding the other 27 lines has resolvent degree 1, by which we mean $\mathrm{RD}(\mathcal{H}_{3,3}(27) \to \mathcal{H}_{3,3}(1)) = 1$. This result is essentially 100 years old. For a nice modern reference, see Dolgachev's book [Dol], Page 480.

Proposition 4.1 (Finding lines on a cubic surface, given a line). *With notation as above:*

$$\mathrm{RD}(\mathcal{H}_{3,3}(27) \to \mathcal{H}_{3,3}(1)) = 1.$$

This is in contrast to Harris's Theorem [Har] that $\mathcal{H}_{3,3}(27) \to \mathcal{H}_{3,3}(1)$ is not solvable by radicals.

Proof. We take the argument from the classic [Hilt], page 349. Suppose that we are given a smooth cubic surface $S = V(f)$ and a line ℓ_0 on S. The line ℓ_0 is given as a zero set of two linear forms : $\ell_0 = V(A_1, A_2)$. Since $\ell_0 \subset S$ this gives

$$f = A_1 Q_1 + A_2 Q_2$$

for quadratic forms Q_1, Q_2. Consider the pencil of planes

$$\Pi(\lambda_1, \lambda_2) = V(\lambda_1 A_1 - \lambda_2 A_2)$$

through the line ℓ_0. Each plane in this pencil intersects S in the union of ℓ_0 and a conic $C(\lambda_1, \lambda_2)$ on S. One can check that the discriminant of each $C(\lambda_1, \lambda_2)$ is a homogeneous polynomial $P(\lambda_1, \lambda_2)$ of degree 5, and that the general $P(\lambda_1, \lambda_2)$ has 5 distinct roots. Each of these solutions gives a reducible conic on S. Since S is smooth none of these is a double line.

We thus have found five distinct pairs of distinct lines $\ell_i, \ell_i', 1 \leq i \leq 5$, and in fact all 10 of these lines are distinct from each other and from ℓ_0, giving 11 lines on S. The important thing for us is to observe that the ℓ_i are pairwise disjoint for $0 \leq i \leq 5$. Since we obtained these with a degree 5 polynomial it follows that

$$\mathrm{RD}\big(\mathcal{H}_{3,3}^{\mathrm{skew}}(5) \to \mathcal{H}_{3,3}(1)\big) \leq \mathrm{RD}(\widetilde{\mathcal{P}_5} \to \mathcal{P}_5) = 1.$$

We can repeat the above procedure with ℓ_0 replaced by any ℓ_i or ℓ_i' to find the remaining 27 lines; that is, to prove

$$\mathrm{RD}\big(\mathcal{H}_{3,3}(27) \to \mathcal{H}_{3,3}^{\mathrm{skew}}(5)\big) \leq 1 \tag{4.5}$$

Alternately, Harris proves in [Har] that the monodromy of the cover $\mathcal{H}_{3,3}(27) \to \mathcal{H}_{3,3}^{\mathrm{skew}}(3)$ is in fact solvable, hence so is the monodromy of $\mathcal{H}_{3,3}(27) \to \mathcal{H}_{3,3}^{\mathrm{skew}}(5)$, giving (4.5). Lemma 2.7 (on RD of a tower) then implies

$$\begin{aligned}\mathrm{RD}\big(\mathcal{H}_{3,3}(27) \to \mathcal{H}_{3,3}(1)\big) &\leq \max\big\{\mathrm{RD}\big(\mathcal{H}_{3,3}(27) \to \mathcal{H}_{3,3}^{\mathrm{skew}}(5)\big),\\ &\qquad\qquad \mathrm{RD}\big(\mathcal{H}_{3,3}^{\mathrm{skew}}(5) \to \mathcal{H}_{3,3}(1)\big)\big\}\\ &= \max\{1,1\} = 1\end{aligned}$$

giving the proposition. □

4.3. Finding a single line. The following fundamental problem still remains. As we will see throughout this paper, it relates to many other problems about resolvent degree.

Problem 4.2. Determine $\mathrm{RD}(\mathcal{H}_{3,3}(1) \to \mathcal{H}_{3,3})$.

While there is a vast literature on lines on smooth cubic surfaces, and while much of it concerns relationships between various intermediate covers of $\mathcal{H}_{3,3}(27) \to \mathcal{H}_{3,3}$, there are far fewer results on Problem 4.2. The best results of which we are aware are due to Burkhardt [Bur], following a suggestion of Klein (see [Hu, Ch. 4.3.2] for a modern treatment).

Theorem 4.3 (Burkhardt, Klein). *Let k be any field of characteristic $\neq 2,3$. Then*

$$\mathrm{RD}_k\big(\mathcal{H}_{3,3}(1) \to \mathcal{H}_{3,3}\big) \leq 3.$$

The proof of Theorem 4.3 will use the following proposition, the first part of which we learned from [DR1, Lemma 6.1].

Proposition 4.4 (Finding the 27 lines is versal). *For any $G \subset W(E_6)$, the k-variety $\mathcal{H}_{3,3}(27)$ is a versal G-variety. In particular*

$$\mathrm{RD}_k\big(W(E_6)\big) = \mathrm{RD}_k\big(\mathcal{H}_{3,3}(27) \to \mathcal{H}_{3,3}\big).$$

Proof. Let $\mathfrak{h}$ denote a Cartan subalgebra of any simple Lie k-algebra of type E_6. Let $W(E_6)$ act on $\mathfrak{h}$ via the defining representation, and let $\mathbb{A}(\mathfrak{h})$ denote the corresponding faithful linear $W(E_6)$-variety. Then by [DR2, Lemma 6.1], there exists a $W(E_6)$-equivariant dominant rational map

$$\mathbb{A}(\mathfrak{h}) \dashrightarrow \mathcal{C}_6'(\mathbb{P}^2) \dashrightarrow \mathcal{H}_{3,3}(27).$$

Applying Proposition 3.16 and Lemma 3.11, the proposition follows. □

Proof of Theorem 4.3. Recall that $W(E_6) \cong W(E_6)^+ \rtimes \mathbb{Z}/2\mathbb{Z}$. By Theorem 3.3,

$$\mathrm{RD}\big(W(E_6)\big) = \max\big\{\mathrm{RD}\big(W(E_6)^+\big), \mathrm{RD}(\mathbb{Z}/2\mathbb{Z})\big\} = \mathrm{RD}\big(W(E_6)^+\big).$$

The group $W(E_6)^+$ has an action on $\mathbb{P}^3$ defined over $\mathbb{Z}[\sqrt{-3}]$ (see, e.g., [Atl]); therefore after adjoining $\sqrt{-3}$ to k ($\mathrm{RD} = 1$), this action is defined over k. By Proposition 3.10, it suffices to prove that $\mathbb{P}^3$ is solvably-versal for $W(E_6)^+$. Note that there is an isomorphism $Sp_4(\mathbb{F}_3)/\mathbb{F}_3^\times \cong W(E_6)^+$ and the $W(E_6)^+$-action on $\mathbb{P}^3$ lifts to a faithful linear action of $Sp_4(\mathbb{F}_3)$ on $\mathbb{A}^4$ defined over $\mathbb{Z}[\sqrt{-3}]$.

Given any $W(E_6)^+$-variety X, the obstruction to realizing it as a quotient of a faithful $Sp_4(\mathbb{F}_3)$-variety is the associated Brauer class in $H^2_{et}(k(X/W(E_6)^+); \mu_2)$. However, by Merkurjev's Theorem [Mer1], any class in $H^2_{et}(k(X)^{W(E_6)^+}; \mu_2)$ trivializes over some multi-quadratic extension of $k(X/W(E_6)^+)$. We conclude that there exists a faithful $Sp_4(\mathbb{F}_3)$-variety $\widetilde{X}$ such that $\widetilde{X}/Sp_4(\mathbb{F}_3) \dashrightarrow X/W(E_6)^+$ is a generically 2-to-1 rational cover. By Proposition 3.16, $\mathbb{A}^4$ is a versal $Sp_4(\mathbb{F}_3)$ variety, and by the definition of versality, there exists an $Sp_4(\mathbb{F}_3)$-equivariant rational map $\widetilde{X} \dashrightarrow \mathbb{A}^4$. Composing with the projection $\mathbb{A}^4 \dashrightarrow \mathbb{P}^3$, we obtain a $W(E_6)^+$-equivariant rational map $\widetilde{X}/\mathbb{Z}/2\mathbb{Z} \dashrightarrow \mathbb{P}^3$. But this shows that $\mathbb{P}^3$ is $W(E_6)^+$-solvably versal as claimed. We conclude

$$\begin{aligned}
&\text{(by Lemma 2.11)}\\
&\mathrm{RD}(\mathcal{H}_{3,3}(1) \to \mathcal{H}_{3,3}) = \mathrm{RD}\big(\mathcal{H}_{3,3}(27) \to \mathcal{H}_{3,3}\big)\\
&\text{(by Proposition 4.4)} \qquad = \mathrm{RD}\big(W(E_6)\big)\\
&\qquad = \mathrm{RD}\big(W(E_6)^+\big)\\
&\qquad = \mathrm{RD}\big(\mathbb{P}^3 \to \mathbb{P}^3/W(E_6)^+\big) \le \dim(\mathbb{P}^3) = 3.
\end{aligned}$$

□

4.4. Moduli of 6 points in $\mathbb{P}^2$. Let $\Sigma \subset (\mathbb{P}^2)^6$ denote the subvariety of 6-tuples of distinct points in $\mathbb{P}^2$ that are *non-generic*; that is, with either 3 colinear or with all 6 points lying on a conic. Let

$$\mathcal{C}_6'(\mathbb{P}^2) := \big((\mathbb{P}^2)^6 \setminus \Sigma\big)/\,\mathrm{PGL}_3$$

be the moduli space of generic 6-tuples in $\mathbb{P}^2$. For any (orbit representative of) $(z_1, \ldots, z_6) \in \mathcal{C}'_6(\mathbb{P}^2)$, blowing up $\mathbb{P}^2$ at each z_i gives a smooth cubic surface $S_{(z_1,\ldots,z_6)}$ equipped with a 6-tuple $(L_1, \ldots, L_6)$ of 6 skew lines corresponding to the exceptional divisors. Every smooth cubic surface arises in this way, and indeed it is classical that the map

$$\psi : \mathcal{C}'_6(\mathbb{P}^2) \to \mathcal{H}^{\mathrm{skew}}_{3,3}(6)$$

defined by $\psi(z_1, \ldots, z_6) := (S_{(z_1,\ldots,z_6)}; L_1, \ldots, L_6)$ is birational, where $\mathcal{H}^{\mathrm{skew}}_{3,3}(6)$ is defined in 4.1. It is classical that 6 skew lines $L_1, \ldots, L_6$ on a smooth cubic surface S determine via explicit formulas the other 21 lines on S; see, e.g., §4 of [Hu]. The ordering on the L_i determines an ordering on the set of all 27 lines, from which we deduce that there is an isomorphism

$$\tau : \mathcal{H}^{\mathrm{skew}}_{3,3}(6) \xrightarrow{\cong} \mathcal{H}_{3,3}(27). \tag{4.6}$$

Composition thus gives an isomorphism

$$\tau \circ \psi : \mathcal{C}'_6(\mathbb{P}^2) \xrightarrow{\cong} \mathcal{H}_{3,3}(27).$$

The permutation action of S_6 on $(\mathbb{P}^2)^6$ leaves invariant Σ and induces a well-defined action of S_6 on $\mathcal{C}'_6(\mathbb{P}^2)$. As explained in, e.g., [Sek, §3], this action extends (via adding a birational automorphism induced by an explicit Cremona transformation) to an action by birational automorphisms of $W(E_6)$ on $\mathcal{C}'_6(\mathbb{P}^2)$ for which the isomorphism $\tau \circ \psi$ is $W(E_6)$-equivariant. We remark that the $W(E_6)$ action on $\mathcal{C}'_6(\mathbb{P}^2)$ is not regular.

As a corollary to Proposition 4.4 and Theorem 4.3, we have the following.

Corollary 4.5. *Let k be a field of characteristic $\neq 2, 3$. For any $G \subset W(E_6)$, the k-variety $\mathcal{C}'_6(\mathbb{P}^2)$ is a versal G-variety. In particular,*

$$\mathrm{RD}\big(\mathcal{C}_6(\mathbb{P}^2) \dashrightarrow \mathcal{C}'_6(\mathbb{P}^2)/W(E_6)\big) = \mathrm{RD}\big(W(E_6)\big) \leq 3.$$

4.5. Pentahedral form. Pentahedral form is a classical normal form for smooth cubic surfaces. We now consider this form from the point of view of resolvent degree.

For any fixed $[a_0 : \cdots : a_4] \in \mathbb{P}^4$ the equations

$$\begin{aligned} a_0X_0^3 + a_1X_1^3 + a_2X_2^3 + a_3X_3^3 + a_4X_4^3 &= 0 \\ X_0 + X_1 + X_2 + X_3 + X_4 &= 0 \end{aligned} \tag{4.7}$$

determine a cubic surface in $\mathbb{P}^3$. Any permutation of the a_i gives an isomorphic cubic surface. We thus have a family $\mathbb{P}^4/S_5$ of cubic surfaces. The elementary symmetric functions $\sigma_1, \dots, \sigma_5$ in the a_i give coordinates on $\mathbb{P}^4/S_5$. The open subset

$$\mathcal{P} := \{[\sigma_1 : \cdots : \sigma_5] : \sigma_5 \neq 0\} \subset \mathbb{P}^4/S_5$$

is the family of smooth cubic surfaces admitting a (*proper*) *pentahedral form*, and the classifying map $\tau : \mathcal{P} \to \mathcal{H}_{3,3}$ is an open embedding (see, e.g., [EJ, Lemma 3.5]). The hyperplane complement

$$\widetilde{\mathcal{P}} := \mathbb{P}^4 - \bigcup_{i=0}^{4} \{a_i = 0\} = \mathbb{P}^4 \times_{\mathbb{P}^4/S_5} \mathcal{P}$$

is the space of smooth cubic surfaces in *proper pentahedral form*. We can pull back the cover $\mathcal{H}_{3,3}(27) \to \mathcal{H}_{3,3}$ along the map

$$\widetilde{\mathcal{P}} \to \mathcal{P} \to^{\tau} \mathcal{H}_{3,3}$$

to obtain a cover $\widetilde{\mathcal{P}}(27) \to \widetilde{\mathcal{P}}$.

Proposition 4.6. *Pentahedral form is an accessory irrationality: the cover $\widetilde{\mathcal{P}}(27) \to \widetilde{\mathcal{P}}$ has Galois group $W(E_6)$. Further, the total space $\widetilde{\mathcal{P}}(27)$ has two connected components, each component is preserved by the index two subgroup $W(E_6)^+ \subset W(E_6)$, and the components are permuted under the action of the full group $W(E_6)$.*

Proof. The cover

$$\mathcal{H}_{3,3}(27)/W(E_6)^+ \to \mathcal{H}_{3,3}$$

corresponds to adjoining a square-root of the discriminant of the cubic. Note that the discriminant of the cubic equals the discriminant of each of its pentahedral forms (cf. [Dol, §9.4.5]). As a consequence, the map $\widetilde{\mathcal{P}} \to \mathcal{H}_{3,3}$ factors through the cover

$$\widetilde{\mathcal{P}} \to \mathcal{H}_{3,3}(27)/W(E_6)^+.$$

The map $\widetilde{\mathcal{P}} \to \mathcal{H}_{3,3}(27)/W(E_6)^+$ is a Galois A_5-cover of its image. On the other hand, because $W(E_6)$ only has proper, nontrivial quotients of order 2; in particular A_5 is not such a quotient. We conclude that $\widetilde{\mathcal{P}} \to \mathcal{H}_{3,3}(27)/W(E_6)^+$ and $\mathcal{H}_{3,3}(27) \to \mathcal{H}_{3,3}(27)/W(E_6)^+$ share no intermediate covers, and thus

$$\mathcal{H}_{3,3}(27) \times_{\mathcal{H}_{3,3}(27)/W(E_6)^+} \widetilde{\mathcal{P}} \to \widetilde{\mathcal{P}}$$

is a connected Galois $W(E_6)^+$ cover. From the above, each of the two components of $\widetilde{\mathcal{P}}(27)$ is isomorphic to this connected $W(E_6)^+$ cover, with the full group $W(E_6)$ interchanging the two components. $\square$

4.6. Hexahedral form. The following is taken from Example 3.7 of [EJ]. Let $H \cong \mathbb{P}^4$ be the hyperplane in $\mathbb{P}^5$ given by $a_0 + \cdots + a_5 = 0$. The group S_6 acts on H with quotient isomorphic to the weighted projective space $\mathbb{P}(2,3,4,5,6)$. The key thing is a sequence of maps (using our notation as above):

$$\mathcal{H}_{3,3}(27) \xrightarrow{t_1} H \xrightarrow{t_2} H/S_6 \xrightarrow{t_3} \mathcal{H}_{3,3} \tag{4.8}$$

where t_1 is an unramified 2-sheeted cover, t_3 is an unramified 36-sheeted cover, and t_2 is a generically 720-to-1 branched cover. Note that the fact that t_1 is 2-sheeted, so that $\mathrm{RD}(\mathcal{H}_{3,3}(27) \to H) = 1$, corresponds to the classical fact that, given a smooth cubic surface S in hexahedral form, one can write down explicitly (as a linear function in the coefficients of S) a formula for 15 of the lines on S (see, e.g., [Dol], Section 9.4). One can obtain the remaining 12 lines by adjoining a square root. By the classification of maximal subgroups in $W(E_6)$ (see [Dol, Theorem 9.5.2]), the stabilizer of an unordered hexahedral form is isomorphic to $S_6 \times \mathbb{Z}/2\mathbb{Z}$. As a consequence, the moduli of unordered hexahedral forms H/S_6 is isomorphic over $\mathcal{H}_{3,3}$ to the moduli of cubics equipped with a double-six:

$$\begin{tikzcd} H/S_6 \arrow[rr, "\cong"] \arrow[dr] & & \mathcal{H}_{3,3}(6,6) \arrow[dl] \\ & \mathcal{H}_{3,3} & \end{tikzcd} .$$

Moreover,

$$\begin{aligned} \mathrm{RD}\big(\mathcal{H}_{3,3}(27) \to \mathcal{H}_{3,3}\big) &= \max\big\{\mathrm{RD}(H \to H/S_6), \mathrm{RD}(H/S_6 \to \mathcal{H}_{3,3})\big\} \\ &\le \max\big\{2, \mathrm{RD}(H/S_6 \to \mathcal{H}_{3,3})\big\} \end{aligned}$$

where the last inequality follows from

$$\begin{aligned} &\text{(by Proposition 3.16 and Lemma 3.11)} && \mathrm{RD}(H \to H/S_6) = \mathrm{RD}(S_6) \\ &\text{(by Hamilton's bound)} && \le 2. \end{aligned}$$

5. Bitangents to plane quartics

The story of 28 bitangents on a smooth plane quartic is analogous to that for the 27 lines on a smooth cubic surface, and indeed the two are directly related, as we will see in §5.3 below.

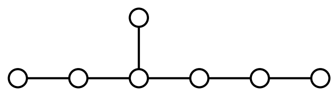
5.1. The moduli space of smooth planar quartics, and its covers. Let $\mathcal{H}_{4,2}$ denote the moduli space of smooth quartic curves in $\mathbb{P}^2$. This is a 6-dimensional quasi-projective variety, the quotient of a hypersurface complement $(\mathbb{P}^{14} - \Sigma)$ by the action of PGL_3 induced from its action on $\mathbb{P}^2$. Let $Gr(2,3)$ denote the Grassmannian of projective lines in $\mathbb{P}^2$. Jacobi proved in 1850 that any smooth plane quartic C has precisely 28 *bitangents*; that is, lines $T \subset \mathbb{P}^2$ that are tangent to C at two points (counted with multiplicity). Let

$$\mathcal{H}_{4,2}(1) := \left\{(C, L) \in (\mathbb{P}^{14} - \Sigma) \times Gr(2,3) : L \text{ bitangent to } C\right\} / \,\mathrm{PGL}_3$$

be the moduli space of smooth plane quartics equipped with a bitangent; here PGL_3 acts diagonally. The map $(C, L) \mapsto C$ is a 28-sheeted covering space. Let $\mathcal{H}_{4,2}(28)$ denote the Galois closure of $\pi : \mathcal{H}_{4,2}(1) \to \mathcal{H}_{4,2}$; this is a (connected) Galois cover of $\mathcal{H}_{4,2}$. We use the notation $\mathcal{H}_{4,2}(28)$ since this cover corresponds to the moduli space of 29-tuples $(C; L_1, \ldots, L_{28})$ of smooth plane quartics equipped with 28 lines with a choice of labelling of the intersection graph of the set of 28 lines.

The deck group of the Galois cover $\mathcal{H}_{4,2}(28) \to \mathcal{H}_{4,2}$ is the same as the monodromy group of the cover $\mathcal{H}_{4,2}(1) \to \mathcal{H}_{4,2}$. This group is isomorphic to the unique simple group of order $1,451,520$, which we denote $W(E_7)^+$. There exists a split injection $W(E_7)^+ \hookrightarrow W(E_7)$, the Weyl group of type E_7. Recall that $W(E_7)$ is the reflection group with Dynkin diagram:

E_7



It is given by order 2 generators s_α, one for each vertex, satisfying the same relations as $W(E_6)$ given above. $W(E_7)$ has order $2,903,040$, and is a direct product of $\mathbb{Z}/2\mathbb{Z}$ with $W(E_7)^+$. The action of $W(E_7)^+$ on $\mathcal{H}_{4,2}(28)$ is free on a Zariski open. $W(E_7)^+ \cong Aut(\mathrm{Pic}(C)[2])$, and for any class $[L_0]$ of a line we have:

$$\mathrm{Stab}([L_0]) \cong W(E_6)$$

This action is most easily seen as follows (cf. [DO, Chapter IX.2]). The moduli $\mathcal{H}_{4,2}(28)$ is the target of a generically 2-to-1 dominant rational map

$$\mathcal{C}_7(\mathbb{P}^2) \dashrightarrow \mathcal{H}_{4,2}(28).$$

Concretely, given 7 points $\{x_1, \ldots, x_7\} \subset \mathbb{P}^2$ in general position, form the degree 2 Del Pezzo surface $V(x_1, \ldots, x_7)$ by blowing up $\mathbb{P}^2$ at these points. The anti-canonical map

$$V \to \mathbb{P}^2. \tag{5.1}$$

realizes V as a 2-fold branched cover, branched over a quartic curve C, and takes every exceptional curve on V to a bitangent of C. By Proposition 1 of [DO, Chapter IX.2], this gives a 2-fold covering map

$$U \to \mathcal{H}_{4,2}(28) \tag{5.2}$$

where $U \subset \mathcal{C}_7(\mathbb{P}^2)$ is the locus of points in general position, and the map sends V with its exceptional curves to C with its 28 bitangents. The Weyl group $W(E_7)$ acts on $\mathcal{C}_7(\mathbb{P}^2)$ (via the Coble representation) and this action factors through the projection

$$W(E_7) \cong \mathbb{Z}/2\mathbb{Z} \times W(E_7)^+ \twoheadrightarrow W(E_7)^+.$$

The map (5.2) is equivariant for this action (see [DO, Chapter IX], esp. p. 194, for a verification of this equivariance). Under the map (5.2), the stabilizer of a bitangent lifts to the stabilizer of a marked point on $\mathcal{C}_7(\mathbb{P}^2)$, i.e., to $W(E_6) \subset W(E_7)^+ \subset W(E_7)$.

Just as for lines on cubics, we will see throughout this paper how many classical problems about smooth quartic curves can be rephrased as understanding various (branched) covers of $\mathcal{H}_{4,2}$; for problems about bitangents the covers are intermediate between $\mathcal{H}_{4,2}(28) \to \mathcal{H}_{4,2}$. We now give several examples.

Aronhold sets. One of the more well-studied types of configurations of bitangents on a smooth plane quartic curve C is the so-called *Aronhold set*. Recall that a collection of $n \geq 3$ bitangents on a smooth plane quartic is *asyzygetic* (resp. *syzygetic*) if the collection of $2n$ points of contact of the bitangents with the quartic are not (resp. are) contained in a conic.

Definition 5.1 (Aronhold set of bitangents). An *Aronhold set* $\mathcal{A}$ on a smooth plane quartic C is an asyzygetic, unordered set of seven bitangents $\{T_1, \ldots, T_7\}$ on C. An *Aronhold basis* is an Aronhold set with an ordering of its elements.

Let $\mathcal{H}_{4,2}(\widetilde{\mathcal{A}})$ denote the moduli of smooth plane quartics equipped with an Aronhold basis, and let $\mathcal{H}_{4,2}(\mathcal{A})$ denote the moduli of smooth plane quartics equipped with an Aronhold set. Note that the forget-the-ordering map is a Galois S_7-cover

$$\mathcal{H}_{4,2}(\widetilde{\mathcal{A}}) \to \mathcal{H}_{4,2}(\mathcal{A}).$$

Aronhold sets have been studied for over a century (for recent treatments, see, e.g., [DO] or [Dol, Chapter 6.1.2]). One of the reasons is that an Aronhold basis on C determines the other 21 bitangents to C, i.e., we have an $W(E_7)^+$-equivariant isomorphism

$$\mathcal{H}_{4,2}(\widetilde{\mathcal{A}}) \to^{\cong} \mathcal{H}_{4,2}(28).$$

Perhaps even more surprising, an Aronhold basis in fact determines the equation for C itself [Leh]. The group $W(E_7)^+$ acts simply transitively on the set of Aronhold bases, and thus acts transitively on the set of Aronhold sets, with stabilizer the symmetric group S_7. There are thus $[W(E_7)^+ : S_7] = 288$ choices of Aronhold sets. The complexity of finding an Aronhold basis, given an Aronhold set, as measured by resolvent degree, is equivalent to Hilbert's 13th problem, as we show in Theorem 8.3.

Steiner Complexes. A second well-studied type of configuration of bitangents on a smooth quartic curve is the *Steiner complex* (cf. [Hilt, Chapter XIX.3] and [Dol, Chapter 6.1.2]).

Definition 5.2 (Steiner complex of bitangents). A *Steiner complex* of bitangents on a smooth plane quartic C is an unordered collection of six unordered pairs of bitangents $\{(\alpha_1, \beta_1), \ldots, (\alpha_6, \beta_6)\}$ such that any two pairs give a syzygetic collection of bitangents.

Any two bitangents determine a Steiner complex, and any one of the six pairs of a Steiner complex determine the same complex, so there are $\binom{28}{2}/6 = 378/6 = 63$ Steiner complexes. Denote the moduli of smooth plane quartics equipped with a Steiner complex by

$$\mathcal{H}_{4,2}(\mathcal{S}) := \big\{(C, S) : C \in \mathcal{H}_{4,2} \text{ and } S \text{ is a Steiner complex for } C\big\}.$$

The group $W(E_7)^+$ acts transitively on the set of Steiner complexes, and the stabilizer of a Steiner complex is isomorphic to $W(D_6) \cong (\mathbb{Z}/2\mathbb{Z})^{\times 5} \rtimes S_6$, where the action of S_6 is via its standard 5-dimensional permutation representation. We can thus make the identification

$$\mathcal{H}_{4,2}(\mathcal{S}) = \mathcal{H}_{4,2}(28)/W(D_6) = \mathcal{H}_{4,2}(\widetilde{\mathcal{A}})/W(D_6). \tag{5.3}$$

where the second equality comes from the fact that an Aronhold basis determines the remaining 21 lines.

Cayley Octads. A third configuration of classical interest is the *Cayley octad* (cf. [Dol, Chapter 6.3.2]).

Definition 5.3. A *Cayley octad* is a collection of 8 distinct unordered points in $\mathbb{P}^3$ that arises as a complete intersection of 3 quadrics. Denote the moduli space of Cayley octads by Cay.

There is a close relationship between Cayley octads and smooth plane quartics, which is summed up in the [Dol, Chapter 6.3] (especially Corollary 6.3.12). In particular, the moduli of plane quartics equipped with an Aronhold set $\mathcal{H}_{4,2}(\mathcal{A})$ admits an 8-to-1 covering map to the moduli space of Cayley octads, which is in turn birational to the moduli space of smooth plane quartics equipped with an even θ-characteristic:

$$\mathcal{H}_{4,2}(\mathcal{A}) \to^{8:1} \mathrm{Cay} \simeq \mathcal{H}_{4,2}(\theta^{\mathrm{ev}}).$$

Moreover, the group $W(E_7)^+$ acts transitively on the set of Cayley octads, respectively even θ-characteristics, and the stabilizer of an octad, respectively even θ-characteristic, is S_8.

5.2. The resolvent degree of finding bitangents to plane quartics. In this subsection we consider the resolvent degree of the problem of finding bitangents on smooth plane quartics.

Proposition 5.4 (Finding **28** bitangents, given **2**). *With the notation as above:*

$$\mathrm{RD}\big(\mathcal{H}_{4,2}(28) \to \mathcal{H}_{4,2}(2)\big) = 1.$$

The proof of Proposition 5.4 that we now give should feel similar to the proof of Proposition 4.1, and indeed we formalize this similarity as a precise statement in §5.3. We include the proof here for its beauty and historical interest.

Proof. Now, since the T_i are distinct, any two intersect in a single point. Let

$$\mathcal{H}'_{4,2}(2) := \big\{(C; T_1, T_2) \in \mathcal{H}_{4,2}(2) : T_1 \cap T_2 \notin C\big\}.$$

This is a Zariski open subset of $\mathcal{H}_{4,2}(2)$. It is enough to prove the theorem for the pullback cover $\mathcal{H}'_{4,2}(28) \to \mathcal{H}'_{4,2}(2)$. The advantage of $\mathcal{H}'_{4,2}(2)$ is that it gives us 4 points of contact, 2 each from $T_1 \cap C$ and $T_2 \cap C$. We can then perform a classical construction, which we take from the 1920 book [Hilt], which posits (see p. 334 of [Hilt]):

> *Through the four points of contact of two bitangents of a non-singular quartic pass five conics each of which passes through the points of contact of two more bitangents.*

More precisely, let $(C; T_1, T_2) \in \mathcal{H}'_{4,2}(2)$ be given. We consider $\mathbb{P}^2$ with coordinates $[x : y : z]$. By picking representatives in the PGL_3 orbit of $(C; T_1, T_2)$, we can assume that T_1 and T_2 are given by the equations $x = 0$ and $y = 0$, respectively. The assumption that C has a bitangent given by $x = 0$ and a bitangent given by $y = 0$ puts the equation of C in a very special form, namely:

$$C := \big\{[x : y : z] \in \mathbb{P}^2 : xy(U + 2kV + t62xy) - (V + txy)^2 = 0\big\} \tag{5.4}$$

for some t, where $U = 0$ and $V = 0$ are conics. Consider the condition that $U + 2kV + t^2xy$ factors as a product of linear forms $p(x, y, z)$ and $q(x, y, z)$.

One can check that this condition is a degree 5 polynomial in t. For such t the equation (5.4) for the quartic C then becomes

$$xyp(x,y,z)q(x,y,z) - W^2 = 0$$

where $W := V + txy$. It is then clear that the lines given by $p = 0$ and $q = 0$ are both bitangent to C. Further, the conic $W = 0$ passes through the eight points of contact of the four bitangents $x = 0, y = 0, p = 0, q = 0$. We have thus proven that

$$\mathrm{RD}\big(\mathcal{H}'_{4,2}(4) \to \mathcal{H}'_{4,2}(2)\big) \leq \mathrm{RD}(\widetilde{\mathcal{P}}_5 \to \mathcal{P}_5) = 1 \tag{5.5}$$

where $\mathcal{H}'_{4,2}(4)$ is the pullback to $\mathcal{H}'_{4,2}(2)$ of the cover $\mathcal{H}_{4,2}(4) \to \mathcal{H}_{4,2}(2)$. Although we will not need it, we remark that there are 5 distinct roots of the degree 5 polynomial determining such t, and so this gives us 5 additional pairs of bitangents to C, for a total of $2 + 5 \cdot 2 = 12$ bitangents.

Harris [Har] proves the following: given any three bitangents whose points of contact lie on a conic, or any four whose points of contact do not, we can solve for the remaining ones in radicals; further, no smaller sets suffice. This in particular gives that the cover $\mathcal{H}'_{4,2}(28) \to \mathcal{H}'_{4,2}(4)$ is solvable by radicals, and so has resolvent degree equal to 1. Combining this with (5.5) thus gives

$$\mathrm{RD}\big(\mathcal{H}_{4,2}(28) \to \mathcal{H}_{4,2}(2)\big) = 1$$

as desired. $\square$

Proposition 5.4 naturally suggests the following fundamental problem.

Problem 5.5 (Finding bitangents on smooth quartics). Compute the following:

(1) $\mathrm{RD}\big(\mathcal{H}_{4,2}(28) \to \mathcal{H}_{4,2}(1)\big)$.

(2) $\mathrm{RD}\big(\mathcal{H}_{4,2}(1) \to \mathcal{H}_{4,2}\big)$.

In the next section, we relate this to the problem of finding lines on cubic surfaces, and in Section 8, we put this problem in the context of Hilbert's 13th problem and Hilbert's Octic Conjecture.

5.3. Relating lines on cubic surfaces to bitangents on plane quartics. In this subsection we relate the resolvent degrees of two classical problems: finding a line on a smooth cubic surface and finding a bitangent on a smooth quartic curve in $\mathbb{P}^2$. We then relate these to the resolvent degrees of other problems.

Theorem 5.6. *For any subgroup* $G \subset W(E_6) \subset W(E_7)^+$*,*

$$\mathrm{RD}(G) = \mathrm{RD}(\mathcal{H}_{3,3}(27) \to \mathcal{H}_{3,3}/G) = \mathrm{RD}(\mathcal{H}_{4,2}(28) \to \mathcal{H}_{4,2}/G).$$

In particular:

(1) $\mathrm{RD}\big(W(D_5)\big) = \mathrm{RD}\big(\mathcal{H}_{3,3}(27) \to \mathcal{H}_{3,3}(1)\big) = \mathrm{RD}\big(\mathcal{H}_{4,2}(28) \to \mathcal{H}_{4,2}(2)\big) = 1.$

(2) $\mathrm{RD}\big(W(E_6)\big) = \mathrm{RD}\big(\mathcal{H}_{3,3}(27) \to \mathcal{H}_{3,3}\big) = \mathrm{RD}\big(\mathcal{H}_{4,2}(28) \to \mathcal{H}_{4,2}(1)\big) \le 3.$

Similarly, for any other subgroup $G \subset W(E_7)^+$*,*

$$\mathrm{RD}(G) = \mathrm{RD}(\mathcal{H}_{4,2}(28) \to \mathcal{H}_{4,2}/G)$$

In particular:

(1) $\mathrm{RD}(S_7) = \mathrm{RD}\big(\mathcal{H}_{4,2}(28) \to \mathcal{H}_{4,2}(\mathcal{A})\big) \le 3.$

(2) $\mathrm{RD}(S_8) = \mathrm{RD}\big(\mathcal{H}_{4,2}(28) \to \mathcal{H}_{4,2}(\theta^{ev})\big) \le 4.$

(3) $\mathrm{RD}\big(W(E_7)^+\big) = \mathrm{RD}(\mathcal{H}_{4,2}(28) \to \mathcal{H}_{4,2}).$

We will deduce Theorem 5.6 from the following, which should be compared with Proposition 4.4 above.

Proposition 5.7 (Versality of the bitangents problem). *For any* $G \subset W(E_7)^+$*, the* k*-variety* $\mathcal{H}_{4,2}(28)$ *is a versal* G*-variety.*

Proof. We recall a construction due to Dolgachev–Ortland [DO, Chapter IX], which in its essentials dates to Coble. We claim there exists a sequence of $W(E_7)$-equivariant dominant rational maps

$$\mathbb{A}(\mathfrak{h}) \dashrightarrow \mathbb{P}(\mathfrak{h}) \dashrightarrow \mathcal{C}_7(\mathbb{P}^2) \dashrightarrow \mathcal{H}_{4,2}(28) \tag{5.6}$$

where $\mathbb{A}(\mathfrak{h})$ denotes the variety given by a Cartan subalgebra of a simple Lie group of type E_7, with its canonical $W(E_7)$-action. By Proposition 3.16, $\mathbb{A}(\mathfrak{h})$ is a versal $W(E_7)$ variety, and in fact a versal G-variety for all $G \subset W(E_7)$. By Lemma 3.11, all the varieties in (5.6) dominated by $\mathbb{A}(\mathfrak{h})$ are also versal G-varieties for all $G \subset W(E_7)$ which act faithfully on them. Since the action of $W(E_7)$ on all but $\mathbb{A}(\mathfrak{h})$ factors through the projection $W(E_7) \cong \mathbb{Z}/2\mathbb{Z} \times W(E_7)^+ \twoheadrightarrow W(E_7)^+$ (cf. [DR2, Remark 7.2]), we conclude the result.

It remains to construct the diagram (5.6). The rational map

$$\mathcal{C}_7(\mathbb{P}^2) \dashrightarrow \mathcal{H}_{4,2}(28)$$

was constructed above as (5.2). The map

$$\mathbb{A}(\mathfrak{h}) \dashrightarrow \mathbb{P}(\mathfrak{h})$$

is just the projectivization, and is thus manifestly $W(E_7)$-equivariant. It remains to construct the map

$$\mathbb{P}(\mathfrak{h}) \dashrightarrow \mathcal{C}_7(\mathbb{P}^2)$$

We again follow [DO, Chapter IX]. We begin by identifying $\mathbb{P}(\mathfrak{h})$ with the set of ordered points $\{x_1, \dots, x_7\}$ in the non-singular locus of a fixed cuspidal cubic, up to projective equivalence (cf. Pinkham [Pin]). Since there are 21 cuspidal cubics through a general collection of 7 points in $\mathbb{P}^2$, forgetting the cubic gives the above 21-sheeted map. This concludes the construction of (5.6) and the proof. $\square$

Proof of Theorem 5.6. By Proposition 5.7, the variety $\mathcal{H}_{4,2}(28)$ is versal for any $G \subset W(E_7)^+$. By Proposition 4.4, the variety $\mathcal{H}_{3,3}(27)$ is versal for any $G \subset W(E_6) \subset W(E_7)^+$. Proposition 3.7 therefore implies that for any $G \subset W(E_6)$

$$\mathrm{RD}(G) = \mathrm{RD}\big(\mathcal{H}_{3,3}(27) \to \mathcal{H}_{3,3}(27)/G\big) = \mathrm{RD}\big(\mathcal{H}_{4,2}(28) \to \mathcal{H}_{4,2}(28)/G\big)$$

and that for any subgroup $G \subset W(E_7)^+$ not contained in $W(E_6)$,

$$\mathrm{RD}(G) = \mathrm{RD}\big(\mathcal{H}_{4,2}(28) \to \mathcal{H}_{4,2}(28)/G\big).$$

The special cases above now follow from the discussions of the quotients of $\mathcal{H}_{3,3}(27)$ and $\mathcal{H}_{4,2}(28)$ of classical interest in Sections 4.1 and 5.1.

The bound

$$\mathrm{RD}\big(W(D_5)\big) = \mathrm{RD}\big(\mathcal{H}_{3,3}(27) \to \mathcal{H}_{3,3}(1)\big) = \mathrm{RD}\big(\mathcal{H}_{4,2}(28) \to \mathcal{H}_{4,2}(2)\big) = 1$$

now follows alternately from Theorem 3.3, Proposition 4.1, or Proposition 5.4. The bound

$$\mathrm{RD}\big(W(E_6)\big) = \mathrm{RD}\big(\mathcal{H}_{3,3}(27) \to \mathcal{H}_{3,3}\big) = \mathrm{RD}\big(\mathcal{H}_{4,2}(28) \to \mathcal{H}_{4,2}(1)\big) \leq 3$$

follows from Theorem 4.3. The bounds

$$\mathrm{RD}(S_7) = \mathrm{RD}\big(\mathcal{H}_{4,2}(28) \to \mathcal{H}_{4,2}(\mathcal{A})\big) \leq 3,$$
$$\mathrm{RD}(S_8) = \mathrm{RD}\big(\mathcal{H}_{4,2}(28) \to \mathcal{H}_{4,2}(\theta^{\mathrm{ev}})\big) \leq 4$$

follow from Corollary 3.17 1, and the Bring–Hamilton bounds $\mathrm{RD}(\widetilde{\mathcal{P}}_7 \to \mathcal{P}_7) \leq 3$ and $\mathrm{RD}(\widetilde{\mathcal{P}}_8 \to \mathcal{P}_8) \leq 4$. $\square$

We now use a classical construction to give a more explicit proof of the first equality of Theorem 5.6.

The classical construction. Let S be a smooth cubic surface containing lines $L_1, \dots, L_{27}$. A choice of a point $p \in S - \cup_{i=1}^{27} L_i$ determines via projection a morphism

$$\pi_p : \mathrm{Bl}_p(S) \to \mathbb{P}^2$$

from the blowup $\mathrm{Bl}_p(S)$ to the plane $\mathbb{P}^2$. This setup has the following remarkable properties:

(1) π_p is a 2-sheeted branched cover, branched over a smooth quartic curve $C_p \subset \mathbb{P}^2$.

(2) The 27 images $\pi_p(L_i), 1 \leq i \leq 27$ are 27 of the 28 bitangents of C_p, with the 28th bitangent to C_p being the image under π_p of the exceptional divisor in $\mathrm{Bl}_p(S)$.

(3) For every smooth quartic curve C in $\mathbb{P}^2$ there exists S and $p \in S$ as above so that C is the branch locus of π_p, as above.

See Figure 1 on Page 310.

Modular interpretation. We can interpret this classical construction in terms of Del Pezzo surfaces of degree 2 and 3, and thus of maps of moduli spaces and their covers.

Consider the universal family

$$\begin{tikzcd} S \arrow[r] & \mathcal{U}_{3,3} \arrow[d, "\pi"] \\ & \mathcal{H}_{3,3} \end{tikzcd}$$

of smooth cubic surfaces. Note that $\mathcal{U}_{3,3}$ can also be thought of as the moduli space of pairs $\{(S,p) : S \in \mathcal{H}_{3,3}, p \in S\}$ and the projection $\pi(S,p) := S$.

We now give a second presentation of $\mathcal{U}_{3,3}$. Recall that

$$\mathcal{H}_{3,3}(27) \cong \mathcal{H}_{3,3}^{\mathrm{skew}}(6) \cong \mathcal{C}_6'(\mathbb{P}^2)$$

Adding the data of a point on a cubic, we get birational maps

$$\mathcal{C}_7(\mathbb{P}^2) \overset{\simeq}{\dashrightarrow} \mathcal{U}_{3,3}^{\mathrm{skew}}(6) \cong \mathcal{U}_{3,3}(27)$$

where $\mathcal{U}_{3,3}^{\mathrm{skew}}(6)$ (resp. $\mathcal{U}_{3,3}(27)$) denotes the space of cubic surfaces equipped with an ordered set of 6 skew lines (resp. an ordered set of 27 lines) and a point on the surface. These isomorphisms are equivariant with respect to the $W(E_6) \subset W(E_7)$ action on $\mathcal{C}_7(\mathbb{P}^2)$ and the $W(E_6)$ actions on $\mathcal{U}_{3,3}^{\mathrm{skew}}(6)$ (resp. $\mathcal{U}_{3,3}(27)$). In particular there is an open embedding

$$\mathcal{C}_7(\mathbb{P}^2)/W(E_6) \subseteq \mathcal{U}_{3,3}$$

onto the cubics equipped with a point not lying on any of the 27 lines.

On the other hand, as discussed above, we have a generically 2-to-1 $W(E_7)$-equivariant dominant map

$$\mathcal{C}_7(\mathbb{P}^2) \dashrightarrow \mathcal{H}_{4,2}(28).$$

Therefore, for any $G \subset W(E_6)$, we obtain a pullback diagram in which the horizontal maps are generically 2-to-1 rational covers

$$\begin{tikzcd} \mathcal{U}_{3,3}(27) \arrow[r, dashed] \arrow[d] & \mathcal{H}_{4,2}(28) \arrow[d] \\ \mathcal{U}_{3,3}(27)/G \arrow[r, dashed] & \mathcal{H}_{4,2}(28)/G \end{tikzcd}$$

This diagram shows that, at the cost of adjoining a square root, any explicit solution for $\mathcal{H}_{4,2}(28) \to \mathcal{H}_{4,2}(28)/G$ determines one for $\mathcal{U}_{3,3}(27) \to \mathcal{U}_{3,3}(27)/G$, and vice versa.

It remains to relate this to solutions of

$$\mathcal{H}_{3,3}(27) \to \mathcal{H}_{3,3}(27)/G.$$

One direction is trivial: because we have a pullback diagram in which all maps are dominant

$$\begin{tikzcd} \mathcal{U}_{3,3}(27) \arrow[r, dashed] \arrow[d] & \mathcal{H}_{3,3}(27) \arrow[d] \\ \mathcal{U}_{3,3}(27)/G \arrow[r, dashed] & \mathcal{H}_{3,3}(27)/G \end{tikzcd}$$

any solution to $\mathcal{H}_{3,3}(27) \to \mathcal{H}_{3,3}(27)/G$ immediately pulls back to give one for $\mathcal{U}_{3,3}(27) \to \mathcal{U}_{3,3}(27)/G$. For the other direction, given an explicit tower solving $\mathcal{U}_{3,3}(27) \to \mathcal{U}_{3,3}(27)/G$

$$\begin{tikzcd} & & & \mathcal{U}_{3,3}(27) \arrow[d] \\ X_r \arrow[r, dashed] \arrow[urrr, dashed] & \cdots \arrow[r, dashed] & X_1 \arrow[r, dashed] & \mathcal{U}_{3,3}(27)/G \end{tikzcd} \tag{5.7}$$

Let $Z \subset \mathcal{U}_{3,3}(27)/G$ be the closure of the complement of the image of X_r in $\mathcal{U}_{3,3}(27)/G$. Because $X_r \dashrightarrow \mathcal{U}_{3,3}(27)/G$ is dominant, Z is a proper subvariety.

Fix a line $L \subset \mathbb{P}^3$ and let $U \subset \mathcal{H}_{3,3}(27)/G$ be the Zariski open consisting of cubic surfaces which intersect L transversely. Define

$$\widetilde{U}_L := \left\{(\tilde{S}, p) : \tilde{S} \in U \subset \mathcal{H}_{3,3}(27)/G, p \in S \cap L\right\}$$

By Bezout's Theorem, the projection

$$\widetilde{U}_L \to U$$

is a 3-to-1 dominant map. Because $Z \subset \mathcal{U}_{3,3}(27)/G$ is a proper closed subvariety, for a generic choice of $L \subset \mathbb{P}^3$, the embedding

$$\widetilde{U}_L \subset \mathcal{U}_{3,3}(27)/G$$

is not contained in Z. We can therefore pull back the solution (5.7) along this embedding to get a tower solving

$$\widetilde{U}_L \times_{\mathcal{H}_{3,3}(27)/G} \mathcal{H}_{3,3}(27) \to \widetilde{U}_L$$

We conclude from Lemma 2.7 and Corollary 3.17 2 that

$$\begin{aligned} \mathrm{RD}\big(\mathcal{H}_{3,3}(27) \to \mathcal{H}_{3,3}(27)/G\big) &\leq \max\big\{\mathrm{RD}\big(\widetilde{U}_L \times_{\mathcal{H}_{3,3}(27)/G} \mathcal{H}_{3,3}(27) \to \widetilde{U}_L\big), \\ &\qquad \mathrm{RD}(\widetilde{U}_L \to U)\big\} \\ &\leq \max\big\{\mathrm{RD}\big(\mathcal{U}_{3,3}(27) \to \mathcal{U}_{3,3}(27)/G\big), 1\big\} \\ &= \mathrm{RD}\big(\mathcal{U}_{3,3}(27) \to \mathcal{U}_{3,3}(27)/G\big). \end{aligned}$$

□

Remark 5.8. The construction above using Bezout's theorem suggests a general method. We develop this further in Section 6.2 below.

The proof of Theorem 5.6 also implies the following.

Corollary 5.9 (RD for Double-Sixes and Steiner Complexes). *The resolvent degree of finding an ordered sixer given a double-six equals the resolvent degree of finding an Aronhold basis given a Steiner complex equals the resolvent degree of S_6, i.e.,*

$$\mathrm{RD}(S_6) = \mathrm{RD}\big(\mathcal{H}_{3,3}^{\mathrm{skew}}(6) \to \mathcal{H}_{3,3}(6,6)\big) = \mathrm{RD}\big(\mathcal{H}_{4,2}(\widetilde{\mathcal{A}}) \to \mathcal{H}_{4,2}(\mathcal{S})\big).$$

Proof. By Theorem 5.6,

$$\mathrm{RD}(S_2 \times S_6) = \mathrm{RD}\big(\mathcal{H}_{3,3}^{\mathrm{skew}}(6) \to \mathcal{H}_{3,3}(6,6)\big)$$

and, because $\mathcal{H}_{4,2}(\widetilde{\mathcal{A}}) \cong \mathcal{H}_{4,2}(28)$ as $W(E_7)^+$-varieties, Theorem 5.6 also gives

$$\mathrm{RD}\big(W(D_6)\big) = \mathrm{RD}\big(\mathcal{H}_{4,2}(\widetilde{\mathcal{A}}) \to \mathcal{H}_{4,2}(\mathcal{S})\big).$$

Because $W(D_6) = (\mathbb{Z}/2\mathbb{Z})^{\times 5} \rtimes S_6$, Theorem 3.3 gives

$$\mathrm{RD}\big(W(D_6)\big) = \max\big\{1, \mathrm{RD}(S_6)\big\} = \mathrm{RD}(S_2 \times S_6) = \mathrm{RD}(S_6).$$ □

6. The resolvent degree of some enumerative problems

Consider an enumerative problem $\widetilde{\mathcal{M}} \dashrightarrow \mathcal{M}$ as in the introduction. As mentioned there, a typical first goal is to prove that this is a branched cover. One then tries to find its degree. The third step is to compute the Galois group of (the normal closure of) the covering. Computing $\mathrm{RD}(\widetilde{\mathcal{M}} \dashrightarrow \mathcal{M})$ can be interpreted as computing the number of parameters needed to specify a point in $\widetilde{\mathcal{M}}$ given a point of $\mathcal{M}$. This seems to us like a fundamental problem. We worked through the explicit examples of lines on a smooth cubic surface and bitangents on a smooth quartic in Sections 4 and 5. In this section we present a few more examples.

6.1. Tangency problems for plane curves. Steiner's 5 conics problem. A classical problem of Steiner asks how many conics in $\mathbb{P}^2$ are tangent to 5 given conics. After many incorrect answers and a long, rich history, the problem was answered around 40 years ago; see, e.g., [EH] and the references contained therein. The answer is 3264. But how to find these conics given the original 5, given by the coefficients of their defining equations?

Harris proves in [Har, IV] that this problem is not solvable by radicals, as follows. Let $W \cong \mathbb{P}^5$ denote the linear system of conics in $\mathbb{P}^2$, and let W_0 denote the Zariski open subset of smooth (i.e., non-degenerate) conics. Let

$$Y := \{(C_1, \ldots, C_5, C) \in W^5 \times W_0 : \ C \text{ is tangent to each } C_i\}.$$

Consider the map $\pi : Y \to W^5$ be $\pi(C_1, \ldots, C_5, C) := (C_1, \ldots, C_5)$. Then π is a 3264-sheeted branched cover. Harris (see §IV of [Har]) computes the monodromy group of this cover to be the full symmetric group S_{3264}. As this group is not solvable, Harris deduces that there is no formula in radicals for the coefficients of C in terms of the coefficients of the C_i.

Problem 6.1 (Refinements of Steiner's problem). Determine the monodromy of the natural branched covers of W^5 lying between Y and W^5. Determine which if any are solvable by radicals. For these, determine explicit formulas.

Problem 6.2 (Resolvent degree of the 5 conics problem). Compute $\mathrm{RD}(Y \to W^5)$.

There are many generalizations of Steiner's Problem, for many of which the associated monodromy group has been computed; see, e.g., [EH, HS]. It would be interesting to work out bounds on the resolvent degree for these problems.

Curves through specified points. There are many more such enumerative problems. For example, we have the following. Let $\mathcal{P}_d \subset (\mathbb{P}^2)^{3d-1}/S_{3d-1}$ be the parameter space of $(3d-1)$-tuples of distinct points in $\mathbb{P}^2$ in general position. A dimension count gives that the number n_d of degree d rational curves that pass through $3d-1$ such points in $\mathbb{P}^2$ is finite. It was known classically that

$n_2 = 1, n_3 = 12$ and $n_4 = 620$. In the early 1990's the following recursive formula for n_d was given by Kontsevich–Manin and Ruan–Tian (see, e.g., [EH] and the references contained therein):

$$n_d = \sum_{d_1+d_2=d, d_1,d_2>0} n_{d_1} n_{d_2} \left(d_1^2 d_2^2 \binom{3d-4}{3d_1-2} - d_1^3 d_2 \binom{3d-4}{3d_1-1} \right).$$

Let $X_d := \mathrm{PGL}_2 \backslash \mathrm{Rat}_d(\mathbb{P}^1, \mathbb{P}^2) / \mathrm{PGL}_3$ denote the moduli space of degree d rational curves. Let

$$Y_d := \{(p_1, \ldots, p_{3d-1}, C_1, \ldots, C_{n_d}) : p_j \in C_k \ \forall j, k\} \subset \mathcal{P}_d \times X_d^{n_d}.$$

Denote by $\pi_d : Y_d \to \mathcal{P}_d$ the natural projection. Then π_d is an n_d-sheeted branched cover.

Problem 6.3. Compute the monodromy of π_d, as well as of the intermediate covers. Compute $\mathrm{RD}(\pi_d)$.

Among many other variations, we mention the following.

Problem 6.4. All general degree n curves through $\frac{1}{2}n(n+3)-1$ fixed points pass through $\frac{1}{2}(n-1)(n-2)$ other fixed points (see, e.g., p. 191 of [Hilt]). Compute RD for the problem of finding one of the $\frac{1}{2}(n-1)(n-2)$ other points, as well as its monodromy.

6.2. Finding a point on a projective subvariety. In relating different problems about varieties in projective space, it will sometimes be useful to pick a basepoint on a variety in a way that varies algebraically over a parameter space. The following proposition, which we isolate because it might be useful in other contexts, states that to compute RD for any algebraic problem for degree d varieties of a fixed dimension in $\mathbb{P}^n$, one can add the data of a basepoint at the cost of finding a root of a degree d polynomial.

Proposition 6.5 (Finding a point on a subvariety of $\mathbb{P}^n$). *Let X be any variety over k, and let*

$$\begin{tikzcd} S \arrow[r] \arrow[dr] & X \times \mathbb{P}^n \arrow[d] \\ & X \end{tikzcd}$$

be any family of r-dimensional, degree d varieties in $\mathbb{P}^n$ such that $S \to X$ is a dominant map. Let

$$\begin{tikzcd} Y \arrow[r, dashed] \arrow[d, dashed] & \widetilde{X} \arrow[d, dashed] \\ S \arrow[r, dashed] & X \end{tikzcd} \tag{6.1}$$

be any pullback diagram with vertical maps being rational covers. Then

$$\mathrm{RD}(Y \dashrightarrow S) \le \mathrm{RD}(\widetilde{X} \dashrightarrow X) \le \max\{\mathrm{RD}(Y \dashrightarrow S), \mathrm{RD}(S_d)\}.$$

Proof. The first inequality follows from Lemma 2.5. We now prove the second inequality. Fix an $n-r$-dimensional linear subspace $L \subset \mathbb{P}^n$. Let $U \subset X$ be the Zariski open consisting of all $x \in X$ such that the variety S_x intersects L transversely. Define

$$U_1 := (U \times L) \cap S.$$

By Bezout's theorem, the map $U_1 \to U$ given by projection is a generically d-to-1 rational cover. Therefore, by Lemma 2.9,

$$\mathrm{RD}(U_1 \to U) \le \mathrm{RD}(\widetilde{\mathcal{P}}_d \to \mathcal{P}_d) = \mathrm{RD}(S_d).$$

By construction, we have a commuting triangle

$$\begin{tikzcd} & S \arrow[d] \\ U_1 \arrow[ur] \arrow[r] & X \end{tikzcd}$$

Form the pullback

$$\begin{tikzcd} U_1 \times_S Y \arrow[r] \arrow[d, dashed] & Y \arrow[d, dashed] \\ U_1 \arrow[r] & S \end{tikzcd}$$

By construction,

$$U_1 \times_S Y \dashrightarrow U_1 \to X$$

is a tower solving $\widetilde{X} \dashrightarrow X$. The definition of resolvent degree and Lemmas 2.5 and 2.7 imply that

$$\begin{aligned} \mathrm{RD}(\widetilde{X} \dashrightarrow X) &\le \mathrm{RD}(U_1 \times_S Y \dashrightarrow X) \\ &\le \max\{\mathrm{RD}(U_1 \times_S Y \dashrightarrow U_1), \mathrm{RD}(U_1 \to X)\} \\ &\le \max\{\mathrm{RD}(Y \dashrightarrow S), \mathrm{RD}(\widetilde{\mathcal{P}}_d \to \mathcal{P}_d)\} \end{aligned}$$

as claimed. $\square$

6.3. Resolvent degree and Bezout's theorem. Recall that $\mathcal{H}_{r,2}$ denotes the moduli space of smooth degree r curves in $\mathbb{P}^2$. Fix $r, s \geq 1$. Bezout's Theorem gives that for each pair of curves $C, C' \subset \mathbb{P}^2$ of degrees r and s, the intersection $C \cap C'$ has rs points, where each $p \in C \cap C'$ is counted with the intersection multiplicity $I_p(C, C')$. Let

$$\mathcal{H}_{(r,s),2} := \left(\left(\mathbb{P}^{\binom{r+2}{2}-1} - \Sigma_r\right) \times \left(\mathbb{P}^{\binom{s+2}{2}-1} - \Sigma_s\right)\right) / \operatorname{PGL}_3$$

denote the moduli of pairs of smooth plane curves (C, C') with $\deg(C) = r$, $\deg(C') = s$ (where Σ_r, and Σ_s denote the loci of singular curves). Let $U_{r,s}$ denote the Zariski open

$$U_{r,s} := \left\{(C, C') : I_p(C, C') = 1 \ \forall p \in C \cap C'\right\} \subset \mathcal{H}_{(r,s),2}$$

and consider the covering

$$\begin{array}{ll} \widetilde{U}_{r,s} & := \left\{(C, C', p) : p \in C \cap C'\right\} \subset U_{r,s} \times \mathbb{P}^2 \\ \pi \big\downarrow & \\ U_{r,s} & \end{array}$$

given by $\pi(C, C', p) := (C, C')$. Note that $\pi^{-1}(C, C') = C \cap C' \subset \mathbb{P}^2$. Bezout's Theorem implies that $\pi : \widetilde{U}_{r,s} \to U_{r,s}$ is an rs-sheeted cover. It is known that the monodromy of this cover is the full symmetric group S_{rs}; see, for example, [HS, Corollary 1]. Thus there is a formula in radicals for the intersection of two curves of degrees $r, s \leq 2$, but there is no such formula when $rs > 4$. It is natural to ask for the minimal number $\operatorname{RD}(\widetilde{U}_{r,s} \to U_{r,s})$ of parameters for any formula for an intersection point of two smooth curves, given the coefficients defining those curves. By the computation of the monodromy, we have

$$\operatorname{RD}(\widetilde{U}_{r,s} \to U_{r,s}) \leq \operatorname{RD}(S_{rs}). \tag{6.2}$$

Problem 6.6. For which r and s does equality hold in (6.2)?

6.4. Finding flexpoints. Let C be a degree $d \geq 2$ plane curve. For a generic point $p \in C$, the tangent line ℓ_p to C at p intersects C with multiplicity $m_p(C \cdot \ell_p) = 2$. Recall that p is a *flex point* of C if $m_p(C \cdot \ell_p) \geq 3$; it is a *simple flex* if $m_p(C \cdot \ell_p) = 3$. It is known that any degree d curve C has $3d(d-2)$ flex points, counted with multiplicity. Recall that $\mathcal{H}_{d,2}$ denotes the moduli space of smooth degree d curves on $\mathbb{P}^2$. Let $\mathcal{H}_{d,2}(\text{flex}) \subset \mathcal{H}_{d,2} \times \mathbb{P}^2$ be the moduli space of pairs (C, p) where $p \in C$ is a flex point. The projection map $\mathcal{H}_{d,2}(\text{flex}) \to \mathcal{H}_{d,2}$ given by $(C, p) \mapsto p$ is a $3d(d-2)$-sheeted covering when restricted to the Zariski open in $\mathcal{H}_{d,2}$ consisting of those degree d curves C all of whose flex points are simple.

The monodromy of $\mathcal{H}_{3,2}(\text{flex}) \to \mathcal{H}_{3,2}$ is solvable (see [Har, II.2]), so that

$$\mathrm{RD}\big(\mathcal{H}_{3,2}(\text{flex}) \to \mathcal{H}_{3,2}\big) = 1.$$

In contrast, Harris proves in II.3 of [Har] that for $d \geq 4$, the monodromy of $\mathcal{H}_{d,2}(\text{flex}) \to \mathcal{H}_{d,2}$ is $S_{3d(d-2)}$, which is not solvable if $d \geq 4$. While Harris concludes from this that there is no formula in radicals for the flex points of a general degree $d \geq 4$ smooth plane curve, the basic question remains as to how complicated any formula not-in-radicals actually is.

Problem 6.7 (Finding flexpoints). Compute the resolvent degree for the problem of finding a flexpoint on a smooth degree $d \geq 4$ plane curve; that is, compute $\mathrm{RD}(\mathcal{H}_{d,2}(\text{flex}) \to \mathcal{H}_{d,2})$.

It is a classical fact that for a degree d curve C, the flexpoints of C are precisely the intersection points of C with its associated Hessian curve H_C, which has degree $3(d-2)$. However, Problem 6.7 is quite different than the situation considered in §6.3. Indeed, while the map

$$\begin{gathered} \mathcal{H}_{d,2} \to^{H} U_{d,3(d-2)} \\ C \mapsto (C, H_C) \end{gathered}$$

fits into a pullback square

$$\begin{tikzcd} \mathcal{H}_{d,2}(\text{flex}) \arrow[r] \arrow[d] & \widetilde{U}_{d,3(d-2)} \arrow[d] \\ \mathcal{H}_{d,2} \arrow[r, "H"] & U_{d,3(d-2)} \end{tikzcd},$$

the codimension of $H(\mathcal{H}_{d,2}) \subset U_{d,3(d-2)}$ is always positive and grows quadratically in d.

7. The resolvent degree of the roots of a polynomial

While the problem of simplifying the formulas needed to solve a general polynomial has been central to the mathematical tradition since the Babylonians, the study of the resolvent degree of polynomials essentially originates with work of Tschirnhaus [Tsch] in the 17th century. Tschirnhaus introduced the *Tschirnhaus transformation*, which remains essentially the only method for providing general upper bounds on $\mathrm{RD}(\widetilde{\mathcal{P}}_n \to \mathcal{P}_n)$. We review Tschirnhaus transformations from a geometric standpoint below, and then we treat several of the classical upper bounds from this perspective.

7.1. Tschirnhaus transformations and classical solutions of polynomials.

Elementary perspective. Consider the general degree n polynomial

$$p(x) := x^n + a_1 x^{n-1} + \cdots + a_n = 0,$$

with roots $x_1, \ldots, x_n$. A *Tschirnhaus transformation* $T(b_0, \ldots, b_{n-1})$ (for some $b_0, \ldots, b_{n-1}$) sends the roots x_i to

$$T(b_0, \ldots, b_{n-1})(x_i) := b_0 x_i^{n-1} + b_1 x_i^{n-2} + \cdots + b_{n-1}.$$

The Tschirnhaus transformation of the polynomial $p(x)$ is defined by

$$T(b_0, \ldots, b_{n-1})(p)(x) := \prod_i \bigl(x - T(b_0, \ldots, b_{n-1})(x_i)\bigr).$$

Because the assignment $x_i \mapsto T(b_0, \ldots, b_{n-1})(x_i)$ is symmetric in the roots, the coefficients of $T(b_0, \ldots, b_{n-1})(p)$ are polynomials in the a_i and the b_j. Accordingly, by solving polynomials in the b_j whose coefficients are polynomials in the a_i, we can find special Tschirnhaus transformations which convert our original polynomial $p(x)$ into a polynomial whose coefficients satisfy special conditions, e.g., some collection of the coefficients are zero.

Note that, given the roots of $T(b_0, \ldots, b_{n-1})(p)$, we can recover the roots of p by a rational transformation. See [Hu, Lemma 4.2.1] for a clear treatment.

As covariants. Tschirnhaus transformations can also be defined as S_n-equivariant maps

$$T \colon \mathbb{A}^n \to \mathbb{A}^n$$

In the setting above, we have an auxiliary affine space parametrizing Tschirnhaus transformations

$$\mathbb{A}^n_T := \bigl\{(b_0, \ldots, b_{n-1})\bigr\}$$

and a map

$$\mathbb{A}^n_T \to \mathrm{Alg}_{S_n}(\mathbb{A}^n, \mathbb{A}^n)$$

from the affine space parametrizing Tschirnhaus transformations to the space of maps of S_n-varieties $\mathbb{A}^n \to \mathbb{A}^n$.

Geometric perspective. Equivalently, we have an S_n-equivariant "evaluation" map

$$\mathbb{A}^n \times \mathbb{A}^n_T \to^{\varepsilon} \mathbb{A}^n$$

where S_n acts trivially on the $\mathbb{A}^n_T$ factor, and via the permutation representation on each $\mathbb{A}^n$. Passing to the quotients, we obtain a commuting square

$$\begin{tikzcd} \mathbb{A}^n \times \mathbb{A}^n_T \arrow[r, "\varepsilon"] \arrow[d] & \mathbb{A}^n \arrow[d] \\ \mathcal{P}_n \times \mathbb{A}^n_T \arrow[r, "\bar{\varepsilon}"] & \mathcal{P}_n \end{tikzcd}$$

To bound the resolvent degree of $\widetilde{\mathcal{P}}_n \to \mathcal{P}_n$ via a Tschirnhaus transformation, one now specifies

(1) a Zariski closed S_n-invariant subvariety $V \subset \mathbb{A}^n$, and

(2) a rational cover $U \dashrightarrow \mathcal{P}_n$ along with a section

$$\begin{tikzcd} & \varepsilon^{-1}(V) \arrow[d] \\ U \arrow[ur, dashed] \arrow[r, dashed] & \mathcal{P}_n \end{tikzcd}$$

Given these data, one obtains

$$\mathrm{RD}(\widetilde{\mathcal{P}}_n \to \mathcal{P}_n) \le \max\bigl\{\mathrm{RD}(U \dashrightarrow \mathcal{P}_n), \dim(V)\bigr\}.$$

Remark 7.1. Standard examples of V are given by

$$V_{1\cdots i} := \bigcap_{j=1}^{i} \{\sigma_j = 0\} \subset \mathbb{A}^n,$$

where the σ_j are the elementary symmetric functions. Finding $U \dashrightarrow \mathcal{P}_n$ with a map $U \dashrightarrow \varepsilon^{-1}(V_{1\cdots i})$ over $\mathcal{P}_n$ is just to find a Tschirnhaus transformation which sets the first i coefficients of the general degree n polynomial to 0.

We now illustrate this procedure in several classical examples.

7.2. The Bring–Hamilton 4-parameter reduction. In 1786 Bring [Bri] proved the following, which was independently discovered by Hamilton [Ham].

Theorem 7.2 (Bring–Hamilton 4-parameter reduction). *For any $n \geq 5$:*

$$\mathrm{RD}(\widetilde{\mathcal{P}}_n \to \mathcal{P}_n) \le n - 4.$$

From the above perspective, Bring's proof is as follows.

Proof. First, restrict to the space of quartic Tschirnhaus transformations, i.e.

$$T(b_0, \ldots, b_4)(x_i) = b_0 x_i^4 + \cdots + b_4.$$

Next, observe that the fiberwise projectivization of $\varepsilon^{-1}(V_1) \to \mathcal{P}_n$ is a trivial $\mathbb{P}^3$ bundle, since the condition that the first coefficient vanish is linear in the b_j, and this 3-plane bundle admits a rational section. Therefore, the fiberwise projectivization of $\varepsilon^{-1}(V_{12}) \to \mathcal{P}_n$ is a bundle of quadric surfaces in $\mathbb{P}^3$. Denote by $\mathcal{H}_{2,3}$ the moduli of quadric surfaces and let $\mathcal{H}_{2,3}(L) \subset \mathcal{H}_{2,3} \times Gr(2,4)$ be the moduli of quadric surfaces equipped with a line, so that the two connected components of $\mathcal{H}_{2,3}(L)$ (corresponding to the two rulings of the quadric) each give a $\mathbb{P}^1$-bundle over $\mathcal{H}_{2,3}$. We have a map

$$\begin{aligned} \mathcal{P}_n &\to \mathcal{H}_{2,3} \\ p &\mapsto \varepsilon^{-1}(V_{12})|_p \end{aligned}$$

By the classical theory of quadratic forms (for a detailed contemporary treatment, see, e.g., [Wol, Lemma 5.2]), after passing to a branched cover $U_1 \to \mathcal{P}_n$ of degree 2^4 (i.e., by adjoining 4 square roots of polynomials in the coefficients), we can diagonalize the associated quadratic form, i.e.,

$$V_{12}|_U \cong V\left(\sum_{i=0}^{3} L_i^2\right)$$

for rational hyperplanes $L_i \subset \mathbb{P}^3_U$. Then $\{L_0 + \sqrt{-1}L_1 = 0, L_2 + \sqrt{-1}L_3 = 0\}$ defines a line on the quadric. In other words, there exists a lift of the map $U_1 \to \mathcal{H}_{2,3}$

$$\begin{tikzcd} & \mathcal{H}_{2,3}(L) \arrow[d] \\ U_1 \arrow[ur, "L"] \arrow[r] & \mathcal{H}_{2,3} \end{tikzcd}$$

By intersecting the family of cubics $\varepsilon^{-1}(V_3)$ with this line, we obtain a map

$$\begin{aligned} U_1 &\to \mathcal{P}_3 \\ u &\mapsto L(u) \cap \varepsilon^{-1}(V_3)|_u \end{aligned}$$

Forming the pullback

$$\begin{tikzcd} U_2 \arrow[r] \arrow[d] & \widetilde{\mathcal{P}}_3 \arrow[d] \\ U_1 \arrow[r] & \mathcal{P}_3 \end{tikzcd}$$

we obtain a branched cover $U_2 \to \mathcal{P}_n$ and a section

$$\begin{tikzcd} & \varepsilon^{-1}(V_{123}) \arrow[d] \\ U_2 \arrow[ur] \arrow[r] & \mathcal{P}_n \end{tikzcd}$$

By construction,

$$\begin{aligned}\mathrm{RD}(U_2 \to \mathcal{P}_n) &= \max\big\{\mathrm{RD}(U_2 \to U_1), \mathrm{RD}(U_1 \to \mathcal{P}_n)\big\}\\ &\le \max\big\{\mathrm{RD}(\widetilde{\mathcal{P}}_3 \to \mathcal{P}_3), 1\big\} = 1.\end{aligned}$$

Therefore

$$\mathrm{RD}(\widetilde{\mathcal{P}}_n \to \mathcal{P}_n) \le \max\big\{\mathrm{RD}(\sqrt{-}), \mathrm{RD}(\widetilde{\mathcal{P}}_3 \to \mathcal{P}_3), \mathrm{RD}(V_{123} \to \mathbb{A}^{n-3})\big\}$$

where the final space $\mathbb{A}^{n-3}$ is the moduli space of all monic degree n polynomials of the form

$$x^n + a_4 x^{n-4} + \cdots + a_{n-1}x + a_n = 0.$$

Restricting to locus $U \subset \mathbb{A}^{n-3}$ where $a_{n-1} \neq 0 \neq a_n$, we can define a linear Tschirnhaus transformation

$$T(x_i) := \frac{a_{n-1}}{a_n} x_i$$

to set the last two coefficients to be equal. This defines a pullback diagram

$$\begin{tikzcd} V_{123}|_U \arrow[r, "T"] \arrow[d] & V_{123,(n-1)=n} \arrow[d] \\ U \arrow[r, "\bar{T}"] & \mathbb{A}^{n-4} \end{tikzcd}$$

where $\mathbb{A}^{n-4}$ denotes the space of all polynomials of the form

$$x^n + b_4 x^{n-4} + \cdots + b_{n-1}x + b_{n-1} = 0.$$

We conclude that, for $n \ge 5$,

$$\begin{aligned}\mathrm{RD}(\widetilde{\mathcal{P}}_n \to \mathcal{P}_n) &\le \max\big\{\mathrm{RD}(\sqrt{-}), \mathrm{RD}(\widetilde{\mathcal{P}}_3 \to \mathcal{P}_3), \mathrm{RD}(V_{123,(n-1)=n} \to \mathbb{A}^{n-4})\big\}\\ &\le n-4\end{aligned}$$

as desired. $\square$

As a consequence of the Bring–Hamilton theorem, we obtain the upper bounds in Hilbert's Sextic and Octic Conjectures Hilbert's and 13th Problem.

Corollary 7.3. $\mathrm{RD}(\widetilde{\mathcal{P}}_6 \to \mathcal{P}_6) = \mathrm{RD}(S_6) \le 2$, $\mathrm{RD}(\widetilde{\mathcal{P}}_7 \to \mathcal{P}_7) = \mathrm{RD}(S_7) \le 3$, *and* $\mathrm{RD}(\widetilde{\mathcal{P}}_8 \to \mathcal{P}_8) \le 4$.

7.3. Brauer's bounds. Hamilton [Ham] was the first to show that

$$\lim_{n\to\infty} n - \mathrm{RD}(\widetilde{\mathcal{P}}_n \to \mathcal{P}_n) = \infty.$$

More precisely, he showed the existence of a function $H\colon \mathbb{N} \to \mathbb{N}$, such that for $n \geq H(r)$, $n - \mathrm{RD}(\widetilde{\mathcal{P}}_n \to \mathcal{P}_n) \geq r$, and he computed the initial values of H:

r	4	5	6	7	8	9
$H(r)$	5	11	47	923	409,619	83,763,206,255

By the mid-20th century, Hamilton's work appears to have been forgotten. Segre [Seg1], building on Hilbert's work on the degree 9 equation, proved that $\mathrm{RD}(\widetilde{\mathcal{P}}_n \to \mathcal{P}_n) \leq n-6$ for $n \geq 157$. He further conjectured that

$$\lim_{n\to\infty} n - \mathrm{RD}(\widetilde{\mathcal{P}}_n \to \mathcal{P}_n) = \infty;$$

that is, he conjectured precisely what Hamilton had shown over a century earlier. Shortly after, in 1945, Brauer [Brau1] and Segre each reproved this statement, but without giving effective bounds. Three decades later, Brauer [Brau2] proved the following theorem, which provides the best general upper bounds on $\mathrm{RD}(\widetilde{\mathcal{P}}_n \to \mathcal{P}_n)$ to date.

Theorem 7.4 (Brauer [Brau2]**).** *Let $n > 3$. For any $r \geq 2$*

$$\mathrm{RD}(\widetilde{\mathcal{P}}_n \to \mathcal{P}_n) \leq n - r \quad \textit{for all } n \geq (r-1)! + 1.$$

We include a streamlined version of Brauer's proof of Theorem 7.4 for completeness.

Proof. We prove this by induction on r. The base case $r = 1$ follows from the Babylonians: $\mathrm{RD}(n) \leq n-1$ for all $n \geq 2$, via a linear translation of the roots.

For the inductive step, consider the full space of Tschirnhaus transformations $\mathbb{P}^{n-1}_T$. Observe that

$$\bar{\varepsilon}^{-1}(V_{1\cdots(r-1)}) \to \mathcal{P}_n$$

is a bundle of $(n-r+1)$-dimensional , degree $(r-1)!$ subvarieties of $\mathbb{P}^{n-1}_T$. By construction, there is an isomorphism of varieties over $\bar{\varepsilon}^{-1}(V_{1\cdots(r-1)})$:

$$\widetilde{\mathcal{P}}_n \times_{\mathcal{P}_n} \bar{\varepsilon}^{-1}\big(V_{1\cdots(r-1)}\big) \cong \bar{\varepsilon}^{-1}\big(V_{1\cdots(r-1)}\big) \times_{\mathbb{A}^{n-(r-1)}} \widetilde{\mathcal{P}}_n|_{\mathbb{A}^{n-r-1}}$$

where $\mathbb{A}^{n-(r-1)} \subset \mathcal{P}_n$ denotes the space of all monic polynomials with the first $(r-1)$ coefficients vanishing. Therefore

$$\mathrm{RD}\Big(\widetilde{\mathcal{P}}_n \times_{\mathcal{P}_n} \bar{\varepsilon}^{-1}\big(V_{1\cdots(r-1)}\big) \to \bar{\varepsilon}^{-1}\big(V_{1\cdots(r-1)}\big)\Big) \leq \mathrm{RD}\big(\widetilde{\mathcal{P}}_n|_{\mathbb{A}^{n-(r-1)}} \to \mathbb{A}^{n-(r-1)}\big).$$

Proposition 6.5 then implies

$$\begin{aligned}\mathrm{RD}(\widetilde{\mathcal{P}}_n \to \mathcal{P}_n) &\le \max\Big\{\mathrm{RD}\Big(\widetilde{\mathcal{P}}_n \times_{\mathcal{P}_n} \bar{\varepsilon}^{-1}\big(V_{1\cdots(r-1)}\big) \to \bar{\varepsilon}^{-1}\big(V_{1\cdots(r-1)}\big)\Big),\\ &\qquad\qquad \mathrm{RD}(\widetilde{\mathcal{P}}_{(r-1)!} \to \mathcal{P}_{(r-1)!})\Big\}\\ &\le \max\Big\{\mathrm{RD}\big(\widetilde{\mathcal{P}}_n|_{\mathbb{A}^{n-(r-1)}} \to \mathbb{A}^{n-(r-1)}\big), \mathrm{RD}\big(\widetilde{\mathcal{P}}_{(r-1)!} \to \mathcal{P}_{(r-1)!}\big)\Big\}.\end{aligned}$$

An analogous linear Tschirnhaus transformation to that in Bring and Hilbert shows

$$\mathrm{RD}\big(\widetilde{\mathcal{P}}_n|_{\mathbb{A}^{n-(r-1)}} \to \mathbb{A}^{n-(r-1)}\big) \le n - r.$$

The inductive hypothesis then gives

$$\mathrm{RD}\big(\widetilde{\mathcal{P}}_{(r-1)!} \to \mathcal{P}_{(r-1)!}\big) \le (r-1)! - (r-1) \le n - r,$$

completing the proof of the induction step. □

Remark 7.5. Note that Brauer's proof does not make use of the Bring–Hamilton idea. Moreover, Hilbert [Hil2] sketched an approach using lines on cubic surfaces to show that $\mathrm{RD}(9) \le 4$. Brauer needs $n \ge 25$ in order to conclude $\mathrm{RD}(\widetilde{\mathcal{P}}_n \to \mathcal{P}_n) \le n - 5$. In [Wol], an extension of Hilbert's argument leads to a substantial improvement over Brauer's bounds for general n.

8. The equivalence of Hilbert's conjectures to classical geometry problems

As with many Hilbert problems, the specific statement of Hilbert's Sextic Conjecture, 13th Problem and Octic Conjecture (see Problem 1.5) turns out to be much broader and more widely connected to other problems than one might at first glance guess. The goal of this section is to use the theory we have developed so far to prove the equivalence of each of these problems with many other natural problems of both geometric and arithmetic natures. We give each statement in English form, and name the corresponding problem in terms of moduli spaces when we have already named them explicitly.

We organize things into five groups of examples, according to the group that is acting. The five classes of examples are ordered in complexity via:

$$\begin{array}{ccc} & \mathrm{RD}\big(W(E_6)\big) & \\ \mathrm{RD}(S_6) \le & & \le \mathrm{RD}\big(W(E_7)\big) \\ & \mathrm{RD}(S_7) \le \mathrm{RD}(S_8) & \end{array}$$

8.1. S_6-varieties and Hilbert's Sextic Conjecture. We start with the Sextic Conjecture.

Theorem 8.1 (RD of S_6 varieties). *The following statements are equivalent:*

(1) *Hilbert's Sextic Conjecture is true:* $\mathrm{RD}(\widetilde{\mathcal{P}}_6 \to \mathcal{P}_6) = 2$.

(2) $\mathrm{RD}(S_6) = 2$.

(3) $\mathrm{RD}(V \to V/S_6) = 2$ *for any faithful, linear* S_6*-variety* V.

(4) $\mathrm{RD}(\mathcal{M}_{0,6} \to \mathcal{M}_{0,6}/S_6) = 2$.

(5) $\mathrm{RD} = 2$ *for the problem of finding a fixed point for the* $\mathbb{Z}/3\mathbb{Z}$ *action on a genus* 4 *curve of the form* $y^3 = P(x)$, *where* $P(x)$ *is a square-free polynomial of degree* 6*:*

$$\mathrm{RD}\big(\widetilde{\mathcal{C}_{3,6}} \to \mathcal{C}_{3,6}\big) = 2.$$

(6) $\mathrm{RD} = 2$ *for the problem of finding a fixed point for the hyperelliptic involution on a genus* 2 *curve:*

$$\mathrm{RD}\big(\mathcal{M}_2(\widetilde{\Delta}) \to \mathcal{M}_2\big) = 2.$$

(7) RD *of finding the* 27 *lines on a cubic, given a double-six:*

$$\mathrm{RD}\big(\mathcal{H}_{3,3}(27) \to \mathcal{H}_{3,3}(6,6)\big) = 2.$$

(8) RD *of finding the* 27 *lines on a smooth cubic surface* S *given the unordered hexahedral form of* S*:*

$$\mathrm{RD}\big(\mathcal{H}_{3,3}(27) \to H/S_6\big) = 2.$$

In fact, the resolvent degrees of all of the above problems coincide.

Proof. We prove the theorem via chains of equivalences.

Equivalence of 1, 2, 3, and 4. The equivalence of the first four follows from Corollary 3.17 1 together with Corollary 3.18.

Equivalence of 4, 5. Consider the moduli space $\mathcal{C}_{3,6}$ of isomorphism classes of algebraic curves of the form $y^3 = P(x)$ where P has is a square-free polynomial of degree 6. These are genus 4 curves equipped with a $\mathbb{Z}/3\mathbb{Z}$ action, the quotient giving a branched cover $\Sigma_4 \to \mathbb{P}^1$ branched over 6 points, each of order 3. Let $\widetilde{\mathcal{C}_{3,6}}$ denote the moduli of curves in $\mathcal{C}_{3,6}$ equipped with an ordering of the $\mathbb{Z}/3\mathbb{Z}$-fixed points. The forgetful map

$$\widetilde{\mathcal{C}_{3,6}} \to \mathcal{C}_{3,6}$$

is a Galois S_6-cover. By mapping the fixed points to $\mathbb{P}^1$ under the $\mathbb{Z}/3\mathbb{Z}$-quotient, we obtain the commutative diagram

$$\begin{tikzcd} \widetilde{\mathcal{C}_{3,6}} \arrow[r] \arrow[d] & \mathcal{M}_{0,6} \arrow[d] \\ \mathcal{C}_{3,6} \arrow[r] & \mathcal{M}_{0,6}/S_6 \end{tikzcd} \tag{8.1}$$

in which the horizontal arrows are birational, equivariant with respect to the S_6 actions, and the bottom row is the quotient of the top row by the S_6 action. The stabilizer of a fixed point is $S_5 \subset S_6$, and thus $\widetilde{\mathcal{C}_{3,6}} \to \mathcal{C}_{3,6}$ is the Galois closure of the cover parametrizing curves in $\mathcal{C}_{3,6}$ with a single choice of fixed point. Together with Lemma 2.11, this proves the equivalence of 4, and 5.

Equivalence of 4 and 6. The *Segre cubic threefold* X_3 is the threefold in $\mathbb{P}^5$ given by

$$X_3 := \left\{[x_0 : \cdots : x_5] \in \mathbb{P}^5 : \sum_{i=0}^{5} x_i = 0 = \sum_{i=0}^{5} x_i^3\right\}.$$

The permutation action of S_6 on $\mathbb{P}^5$ leaves invariant X_3, permuting its 10 nodes. It's classically known that $X_3 \cong \mathcal{M}_{0,6}$ as S_6-varieties.

Hunt proves in [Hu, Theorem 3.3.11] that the dual variety to X_3 is the so-called *Igusa quartic* $\mathcal{I}_4$, which is the moduli space of 6 points on a conic in $\mathbb{P}^2$. The two varieties X_3 and $\mathcal{I}_4$ are S_6-equivariantly birational. The Igusa quartic $\mathcal{I}_4$ is the Satake compactification of the moduli space $\mathcal{M}_2(\widetilde{\Delta})$ of hyperelliptic curves of genus 2 with a marking of the 6 branch points. The group S_6 acts by permuting these marked points. We thus obtain a commutative diagram in which all horizontal arrows are birational equivalences

$$\begin{tikzcd} \mathcal{M}_{0,6} \arrow[r, "\sim"] \arrow[d] & \mathcal{I}_4 \arrow[d] & \mathcal{M}_2(\widetilde{\Delta}) \arrow[l, "\sim"'] \arrow[d] \\ \mathcal{M}_{0,6}/S_6 \arrow[r, "\sim"] & \mathcal{I}_4/S_6 & \mathcal{M}_2 \arrow[l, "\sim"'] \end{tikzcd} \tag{8.2}$$

Thus each of the rational covers in (8.2) have equal resolvent degree.

Equivalence of 2, 7 and 8. As explained in (4.4), the moduli space of pairs (S, D) where $S \in \mathcal{H}_{3,3}$ and D is a double-six in S can be identified with $\mathcal{H}_{3,3}(27)/S_6$. Thus the problem of finding all 27 lines on a smooth cubic surface given a double-six is $\mathrm{RD}(\mathcal{H}_{3,3}(27) \to \mathcal{H}_{3,3}(27)/S_6)$. By Proposition 4.4, $\mathcal{H}_{3,3}(27)$ is versal for any $G \subset W(E_6)$. Therefore, by Proposition 3.7,

$$\mathrm{RD}\big(\mathcal{H}_{3,3}(27) \to \mathcal{H}_{3,3}(27)/S_6\big) = \mathrm{RD}(S_6),$$

proving the equivalence of 2 and 7 .

Now recall from §4.8 that the moduli space of unordered hexahedral forms for smooth cubic surfaces fits in to the sequence of branched covers (see (4.8)) :

$$\mathcal{H}_{3,3}(27) \xrightarrow{t_1} H \xrightarrow{t_2} H/S_6 \xrightarrow{t_3} \mathcal{H}_{3,3}$$

where t_1 is an unramified 2-sheeted cover, t_3 is an unramified 36-sheeted cover, and t_2 is a generically 720-to-1 branched cover. The composite is a Galois branched cover, with deck group $S_2 \times S_6 \subset W(E_6)$, i.e.

$$H/S_6 = \mathcal{H}_{3,3}/(S_2 \times S_6)$$

Proposition 4.4 therefore implies

$$\mathrm{RD}\big(\mathcal{H}_{3,3}(27) \to H/S_6\big) = \mathrm{RD}(S_2 \times S_6) = \mathrm{RD}(S_6),$$

proving the equivalence of 8 and 2. □

8.2. $W(E_6)$-varieties and lines on a smooth cubic surface. In this section we summarize the equality of the resolvent degree of different $W(E_6)$-varieties proven above.

Theorem 8.2 (RD of $W(E_6)$ varieties). *The following are equal:*

1. $\mathrm{RD}\big(W(E_6)\big)$.
2. $\mathrm{RD}\big(V \to V/W(E_6)\big)$ *for* V *any faithful representation of* $W(E_6)$.
3. RD *of finding all 27 lines on a smooth cubic surface:*

$$\mathrm{RD}\big(\mathcal{H}_{3,3}(27) \to \mathcal{H}_{3,3}\big).$$

4. RD *of finding a line on a smooth cubic surface:*

$$\mathrm{RD}\big(\mathcal{H}_{3,3}(1) \to \mathcal{H}_{3,3}\big).$$

5. RD *of finding* 28 *bitangents on a smooth plane quartic, given one of them:*

$$\mathrm{RD}\big(\mathcal{H}_{4,2}(28) \to \mathcal{H}_{4,2}(1)\big).$$

Further, all of the above are at most 3.

Proof. We prove the theorem in chains of equivalences.

Equivalence of 1, 2, 3 and 4. This follows from the proof of Theorem 4.3. Moreover, from Theorem 4.3, we obtain the upper bound of 3.

Equivalence of 3 and 5. This is the statement of Theorem 5.6 above. □

8.3. S_7-varieties and Hilbert's 13th Problem. We now prove the equivalence of Hilbert's 13th problem with various other problems. Recall that $\mathcal{C}_n(\mathbb{P}^m)$ denotes the moduli space of ordered n-tuples of distinct points in P^m modulo the action of PGL_{m+1}.

Theorem 8.3 (**RD of S_7 varieties**). *The following are equivalent:*

(1) *Hilbert's 13th problem:* $\mathrm{RD}(\widetilde{\mathcal{P}}_7 \to \mathcal{P}_7) = 3$.

(2) $\mathrm{RD}(V \to V/S_7 = 3)$ *for any faithful linear representation* V *of* S_7.

(3) $\mathrm{RD}(S_7) = 3$.

(4) $\mathrm{RD}(\mathcal{C}_7(\mathbb{P}^n) \to \mathcal{C}_7(\mathbb{P}^n)/S_7) = 3$ *for* $n \leq 4$*; in particular*

$$\mathrm{RD}(\mathcal{M}_{0,7} \to \mathcal{M}_{0,7}/S_7) = 3.$$

(5) $\mathrm{RD} = 3$ *for the problem of finding the* 28 *bitangents on a smooth quartic* C*, given an Aronhold set on* C*:*

$$\mathrm{RD}\big(\mathcal{H}_{4,2}(28) \to \mathcal{H}_{4,2}(\mathcal{A})\big) = 3.$$

In fact, the resolvent degrees of all of the above problems coincide.

Proof. **Equivalence of 1, 2, 3 and 4.** This follows from Corollary 3.17 1 together with Corollary 3.18.

Equivalence of 3 and 5. The equivalence of 3 and 5 follows from Theorem 5.6. □

8.4. S_8-varieties and Hilbert's Octic Conjecture. We now prove the equivalence of Hilbert's Octic Conjecture to several problems about plane quartics and genus 3 curves.

Theorem 8.4 (RD of S_8-varieties). *The following are equivalent:*

1. *Hilbert's Octic Conjecture:* $\mathrm{RD}(\widetilde{\mathcal{P}}_8 \to \mathcal{P}_8) = 4$.
2. $\mathrm{RD}(V \to V/S_8 = 4)$ *for any faithful linear representation* V *of* S_8.
3. $\mathrm{RD}(S_8) = 4$.

4. $\mathrm{RD}(\mathcal{C}_8(\mathbb{P}^n) \to \mathcal{C}_8(\mathbb{P}^n)/S_8) = 4$, *for* $n \leq 5$; *in particular*

$$\mathrm{RD}(\mathcal{M}_{0,8} \to \mathcal{M}_{0,8}/S_8) = 4.$$

5. $\mathrm{RD} = 4$ *for the problem of finding the* 28 *bitangents on a smooth quartic* C, *given an even* θ*-characteristic:*

$$\mathrm{RD}\big(\mathcal{H}_{4,2}(28) \to \mathcal{H}_{4,2}(\theta^{\mathrm{ev}})\big) = 4,$$

6. $\mathrm{RD} = 4$ *for the problem of finding an Aronhold set on a smooth plane quartic* C *given an even* θ*-characteristic:*

$$RD\big(\mathcal{H}_{4,2}(\mathcal{A}) \to \mathcal{H}_{4,2}(\theta^{\mathrm{ev}})\big) = 4,$$

7. $\mathrm{RD} = 4$ *for the problem of finding the 28 bitangents on a quartic, given a Cayley octad:*

$$\mathrm{RD}\big(\mathcal{H}_{4,2}(28) \to \mathrm{Cay}\big) = 4.$$

In fact, the resolvent degrees of all of the above problems coincide.

Proof. The equivalence of (1), (2) and (3) follows from Corollary 3.17 1.

For the equivalence of (3), (4), and (5), observe that there exists a diagram of $W(E_7)^+$-equivariant maps

$$\mathbb{A}(\mathfrak{h}) \dashrightarrow \mathbb{P}(\mathfrak{h}) \dashrightarrow \mathcal{C}_7(\mathbb{P}^2) \dashrightarrow \mathcal{H}_{4,2}(28) \tag{8.3}$$

Indeed, the sequence

$$\mathbb{A}(\mathfrak{h}) \dashrightarrow \mathbb{P}(\mathfrak{h}) \dashrightarrow \mathcal{C}_7(\mathbb{P}^2) \dashrightarrow \mathcal{H}_{4,2}(28)$$

was constructed as (5.6) in the proof of Proposition 5.7. Because $W(E_7)^+$ is simple, all the varieties in (8.3) are faithful $W(E_7)^+$-varieties. By Proposition 3.16 and Lemma 3.11, we conclude that all of these varieties are versal G-varieties for any $G \subset W(E_7)^+$, in particular for $G = S_8$. The equivalence of (3), (4), and (5) now follows from Proposition 3.7. The equivalence of (5) and (6) follows from Lemma 2.11 and the fact that

$$\mathcal{H}_{4,2}(28) \to \mathcal{H}_{4,2}(\theta^{\mathrm{ev}})$$

is a Galois closure of the cover

$$\mathcal{H}_{4,2}(\mathcal{A}) \to \mathcal{H}_{4,2}(\theta^{\mathrm{ev}}).$$

Finally, the equivalence of (3) and (7) follows from the classical fact that there is a birational map

$$\mathcal{H}_{4,2}(28)/S_8 \simeq \mathrm{Cay}$$

from the S_8 quotient of the moduli of smooth plane quartics with an ordering of their 28 bitangents to the moduli of Cayley octads. $\square$

8.5. $W(E_7)$ and bitangents to a planar quartic. In this section we prove the equality of the resolvent degree of different $W(E_7)^+$-varieties.

Theorem 8.5 (RD of $W(E_7)$ and bitangents to a planar quartic). *The following are equal:*

1. $\mathrm{RD}\big(W(E_7)\big)$.
2. $\mathrm{RD}\big(W(E_7)^+\big)$
3. $\mathrm{RD}(V \to V/G)$ *for* $G = W(E_7)^+, W(E_7)$ *and* V *any faithful representation of* G.
4. $\mathrm{RD}\big(\mathcal{C}_7(\mathbb{P}^2) \to \mathcal{C}_7(\mathbb{P}^2)/W(E_7)^+\big)$.
5. $\mathrm{RD}\big(\mathcal{H}_{4,2}(28) \to \mathcal{H}_{4,2}\big)$.

Proof. As noted above, there is an isomorphism

$$W(E_7) \cong W(E_7)^+ \times \mathbb{Z}/2\mathbb{Z};$$

Theorem 3.3 implies that

$$\mathrm{RD}\left(W(E_7)\right) = \max\big\{\mathrm{RD}(\mathbb{Z}/2\mathbb{Z}), \mathrm{RD}\big(W(E_7)^+\big)\big\} = \mathrm{RD}\big(W(E_7)^+\big).$$

In the proof of Theorem 8.4, we constructed a diagram (8.3) of varieties which are versal for every $G \subset W(E_7)^+$, in particular for $G = W(E_7)^+$. By Proposition 3.7, we conclude that

$$\mathrm{RD}\big(X \to X/W(E_7)^+\big) = \mathrm{RD}\big(W(E_7)^+\big)$$

for all X in the diagram (8.3). The theorem now follows. $\square$

Acknowledgements. This paper owes a huge intellectual debt to many people. First, the ideas of Klein, Hilbert and their contemporaries are seminal to most work in this area. The idea of resolvent degree was implicit in their work, but it was first defined formally by Brauer, to whom we owe the modern start of the theory. We have benefited greatly from the work of Igor Dolgachev, which has (among other things) helped to explain and place in modern terms the work of the classical algebraic geometers. We mention in particular his book [Dol] and his book [DO] with Ortland. We have also benefitted greatly from the point of view of Bruce Hunt's book [Hu], which emphasizes the connections with locally symmetric varieties. The first author would like to thank Eduard Looijenga, from whom he learned many of the classical constructions used in this paper, and the modern take on these. Finally, this paper builds on the theory of essential dimension, introduced by Buhler–Reichstein [BR1] and developed by Merkurjev, Reichstein and many others.

It is a pleasure to thank the following people for useful conversations, correspondence and comments: Maxime Bergeron, Izzet Coskun, Igor Dolgachev, Jordan Ellenberg, Etienne Ghys, Sam Grushevsky, Nate Harman, Eriko Hironaka, Heisuke Hironaka, Sean Howe, Mark Kisin, Eduard Looijenga, Curt McMullen, Madhav Nori, Daniil Rudenko, Aaron Silberstein and Amie Wilkinson. We especially thank Nat Mayer and Zinovy Reichstein for careful readings and numerous detailed comments on an earlier draft of this paper. We would also like to thank the algebraic geometry/topology/representation theory working group at the University of Chicago for many conversations. It a pleasure to thank Sebastian Hensel for translating Hilbert's paper [Hil2] for us. Finally, we thank the anonymous referee, whose comments helped to greatly improve this paper.

The first author was supported in part by National Science Foundation Grant Nos. DMS-1105643 and DMS-1406209, and the Jump Trading Mathlab Research Fund. The second author was supported in part by National Science Foundation Grant No. DMS-1400349.

A. Appendix

Versal covers for subgroups of $W(E_6)$ and covers related to lines on cubics

$$
\begin{tikzcd}
\mathbb{A}(\mathfrak{h}_6) \arrow[r, dashed] & \mathbb{P}(\mathfrak{h}_6) \arrow[r, dashed] & \mathcal{C}_6'(\mathbb{P}^2) \arrow[r, "\cong"] \arrow[d, dashed, "S_2^{\times 4}"] & \mathcal{H}_{3,3}(27) \arrow[d, "S_2^{\times 4}"] \arrow[dr, "S_6"] \arrow[drr, "W(E_6)^+"] & & & \\
 & & \mathcal{M}_{0,7}/S_2 \arrow[r, dashed, "\simeq"] \arrow[d, "S_5"] & \mathcal{H}_{3,3}(27)/S_2^{\times 4} \arrow[d, "S_5"] & \mathcal{H}_{3,3}^{skew}(6)/S_6 \arrow[d, "S_2"] & \mathcal{H}_{3,3}(\sqrt{\Delta}) \arrow[ddl, "S_2"] & \widetilde{\mathcal{P}} \arrow[l, "A_5"'] \\
 & & \mathcal{M}_{0,7}/S_2 \times S_5 \arrow[r, dashed, "\simeq"] & \mathcal{H}_{3,3}(1) \arrow[dr, "27:1"] & \mathcal{H}_{3,3}(6,6) \arrow[d, "36:1"] & & \\
 & & & & \mathcal{H}_{3,3} & &
\end{tikzcd}
$$

The diagram above shows the relation between many covers of classical interest of the moduli space $\mathcal{H}_{3,3}$ of smooth cubic surfaces. The column involving $\mathcal{M}_{0,7}$ was constructed by Doran [Dor].

Versal covers for subgroups of $W(E_7)^+$ and covers related to bitangents on plane quartics

$$
\begin{tikzcd}
\mathbb{A}(\mathfrak{h}_7) \arrow[r, dashed] & \mathbb{P}(\mathfrak{h}_7) \arrow[r, dashed] & \mathcal{C}_7(\mathbb{P}^2) \arrow[r, dashed, "2:1"] \arrow[d, "W(D_5)"'] & \mathcal{H}_{4,2}(28) \arrow[d, "W(D_5)"'] \arrow[r, "S_7"] \arrow[dr, "S_8"'] \arrow[rr, "W(D_6)"] & \mathcal{H}_{4,2}(\mathcal{A}) \arrow[d, "8:1"] & \mathcal{H}_{4,2}(\mathcal{S}) \arrow[ddl, "63:1"] \\
 & & \mathcal{U}_{3,3}(1) \arrow[r, dashed, "2:1"] \arrow[d, "27:1"'] & \mathcal{H}_{4,2}(2) \arrow[d, "27:1"'] & & \\
 & & \mathcal{U}_{3,3} \arrow[r, dashed, "2:1"] & \mathcal{H}_{4,2}(1) \arrow[dr, "28:1"'] & \mathcal{H}_{4,2}(\theta^{\mathrm{ev}}) \arrow[d, "36:1"] & \\
 & & & & \mathcal{H}_{4,2} &
\end{tikzcd}
$$

The diagram above shows the relation between many covers of classical interest of the moduli space $\mathcal{H}_{4,2}$ of smooth plane quartics.

References

[Arn] V. I. Arnol'd, On the representation of continuous functions of three variables by superpositions of continuous functions of two variables. *Mat. Sb. (N. S.)* **48** **(90)** (1959), 3–74. Zbl 0125.30802 MR 0121453

[AS] V. Arnold and G. Shimura, Superpositions of algebraic functions. *Proc. Symposia in Pure Math.* vol. 28 (1976), AMS, Providence, 45–46.

[Atl] *Atlas of Finite Group Representations*, v. 3. `http://brauer.maths.qmul.ac.uk/Atlas/v3/`, accessed Jan. 5, 2018.

[Brau1] R. Brauer, A note on systems of homogeneous algebraic equations. *Bull. AMS* **51** (1945), 749–755. Zbl 0063.00599 MR 0013127

[Brau2] —— On the resolvent problem. *Ann. Mat. Pura Appl. (4)* **102** (1975), 45–55. Zbl 0299.12105 MR 0371854

[BR1] J. Buhler and Z. Reichstein, On the essential dimension of a finite group. *Compositio Math.* **106** (1997), 159–179. Zbl 0905.12003 MR 1457337

[BR2] —— On Tschirnhaus transformations. *Topics in Number Theory*, (University Park, PA, 1997), 127–142, Math. Appl., 467, Kluwer Acad. Publ., Dordrecht, 1999. Zbl 0937.12001 MR 1691314

[Bri] E. Bring, Meletemata quædam Mathematica circa Transformationem Æquationum Algebraicarum ("Some Selected Mathematics on the Transformation of Algebraic Equations"), Lund, 1786.

[Bur] H. Burkhardt, Untersuchungen aus dem Gebiet der hyperelliptischen Modulfunctionen, II. *Math. Ann.* **38** (1890), 161–224. JFM 23.0490.01 MR 1510670

[CGR] V. Chernousov, P. Gille and Z. Reichstein, Resolving G-torsors by abelian base extensions. *J. Algebra* **296** (2006), 561–581. Zbl 1157.14311 MR 2201056

[CHM] A. Chen, Y.-H. He, and J. McKay, Erland Samuel Bring's "Transformation of algebraic equations". arXiv:1711.09253v1

[Di] J. Dixmier, Histoire de 13e problème de Hilbert. *Cahiers du séminaire d'histoire des mathématiques*, 2e série, tome 3 (1993), 85–94. Zbl 0795.01012 MR 1240756

[DO] I. Dolgachev and D. Ortland, Point sets in projective spaces and theta functions. *Asterisque* **165** (1988). Zbl 0685.14029 MR 1007155

[Dol] I. Dolgachev, *Classical Algebraic Geometry: A Modern Viewpoint*. Cambridge Univ. Press, 2012. Zbl 1252.14001 MR 2964027

[Dor] B. Doran, Hurwitz spaces and moduli spaces as ball quotients via pull-back. arXiv:math/0404363v1

[DM] P. Doyle and C. McMullen, Solving the quintic by iteration. *Acta Math.* **163** (1989), 151–180. Zbl 0705.65036 MR 1032073

[DR1] A. Duncan and Z. Reichstein, Versality of algebraic group actions and rational points on twisted varieties, with an appendix containing a letter from J.-P. Serre. *J. Algebraic Geom.* **24** (2015), 499–530. Zbl 1327.14210 MR 3344763

[DR2] —— Pseudo-reflection groups and essential dimension. *J. Lond. Math. Soc.* (2) **90** (2014), 879–902. Zbl 1317.20039 MR 3291805

[EH] D. Eisenbud and J. Harris, 3264 *and All That – A Second Course in Algebraic Geometry*. Cambridge Univ. Press, 2016. Zbl 1341.14001 MR 3617981

[EJ] A.-S. Elsenhans and J. Jahnel, Moduli spaces and the inverse Galois problem for cubic surfaces. *Trans. Amer. Math. Soc.* **367** (2015), 7837–7861. Zbl 1331.14039 MR 3391901

[Gre] M. Green, On the analytic solution of the equation of fifth degree. *Compos. Math.* **37**, (1978), 233–241. Zbl 0405.30034 MR 0511743

[FKW] B. Farb, M. Kisin and J. Wolfson, Modular functions and resolvent problems (with an appendix by Nate Harman). arXiv:1912.12536

[Ham] W. Hamilton, Inquiry into the validity of a method recently proposed by George B. Jerrard, esq., for transforming and resolving equations of elevated degrees. *Report of the Sixth Meeting of the British Association for the Advancement of Science* (1836), Bristol, 295–348.

[Har] J. Harris, Galois groups of enumerative problems. *Duke Math. J.* **46** (1979), 685–724. Zbl 0433.14040 MR 0552521

[He] C. Hermite, Sur l'invariant du dix-huitième ordre des formes du cinquième degré. *J. Reine Angew. Math.* **59** (1861), 304–305. ERAM 059.1567cj MR 1579180

[Hil1] D. Hilbert, Mathematical Problems. *Proceedings of the 1900 ICM*, English translation reprinted in *Bull. AMS* **37** (2000), 407–436. Zbl 0979.01028 MR 1779412

[Hil2] —— Über die Gleichung neunten Grades. *Math. Ann.* **97** (1927), 243–250. JFM 52.0103.02 MR 1512361

[Hilt] H. Hilton, *Plane Algebraic Curves*. Oxford Univ. Press, 1920. JFM 47.0611.03

[HS] A. Hefez and G. Sacchiero, The Galois group of the tangency problem for plane curves. *Math. Scand.* **56** (1985), 171–190. Zbl 0566.14024 MR 0813635

[Hu] B. Hunt, *The Geometry of Some Special Arithmetic Quotients*. Springer Lect. Notes in Math., Vol. 1637, 1996. Zbl 0904.14025 MR 1438547

[Jou] P. Joubert, Sur l'equation du sixième degré. *C. R. Acad. Sci. Paris* **64** (1867), 1025–1029.

[KK] M. Kracht and E. Kreyszig, E. W. von Tschirnhaus: His role in early calculus and his work and impact on algebra. *Historia Mathematica* **17** (1990), 16–35. Zbl 0696.01005 MR 1045714

[Kle1] F. Klein, Ueber eine geometrische Repräsentation der Resolventen algebraischer Gleichungen. *Math. Ann.* **4** (1871), 346–358.

[Kle2] —— *Vorlesungen über das Ikosaeder und die Auflösung der Gleichungen vom fünften Grade*. Teubner, Leipzig, 1884. (English translation: *Lectures on the Icosahedron and Solution of EquationS of the Fifth Degree*, translated by G. G. Morrice, 2nd and rev. edition, New York, Dover Publications, 1956.) JFM 16.0061.01 MR 1315530

[Kle3] —— Sur la résolution, par fonctions hyperelliptique, de l'équation du vingt-septième degré, de laquelle dépend la détermination des vingt-sept droites d'une surface cubique. *Jour. de math. pure et appl.* (*4*) **4**, (1888).

[Kro] L. Kronecker, Ueber die Gleichungen fünften Grades. *Journal für die reine und angewandte Mathematik* **59** (1861), 306–310. ERAM 059.1568cj MR 1579181

[Leh] D. Lehavi, Any smooth plane quartic can be reconstructed from its bitangents. *Israel J. Math* **146** (2005), 371–379. Zbl 1076.14037 MR 2151609

[Man] L. Manivel, Configurations of lines and models of lie algebras. *J. Algebra* **304** (2006), 457–486. Zbl 1167.17001 MR 2256401

[Mer1] A. Merkurjev, On the norm residue symbol of degree 2. *Dokl. Akad. Nauk SSSR* **261** (1981), 542–547.

[Mer2] A. Merkurjev, Essential dimension: A survey. *Transformation Groups* **18** (2013), 415–481. Zbl 1278.14066 MR 3055773

[MR] A. Meyer and Z. Reichstein, Some consequences of the Karpenko–Merkurjev theorem. *Documenta Math.* Extra vol.: Andrei A. Suslin's Sixtieth Birthday (2010), 445–457. Zbl 1277.20059 MR 2804261

[Pin] H. Pinkham, *Résolutions simultanée de points doubles rationnels*. Lecture Notes in Math. 777 (1980), Springer-Verlag, 179–204. Zbl 0457.14004

[PSV] D. PLAUMAN, B. STURMFELS and C. VINZANT, Supplementary material to "Quartic curves and their bitangents". *Jour. of Symb. Comp.* **46** (2011), 712–733. Available at http://www4.ncsu.edu/~clvinzan/quartics.html. Zbl 1214.14049 MR 2781949

[Rei] Z. REICHSTEIN, *Proceedings of the Inter. Cong. of Mathematicians*, Vol. II, 162–188, Hindustan Book Agency, New Delhi, 2010.

[Reid] M. REID, The complete intersection of two or more quadrics, 1972 preprint, Trinity College, Cambridge.

[Seg1] B. SEGRE, The algebraic equations of degrees 5, 9, 157, ..., and the arithmetic upon an algebraic variety. *Ann. of Math.* (2) **46** (1945), 287–301. Zbl 0061.01807 MR 0013126

[Seg2] —— *Arithmetical Questions on Algebraic Varieties*. University of London, Athlone Press, London, 1951. Zbl 0042.15204 MR 0043498

[Sek] J. SEKIGUCHI, The configuration space of 6 points in $\mathbb{P}^2$, the moduli space of cubic surfaces and the Weyl group of type E_6. Kyoto University Research Information Repository, 1993-09, http://hdl.handle.net/2433/83660. Zbl 0939.14502 MR 1311274

[SH1] J. SYLVESTER and J. HAMMOND, On Hamilton's Numbers. *Phil. Trans. R. Soc. London A* **178** (1887), 285–312. JFM 19.0080.02

[SH2] —— On Hamilton's Numbers II. *Phil. Trans. R. Soc. London A* **179** (1888), 65–71. JFM 20.0081.01

[SS] M. SCHÜTT and T. SHIODA, *Mordell–Weil Lattices*. Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics], 70. Zbl 07105781 MR 3970314

[Syl] J. SYLVESTER, On the so-called Tschirnhausen transformation. *J. Reine Angew. Math.* **100** (1887), 465–486. JFM 19.0079.02 MR 1580113

[Tsch] E. W. von TSCHIRNHAUS, Methodus auferendi omnes terminos intermedios ex data aeqvatione (Method of eliminating all intermediate terms from a given equation). *Acta Eruditorum* (1683), 204–207.

[Wol] J. WOLFSON, Tschirnhaus transformations after Hilbert. arXiv:2001.06515

(*Reçu le 8 mai 2019*)

Benson FARB, Dept. of Mathematics, University of Chicago,
5734 University Avenue, Chicago, IL 60637-1514, USA

e-mail: farb@math.uchicago.edu

Jesse WOLFSON, Dept. of Mathematics, University of California, Irvine,
340 Rowland Hall, Irvine, CA 92697-3875, USA

e-mail: wolfson@uci.edu