18 August 2021 ArXiv.org/2108.07905

GALOIS GROUPS IN ENUMERATIVE GEOMETRY AND APPLICATIONS

FRANK SOTTILE AND THOMAS YAHL

ABSTRACT. As Jordan observed in 1870, just as univariate polynomials have Galois groups, so do problems in enumerative geometry. Despite this pedigree, the study of Galois groups in enumerative geometry was dormant for a century, with a systematic study only occuring in the past 15 years. We discuss the current directions of this study, including open problems and conjectures.

INTRODUCTION

We are all familiar with Galois groups: They play important roles in the structure of field extensions and control the solvability of equations. Less known is that they have a long history in enumerative geometry. In fact, the first comprehensive treatise on Galois theory, Jordan's "Traité des Substitutions et des Équations algébriques" [43, Ch. III], also discusses Galois theory in the context of several classical problems in enumerative geometry.

While Galois theory developed into a cornerstone of number theory and of arithmetic geometry, its role in enumerative geometry lay dormant until Harris's 1979 paper "Galois groups of enumerative problems" [31]. Harris revisited Jordan's treatment of classical problems and gave a proof that, over $\mathbb{C}$, the Galois and monodromy groups coincide. He used this to introduce a geometric method to show that an enumerative Galois group is the full symmetric group and showed that several enumerative Galois groups are full-symmetric, including generalizations of the classical problems studied by Jordan.

We sketch the development of Galois groups in enumerative geometry since 1979. This includes some new and newly applied methods to study or compute Galois groups in this context, as well as recent results and open problems. A theme that Jordan initiated is that intrinsic structure of the solutions to an enumerative problem constrains its Galois group G giving an "upper bound" for G. The problem of identifying the Galois group G becomes that of showing it is as "large as possible". In all cases when G has been determined, it is as large as possible given the intrinsic structure. Thus we may view G as encoding the intrinsic structure of the enumerative problem.

Consider the problem of lines on a cubic surface. Cayley [14] and Salmon [70] showed that a smooth cubic surface $\mathcal{V}(f)$ in $\mathbb{P}^3$ (f is a homogeneous cubic in four variables) contains 27 lines. (See Figure 1.) This holds over any algebraically closed field. When f

1991 *Mathematics Subject Classification.* 14M25, 65H20, 65H10, Need more.

Key words and phrases. Galois group, enumerative geometry, sparse polynomial systems, Schubert caculus, Fano problem, homotopy continuation.

Research of Sottile and Yahl supported by grant 636314 from the Simons Foundation.

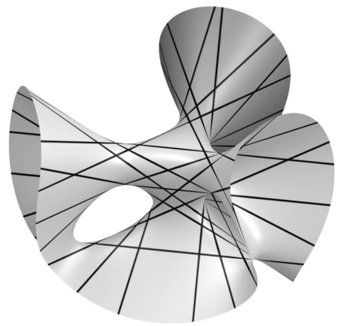


FIGURE 1. A cubic with 27 lines. (Image courtesy of Oliver Labs)

has rational coefficients, the field $\mathbb{K}$ of definition of the lines is a Galois extension of $\mathbb{Q}$, and its Galois group G has a faithful action on the 27 lines.

As the lines lie on a surface, we expect that some will meet, and Schläfli [71] showed that for a general cubic, these lines form a remarkable incidence configuration whose symmetry group is the reflection group E_6. As Jordan observed, this implies that G is a subgroup of E_6, and it is now known that for most cubic surfaces $G = E_6$.

A modern view begins with the incidence variety of this enumerative problem. The space of homogeneous cubics on $\mathbb{P}^3$ forms a 19-dimensional projective space, as a cubic in four variables has $\binom{3+(4-1)}{3} = 20$ coefficients. Writing $\mathbb{G}(1, \mathbb{P}^3)$ for the (four-dimensional) Grassmannian of lines in $\mathbb{P}^3$, we have the incidence variety.

$$\begin{array}{c} \Gamma := \{(\ell, f) \in \mathbb{G}(1, \mathbb{P}^3) \times \mathbb{P}^{19}_{\text{cubics}} \mid f|_\ell \equiv 0\}. \\ \Big\downarrow \pi \\ \mathbb{P}^{19}_{\text{cubics}} \end{array} \tag{1}$$

Write $\Bbbk$ for our ground field, which we assume for now to be algebraically closed. Both Γ and $\mathbb{P}^{19}$ are irreducible; Let us consider their fields of rational functions, $\Bbbk(\Gamma)$ and $\Bbbk(\mathbb{P}^{19})$. As the typical fiber of π consists of 27 points and π is dominant, $\pi^*(\Bbbk(\mathbb{P}^{19}))$ is a subfield of $\Bbbk(\Gamma)$, and the extension has degree 27. The Galois group G of the normal closure of this extension acts on the lines in the generic cubic surface over $\mathbb{P}^{19}$, and we have that $G = E_6$.

Suppose that $\Bbbk = \mathbb{C}$. If $B \subset \mathbb{P}^{19}$ is the set of singular cubics (a degree 32 hypersurface) then over $\mathbb{P}^{19} \smallsetminus B$, Γ is a covering space of degree 27. Lifting based loops gives the monodromy action of the fundamental group of $\mathbb{P}^{19} \smallsetminus B$ on the fiber above the base point. Permutations of the fiber obtained in this way constitute the *monodromy group* of π. For the same reasons as before, this is a subgroup of E_6. In fact, it equals E_6.

This situation, a dominant map $\pi\colon X \to Z$ of irreducible equidimensional varieties, is called a *branched cover*. Branched covers are common in enumerative geometry and applications of algebraic geometry. For the problem of 27 lines, that the algebraic Galois group equals the geometric monodromy group is no accident; While Harris [31] gave a modern proof, the equality of these two groups may be traced back to Hermite [39]. We sketch a proof, valid over arbitrary fields, in Section 1.

Harris's article brought this topic into contemporary algebraic geometry. He also introduced geometric methods to show that the Galois group of an enumerative problem is *fully symmetric* in that it is the full symmetric group on the solutions. In the 25 years following its publication, the Galois group was determined in only a handful of enumerative problems. For example, D'Souza [18] showed that the problem of lines in $\mathbb{P}^3$ tangent to a smooth octic surface at four points (everywhere tangent lines) had Galois group that is fully symmetric. Interestingly, he did not determine the number of everywhere tangent lines.

This changed in 2006 when Vakil introduced a method [89] to deduce that the Galois group of a Schubert problem on a Grassmannian (a *Schubert Galois group*) contains the alternating group on its solutions. Such a Galois group is *at least alternating*. He used that to show that most Schubert problems on small Grassmannians were at least alternating, and to discover an infinite family of Schubert problems whose Galois groups were not the full symmetric group. As we saw in the problem of 27 lines on a cubic surface, such an enumerative problem with a small Galois group typically possesses some internal structure. Consequently, we use the adjective *enriched* to describe such a problem or Galois group. Enriched Schubert problems were also found on more general flag manifolds [69]. These discoveries inspired a more systematic study of Schubert Galois groups, which we discuss in Section 6. Despite significant progress, the *inverse Galois problem* for Schubert calculus remains open.

Galois groups of enumerative problems are usually transitive permutation groups. There is a dichotomy between those transitive permutation groups that preserve no nontrivial partition, called *primitive* groups, and the *imprimitive* groups that do preserve a nontrivial partition. The Galois group of the 27 lines is primitive, but most known enriched Schubert problems have imprimitive Galois groups.

Another well-understood class of enumerative problems comes from the Bernstein-Kushnirenko Theorem [8, 49]. This gives the number of solutions to a system of polynomial equations that are general given the monomials occurring in the equations. Esterov [24] determined which of these problems have fully symmetric Galois group and showed that all others have an imprimitive Galois group. Here, too, the inverse Galois problem remains open. We discuss this in Section 4.

The problem of lines on a cubic surface is the first in the class of *Fano problems*, which involve counting the number of linear subspaces that lie on a general complete intersection in projective space. Recently, Hashimoto and Kadets [32] nearly determined the Galois groups of all Fano problems. Most are at least alternating, except for the lines on a cubic surface and the r-planes lying on the intersection of two quadrics in $\mathbb{P}^{2r+2}$. We explain this in Section 3, and discuss computations which show that several small Fano problems are full-symmetric.

Branched covers arise from families of polynomial systems, which are common in the applications of mathematics. Oftentimes the application or the formulation as a system of polynomials possesses some intrinsic structure, which is manifested in the corresponding Galois group being enriched. In Section 7, we discuss two occurrences of enriched Galois groups in applications and a computational method that exploits structure in Galois groups for computing solutions to systems of equations.

We begin in Section 1 with a general discussion of Galois groups in enumerative geometry, and sketch some methods from numerical algebraic geometry in Section 2. Later, in Section 5, we present methods, both numerical and symbolic, to compute and study Galois groups in enumerative geometry.

1. Galois groups of branched covers

We will let $\Bbbk$ be a field with algebraic closure $\overline{\Bbbk}$. We adopt standard terminology from algebraic geometry: An affine (projective) scheme $\mathcal{V}(F)$ is defined in $\mathbb{A}^n$ ($\mathbb{P}^n$) by polynomials (homogeneous forms) $F = (f_1, \dots, f_m)$ in n ($n+1$) variables with coefficients in $\Bbbk$. We will call the collection F a system (of equations) and say the isolated points of $\mathcal{V}(F)$ (over $\overline{\Bbbk}$) are the *solutions* to F. The affine scheme $\mathcal{V}(F)$ is a variety when every irreducible component of $\mathcal{V}(F)$ is reduced. We may also use variety to refer to the underlying variety. We write $X(\overline{\Bbbk})$ for the points of a variety X with coordinates in $\overline{\Bbbk}$.

Recall that the Galois group of a separable univariate polynomial $f(x) \in \Bbbk[x]$ is the Galois group of the splitting field of f, which is generated over $\Bbbk$ by the roots of f. Given a system F of multivariate polynomials over $\Bbbk$, its splitting field is the field generated by over $\Bbbk$ by the coordinates of all solutions to F, and its Galois group is the Galois group of this field extension.

A separable map $\pi\colon X \to Z$ of irreducible varieties is a *branched cover* when X and Y have the same dimension and $\pi(X)$ is dense in Z (π is *dominant*). Branched covers are ubiquitous in enumerative geometry and in applications of algebraic geometry. When the varieties are complex, there is a proper subvariety $B \subset Z$ (the *branch locus*) such that π is a covering space over $Z \smallsetminus B$. We explain how to associate a Galois/monodromy group to a branched cover and then give some background on permutation groups, and the relation between imprimitivity of the Galois group and decomposability of the branched cover.

1.1. **Galois and monodromy groups of branched covers.** Let $\pi\colon X \to Z$ be a branched cover. As π is dominant, the function field $\Bbbk(Z)$ of Z embeds as a subfield of the function field $\Bbbk(X)$ of X. This realizes $\Bbbk(X)$ as a finite extension of $\Bbbk(Z)$ of degree d, the degree of π. Let $\mathbb{K}$ be the normal closure of this extension. The Galois group of the branched cover π, denoted Gal_π, is the Galois group of $\mathbb{K}/\Bbbk(Z)$. This is a transitive subgroup of the symmetric group S_d that is well-defined up to conjugation.

There is also a geometric construction of Gal_π. For $1 \le s \le d$, let X^s_Z be the s-th fold iterated fiber product of $\pi\colon X \to Z$,

$$X^s_Z \ := \ \underbrace{X \times_Z X \times_Z \cdots \times_Z X}_{s} \, .$$

The fiber of $\pi^s\colon X^s_Z \to Z$ over a point $z \in Z$ is the s-fold Cartesian product $(\pi^{-1}(z))^s$ of the fiber of π over z.

The fiber product has many irreducible components when $s > 1$, possibly of different dimensions. Let $U \subset Z$ be the maximal dense open subset over which π is étale—fibers $\pi^{-1}(z)$ for $z \in U$ are zero-dimensional reduced schemes of degree d. Its complement is the *branch locus* B of π. The *big diagonal* of X^s_Z is the closed subscheme consisting of s-tuples with a repeated coordinate. Let $X^{(s)}_Z$ be the closure in X^s_Z of the complement of the big diagonal in $(\pi^s)^{-1}(U)$. The fiber of $X^{(s)}_Z$ over a point $z \in U(\overline{\Bbbk})$ consists of s-tuples of distinct points of the fiber $\pi^{-1}(z)$.

When $s = d$, the symmetric group S_d acts on $X^{(d)}_Z$, permuting each d-tuple. It permutes the irreducible components and acts simply transitively on the fiber above a point $z \in U(\overline{\Bbbk})$. Let $X' \subset X^{(d)}_Z$ be an irreducible component (they are all isomorphic when $s = d$).

We compare this to the construction of the splitting field of a univariate polynomial. Replacing X and Z by appropriate affine open subsets, we may embed X as a hypersurface in $Z \times \mathbb{A}^1_t$ with $X \to Z$ the projection. Writing $\Bbbk[X]$ and $\Bbbk[Z]$ for their coordinate rings, there is a monic irreducible polynomial $f \in \Bbbk[Z][t]$ of degree d such that $\Bbbk[X] = \Bbbk[Z][t]/\langle f\rangle$. Thus $\Bbbk(X) = \Bbbk(Z)[t]/\langle f\rangle = \Bbbk(Z)(\alpha)$, where α is the image of t in $\Bbbk[X]$. If X' is an irreducible component of $X^{(d)}_Z$, then $\Bbbk(X') = \Bbbk(Z)(\alpha_1, \ldots, \alpha_d)$ where $\alpha_i \in \Bbbk[X']$ is given by the composition of inclusion $X' \subset X^{(d)}_Z$, the ith coordinate projection $X^{(d)}_Z \to X$, and the function α. As $i \neq j \Rightarrow \alpha_i \neq \alpha_j$ (X' does not lie in the big diagonal), we see that $\alpha_1, \ldots, \alpha_d$ are the roots of f in $\Bbbk(X')$. Thus $\Bbbk(X')$ is the splitting field of f and Galois over $\Bbbk(Z)$.

The *monodromy group* Mon_π of the branched cover is the subgroup of S_d that preserves X'. Elements of Mon_π are automorphisms of the extension $\Bbbk(X')/\Bbbk(Z)$ so that $\mathrm{Mon}_\pi \subset \mathrm{Gal}(\Bbbk(X')/\Bbbk(Z))$, the Galois group of $\Bbbk(X')/\Bbbk(Z)$. Since Mon_π acts simply transitively on fibers of $X' \to Z$ above points in $U(\overline{\Bbbk})$, its order is the degree of the map $X' \to Z$, which is the order of the field extension $\Bbbk(X')/\Bbbk(Z)$. Hence we arrive at the result $\mathrm{Mon}_\pi = \mathrm{Gal}(\Bbbk(X')/\Bbbk(Z))$.

Theorem 1 (Galois equals monodromy)**.** *For a branched cover $\pi\colon X \to Z$ defined over a field $\Bbbk$, the Galois group is equal to the monodromy group,*

$$\mathrm{Gal}_\pi \;=\; \mathrm{Mon}_\pi\,.$$

The enumerative problem of 27 lines on a cubic surface has a corresponding incidence variety (1) which is a branched cover, and its Galois/monodromy group is a special case of the results of this section. Incidence varieties of enumerative problems typically are branched covers and therefore have Galois groups as we will see throughout this survey.

We make an important observation. While the Galois group of a branched cover $\pi\colon X \to Z$ is defined via a geometric construction, it does depend upon the field of definition. For example, consider the branched cover $\pi\colon \mathbb{A}^1 \to \mathbb{A}^1$ given by $x \mapsto x^3$. Assume that $\Bbbk$ does not have characteristic 3, for otherwise π is inseparable. Over the rational numbers, that is $\pi\colon \mathbb{A}^1(\mathbb{Q}) \to \mathbb{A}^1(\mathbb{Q})$, it has Galois group S_3, but over any field containing $\sqrt{-3}$ (e.g. -3 is a square in $\Bbbk$) its Galois group is $A_3 = \mathbb{Z}/3\mathbb{Z}$. This is because the discriminant of the cubic $x^3 - t$ defining π is $-27t^2$, which is a square only in fields containing $\sqrt{-3}$. When necessary, we write $\mathrm{Gal}_\pi(\Bbbk)$ to indicate that the branched cover is defined over $\Bbbk$.

If $\pi\colon X \to Z$ is a branched cover defined over $\Bbbk$ and $\mathbb{F}/\Bbbk$ is any field extension, $\mathrm{Gal}_\pi(\mathbb{F})$ is isomorphic to the subgroup of $\mathrm{Gal}_\pi(\Bbbk)$ corresponding to the extension $\mathbb{K}/\mathbb{E}$, where $\mathbb{K}$ is the normal closure of $\Bbbk(X)/\Bbbk(Z)$ and $\mathbb{E} = \mathbb{K} \cap \mathbb{F}(Z)$.

1.2. **Complex branched covers.** Suppose that $\pi\colon X \to Z$ is a branched cover of complex varieties. Then the étale locus $U \subset Z$ is the open subset that is maximal with respect to inclusion such that the restriction $\pi\colon \pi^{-1}(U) \to U$ is a covering space. We will also call U the set of regular values of π.

The monodromy group Mon_π as defined in Section 1.1 agrees with the usual notion of the monodromy group of the covering space

$$\pi \;:\; \pi^{-1}(U) \;\longrightarrow\; U\,.$$

This is the group of permutations of a fiber $\pi^{-1}(z)$ obtained by lifting loops in U that are based at z to paths in $\pi^{-1}(U)$ that connect points in the fiber. If d is the degree of π, lifting based loops in U to paths in a component X' of $X_Z^{(d)}$ gives this equality. For more on covering spaces and monodromy groups, see [33, 64].

The complement of any (Zariski) open subset V of Z has real codimension at least 2. The loops in U that generate the monodromy group can be chosen to lie in V (by a change of base point if necessary). A consequence is that the monodromy group Mon_π is equal to the monodromy group of any restriction $\pi\colon \pi^{-1}(V) \to V$ to a Zariski open set V such that this map is a covering space.

1.3. **Enriched Galois groups.** As Harris showed [31], many enumerative problems have Galois groups that are the full symmetric group S_d on their solutions. We call such a Galois group/enumerative problem *fully symmetric*. It is a standard part of the Algebra curriculum that any finite group may arise as the Galois group of a branched cover. Nevertheless, determining the possible Galois groups of a given class of enumerative problems (the *inverse Galois problem* for that class), as well as the Galois group of any particular enumerative problem is an interesting problem that is largely open.

Many techniques to study Galois groups in enumerative geometry are able to show that the Galois group Gal_π is either S_d or contains its subgroup A_d of alternating permutations. We call such an enumerative problem/Galois group *at least alternating*. While many enumerative Galois groups are at least alternating, we know of no natural enumerative problem whose Galois group is the alternating group (besides those similar to $x \mapsto x^3$).

As we saw in the problem of 27 lines, when a Galois group fails to be fully symmetric, we expect there is a geometric reason for this failure. That is, the set of solutions is enriched with extra structure that prevents the Galois group from being fully symmetric. Consequently, we will call a Galois group or enumerative problem *enriched* if its Galois group is not fully symmetric.

Let us recall some aspects of permutation groups. A permutation group of degree d is a subgroup G of S_d. Thus G has a natural action on the set $[d] := \{1, \ldots, d\}$, as well as on the subsets of $[d]$. The group is *transitive* if for any $i, j \in [d]$, there is an element $g \in G$ with $g(i) = j$. More generally, for any $1 \leq s \leq d$, G is *s-transitive* if for any distinct $i_1, \ldots, i_s \in [d]$ and distinct $j_1, \ldots, j_s \in [d]$, there is an element $g \in G$ with $g(i_m) = j_m$ for $m = 1, \ldots, s$. That is, G is s-transitive when it acts transitively on the set of distinct s-tuples of elements of $[d]$. This has the following consequence.

Proposition 2. *The monodromy group* Mon_π *of a branched cover* $\pi\colon X \to Z$ *is s-transitive if and only if the variety* $X_Z^{(s)}$ *is irreducible.*

Let G be a transitive permutation group of degree d. A *block* of G is a subset $B \subset [d]$ such that for every $g \in G$, either $gB = B$ or $gB \cap B = \emptyset$. The subsets $\emptyset$, $[d]$, and every singleton are blocks of every permutation group. If these trivial blocks are the only blocks, then G is *primitive* and otherwise it is *imprimitive*.

The Galois group E_6 for the problem of 27 lines is primitive, but it is not 2-transitive. For the latter, observe that some pairs of lines on a cubic surface meet, while other pairs are disjoint. These incidences provide an obstruction to 2-transitivity.

When G is imprimitive, we have a factorization $d = ab$ with $1 < a, b < d$ and there is a bijection $[a] \times [b] \leftrightarrow [d]$ such that G preserves the projection $[a] \times [b] \to [b]$. That is, the fibers $\{[a] \times \{i\} \mid i \in [b]\}$ are blocks of G and its action on this set of blocks gives a homomorphism $G \to S_b$ with transitive image. In particular, G is a subgroup of the group of permutations of $[d] = [a] \times [b]$ which preserve the fibers of the projection $[a] \times [b] \to [b]$. This group is the wreath product $S_a \wr S_b$, which is the semi-direct product $(S_a)^b \rtimes S_b$, where S_b acts on $(S_a)^b$ by permuting factors.

Imprimitivity has a geometric manifestation. A branched cover $\pi\colon X \to Z$ is *decomposable* if there is a nonempty Zariski open subset $V \subset Z$ and a variety Y such that π factors over V,

$$\pi^{-1}(V) \xrightarrow{\varphi} Y \xrightarrow{\psi} V\,, \tag{2}$$

with φ and ψ both nontrivial branched covers. The fibers of φ over points of $\psi^{-1}(v)$ are blocks of the action of Gal_π on $\pi^{-1}(v)$, which implies that Gal_π is imprimitive. Pirola and Schlesinger [66] observed that decomposability of π is equivalent to imprimitivity of Gal_π.

Proposition 3. *A branched cover is decomposable if and only if its Galois group is imprimitive.*

Harris's geometric method to show that a Galois group of an enumerative problem over $\mathbb{C}$ is fully-symmetric involves two steps. First, show that $X_Z^{(2)}$ is irreducible, so that Mon_π is 2-transitive. Next, identify an instance of the enumerative problem (a point $z \in Z$) with $d-1$ solutions, where exactly one solution has multiplicity 2. This implies that a small loop in Z around z induces a simple transposition in Mon_π. This implies that $\mathrm{Mon}_\pi = S_d$, as S_d is its only 2-transitive subgroup containing a simple transposition. Jordan [43] gave a useful generalization of this last fact about S_d, which we use in Section 5.

Proposition 4. *Suppose that $G \subset S_d$ is a permutation group. If G is primitive and contains a p-cycle for some prime number $p < d-2$, then G is at least alternating.*

If G contains a d-cycle, a $d-1$-cycle, and a p-cycle for some prime number $p < d-2$ then $G = S_d$.

2. Numerical Algebraic Geometry

Methods from numerical analysis underlie algorithms that readily solve systems of polynomial equations. Numerical algebraic geometry uses this to represent and study algebraic varieties on a computer. We sketch some of its fundamental algorithms, which will later be used for studying Galois groups.

2.1. **Homotopy continuation.** When $\Bbbk = \mathbb{C}$, solutions to enumerative problems, fibers of branched covers, and monodromy are all effectively computed using algorithms based on numerical homotopy continuation. This begins with a *homotopy*, which is a family $\mathcal{H}(x;t)$ of systems of polynomials that interpolate between the systems at $t = 0$ and $t = 1$ in a particular way: We require that the variety $\mathcal{V}(\mathcal{H}(x;t)) \subset \mathbb{C}^n_x \times \mathbb{C}_t$ contains a curve C that is the union of the 1-dimensional irreducible components of $\mathcal{V}(\mathcal{H})$ which project dominantly to $\mathbb{C}_t$. We further require that $1 \in \mathbb{C}_t$ is a regular value of the projection $\pi\colon C \to \mathbb{C}_t$, that π is proper near 1, and that $\mathcal{V}(\mathcal{H}(x;t))$ is smooth at all points of the fiber $W := \pi^{-1}(1)$. The *start system* is $\mathcal{H}(x;1)$ and write W for its set of isolated solutions, which we assume are known. The *target system* is $\mathcal{H}(x;0)$ and we wish to use $\mathcal{H}$ to compute the isolated solutions to the target system.

Given a homotopy $\mathcal{H}(x;t)$, we restrict C to the points above an arc $\gamma \subset \mathbb{C}_t$ with endpoints $\{0,1\}$ such that γ avoids the critical values of $\pi\colon C \to \mathbb{C}_t$, except possibly at $t = 0$. In what follows, we will take γ to be the interval $[0,1]$, for simplicity. This restriction is a collection of arcs in C, one for each point of W, which start at points of W at $t = 1$ and lie above $(0,1]$. Some arcs may be unbounded near $t = 0$, while the rest end in points of $\pi^{-1}(0)$, and all points of $\pi^{-1}(0)$ are reached. Beginning with the (known) points of W, standard path-tracking algorithms [1] from numerical analysis may follow these arcs and compute the points of $\pi^{-1}(0)$. When $\pi\colon C \to \mathbb{C}_t$ is proper near $t = 0$ and smooth above $t = 0$, there are $|W|$ points in $\pi^{-1}(0)$ so that each path gives a point of $\pi^{-1}(0)$. In this case, the homotopy is *optimal*. For more on numerical homotopy continuation, see [58, 79].

The most straightforward optimal homotopy is a *parameter homotopy* [55, 59], in which the structure and number of solutions of the start, target, and intermediate systems are the same. A source for parameter homotopies is a branched cover $X \to Z$, where Z is a rational variety and X is a subvariety of $\mathbb{C}^n \times Z$. Suppose that $f\colon \mathbb{C}_t \to Z$ is a rational curve with $f(0)$ and $f(1)$ lying in the open set U of regular values of $X \to Z$. Pulling back $X \to Z$ along f gives a dominant map $\pi\colon f^*(X) \to \mathbb{C}_t$ with the same degree d as $X \to Z$. A generating set $\mathcal{H}(x;t)$ of the ideal of $f^*(X) \subset \mathbb{C}^n \times \mathbb{C}_t$ gives a homotopy that is optimal as there are d solutions to both the start and target systems.

For example, suppose that $X \to Z = \mathbb{P}^{19}$ is the branched cover (1) from the problem of 27 lines. Given smooth cubics f_1 and f_0, the pencil $f(t) := tf_1 + (1-t)f_0$ is a map $\mathbb{C}_t \to \mathbb{P}^{19}$ as above. A general line ℓ in $\mathbb{P}^3$ is the span of points $[x_1, x_2, 1, 0]$ and $[x_3, x_4, 0, 1]$, for $(x_1, x_2, x_3, x_4) \in \mathbb{C}^4$. A general point on ℓ has the form $[ux_1 + x_3, xu_2 + x_4, u, 1]$, for $u \in \mathbb{C}$, and ℓ lies on the cubic $\mathcal{V}(f(t))$ when $f(t)(ux_1+x_3, xu_2+x_4, u, 1)$ is identically zero. Thus, if we expand $f(t)(ux_1 + x_3, xu_2 + x_4, u, 1)$ as a polynomial in u, the four coeffcients of the resulting cubic are equations in $x_1, \ldots, x_4, t$ for the general line ℓ to lie on the cubic $\mathcal{V}(f(t))$. Let $\mathcal{H}(x;t)$ be these four coefficients. When $\mathcal{V}(f_1)$ has 27 lines of the given form, this is a homotopy, and if we knew the coordinates of those 27 lines, numerical homotopy continuation using $\mathcal{H}(x;t)$ could be used to compute the lines on $\mathcal{V}(f_0)$.

2.2. **Witness sets.** Numerical homotopy continuation enables the reliable computation of solutions to systems of polynomial equations. Numerical algebraic geometry uses this ability to solve as a basis for algorithms that study and manipulate varieties on a computer.

Its starting point is a witness set, which is a data structure for varieties in $\mathbb{C}^n$ [77, 78]. Suppose that $X \subset \mathbb{C}^n$ is a union of irreducible components of the same dimension m of a variety $\mathcal{V}(F)$, where F is a system of polynomials. If $L \subset \mathbb{C}^n$ is a general linear subspace of codimension m, then $W := X \cap L$ is a transverse intersection consisting of $\deg(X)$ points, called a *linear section* of X. The triple (W, F, L) is a *witness set* for X (typically, L is represented by m linear forms).

Given a witness set (W, F, L) for X and a general codimension m linear subspace L', we may compute the linear section $W' = X \cap L'$ and obtain another witness set (W', F, L') for X as follows. Let $L(t) := tL + (1-t)L'$ be the convex combination of (the equations for) L and L', and form the homotopy $\mathcal{H}(x;t) := (F, L(t))$. Path-tracking using $\mathcal{H}(x;t)$ starting from the points of W at $t = 1$ will compute the points of W' at $t = 0$. This instance of the parameter homotopy is called "moving the witness set".

Suppose that we have a third codimension m linear subspace L''. We may then use W' to compute the linear section $W'' = X \cap L''$, and then use W'' to return to W. The arcs connect every point $w \in W$ to a point $w' \in W'$, then to a point $w'' \in W''$, and finally to a possibly different point $\sigma(w) \in W$. This defines a permutation σ of W. The four points, as they are connected by smooth arcs, lie in the same irreducible component of X. Thus the cycles in the permutation σ refine the partition of W given by the irreducible components of X. Repeating this procedure with possible different linear subspaces L', L'', and then applying the trace test [53, 76], leads to a *numerical irreducible decomposition* of X; that is, it computes the partition $W = W_1 \sqcup W_2 \sqcup \cdots \sqcup W_r$, where $X_1, \ldots, X_r$ are the irreducible components of X and $W_i := X_i \cap L$. This algorithm was developed in [74, 75, 76].

Several freely available software packages have implementations of the basic algorithms of Numerical Algebraic Geometry. These include Macaulay 2 [30] in its Numerical Algebraic Geometry package [52], in Bertini [5], and in HomotopyContinuation.jl [10].

3. Fano Problems

Debarre and Manivel determined the dimension and degree of the variety of r-planes lying on general complete intersections in $\mathbb{P}^n$. When this is zero-dimensional it is called a *Fano problem*. For example, the problem of 27 lines is a Fano problem. Galois groups of Fano problems were studied classically by Jordan and Harris and recently by Hashimoto and Kadets, who nearly determined the Galois group for each Fano problem.

3.1. Combinatorics of Fano Problems.

Let $\mathbb{G}(r, \mathbb{P}^n)$ be the Grassmann variety defined over the complex numbers of r-dimensional linear subspaces of $\mathbb{P}^n$, which has dimension $(r+1)(n-r)$. Given a variety $X \subseteq \mathbb{P}^n$, its *Fano scheme* is the subscheme of $\mathbb{G}(r, \mathbb{P}^n)$ of r-planes lying on X.

Fano schemes may be studied uniformly when $X \subset \mathbb{P}^n$ is a complete intersection. For this, let $d_\bullet := (d_1, \ldots, d_s)$ be a weakly increasing list of integers greater than 1. Suppose that $F = (f_1, \ldots, f_s)$ are homogeneous polynomials on $\mathbb{P}^n$ with f_i of degree d_i. Let $\mathcal{V}_r(F)$ be the Fano scheme of r-planes in $\mathcal{V}(F)$.

Just as $\mathcal{V}(F)$ has expected dimension $n-s$, there is an expected dimension for $\mathcal{V}_r(F)$. Let f be a form on $\mathbb{P}^n$ of degree d. Its restriction to $H \in \mathbb{G}(r, \mathbb{P}^n)$ is a form of degree d

on H; as the dimension of the vector space of such forms is $\binom{d+r}{r}$, we expect this to be the codimension of $\mathcal{V}_r(f)$ in $\mathbb{G}(r,\mathbb{P}^n)$. Thus the expected dimension of $\mathcal{V}_r(F)$ is

$$\delta = \delta(r,n,d_\bullet) \;:=\; (r+1)(n-r) \;-\; \sum_{i=1}^{s}\binom{d_i+r}{r}.$$

Write $\mathbb{C}^{(r,n,d_\bullet)}$ for the vector space of homogeneous polynomials $F=(f_1,\dots,f_s)$ in $n+1$ variables with f_i of degree d_i. Debarre and Manivel [16] showed that there is a dense open subset $U = U_{(r,n,d_\bullet)} \subset \mathbb{C}^{(r,n,d_\bullet)}$ with the following property: For $F\in U$, if $\delta\geq 0$ and $n-s\geq 2r$, then $\mathcal{V}_r(F)$ is a smooth variety of dimension δ, and if $\delta<0$ or $n-s<2r$, then $\mathcal{V}_r(F)$ is empty. A *Fano problem* is the enumerative problem of determining $\mathcal{V}_r(F)$ for $F\in U_{(r,n,d_\bullet)}$, when $\delta(r,n,d_\bullet)=0$ and $n-s\geq 2r$.

Since the Grassmannian has Picard group generated by $O(1)$ induced by its Plücker embedding, when $\delta\geq 0$ and $n-s\geq 2r$ and $F\in U$, the Fano variety $\mathcal{V}_r(F)$ has a well-defined degree. Standard techniques in intersection theory allow this degree to be computed, using that $\mathcal{V}_r(F)$ is the vanishing of sections of appropriate vector bundles on $\mathbb{G}(r,\mathbb{P}^n)$. (These are $\mathrm{Sym}_{d_i}(T)$, where T is the dual of the tautological $(r+1)$-subbundle on the Grassmannian.)

This leads to a formula for this degree. For that, define the polynomials

$$Q_{r,d}(x) \;=\; \prod_{a_0+\cdots+a_r=d}(a_0x_0+\cdots+a_rx_r)\in\mathbb{Z}[x_0,\dots,x_r] \qquad a_i\in\mathbb{Z}_{\geq 0}$$

as well as $Q_{r,d_\bullet}=Q_{r,d_1}(x)\cdots Q_{r,d_s}(x)$ and the Vandermonde polynomial

$$\mathrm{V}_r(x) \;=\; \prod_{0\leq i<j\leq r}(x_i-x_j)\,.$$

When $\delta(r,n,d_\bullet)=0$, $n-s\geq 2r$, and $F\in U_{(r,n,d_\bullet)}$, the degree $\deg(r,n,d_\bullet)$ of $\mathcal{V}_r(F)$ is the coefficient of $x_0^n x_1^{n-1}\cdots x_r^{n-r}$ in the product $Q_{r,d_\bullet}(x)\mathrm{V}_r(x)$ [16, Thm. 4.3]. Table 1 gives these degrees for all Fano problems with a small number of solutions.

TABLE 1. Small finite Fano problems

r	n	$d_\bullet$	# of solutions	Galois Group
1	4	$(2,2)$	16	D_5
1	3	(3)	27	E_6
2	6	$(2,2)$	64	D_7
3	8	$(2,2)$	256	D_9
1	7	$(2,2,2,2)$	512	S_{512}
1	6	$(2,2,3)$	720	S_{720}
2	8	$(2,2,2)$	1024	S_{1024}
1	5	$(3,3)$	1053	S_{1053}

3.2. **Galois groups of Fano problems.** Consider the incidence correspondence,

$$\begin{array}{l} \Gamma := \{(F,H) \in \mathbb{C}^{(r,n,d_\bullet)} \times \mathbb{G}(r,\mathbb{P}^n) \ \mid\ F|_H = 0\}. \\ \Big\downarrow \pi \\ \mathbb{C}^{(r,n,d_\bullet)} \end{array}$$

The fiber over a general complete intersection $F \in U_{(r,n,d_\bullet)}$ is the Fano variety $\mathcal{V}_r(F)$. When we have a Fano problem, $\delta(r,n,d_\bullet) = 0$ and $n - s \geq 2r$, π is a branched cover of degree $\deg(r,n,d_\bullet)$. We define the Galois group of the Fano problem to be $\mathrm{Gal}_{(r,n,d_\bullet)} = \mathrm{Gal}_\pi$.

The study of Galois groups of Fano problems began with Jordan [43] with the problem of 27 lines on a smooth cubic surface, which has data $(1,3,(3))$. By observing the incidence structure of the lines on a smooth cubic, Jordan determined that the Galois group over $\mathbb{C}$ is a subgroup of E_6, $\mathrm{Gal}_{(1,3,(3))} \subseteq E_6$.

Harris [31] showed that Jordan's inclusion is an equality, $\mathrm{Gal}_{(1,3,(3))} = E_6$, and then generalized this, showing that $\mathrm{Gal}_{(1,n,(2n-3))}$ is fully symmetric for $n \geq 4$. For this, he used the interpretation of the Galois group as a monodromy group. Using arguments from algebraic geometry, when $n \geq 4$ he showed that the monodromy group is 2-transitive and contains a simple transposition.

Hashimoto and Kadets [32] recently revisited this topic, determining these groups in many cases. There are two special cases of finite Fano problems, that of lines on a cubic surface and that of linear spaces on the intersection of two quadrics. Hashimoto and Kadets showed that these problems are enriched and that

$$\mathrm{Gal}_{(1,3,(3))} \;=\; E_6 \qquad \text{and} \qquad \mathrm{Gal}_{(r,2r+2,(2,2))} \;=\; W(D_{2r+3})\,.$$

The enriched Galois structure is reflected in that these are the only Fano problems where the r-planes on $\mathcal{V}(F)$ will intersect. As in the problem of 27 lines, the generic incidence structure prevents the Galois group from being fully symmetric. In all other cases, they showed that the Galois group is at least alternating. In Section 5.2, we describe a method based on numerical homotopy continuation to compute monodromy permutations, when $\Bbbk = \mathbb{C}$. We used this to show that some small Fano problems have full symetric Galois groups.

Theorem 5. *Each of the Fano problems*

$$(1,7,(2,2,2,2))\,,\ (1,6,(2,2,3))\,,\ (2,8,(2,2,2,2))\,,\ \textit{and}\ (1,5,(3,3))\,,$$

has full symmetric Galios group.

4. Galois groups of sparse polynomial equations

We work over the complex numbers. With modifications due to separability, much of this holds over an arbitrary field. However, a key argument in Esterov's proof for Theorem 7 uses that the field is uncountable, together with topological properties of $\mathbb{C}$.

The Bernstein-Kuchnirenko Theorem gives an upper bound on the number of solutions in the algebraic torus $(\mathbb{C}^\times)^n$ to a system of polynomials. This bound depends on the monomials which appear in the equations (their support). When the equations are general given their support, this bound is attained. The family of all systems with a given support forms a branched cover and therefore has a Galois group. Esterov identified two structures in the support which imply that the Galois group is imprimitive, and showed that if they are not present, then the Galois group is full symmetric. It remains an open problem to determine the Galois group when it is imprimitive.

4.1. **Systems of sparse polynomial equations.** A *(Laurent) monomial* in n variables $x_1, \dots, x_n$ with exponent vector $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{Z}^n$ is

$$x^\alpha \ := \ x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n} \,.$$

This is a character of the algebraic torus $(\mathbb{C}^\times)^n$. A *(Laurent) polynomial* f over $\mathbb{C}$ is a linear combination of monomials,

$$f \ = \ \sum c_\alpha x^\alpha \qquad c_\alpha \in \mathbb{C}\,.$$

For a nonempty finite set $\mathcal{A} \subseteq \mathbb{Z}^n$, the space of *polynomials supported on $\mathcal{A}$* is written $\mathbb{C}^{\mathcal{A}}$. This is the set of polynomials f such that $c_\alpha \neq 0$ implies $\alpha \in \mathcal{A}$.

Given a collection $\mathcal{A}_\bullet = (\mathcal{A}_1, \mathcal{A}_2, \dots, \mathcal{A}_n)$ of nonempty finite subsets of $\mathbb{Z}^n$, write

$$\mathbb{C}^{\mathcal{A}_\bullet} \ := \ \mathbb{C}^{\mathcal{A}_1} \times \cdots \times \mathbb{C}^{\mathcal{A}_n}$$

for the vector space of n-tuples $F = (f_1, \dots, f_n)$ of polynomials, where f_i has support $\mathcal{A}_i$, for each $i = 1, \dots, n$. An element $F \in \mathbb{C}^{\mathcal{A}_\bullet}$ is a square system of polynomials whose solutions are those $x \in (\mathbb{C}^\times)^n$ such that

$$f_1(x_1, \dots, x_n) \ = \ f_2(x_1, \dots, x_n) \ = \ \cdots \ = \ f_n(x_1, \dots, x_n) \ = \ 0\,,$$

written $F(x) = 0$. We call F a *sparse polynomial system with support $\mathcal{A}_\bullet$*.

Given supports $\mathcal{A}_\bullet = (\mathcal{A}_1, \dots, \mathcal{A}_n)$, define the incidence variety

$$\Gamma = \Gamma_{\mathcal{A}_\bullet} \ := \ \left\{(F, x) \in \mathbb{C}^{\mathcal{A}_\bullet} \times (\mathbb{C}^\times)^n \mid F(x) = 0\right\}\,.$$

It is equipped with projections $\pi\colon \Gamma \to \mathbb{C}^{\mathcal{A}_\bullet}$ and $p\colon \Gamma \to (\mathbb{C}^\times)^n$. The fiber $p^{-1}(x)$ for $x \in (\mathbb{C}^\times)^n$ is the set of all polynomials $(f_1, \dots, f_n)$ with $f_i(x) = 0$ for each i. Observing that $f_i(x) = 0$ is a non-zero linear equation on $\mathbb{C}^{\mathcal{A}_i}$, we see that $p^{-1}(x) \subset \mathbb{C}^{\mathcal{A}_\bullet}$ is the product of n hyperplanes and thus has codimension n. Consequently, $\Gamma \to (\mathbb{C}^\times)^n$ is a vector bundle, and therefore irreducible, and it has dimension equal to $\dim \mathbb{C}^{\mathcal{A}_\bullet}$.

Thus the map $\pi\colon \Gamma \to \mathbb{C}^{\mathcal{A}_\bullet}$ is a branched cover when π is dominant, equivalently, when a generic system $F \in \mathbb{C}^{\mathcal{A}_\bullet}$ has a positive, finite number of solutions in $(\mathbb{C}^\times)^n$. The number of solutions to a generic system is determined by the polyhedral geometry of its support, which we review. For convex bodies $K_1, \dots, K_n \subset \mathbb{R}^n$ and nonnegative real numbers, $t_1, \dots, t_n \in \mathbb{R}_{\geq 0}$, Minkowski proved that the volume of the Minkowski sum

$$t_1 K_1 + \cdots + t_n K_n \ := \ \{t_1 x_1 + \cdots + t_n x_x \mid x_i \in K_i\}$$

is a homogeneous polynomial of degree n in $t_1, \dots, t_n$. Its coefficient of $t_1 \cdots t_n$ is the *mixed volume* of $K_1, \dots, K_n$. For supports $\mathcal{A}_\bullet = (\mathcal{A}_1, \dots, \mathcal{A}_n)$, let $\mathrm{MV}(\mathcal{A}_\bullet)$ be the mixed volume of their convex hulls, $\mathrm{conv}(\mathcal{A}_1), \dots, \mathrm{conv}(\mathcal{A}_n)$. This is described in detail in [26]. We state the Bernstein-Kushnirenko Theorem [8, 48].

Theorem 6 (Bernstein-Kushnirenko). *A system $F \in \mathbb{C}^{\mathcal{A}_\bullet}$ has at most $\mathrm{MV}(\mathcal{A}_\bullet)$ isolated solutions in $(\mathbb{C}^\times)^n$. This bound is sharp and attained for generic $F \in \mathbb{C}^{\mathcal{A}_\bullet}$.*

Thus $\pi\colon X_{\mathcal{A}_\bullet} \to \mathbb{C}^{\mathcal{A}_\bullet}$ is a branched cover of degree $\mathrm{MV}(\mathcal{A}_\bullet)$ if and only if $\mathrm{MV}(\mathcal{A}_\bullet) > 0$, which Minkowski determined as follows. For a nonempty subset $I \subseteq [n] := \{1, \dots, n\}$, write $\mathcal{A}_I := (\mathcal{A}_i \mid i \in I)$ and let $\mathbb{Z}\mathcal{A}_I$ be the affine span of the supports in $\mathcal{A}_I$. This is the free abelian group generated by all differences $\alpha - \beta$ for $\alpha, \beta \in \mathcal{A}_i$ for some $i \in I$. Then $\mathrm{MV}(\mathcal{A}_\bullet) = 0$ if and only if there exists a subset $I \subseteq [n]$ such that $|I| > \mathrm{rank}(\mathbb{Z}\mathcal{A}_I)$. One direction is obvious. When $|I| > \mathrm{rank}(\mathbb{Z}\mathcal{A}_I) = m$, then there is a change of variables so that the subsystem of polynomials with indices in I has more equations than variables. In particular, $\mathrm{MV}(\mathcal{A}_\bullet) \neq 0$ implies that $\mathbb{Z}\mathcal{A}_\bullet := \mathbb{Z}\mathcal{A}_{[n]}$ has full rank n.

4.2. **Galois groups of sparse polynomial systems.** Suppose that $\mathcal{A}_\bullet$ is a collection of supports with $\mathrm{MV}(A_\bullet) > 0$. Write $\mathrm{Gal}_{\mathcal{A}_\bullet}$ for the Galois group of the corresponding branched cover $\pi\colon \Gamma_{\mathcal{A}_\bullet} \to \mathbb{C}^{\mathcal{A}_\bullet}$. Esterov [24] studied these groups, identifying two structures which imply that $\mathrm{Gal}_{\mathcal{A}_\bullet}$ is imprimitive.

We call $\mathcal{A}_\bullet$ *lacunary* if $\mathbb{Z}\mathcal{A}_\bullet \neq \mathbb{Z}^n$. If $\mathrm{MV}(\mathcal{A}_\bullet) > [\mathbb{Z}^n \colon \mathbb{Z}\mathcal{A}_\bullet]$, then it is *strictly lacunary*. Lacunary systems generalize the following example. Let $n = 1$ and suppose that we have a univariate polynomial $f(x)$ of the form $g(x^3)$, for g a univariate polynomial with $g(0) \neq 0$. Observe that $\mathbb{Z}\mathcal{A}_\bullet \subset 3\mathbb{Z}$. The zeroes of f ($\{x \in \mathbb{C} \mid f(x) = 0\}$) are cube roots of the zeroes of g, and the group of cubic roots of unity acts freely on the zeroes of f. These orbits are blocks of the action of the Galois group of f. When g has two or more roots, there is more than one orbit, and the action of the Galois group is imprimitive.

We call $\mathcal{A}_\bullet$ *triangular* if there exists a nonempty proper subset $I \subsetneq [n]$ such that $\mathrm{rank}(\mathbb{Z}\mathcal{A}_I) = |I|$. In this case there is a change of variables so that the equations indexed by I involve only the first $|I|$ variables. We write $\mathrm{MV}(\mathcal{A}_I)$ for the mixed volume of the supports of the polynomials indexed by I as polynomials in the first $|I|$ variables. We say $\mathcal{A}_\bullet$ is *strictly triangular* if $1 < \mathrm{MV}(\mathcal{A}_I) < \mathrm{MV}(\mathcal{A}_\bullet)$.

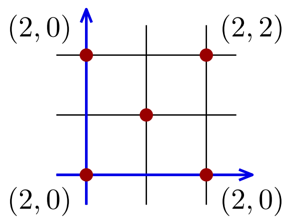
Strictly triangular systems generalize the following example. Let $n = 2$ and write our variables as (y, z) and suppose that we have a system F of the form $f(y) = g(y, z) = 0$, where $\deg(f)$, $\deg_z(g)$ are both at least 2. (Here, $\deg_z(g)$ is the degree of g as a polynomial in z.) Since the first coordinate of a solution (y^*, z^*) of F is a solution of f, the action of the Galois group of F has blocks given by the fibers of the projection to the first coordinate. When f and g are general given their supports, there are $\deg(f)$ blocks, each of size $\deg_z(g)$, and the action of the Galois group is imprimitive.

We provide more details in Section 7. This is explained fully in [24], and algorithmically in [12, Sect. 2.3]. When $\mathcal{A}_\bullet$ is neither lacunary nor strictly triangular, Esterov showed that $\mathrm{Gal}_{\mathcal{A}_\bullet}$ is 2-transitive using that a countable union of subvarieties is nowhere dense. Then, he showed that a small loop around the discriminant of these systems generates a simple transposition, which shows that $\mathrm{Gal}_{\mathcal{A}_\bullet}$ is full symmetric.

Theorem 7 (Esterov). *Let $\mathcal{A}_\bullet$ be a set of supports with $\mathrm{MV}(\mathcal{A}_\bullet) > 0$. If $\mathcal{A}_\bullet$ is neither strictly lacunary nor strictly triangular, then $\mathrm{Gal}_{\mathcal{A}_\bullet}$ is the full symmetric group. If $\mathcal{A}_\bullet$ is strictly lacunary or strictly triangular, then $\mathrm{Gal}_{\mathcal{A}_\bullet}$ is imprimitive. If $\mathcal{A}_\bullet$ is lacunary but not strictly lacunary, then $\mathrm{Gal}_{\mathcal{A}_\bullet}$ is the group $\mathrm{Hom}(\mathbb{Z}^n/\mathbb{Z}\mathcal{A}_\bullet, \mathbb{C}^\times)$ of roots of unity.*

When $\mathcal{A}_\bullet$ is either strictly lacunary or strictly triangular, Esterov's theorem does not determine the group $\mathrm{Gal}_{\mathcal{A}_\bullet}$ explicitly. As it is imprimitive, the Galois group $\mathrm{Gal}_{\mathcal{A}_\bullet}$ is a subgroup of a certain wreath product. It may be a proper subgroup, as the following example shows.

Example 8. Let $n = 2$ and suppose that $\mathcal{A}$ is consists of the vertices of the 2×2 square and its center point $(1, 1)$, which we show below.



Let $\mathcal{A}_\bullet := (\mathcal{A}, \mathcal{A})$. Its mixed volume is $\mathrm{MV}(\mathcal{A}_\bullet) = 8$, which is twice the area of the square. Thus a general system of polynomials with support $\mathcal{A}_\bullet$ has eight solutions in $(\mathbb{C}^\times)^n$. The lattice $\mathbb{Z}\mathcal{A}_\bullet$ has index 2 in $\mathbb{Z}^2$, so solutions come in four pairs of symmetric points, (x, y) and $(-x, -y)$. These pairs are preserved by the Galois group, showing that it is a subgroup of the wreath product $S_2 \wr S_4$. It can be shown that $\mathrm{Gal}_{\mathcal{A}_\bullet} = (S_2 \wr S_4) \cap A_8$ and is thus a proper subgroup of this wreath product. $\diamond$

This example is due to Esterov and Lang [25], who gave conditions which imply that the Galois group is the full wreath product, for certain lacunary systems. Despite this, there is no known criteria for when that occurs, not even a conjecture about which groups can occur as Galois groups of sparse polynomial systems. Also, it is not clear what can be said about Galois groups of sparse polynomials over other fields than the complex numbers.

5. Computing Galois Groups

Understanding Galois groups of enumerative problems has both benefited from and inspired the development of and use of computational tools. We discuss an adaptation of the well-known symbolic method of computing cycle types of Frobenius elements and then several methods based on numerical homotopy continuation. For a prime $p \in \mathbb{Z}$, write $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ for the field with p elements.

5.1. **Frobenius elements.** Let $f \in \mathbb{Z}[x]$ be a monic irreducible univariate polynomial and $\mathbb{K}$ its splitting field, a finite Galois extension of $\mathbb{Q}$. Let $\mathcal{O} \subset \mathbb{K}$ be those elements that are integral over $\mathbb{Z}$. For every prime $p \in \mathbb{Z}$ not dividing the discriminant of f, there is a unique *Frobenius element* $\sigma_p \in \mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ in the Galois group of $\mathbb{K}$ over $\mathbb{Q}$ that restricts to the Frobenius automorphism above p: For every prime ϖ of $\mathcal{O}$ with $\varpi \cap \mathbb{Z} = \langle p \rangle$ (ϖ is *above* p), and every $z \in \mathcal{O}$, we have $\sigma_p(z) \equiv z^p \mod \varpi$. If f is not monic, then we first invert the primes dividing the leading coefficient of f. This is explained in [50, §§ VII.2].

The cycle type of σ_p (as a permutation of the roots of f) is given by the degrees of the irreducible factors in $\mathbb{F}_p[x]$ of $f_p := f \mod p$, as these factors give primes ϖ above p. Indeed, if g is an irreducible factor of degree r, then $\mathcal{O}/\varpi \simeq \mathbb{F}_p[x]/\langle g \rangle$ is a finite field with p^r elements. The cycle type of σ_p records how p splits in $\mathcal{O}$ and is also called the *splitting type* of σ_p or of f_p. The prime p does not divide the discriminant exactly when f_p is squarefree with the same degree as f. This gives a method to compute cycle types of elements of $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$: For a prime p with $\deg(f_p) = \deg(f)$, factor the reduction f_p, and if no factor is repeated, record the degrees of the factors.

This is particularly effective due to the Chebotarev Density Theorem [86, 87]: Let $\mathbb{K}/\mathbb{Q}$ be a Galois extension and λ a cycle type of an element in $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$. Let n_λ be the fraction of elements in $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ with cycle type λ. Then the density of primes $p \leq N$ such that the Frobenius element σ_p has splitting type λ tends to n_λ as $N \to \infty$. Loosely, for p sufficiently large, Frobenius elements are distributed uniformly in $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$.

Table 2 illustrates this when f is $x^6 - 503x^5 - 544x^4 - 69x^3 - 152x^2 - 49x - 763$, which

TABLE 2. Frobenius elements for f

1^6	$1^4,2$	$1^2,2^2$	2^3	$1^3,3$	$1,2,3$	3^2	$1^2,4$	$2,4$	$1,5$	6
1	15	45	15	40	120	40	90	90	144	120
3	12	24	9	47	146	32	112	71	121	143
.989	15.02	44.97	14.99	40.07	120.03	39.95	89.87	89.97	144.24	119.9

has Galois group S_6. The headers in the first row are the cycle types (conjugacy classes) of permutations in S_6, expressed using the frequency representation for cycles type in which (2^3) indicates three 2-cycles. The second row contains the sizes of each conjugacy class. The third row records how many of the first $720 = 6!$ primes p not dividing the discriminant[1] did f_p have the corresponding splitting type. For the last row, we repeated this calculation for the first $720 \cdot 10^5$ primes larger than 10^8. We display the observed number that had a given splitting type, divided by 10^5 for comparison.

Determining the splitting type of Frobenius elements gives information about Galois groups, including information about the distribution of cycle types in a Galois group. For example, if the Galois group Gal is known to be a subgroup of a particular permutation group G, knowing the cycle types of relatively few elements often suffices to show that $\mathrm{Gal} = G$, as Proposition 4 does for the symmetric group. If we do not have a candidate for Gal, then computing many Frobenius elements may help to predict the Galois group with a high degree of confidence, by the Chebotarev density theorem.

Frobenius elements are also a tool for studying Galois groups in enumerative geometry. Let $\pi\colon X \to Z$ be a branched cover of irreducible varieties defined over $\mathbb{Z}$ with Z smooth and rational. For any regular value $z \in Z(\mathbb{Q})$ of π, let $\mathbb{K}_z$ be the field generated by the coordinates of the points in the fiber $\pi^{-1}(z)$ (in $X(\overline{\mathbb{Q}})$). This is a finite Galois extension of $\mathbb{Q}$ whose Galois group is a subgroup of $\mathrm{Gal}_\pi(\mathbb{Q})$. For all except finitely many primes p, both z and $\pi^{-1}(z)$ have reductions z_p and $\pi^{-1}(z_p)$ modulo p, and there is a Frobenius element $\sigma_{p,z} \in \mathrm{Gal}(\mathbb{K}_z/\mathbb{Q})$. This is also a consequence of [50, §§ VII.2].

Given a prime p and a cycle type λ of an element in the Galois group $\mathrm{Gal}_\pi(\mathbb{Q})$, we may consider the density of points $z \in Z(\mathbb{F}_p)$ that are regular values of π such that the

[1] $1897200677467777300238674815969 6 = 2^4 \cdot 3^{12} \cdot 7 \cdot 29 \cdot 2633 \cdot 88805021 \cdot 47006055979$.

corresponding Frobenius element has conjugacy class λ. Ekedahl [21] showed that in the limit as $p \to \infty$, this density tends to n_λ, the density of the conjugacy class in $\mathrm{Gal}_\pi(\mathbb{Q})$.

This theoretical result may be used in an algorithm. Assume that $\pi\colon X \to Z$ is a branched cover of irreducible varieties defined over $\mathbb{Z}$ with Z an open subset of an affine space $\mathbb{A}^m(\mathbb{Z})$. All enumerative problems we discuss have this form, as Z is typically a variety of parameters (coefficients of polynomials or entries of matrices representing flags). Replacing X by an open subset, we have that $X \subset \mathbb{A}^m(\mathbb{Z}) \times \mathbb{A}^n(\mathbb{Z})$ is an affine variety with ideal $I \subset \mathbb{Z}[z, x]$. Specializing I at an integer point $z \in Z(\mathbb{Z})$ gives the ideal $I(z)$ of the fiber $\pi^{-1}(z)$. The splitting type of the fiber at p may determined by a primary decomposition of the ideal $I(z)$ modulo p.

Consider this for the branched cover $\pi\colon \Gamma \to \mathbb{P}^{19}$ of lines on cubic surfaces (1). For each of 69 primes p between 5 and 11579, we determined the splitting type of the 27 lines for many (70 to 220 million) randomly chosen smooth cubic surfaces in $\mathbb{P}^{19}(\mathbb{F}_p)$, and compared that to the distribution of cycle types in the Galois group E_6. More specifically, let n_λ be the density of elements in E_6 with cycle type λ. For a prime p, let $E_{p,\lambda}$ be the empirical density, the observed fraction of surfaces whose lines had splitting type λ. By Ekedahl's Theorem, $\lim_{p\to\infty} E_{p,\lambda} = n_\lambda$. (This same limit holds if we replace smooth cubics in $\mathbb{P}^{19}(\mathbb{F}_p)$ by isomorphism classes of smooth cubics over $\mathbb{F}_p$ [4].) Figure 2 presents some data from our calculation. The full computation is archived on the web page[2].

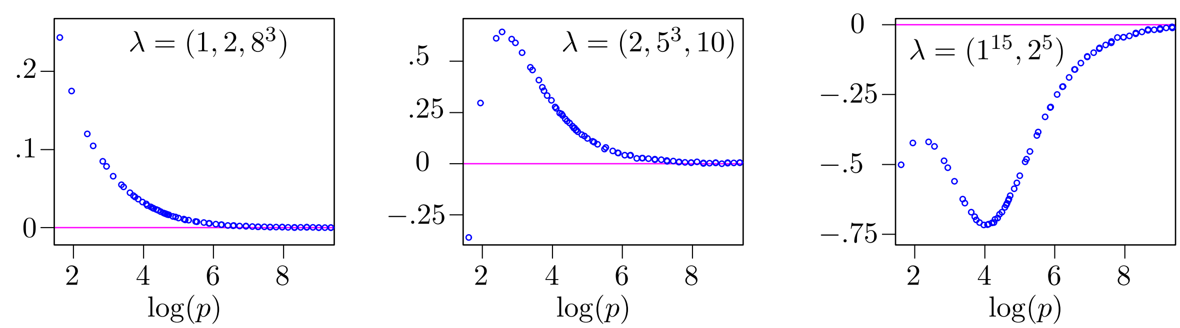


FIGURE 2. Relative discrepancy, $\frac{E_{p,\lambda}}{n_\lambda} - 1$, against $\log(p)$ at 69 primes p, for splitting types $\lambda \in \{(1, 2, 8^3), (2, 5^3, 10), (1^{15}, 2^5)\}$.

There are algorithms to compute this decomposition implemented in software such as Macaulay2 [30] or Singular [17]. While these rely on Gröbner bases, they are unreasonably effective, as they also take advantage of fast Gröbner basis calculation in positive characteristic, for example the F5 algorithm [27].

5.2. **Computing Galois groups numerically.** In Section 2.2, we discussed how moving a witness set W to another one, W', to a third, W'', and then back to W computes a permutation σ of W. This is readily adapted to computing a permutation of a fiber of a branched cover, which is an element of its Galois group Gal_π. While computing several such monodromy permutations only gives a subgroup of Gal_π, that may be sufficient to

[2] https://www.math.tamu.edu/~sottile/research/stories/27_Frobenius/

determine it [54]. We explain a numerical method from [35] that computes a generating set for the Galois group and another numerical method to study transitivity.

Given a branched cover $\pi\colon X \to Z$ of degree d over $\mathbb{C}$ with Z rational, let $U \subset Z$ be the regular locus so that $\pi^{-1}(U) \to U$ is a covering space. Suppose that we have computed all points in a fiber $\pi^{-1}(z)$ for some point $z \in U$. Choosing other points $z', z'' \in U$, we may construct three parameter homotopies that move the points of $\pi^{-1}(z)$ to those of $\pi^{-1}(z')$, to $\pi^{-1}(z'')$, and then back to $\pi^{-1}(z)$. The tracked paths give a permutation σ of the fiber $\pi^{-1}(z)$.

Writing the points of $\pi^{-1}(z)$ in some order $(w_1, \dots, w_d)$ gives a point in the fiber of $X_Z^{(d)}$ over z. (Recall that $X_Z^{(d)}$ was used in Section 1.1 to give a geometric construction of Gal_π.) The d-tuples of computed paths between the fibers $\pi^{-1}(z)$, $\pi^{-1}(z')$, $\pi^{-1}(z'')$, and back to $\pi^{-1}(z)$ give a path in $X_Z^{(d)}$ from the point $(w_1, \dots, w_d)$ and the point $(\sigma(w_1), \dots, \sigma(w_d))$ in the same fiber. These paths all lie in the same irreducible component of $X_Z^{(d)}$, showing that $\sigma \in \mathrm{Gal}_\pi$.

This may be used to compute many permutations in Gal_π, giving an increasing sequence of subgroups of Gal_π. As with computing Frobenius elements, this may suffice to determine Gal_π. For example, if the computed subgroup of Gal_π is S_d, then $\mathrm{Gal}_\pi = S_d$ is full-symmetric. This method was used in [54] to show that several Schubert Galois groups (see Section 6) were full-symmetric, including one with $d = 17589$. In that computation, every time a new permutation π was found, GAP [29] was called to test if the computed set of permutations generated the symmetric group.

A drawback is that numerical path tracking may be inexact, which can lead to false conclusions (this is known as path-crossing). A consequence of the calculation in [54] was the implementation of an algorithm [36] for *a posteriori* certification of the computed solutions to a system of polynomials, based on Smale's α-theory [73]. Certification using Krawczyk's method from interval arithmetic [46] has also been implemented [9], providing another approach. More substantially, algorithms were developed [6, 7] to certify path-tracking and thereby certifiably compute monodromy.

This approach of computing monodromy may be improved to compute a generating set of the Galois group [35]. Given a branched cover $\pi\colon X \to Z$ as above, restricting to an open subset of Z and compactifying, we may assume that $Z = \mathbb{P}^N$. The branch locus of $\pi\colon X \to \mathbb{P}^N$ is a hypersurface $B \subset \mathbb{P}^N$. Let $z \in U := \mathbb{P}^n \smallsetminus B$. Lifting loops in U based at z gives a surjective homomorphism from the fundamental group of U to the monodromy group of the cover $\pi^{-1}(U) \to U$ [33, 64].

A witness set for B can be used to obtain a generating set for the fundamental group of U. Suppose that $\ell \cap B$ is a linear section of the hypersurface B, so that $\ell \simeq \mathbb{P}^1$ is a line. Zariski [93] showed that the inclusion $\ell \cap U \hookrightarrow U$ induces a surjection from the fundamental group of $\ell \cap U$ to the fundamental group of U. As the fundamental group of $\ell \cap U$ is generated by based loops around each of the (finitely many) points of $\ell \smallsetminus (B \cap \ell)$, lifts of these loops generate the Galois group Gal_π of the branched cover.

In [35], this method is demonstrated on the branched cover $\Gamma \to \mathbb{P}^{19}$ (1) from the problem of 27 lines. The branch locus B is the set of singular cubics, which forms a hypersurface on $\mathbb{P}^{19}$ of degree 32, so that a general line ℓ in $\mathbb{P}^{19}$ meets B transversally in 32 points. The computed permutations for a particular choice of ℓ (given in Figure 5 in [35]) generate E_6. Each permutation is a product of six disjoint 2-cycles in S_{27}. Here is one,

$$(1,6)(4,13)(8,25)(10,19)(11,16)(20,27)\ .$$

That a loop around a point of $\ell\cap B$ gives a permutation that is the product of six disjoint 2-cycles is a manifestation of the enriched structure of this enumerative problem; Above a general point of B, there are six solutions of multiplicity 2. Contrast this with the result of Esterov [24] from Section 4 where a single loop around B gave a simple transposition.

Similar ideas were used to establish Theorem 5, except that rather than compute a full witness set for the branch locus, a single point $z\in\ell\cap B$ in a linear section of the branch locus was computed. Lifting one loop around z gave a simple transposition, which was sufficient to show that those Fano problems wre full symmetric.

We mention another method from [35] involving transitivity. Let $\pi\colon X\to Z$ be a branched cover of degree d. By Proposition 2, for any $1\leq s\leq d$, s-transitivity of the Galois group Gal_π is equivalent to the irreducibility of the variety $X_Z^{(s)}$. Numerical irreducible decomposition may be used to determine the (ir)reducibility of $X_Z^{(s)}$ and therby determine whether or not Gal_π is s-transitive. Details and an example involving the problem of 27 lines are given in [35, Sect. 4].

6. Galois groups in Schubert calculus

In his seminal book, "Kalkul der abzählenden Geometrie" [72] Schubert presented methods for computing the number of solutions to problems in enumerative geometry. Justifying these methods was Hilbert's 15th problem [40], and they collectively came to be known as "Schubert's Calculus". A central role was played by the Grassmannian and its Schubert cycles/varieties. Schubert and others studied these objects further, and now Schubert varieties and the interplay of their geometry, combinatorics, and algebra make them central objects in combinatorial algebraic geometry [28] and other areas of mathematics. This study is also called Schubert calculus. We are concerned with the overlap of these versions of Schubert calculus—problems in enumerative geometry that involve intersections of Schubert varieties in Grassmannians and flag manifolds.

These *Schubert problems* form a rich and well-understood class of examples that has long served as a laboratory for investigating new phenomena in enumerative geometry [45]. Thousands to millions of Schubert problems are computable and therefore may be studied on a computer. Recently, this has also included reality in enumerative geometry [81], and the resulting experimentation generated conjectures [37, 69, 80] and examples [38] concerning reality in Schubert calculus. These in turn helped to inspire proofs of some conjectures [22, 23, 51, 62, 63, 61, 67].

Vakil's geometric Littlewood-Richardson rule [88] gave a new tool [89] for investigating Galois groups of Schubert problems (*Schubert Galois groups*) on Grassmannians. He used it to discover an infinite family of Schubert problems on Grassmannians with enriched Galois groups. The study of reality in flag manifolds uncovered another infinite family of enriched Schubert problems in manifolds of partial flags [69, Thm. 2.18]. Subsequent results and constructions have led to the expectation that a Schubert Galois group should be an iterated wreath product of symmetric groups, together with an understanding of the structure of enriched Schubert problems. Despite this, we are far from a classification, and the study has been limited to Grassmannians and type A flag manifolds.

After describing Schubert problems in Grassmannians, in Section 6.2 we construct Schubert problems whose Galois groups are symmetric groups S_b acting on flags of subsets of $[b] := \{1, \ldots, b\}$; This gives many enriched Schubert problems on flag manifolds in type A. We also present a conjectural solution to the inverse Galois problem for Schubert calculus. In Section 6.3 we describe a general construction of Schubert problems whose Galois groups are expected to be wreath products of two Schubert Galois groups. Our last section discusses results on Schubert Galois groups that are leading to an emerging picture of a possible classification of Schubert problems by their Galois groups.

6.1. **Schubert problems.** Consider the classical Schubert problem: "Which lines in $\mathbb{P}^3$ meet each of four general lines?" Three mutually skew lines ℓ^1, ℓ^2, and ℓ^3 lie on a unique hyperboloid (Fig. 3). This hyperboloid has two rulings. One contains ℓ^1, ℓ^2, and ℓ^3,

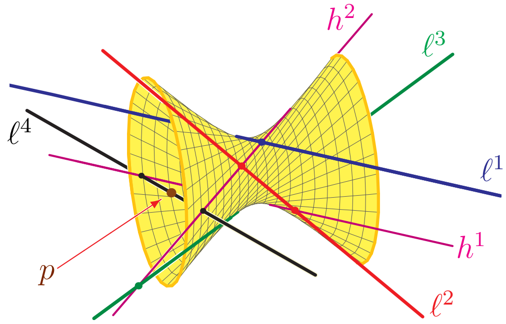


FIGURE 3. Problem of four lines

and the second consists of the lines meeting them. A general fourth line, ℓ^4, meets the hyperboloid in two points, and through each of these points there is a unique line in the second ruling. These two lines, h^1 and h^2, are the solutions to this instance of the problem of four lines. Its Galois group is the symmetric group S_2: Indeed, the solutions move as ℓ_4 moves and rotating ℓ_4 180° about the point p will interchange the two lines.

More generally, a Schubert problem involves determining the linear subspaces of a vector space that have specified positions with respect to certain fixed, but general linear subspaces. For the problem of four lines, if we replace projective space $\mathbb{P}^3$ by $\mathbb{C}^4$, the lines become 2-dimensional linear subspaces. Thus the problem of four lines is to determine the 2-planes in $\mathbb{C}^4$ that meet four given 2-planes nontrivially.

We introduce some terminology. First, fix integers $1 \leq m < n$. The collection of all m-dimensional subspaces of $\mathbb{C}^n$ is the *Grassmannian* $\mathrm{Gr}(m, n)$ (also written $\mathrm{Gr}(m, \mathbb{C}^n)$), which is an algebraic manifold of dimension $m(n-m)$. In Section 3, this space was written $\mathbb{G}(m-1, \mathbb{P}^{n-1})$.

The Grassmannian has distinguished Schubert varieties. These depend upon the choice of a (complete) flag, which is a collection $F\colon F_1 \subset F_2 \subset \cdots \subset F_n = \mathbb{C}^n$ of linear subspaces with $\dim F_i = i$. Given a flag F, a Schubert variety is the collection of all m-planes having a given position with respect to F. A position is encoded by a *partition*, which is a weakly decreasing sequence of nonnegative integers λ: $\lambda_1 \geq \cdots \geq \lambda_m \geq 0$ with $\lambda_1 \leq n-m$. For a flag F and partition λ, the corresponding Schubert variety is

$$\Omega_\lambda F \ := \ \{H \in \mathrm{Gr}(m,n) \mid \dim H \cap F_{n-m+i-\lambda_i} \geq i \ \text{ for } i = 1, \dots, m\}. \tag{3}$$

Setting $|\lambda| := \lambda_1 + \cdots + \lambda_m$, the Schubert variety $\Omega_\lambda F$ has codimension $|\lambda|$ in $\mathrm{Gr}(m,n)$.

Only m of the n subspaces F_i in F appear in the definition (3) of the Schubert variety $\Omega_\lambda F$. If $i < m$ and $\lambda_i = \lambda_{i+1}$, then the condition on H in (3) from λ_{i+1} implies the condition on H for λ_i. Those i with $\lambda_i > \lambda_{i+1}$ (or $i = m$ with $\lambda_m > 0$) are *essential*. When $(m,n) = (2,4)$ and $\lambda = (1,0)$, the essential condition is when $i = 1$. Indeed, $\Omega_{(1,0)} F = \{H \in \mathrm{Gr}(2,4) \mid \dim H \cap F_2 \geq 1\}$. In $\mathbb{P}^3$, this is the set of lines $\mathbb{P}H$ that meet the fixed line $\mathbb{P}F_2$.

A *Schubert problem* is a list $\lambda^\bullet = \lambda^1, \dots, \lambda^s$ of partitions with $\sum_j |\lambda^j| = m(n-m)$, the dimension of the Grassmannian. An *instance* of $\lambda^\bullet$ is given by a choice $F^\bullet = (F^1, \dots, F^s)$ of flags. The solutions to this instance form the set of m-planes H that have position λ^j with respect to the flag F^j, for each j. This set is the intersection

$$\Omega_{\lambda^1} F^1 \bigcap \Omega_{\lambda^2} F^2 \bigcap \cdots \bigcap \Omega_{\lambda^s} F^s \,. \tag{4}$$

Kleiman [44] showed that this intersection is transverse when the flags are general. When the flags are general, this implies that for each solution (point H in (4)), the inequalities in (3) for each pair λ^j, F^j hold with equality. Also, the number of solutions does not depend upon the (general) flags. Write $d(\lambda^\bullet)$ for this number, which may be computed using algorithms in Schubert's calculus.

Let $\mathbb{F}\ell(n)$ be the space of complete flags in $\mathbb{C}^n$ and consider the incidence variety:

$$\begin{array}{ll} \Gamma_{\lambda^\bullet} := \{(H, F^1, \dots, F^s) \in \mathrm{Gr}(m,n) \times \mathbb{F}\ell(n)^s \ \mid \\ \qquad\qquad\qquad\qquad\qquad H \in \Omega_{\lambda^i} F^i \text{ for } i = 1, \dots, s\} \\ \Big\downarrow \pi_{\lambda^\bullet} \\ \mathbb{F}\ell(n)^s \end{array} \tag{5}$$

The total space $\Gamma_{\lambda^\bullet}$ of this Schubert problem is irreducible, as it is a fiber bundle over the Grassmannian $\mathrm{Gr}(m,n)$ with irreducible fibers (this is explained in [82, Sect. 2.2]). The fiber of $\pi_{\lambda^\bullet}$ over $(F^1, \dots, F^s) \in \mathbb{F}\ell(n)^s$ is the intersection (4). Since this is transverse and consists of $d(\lambda^\bullet)$ points for general flags, $\pi_{\lambda^\bullet}$ is a branched cover of degree $d(\lambda^\bullet)$. We write $\mathrm{Gal}_{\lambda^\bullet}$ for its Galois group, which we call a *Schubert Galois group*.

6.2. **Some enriched Schubert problems.** We present a construction of many enriched Schubert problems on Grassmannians and flag manifolds. These are based on the following generalization of the problem of four lines: Let $1 < b$ be an integer and consider the 2-planes $h \subset \mathbb{C}^{2b}$ that meet each of four general b-planes $K^1, \dots, K^4$ in at least a one-dimensional subspace. Since $2b - 2 + 1 - (b-1) = b$, this Schubert problem is given by four partitions, each equal to $(b-1, 0)$.

This has b solutions, which we now describe. As the K^i are general, we have $K^i \oplus K^j = \mathbb{C}^{2b}$ for $i \neq j$. Then K^3, K^4 are graphs of isomorphisms $f_3, f_4 \colon K^1 \to K^2$, and $\varphi := f_4^{-1} \circ f_3$ is a linear isomorphism of K^1. If $\ell = \varphi(\ell) \subset K^1$ is a φ-stable line (one-dimensional subspace) in K^1, then $f_3(\ell) = f_4(\ell)$ and $H := \ell \oplus f_3(\ell)$ is a solution to this enumerative problem. Furthermore, all solutions have this form, as $H \cap K^i$ for $i = 1, \ldots, 4$ are four lines in the same 2-plane H. As the subspaces K^i are general, the linear transformation φ is semi-simple and therefore has $b = \dim(K^1)$ distinct stable lines (generated by its eigenvectors). Thus this Schubert problem has b solutions.

Note that the monodromy group for the eigenvectors of semi-simple linear transformations φ is the full symmetric group S_b acting on the set of 1-dimensional φ-stable linear subspaces of K^1. Thus the Galois group of this Schubert problem is the full symmetric group S_b acting naturally as permutations on the set $[b] := \{1, \ldots, b\}$.

Example 9. Vakil [89, § 3.14] used these problems in $\mathrm{Gr}(2, 2b)$ to construct an infinite family of Schubert problems with enriched Galois groups. Let $1 \leq a < b$ and consider the Schubert problem in $\mathrm{Gr}(2a, 2b)$ of $2a$-planes that meet each of four general b-planes $K^1, \ldots, K^4$ in at least an a-dimensional linear subspace. The previous argument generalizes: Let $f_3, f_4 \colon K^1 \to K^2$ and $\varphi := f_4^{-1} \circ f_3 \colon K^1 \to K^1$ be the linear isomorphisms determined by $K^1, \ldots, K^4$. Every solution has the form $L \oplus f_3(L)$ for $L = \varphi(L) \subset K^1$ a φ-stable a-dimensional linear subspace. Consequently, L is spanned by a linearly independent eigenvectors of φ. Thus this Schubert problem has $\binom{b}{a}$ solutions.

The symmetric group S_b acts naturally on the set $\binom{[b]}{a}$ of subsets of $[b]$ of cardinality a, and this argument shows that this permutation group (written $S\binom{[b]}{a}$) is the Galois group of this Schubert problem. This action is not 2-transitive when $1 < a < b-1$. It preserves the dimension of the intersection of a pair of solutions, and thus has at least $\min\{a, b-a\}$ distinct orbits on pairs of solutions. $\diamond$

We generalize Vakil's examples, while also generalizing [69, Thm. 2.18].

Example 10. Suppose that $1 \leq a_1 < \cdots < a_r < b$ are integers and write $a_\bullet$ for the sequence $a_1 < \cdots < a_r$. Let $\mathbb{F}\ell(2a_\bullet, 2b)$ be the space of partial flags of the form

$$F \,:\, F_{2a_1} \subset F_{2a_2} \subset \cdots \subset F_{2a_r} \subset \mathbb{C}^{2b},$$

where $\dim F_{2a_i} = 2a_i$. Fix four general b-planes K^1, K^2, K^3, K^4 in $\mathbb{C}^{2b}$. Consider the Schubert problem that seeks the partial flags $F \in \mathbb{F}\ell(2a_\bullet, 2b)$ such that for $i = 1, \ldots, r$,

$$\dim F_{2a_i} \bigcap K^j \;\geq\; a_i \qquad \text{for all} \;\; j = 1, \ldots, 4\,. \tag{6}$$

As before, $K^1, \ldots, K^4$ give isomorphisms $f_3, f_4 \colon K^1 \to K^2$ and $\varphi = f_4^{-1} \circ f_3 \colon K^1 \to K^1$. For each $1 \leq i \leq r$, the solutions to (6) are given by $L_{a_i} \oplus f_3(L_{a_i})$ where $L_{a_i} \subset K^1$ is a φ-stable linear subspace of dimension a_i.

Consequently, the solutions to (6) for all i are in bijection with φ-stable flags

$$L_{a_1} \subset L_{a_2} \subset \cdots \subset L_{a_r} \subset K^1,$$

where $\dim L_{a_i} = a_i$. Since L_{a_i} is necessarily spanned by a_i independent eigenvectors of φ, these are in bijection with flags of subsets of $[b]$:

$$\binom{[b]}{a_\bullet} \;:=\; \{T_1 \subset T_2 \subset \cdots \subset T_r \subset [b] \mid |T_i| = a_i\}\,.$$

Thus $\binom{[b]}{a_\bullet}$ counts solutions to this Schubert problem and its Galois group is the symmetric group S_b, with its natural action on the set $\binom{[b]}{a_\bullet}$ of flags of subsets. Write $S\binom{[b]}{a_\bullet}$ for this permutation group. $\diamond$

This completes the following existence proof concerning Schubert Galois groups.

Theorem 11. *For any positive integers $1 \leq a_1 < \cdots < a_r < b$, there is a Schubert problem on the flag manifold $\mathbb{F}\ell(2a_\bullet, 2b)$ with Galois group $S\binom{[b]}{a_\bullet}$.*

These Schubert Galois groups form the basis for a conjectured solution to the Inverse Galois Problem in Schubert calculus.

Conjecture 12. *A Galois group for a Schubert problem on a type A flag manifold is an iterated wreath product of permutation groups $S\binom{[b]}{a_\bullet}$, and all such wreath products occur.*

Schubert Galois groups for Grassmannians are iterated wreath products of permutation groups $S\binom{[b]}{a}$, and all such wreath products occur.

Conjecture 12 describes all known Schubert Galois groups—we discuss that and more in Section 6.4. Additionally, all Schubert problems we know of with enriched Galois groups are either among those described in Examples 9 or 10 or they are fibrations of Schubert problems, a structure we discuss in Section 6.3 which is conjectured to give such wreath products.

6.3. **Compositions of Schubert problems.** By Proposition 3, when a branched cover is decomposable, its Galois group is a subgroup of the wreath product of the Galois groups of its factors. We explain how to construct a Schubert problem on a Grassmannian $\mathrm{Gr}(2a+m, 2b+n)$ with decomposable branched cover. This is built from one of the Schubert problems of Example 9 on $\mathrm{Gr}(2a, 2b)$ and any Schubert problem $\mu^\bullet$ on $\mathrm{Gr}(m, n)$ with $d(\mu^\bullet) > 1$. Conjecturally, its Galois group is the wreath product $(\mathrm{Gal}_{\mu^\bullet})^{\binom{b}{a}} \rtimes S\binom{[b]}{a}$. This conjecture would establish existence in the Inverse Galois Problem for Schubert problems on Grassmannians.

It is convenient to represent a partition μ by its (Young) diagram, which is a left-justified array of boxes with μ_i boxes in row i. Thus

$$(1) \longleftrightarrow \square, \qquad (2,2) \longleftrightarrow \ydiagram{2,2}, \quad \text{and} \quad (3,2,1,1) \longleftrightarrow \ydiagram{3,2,1,1}\,.$$

We omit any trailing 0s in a partition μ. Observe that the essential conditions in μ correspond to the boxes that form south east corners. Consequently, a rectangular partition imposes a single incidence condition.

As the number $d(\mu^\bullet)$ of solutions to a Schubert problem $\mu^\bullet$ may be computed in the cohomology ring of the corresponding Grassmannian [28], we often write a Schubert problem multiplicatively. Thus $(\square, \square, \square, \square)$, which is the problem of four lines, is also written $\square \cdot \square \cdot \square \cdot \square$ or as $\square^4$. The construction of a composition of Schubert problems is a bit technical, we will illustrate it first on the simplest example, when $\lambda^\bullet = \mu^\bullet$ are both the problem of four lines.

Example 13. Consider the Schubert problem $\kappa^\bullet$ in $\mathrm{Gr}(4,8)$ given by the partitions

$$\kappa^\bullet \;=\; \square\!\square\!\square \cdot \square\!\square\!\square \cdot \begin{smallmatrix}\square\\\square\end{smallmatrix} \cdot \begin{smallmatrix}\square\\\square\end{smallmatrix} \cdot \square \cdot \square \cdot \square \cdot \square\,. \tag{7}$$

An instance of this Schubert problem is given by two 2-planes ℓ_2^1, ℓ_2^2, two 6-planes L_6^3, L_6^4, and four 4-planes $K_4^1, \dots, K_4^4$, and its solutions are

$$\left\{H \in \mathrm{Gr}(4,8) \;\middle|\; \begin{array}{ll} \dim H \cap \ell_2^i \geq 1 & \text{for } i = 1,2 \\ \dim H \cap L_6^j \geq 3 & \text{for } j = 3,4 \end{array} \quad \dim H \cap K_4^t \geq 1 \;\; \text{for } t = 1, \dots, 4\right\}. \tag{8}$$

Assume that these linear subspaces ℓ_2^i, L_6^j, K_4^t are in general position, which implies the dimension assertions that follow. Let $\Lambda := \ell_2^1 \oplus \ell_2^2 \simeq \mathbb{C}^4$ and $M := L_6^3 \cap L_6^4 \simeq \mathbb{C}^4$.

If H is a solution to (8), then $\dim H \cap \Lambda \geq 2$ and $\dim H \cap M \geq 2$. As $\Lambda \cap M = \{0\}$ and $\dim H = 4$, these inequalities are equalities. Set $h := H \cap \Lambda \in G(2, \Lambda)$. For $j = 3, 4$, the intersection $H \cap L_6^j$ has codimension 1 in H and therefore $\dim h \cap L_6^j = 1$. Setting $\ell_2^j := \Lambda \cap L_6^j$, we see that h is a solution to the instance of the problem of four lines given by $\ell_2^1, \dots, \ell_2^4$.

Similarly, for each $i = 1, \dots, 4$, $H \cap M$ meets the 2-plane $k_2^i(h) := (h \oplus K_4^i) \cap M$. Thus $H \cap M$ is a solution to the problem of four lines given by $k_2^1(h), \dots, k_2^4(h)$. Conversely, given a solution $h \subset \Lambda$ to the problem of four lines given by $\ell_2^1, \dots, \ell_2^4$ and a solution $h' \subset M$ to the problem of four lines given by $k_2^1(h), \dots, k_2^4(h)$, their sum $h \oplus h'$ is a solution to the Schubert problem (8). $\diamond$

Thus the branched cover $\pi \colon \Gamma_{\kappa^\bullet} \to \mathbb{F}\ell(8)^8$ of this Schubert problem (5) is decomposable. Indeed, let $U \subset \mathbb{F}\ell(8)^8$ be the subset of flags in the general position used in Example 13. If we let $X := \pi^{-1}(U)$ be the restriction of $\Gamma_{\kappa^\bullet}$ to this set of general instances, then Example 13 shows that we have a factorization $X \to Y \to U$. Here, the fiber of $Y \to U$ over an instance in U is the instance of $\square^4$ in $\mathrm{Gr}(2, \Lambda)$ given by $\ell_2^1, \dots, \ell_2^4$, and given a solution h to this instance, the fiber of $X \to Y$ over h is the instance of $\square^4$ in $\mathrm{Gr}(2, M)$ given by $k_2^1(h), \dots, k_2^4(h)$.

We make a definition inspired by this structure.

Definition 14. A Schubert problem $\kappa^\bullet$ is *fibered* over a Schubert problem $\lambda^\bullet$ with fiber $\mu^\bullet$ if the branched cover $\Gamma_{\kappa^\bullet} \to \mathbb{F}\ell(n)^s$ is decomposable, and it admits a decomposition

$$X \longrightarrow Y \longrightarrow U \quad (U \subset \mathbb{F}\ell(n)^s \text{ is open and dense})$$

such that

(1) fibers of $Y \to U$ are instances of $\lambda^\bullet$,
(2) fibers of $X \to Y$ are instances of $\mu^\bullet$, and
(3) general instances of $\lambda^\bullet$ and $\mu^\bullet$ occur as fibers in this way.

We will call $\kappa^\bullet$ a *fibration*. This notion is developed in [57] and [84], where the following is proven, which is a special case of [57, Lemma 15].

Proposition 15. *If a Schubert problem $\kappa^\bullet$ is fibered over $\lambda^\bullet$ with fiber $\mu^\bullet$, then $d(\kappa^\bullet) = d(\lambda^\bullet) \cdot d(\mu^\bullet)$, and its Galois group is a subgroup of the wreath product*

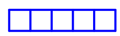
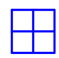
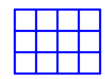
$$\mathrm{Gal}_{\kappa^\bullet} \;\subset\; (\mathrm{Gal}_{\mu^\bullet})^{d(\lambda^\bullet)} \rtimes \mathrm{Gal}_{\lambda^\bullet}\,.$$

Consequently, the Schubert Galois group from Example 13 is a subgroup of the wreath product $(S_2)^2 \rtimes S_2$. In fact, its Galois group equals this wreath product [56, Sect. 5.5.2].

The construction of Example 13 was generalized in [84]. Given two Schubert problems $\lambda^\bullet$ and $\mu^\bullet$ on possibly different Grassmannians, that paper describes how to use them to build a new Schubert problem $\lambda^\bullet \circ \mu^\bullet$ on another Grassmannian, called their *composition*. It uses combinatorics to prove that $d(\lambda^\bullet \circ \mu^\bullet) = d(\lambda^\bullet) \cdot d(\mu^\bullet)$, and it is expected—but not proven—that $\lambda^\bullet \circ \mu^\bullet$ is fibered over $\lambda^\bullet$ with fiber $\mu^\bullet$.

Next, it identifies a family of Schubert problems and shows that for any Schubert problem $\lambda^\bullet$ in that family, any composition $\lambda^\bullet \circ \mu^\bullet$ is fibered over $\lambda^\bullet$ with fiber $\mu^\bullet$. This family includes all the Schubert problems of Example 9. We explain this construction when λ is a Schubert problem of Example 9, which is a motivation for Conjecture 12.

Write $\square_{a,b}$ for the rectangular partition with a rows, each of length $b-a$. For example,

$\square_{1,2}$ = , $\square_{1,6}$ = , $\square_{2,4}$ = , and $\square_{3,7}$ = .

Every Schubert problem in Example 9 has the form $\square_{a,b}^4$.

Fix integers $1 \leq a < b$ and $1 \leq m < n$, and let $\mu^\bullet = (\mu^1, \ldots, \mu^s)$ be any Schubert problem on $\mathrm{Gr}(m,n)$. Set $r := n-m$. The composition, $\square_{a,b}^4 \circ \mu^\bullet$, of $\square_{a,b}^4$ and $\mu^\bullet$ is the Schubert problem on $\mathrm{Gr}(2a+m, 2b+n)$ given by the following partitions

$$\square_{a,b+r}\,,\, \square_{a,b+r}\;,\; \square_{a+m,b+m}\,,\, \square_{a+m,b+m}\;,\; \mu^1, \ldots, \mu^s\,.$$

Suppose that $a=1$, $b=2$, and $\mu^\bullet = \square^4$. Then $m=r=2$ and $n=4$, so that these partitions are

$$\square_{1,4}\,,\, \square_{1,4}\;,\; \square_{3,4}\,,\, \square_{3,4}\;,\; \square, \square, \square, \square\,,$$

which is the Schubert problem $\kappa^\bullet$ (7) of Example 13.

Proposition 16 (Theorem 3.8 of [84]). *The Schubert problem $\square_{a,b}^4 \circ \mu^\bullet$ is fibered over the Schubert problem $\square_{a,b}^4$ on $\mathrm{Gr}(2a,2b)$ with fiber the Schubert problem $\mu^\bullet$ on $\mathrm{Gr}(m,n)$. We have*

$$\mathrm{Gal}_{\square_{a,b}^4 \circ \mu^\bullet} \;\subset\; (\mathrm{Gal}_{\mu^\bullet})^{\binom{b}{a}} \rtimes S\tbinom{[b]}{a}\,.$$

We conjecture this inclusion is an equality—that would prove the existence statement in Conjecture 12, for Grassmannians.

Sketch of proof. We explain how to decompose a general instance of the Schubert problem $\square_{a,b}^4 \circ \mu^\bullet$. This is similar to Example 13. This involves constructing an instance of $\square_{a,b}^4$ as an auxiliary problem, and for each of its solutions, constructing an instance of $\mu^\bullet$.

An instance of the Schubert problem $\square_{a,b}^4 \circ \mu^\bullet$ is given by two b-planes K_b^1, K_b^2, two codimension b-planes L_{b+n}^3, L_{b+n}^4, and flags $F^1, \ldots, F^s$ in $\mathbb{C}^{2b+n}$. The Schubert problem seeks the $(2a+m)$-planes H such that for every $i = 1,2$, $j = 3,4$, and $t = 1, \ldots, s$, we have

$$\dim H \cap K_b^i \;\geq\; a\,,\quad \dim H \cap L_{b+n}^j \;\geq\; a+m\,,\quad \text{and}\quad H \in \Omega_{\mu^t} F^t\,.$$

Suppose that the linear subspaces K_b^i, L_{b+n}^j, and the flags F^t are in general position. Let H be a solution to this instance of $\square_{a,b}^4 \circ \mu^\bullet$. If we set $\Lambda := K_b^1 \oplus K_b^2 \simeq \mathbb{C}^{2b}$ and $M := L_{b+n}^3 \cap L_{b+n}^4 \simeq \mathbb{C}^n$, then $\dim H \cap \Lambda = 2a$ and $H \cap M = m$. Setting $K_b^j := \Lambda \cap L_{b+n}^j$

for $j = 3, 4$, we have that $h := H \cap \Lambda$ is a solution to the Schubert problem $\square^4_{a,b}$ in $\mathrm{Gr}(2a, \Lambda)$ given by $K^1_b, \dots, K^4_b$. Let $1 \le t \le s$. Since the flag F^t is in general position, $\dim(h+F^t_r) = \dim(h)+\dim(F^t_r) = 2a+r$. As M has codimension $2b$ and also meets $h+F^t_r$ properly, $(h + F^t_r) \cap M$ has dimension $2a+r-2b$. Thus for $1 \le r \le n$, $(h + F^t_{r+2b-2a}) \cap M$ defines a flag $F^t(h)$ in M. A further exercise in dimension-counting and the definition of Schubert variety (3) shows that $H \cap M \in \Omega_{\mu^t} F^t(h)$.

Furthermore, for every solution h to the auxiliary problem $\square^4_{a,b}$ in $\mathrm{Gr}(2a, \Lambda)$, if we define flags $F^i(h)$ in M as above, then, for every solution h' to the instance of the Schubert problem $\mu^\bullet$ in $\mathrm{Gr}(m, M)$ given by the flags $F^\bullet(h)$, the direct sum $h \oplus h'$ is a solution to the original Schubert problem. $\square$

6.4. **An emerging landscape of Schubert Galois groups.** The constructions and results described in Sections 6.2 and 6.3 arose from a sustained investigation of Schubert Galois groups in which computer experimentation informed theoretical advances. This began with Vakil's seminal paper [89]. There, he used his geometric Littlewood-Richardson rule [88] in a method used to show a Schubert Galois group is at least alternating. He applied this method to study Schubert Galois groups in small Grassmannians. Subsequent experimentation and results this inspired is leading to an understanding what to expect for Schubert Galois groups, and an outline of a potential classification is emerging from this study.

Without delving into its (considerable) details, we sketch salient features of Vakil's geometric Littlewood-Richardson rule [89]. Given a Schubert problem $\mu^\bullet$ on a Grassmannian $G(m, n)$, it constructs a tree $\mathcal{T}_{\mu^\bullet}$ with $d(\mu^\bullet)$ leaves that encodes a sequence of deformations of intersections of Schubert varieties as the flags move into special position. Each node $\bullet\bullet$ of $\mathcal{T}_{\mu^\bullet}$ determines an enumerative problem which involves intersecting a subset of the Schubert varieties in $\mu^\bullet$ with a *checkerboard variety* $Y_{\bullet\bullet}(E, M)$. Here E, M are two flags in a special position (determined by $\bullet\bullet$) and $Y_{\bullet\bullet}(E, M)$ is the set of m-planes in $G(m, n)$ having a particular position with respect to E, M (again specified by $\bullet\bullet$). Let $d(\bullet\bullet)$ be the number of solutions to this enumerative problem and $\mathrm{Gal}(\bullet\bullet)$ be its Galois group.

The root of the tree $\mathcal{T}_{\mu^\bullet}$ is labeled by $\mu^\bullet$. For a leaf node $\bullet\bullet$, $d(\bullet\bullet) = 1$. Every node $\bullet\bullet$ of $\mathcal{T}_{\mu^\bullet}$ that is not a leaf has either one child $\bullet\bullet'$ or two children $\bullet\bullet'$ and $\bullet\bullet''$, and we have $d(\bullet\bullet) = d(\bullet\bullet')$, respectively $d(\bullet\bullet) = d(\bullet\bullet') + d(\bullet\bullet'')$, when there is one child, respectively two children. The children of a node are in bijection with the irreducible components of the checkerboard variety $Y_{\bullet\bullet}(E, M)$ as the flags E, M become more degenerate.

Theorem 17 (Thms 3.2 and 3.10 of [89])**.** *Let $\bullet\bullet$ be a node in $\mathcal{T}_{\mu^\bullet}$. Suppose that the Galois group of each child of $\bullet\bullet$ is at least alternating. Then $\mathrm{Gal}(\bullet\bullet)$ is at least alternating if one of the following conditions* (1), (2a), *or* (2b) *hold.*

(1) *$\bullet\bullet$ has a unique child.*
(2) *$\bullet\bullet$ has two children $\bullet\bullet'$ and $\bullet\bullet''$, and*
   (a) *$d(\bullet\bullet') \ne d(\bullet\bullet'')$ or both are equal to 1, or*
   (b) *$\mathrm{Gal}(\bullet\bullet)$ is 2-transitive, and we do not have $d(\bullet\bullet') = d(\bullet\bullet'') = 6$.*

When $\bullet\bullet$ is a leaf, $d(\bullet\bullet) = 1$ so that $\mathrm{Gal}(\bullet\bullet) = S_1$ is at least alternating. Theorem 17 leads to Vakil's recursive method that may conclude $\mathrm{Gal}(\mu^\bullet)$ is at least alternating. Given a Schubert problem $\mu^\bullet$, this method first constructs $\mathcal{T}_{\mu^\bullet}$, which it then investigates. If, for every non-leaf node ●●, either (1) or (2a) hold at ●●, then it declares that $\mathrm{Gal}_{\mu^\bullet}$ is at least alternating. Otherwise, the method is inconclusive. It is not a decision procedure, but it is a useful filter to identify Schubert problems that may have enriched Galois groups and thus are worthy of further study.

Vakil wrote a Maple script[3] that runs his method on all Schubert problems on a given Grassmannian. He ran this on all small Grassmannians. Every Schubert Galois group on $\mathrm{Gr}(2,n)$ for $n \leq 16$ and on $\mathrm{Gr}(3,n)$ for $n \leq 9$ was found to be at least alternating (for $\mathrm{Gr}(3,n)$, Condition (2b) in Theorem 17 was needed). As $\mathrm{Gr}(4,6) \simeq \mathrm{Gr}(2,6)$ and $\mathrm{Gr}(4,7) \simeq \mathrm{Gr}(3,7)$, the next Grassmannian was $\mathrm{Gr}(4,8)$. His algorithm was inconclusive for 14 (out of 3501) Schubert problems on $\mathrm{Gr}(4,8)$. These 14 include the problem $\square^4_{2,4}$ from Example 9 and the problem of Example 13. The Galois groups of these 14 problems are known and none are 2-transitive [56, Sect. 5.5].

A Schubert problem $\mu^\bullet$ on $\mathrm{Gr}(m,n)$ is *simple* if at most two of the conditions in $\mu^\bullet$ are not $\square = (1,0,\dots,0)$. Using the Pieri homotopy algorithm [41] to compute solutions to simple Schubert problems and monodromy, Galois groups of many simple Schubert problems (including one with 17,589 solutions) were shown to have full-symmetric Galois groups [54].

The first general result concerning Schubert Galois groups was given in [11]. Using Vakil's algorithm and combinatorial reasoning, it was shown that every Schubert problem on $\mathrm{Gr}(2,n)$ for all n has at least alternating Galois group. With an eye towards Condition (2b) in Theorem 17, another general result showed that Galois groups of Schubert problems on $\mathrm{Gr}(3,n)$, for every n are 2-transitive [82]. Yet another general result is that all simple Schubert problems are at least alternating [83]. These results and computations described below suggest the following dichotomy for Schubert Galois groups.

Conjecture 18. *A Schubert Galois group is either the full symmetric group or it is not 2-transitive.*

Robert Williams used the method of computing Frobenius elements to show that many Schubert problems have full symmetric Galois groups over $\mathbb{Q}$ [92]. These include all Schubert problems on a Grassmannian $\mathrm{Gr}(2,n)$ with up to 500 solutions, as well as all simple Schubert problems on any Grassmannian with up to 500 solutions [83], and all Schubert problems on $\mathrm{Gr}(4,9)$ with at most 300 solutions [57]. The numbers here, 300 and 500, are approximate and they represent the limit of the software used—Singular [17]—to solve a Schubert problem over a prime field (typically $\mathbb{F}_{1009}$) in a few hours.

We close with a sketch of the results from [57], which determined all enriched problems on $\mathrm{Gr}(4,9)$. This began by using Vakil's method, both his maple implementation and a perl implementation by C. Brooks, to identify many Schubert problems on $\mathrm{Gr}(4,9)$ that were at least alternating. For only 233 of the 38,760 Schubert problems was the method inconclusive, and further study found exactly 149 Schubert problems on $\mathrm{Gr}(4,9)$ that had enriched Galois groups. We remark that this (and earlier computations on $\mathrm{Gr}(4,8)$) only

[3] http://math.stanford.edu/~vakil/programs/galois

tested Schubert problems that could not be reduced to a Schubert problem on a smaller Grassmannian.

Each of these 149 enriched Schubert problems was shown to be a fibration as in Definition 14, where the constituent Schubert problems were on a $\mathrm{Gr}(2,4)$ or a $\mathrm{Gr}(2,5)$, and had full symmetric Galois groups, either S_2 or S_3 or S_5. By Proposition 15, the Schubert Galois group of each was a subgroup of a wreath product of symmetric groups. Computing sufficiently many Frobenius elements showed that in each case, the Galois group was the expected wreath product. This computation is explained and archived on the web page[4]. Of these, 120 are compositions of Schubert problems as in Proposition 16, while the remaining 29 had a different structure.

While these results on Schubert Galois groups have not resulted in a classification, there is an emerging landscape of what to expect, which we summarize for Grassmannians $\mathrm{Gr}(m,n)$.

- If $\min\{m, n-m\} = 1$, then $\mathrm{Gr}(m,n) \simeq \mathbb{P}^{n-1}$, and Schubert calculus becomes linear algebra; all Schubert problems have one solution. There are no non-trivial Galois groups.
- If $\min\{m, n-m\} = 2$, then $\mathrm{Gr}(m,n) \simeq \mathrm{Gr}(2,n)$ and all Schubert Galois groups are at least alternating [11] and conjectured to be fully symmetric.
- If $\min\{m, n-m\} = 3$, then $\mathrm{Gr}(m,n) \simeq \mathrm{Gr}(3,n)$ and all Schubert Galois groups are 2-transitive [82] and conjectured to be fully symmetric.
- If $\min\{m, n-m\} \geq 4$, then $\mathrm{Gr}(m,n)$ has enriched Schubert problems. An enriched Schubert problem is either equivalent to one of Vakil's problems from Example 9, or it is a fibration of Schubert problems.

We also remark that we do not know whether or not Schubert Galois groups depend upon the base field. In particular, are they the same for $\mathbb{Q}$ and for $\mathbb{C}$, or different?

7. Galois groups in applications

Structures in polynomial systems or in enumerative geometry give information about the associated Galois groups. In a growing number of applications of algebraic geometry, information about associated Galois groups may be used to detect these structures and then exploit them for solving or for understanding the application. We sketch this in three application realms. Esterov's partial determination of Galois groups for sparse polynomial systems leads to a surprisingly efficient algorithm to recursively decompose and solve sparse systems. Work in vision reconstruction problems uses Galois groups to detect decompositions, which are then used in efficient solvers. The classical problem of Alt, to determine four-bar mechanisms whose coupler curve passes through nine given points, has a hidden symmetry of order six coming from the structure of the problem and its formulation as a system of equations.

7.1. **Solving decomposable sparse polynomial systems.** By Proposition 3, when a branched cover $\pi\colon X \to Z$ is decomposable in that there is a Zariski open subset $V \subset Z$

[4] `https://www.math.tamu.edu/~sottile/research/stories/GIVIX/`

over which π factors,

$$\pi^{-1}(V) \xrightarrow{\varphi} Y \xrightarrow{\psi} V\,, \tag{2}$$

then its Galois group Gal_π is imprimitive (and *vice-versa*). Améndola, Lindberg, and Rodriguez [3] proposed methods to exploit this structure in numerical algebraic geometry. For example, when the decomposition (2) is known explicitly, fibers of $\pi\colon X \to Z$ may be recovered from the partial data consisting of one fiber of $\varphi\colon \pi^{-1}(V) \to Y$ and one fiber of $\psi\colon Y \to V$. They illustrated this on examples where $V = Z$ and the first map $\varphi\colon X \to Y$ comes from the invariants of a group acting on the fibers of π. Interestingly, their methods do not require knowledge of the full Galois group, only of the decomposition (2).

This approach is particularly fruitful for the sparse polynomial systems of Section 4, whose notation and definitions we use. Let $\mathcal{A}_\bullet$ be a collection of supports for a sparse polynomial system. By Esterov's Theorem 7, if $\mathcal{A}_\bullet$ is either strictly lacunary or strictly triangular, then $\mathrm{Gal}_{\mathcal{A}_\bullet}$ is imprimitive, and $\mathrm{Gal}_{\mathcal{A}_\bullet}$ is completely determined (either a group of units or full symmetric) in all other cases. Not only does this characterize when the branched cover $\pi\colon \Gamma_{\mathcal{A}_\bullet} \to \mathbb{C}^{\mathcal{A}_\bullet}$ is decomposable, but it leads to an algorithmic procedure for an explicit description of the decomposition. We sketch that; As complete description is given in [12].

When $\mathcal{A}_\bullet$ is lacunary, $\mathbb{Z}^n/\mathbb{Z}\mathcal{A}_\bullet$ is a nontrivial finite group. Let $\varphi\colon (\mathbb{C}^\times)^n \twoheadrightarrow (\mathbb{C}^\times)^n$ be the map induced by the inclusion $\mathbb{Z}^n \xrightarrow{\sim} \mathbb{Z}\mathcal{A}_\bullet \subset \mathbb{Z}^n$ and the functor $\mathrm{Hom}(\_\,, \mathbb{C}^\times)$. This has kernel $\mathrm{Hom}(\mathbb{Z}^n/\mathbb{Z}\mathcal{A}_\bullet, \mathbb{C}^\times)$, a group of units in $(\mathbb{C}^\times)^n$. If $\mathcal{B}_\bullet$ is the preimage of $\mathcal{A}_\bullet$ under the identification $\mathbb{Z}^n \xrightarrow{\sim} \mathbb{Z}\mathcal{A}_\bullet$, then a system $F(x)$ with support $\mathcal{A}_\bullet$ has the form $G(\varphi(x))$, where the system G has support $\mathcal{B}_\bullet$. Thus $\mathrm{Hom}(\mathbb{Z}^n/\mathbb{Z}\mathcal{A}_\bullet, \mathbb{C}^\times)$ acts on the solutions of any system $F \in \mathbb{C}^{\mathcal{A}_\bullet}$, and in fact on the branched cover $\pi\colon \Gamma_{\mathcal{A}_\bullet} \to \mathbb{C}^{\mathcal{A}_\bullet}$. This action is free, and the quotient variety is the branched cover $\psi\colon \Gamma_{\mathcal{B}_\bullet} \to \mathbb{C}^{\mathcal{B}_\bullet}(= \mathbb{C}^{\mathcal{A}_\bullet})$. We have $\mathrm{MV}(\mathcal{A}_\bullet) = |\mathbb{Z}^n/\mathbb{Z}\mathcal{A}_\bullet| \cdot \mathrm{MV}(\mathcal{B}_\bullet)$ and when $\mathrm{MV}(\mathcal{A}_\bullet) > |\mathbb{Z}^n/\mathbb{Z}\mathcal{A}_\bullet|$, the decomposition of $\pi\colon \Gamma_{\mathcal{A}_\bullet} \to \mathbb{C}^{\mathcal{A}_\bullet}$ through the intermediate variety $\Gamma_{\mathcal{B}_\bullet}$ is nontrivial.

The first of the maps in this decomposition is induced from the inclusions $\Gamma_{\mathcal{A}_\bullet} \subset \mathbb{C}^{\mathcal{A}_\bullet} \times (\mathbb{C}^\times)^n$ and $\Gamma_{\mathcal{B}_\bullet} \subset \mathbb{C}^{\mathcal{B}_\bullet} \times (\mathbb{C}^\times)^n$ by the identification $\mathbb{C}^{\mathcal{A}_\bullet} = \mathbb{C}^{\mathcal{B}_\bullet}$ and the monomial map $\varphi\colon (\mathbb{C}^\times)^n \to (\mathbb{C}^\times)^n$, from which fibers may be explicitly computed. The map φ is computed from the Smith normal form of a matrix whose columns are generators of $\mathbb{Z}\mathcal{A}_\bullet$. Similarly, the second map is simply the branched cover associated to the family of sparse systems of support $\mathcal{B}_\bullet$. If $\mathcal{B}_\bullet$ is lacunary or triangular, then this may be further decomposed. If not, then its fibers are readily computed by numerical software such as `PHCpack` [90] or `HomotopyContinuation.jl` [10], using the polyhedral homotopy [42].

Suppose now that $\mathcal{A}_\bullet$ is strictly triangular with witness $\emptyset \neq I \subsetneq [n]$, so that $\mathrm{rank}(\mathbb{Z}\mathcal{A}_I) = |I|$ and $1 < \mathrm{MV}(\mathcal{A}_I) < \mathrm{MV}(\mathcal{A}_\bullet)$. Then there is a monomial change of coordinates on $(\mathbb{C}^\times)^n$ and a reindexing of the supports so that $I = [m]$ and $\mathcal{A}_1, \dots, \mathcal{A}_m \subset \mathbb{Z}^m$, which is the first m coordinates of $\mathbb{Z}^n$. Writing $(\mathbb{C}^\times)^n = (\mathbb{C}^\times)^m \times (\mathbb{C}^\times)^{n-m}$ for the corresponding splitting, points $x \in (\mathbb{C}^\times)^n$ are ordered pairs $x = (y, z)$ with $y \in (\mathbb{C}^\times)^m$ and $z \in (\mathbb{C}^\times)^{n-m}$. Then a system F with support $\mathcal{A}_\bullet$ has the form $F(x) = (G(y), H(y, z))$, where G has support $\mathcal{A}_I$ and H has support $\mathcal{A}_{I^c}$, where $I^c := \{m{+}1, \dots, n\}$. Any solution to $F = 0$ is a pair (y^*, z^*), where y^* is a solution to $G(y) = 0$, and z^* is a solution to the system $H(y^*, z) = 0$

on $(\mathbb{C}^\times)^{n-m}$. This structure is apparent in the decomposition

$$\Gamma_{\mathcal{A}_\bullet} \longrightarrow \Gamma_{\mathcal{A}_I} \times \mathbb{C}^{\mathcal{A}_{I^c}} \longrightarrow \mathbb{C}^{\mathcal{A}_I} \times \mathbb{C}^{\mathcal{A}_{I^c}} = \mathbb{C}^{\mathcal{A}_\bullet}, \tag{9}$$

where the first map is induced by the projection $(\mathbb{C}^\times)^n \to (\mathbb{C}^\times)^m$ onto the first m coordinates applied to solutions (y^*, z^*).

Let $p\colon \mathbb{Z}^n \to \mathbb{Z}^{n-m}$ be the projection to the last $n-m$ coordinates and observe that for any solution y^* to $G(y) = 0$, $H(y^*, z)$ has support $p(\mathcal{A}_{I^c})$. We have the following product formula (see [85, Lem. 6] or [24, Thm. 1.10]),

$$\mathrm{MV}(\mathcal{A}_\bullet) = \mathrm{MV}(\mathcal{A}_I) \cdot \mathrm{MV}(p(\mathcal{A}_{I^c})).$$

Since $1 < \mathrm{MV}(\mathcal{A}_I)$ and $1 < \mathrm{MV}(\mathcal{A}_\bullet)/\mathrm{MV}(\mathcal{A}_I) = \mathrm{MV}(p(\mathcal{A}_{I^c}))$, the decomposition (9) is nontrivial. When either $\mathcal{A}_I$ or $p(\mathcal{A}_{I^c})$ is lacunary or triangular, these maps may be further decomposed. If one is neither lacunary or triangular, then its fibers are readily computed by numerical software as above.

This leads to an algorithm to recursively decompose the branched cover $\pi\colon \Gamma_{\mathcal{A}_\bullet} \to \mathbb{C}^{\mathcal{A}_\bullet}$. In each decomposition, the decomposability of each factor is determined by examining another sparse family. Given a blackbox solver (e.g. `HomotopyContinuation.jl` [10] or `PHCpack` [90]) to compute fibers of indecomposable branched covers, combined with the methods of Améndola, et. al [3], results in an efficient algorithm for solving sparse polynomial systems, which was developed in [12]. These methods have been implemented in the Macaulay2 [30] package `DecomposableSparseSystems.m2` [13]. In [12] this package was used in an experiment in which thousands of decomposable systems were solved, both using the black box solver `PHCpack` and that package (called Algorithm 9 in [12]). Figure 4 shows a box plot of the timings.

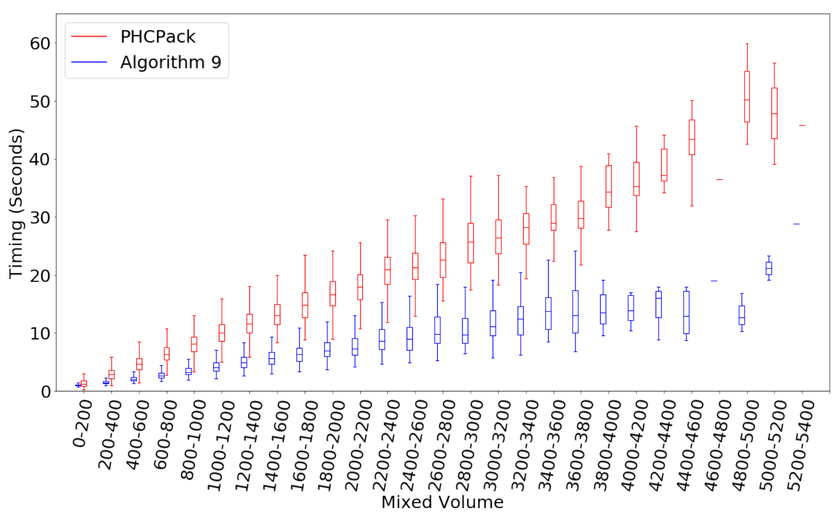


FIGURE 4. Box plot of timings comparing `PHCpack` and Algorithm 9.

7.2. **Vision Problems.** A camera takes a 2-dimensional image of a 3-dimensional scene. The fundamental problem of image reconstruction is to recover the scene from images taken by cameras at different unknown locations. For this, some features (e.g. points, lines, and incidences) are matched between images. This matching is used to infer the camera positions, which are then used for the full reconstruction. There are many versions of this nonlinear problem of determining camera positions—different types of cameras and different configurations of matched features.

A calibrated perspective camera consists of a *focal point* $\mathbf{t} \in \mathbb{R}^3$ and a direction vector $\mathbf{v}$. The image is the projection of $\mathbb{R}^3 \smallsetminus \{\mathbf{t}\}$ from the point $\mathbf{t}$ onto a plane with normal vector $\mathbf{v}$ lying a distance 1 from $\mathbf{t}$ in the direction of $\mathbf{v}$. The image of a point $\mathbf{x} \in \mathbb{R}^3$ is the intersection of the line between $\mathbf{t}$ and $\mathbf{x}$ with this plane. The considered features are some points, lines, and their incidences, which are assumed to be present in each image.

An *image reconstruction problem* is specified by the number of cameras (images) and the matched features. For example, we may have two cameras and five points in each image. Such a problem is *minimal* if, for general data, there is a positive, finite number of solutions (camera positions). The *degree* of the minimal problem is this number of (complex) solutions for general data, which is a measure of the algebraic complexity of solving the minimal problem. Highly optimized solvers have been developed for some minimal problems [47, 65]. The minimal reconstruction problems were recently classified [20], finding many new minimal problems. Among these new minimal reconstruction problems are some which have imprimitive Galois groups, whose corresponding decomposable structure may be exploited for solving [3].

We present some of the formulation of reconstruction problems. Fix a reference frame, choosing one camera to be at the origin and to face upwards. Any other camera is the translation of the first by an element of the special Euclidean group, $\mathrm{SE}_{\mathbb{R}}(3)$. A element of $\mathrm{SE}_{\mathbb{R}}(3)$ is a pair $[\mathbf{R} \mid \mathbf{t}]$, where $\mathbf{R} \in \mathrm{SO}(3)$ is a rotation matrix and $\mathbf{t} \in \mathbb{R}^3$ is a translation vector. Then $[\mathbf{R} \mid \mathbf{t}]$ represents a camera with focal point $\mathbf{t}$ and direction vector $\mathbf{Rk}$, where $\mathbf{k}$ is the upward-pointing unit vector. In this way, elements of $\mathrm{SE}_{\mathbb{R}}(3)$ give coordinates for cameras. The fixed camera has coordinate $[\mathbf{I} \mid \mathbf{0}]$ where $\mathbf{I}$ is the identity matrix and $\mathbf{0}$ is the zero vector.

The image plane Π of a camera $[\mathbf{R} \mid \mathbf{t}]$ consists of the points $\mathbf{p} \in \mathbb{R}^3$ satisfying the equation $(\mathbf{Rk}) \cdot (\mathbf{p} - \mathbf{t}) = 1$. For $\mathbf{x} \in \mathbb{R}^3 \smallsetminus \{\mathbf{t}\}$, its image in Π is the point

$$\mathbf{t} \;+\; \frac{\mathbf{x} - \mathbf{t}}{(\mathbf{Rk}) \cdot (\mathbf{x} - \mathbf{t})}\;.$$

Translating by $-\mathbf{t}$ and applying $\mathbf{R}^{-1}$ sends the image plane Π to the standard reference plane $\Pi_{\mathbf{0}} := \{(x, y, 1) \mid x, y \in \mathbb{R}\}$ for the camera $[\mathbf{I} \mid \mathbf{0}]$. We use the coordinates from $\Pi_{\mathbf{0}}$ to represent images of points for all camera. Thus a point $\mathbf{y} \in \Pi_{\mathbf{0}}$ is the image of a point $\mathbf{x} \in \mathbb{R}^3$ under the camera $[\mathbf{R} \mid \mathbf{t}]$ if

$$\mathbf{x} \;=\; \mathbf{R}\alpha\mathbf{y} \;+\; \mathbf{t}\,, \tag{10}$$

where $\alpha = (\mathbf{Rk}) \cdot (\mathbf{x} - \mathbf{t})$ is the *focal depth* of the point $\mathbf{x}$ relative to $[\mathbf{R} \mid \mathbf{t}]$. Figure 5 is a schematic showing the correspondence between five points $\mathbf{x} \in \mathbb{R}^3$ and their images in the planes Π, for two cameras.

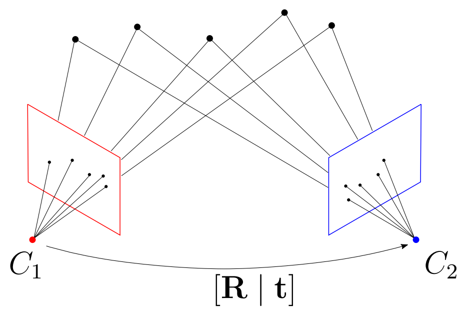


FIGURE 5. Minimal problem of two cameras with five points.

Given matched configurations of points, lines, and incidences in $\Pi_{\mathbf{0}}$ for each of several, say n, cameras, equations based on (10) formulate the image reconstruction problem as a system of equations on $(\mathrm{SE}_{\mathbb{R}}(3))^{n-1}$. Complexifying gives a system of polynomials that depends upon the input configuration. When the problem is minimal, this gives a branched cover over the parameter space of all input configurations. The degree of the branched cover is the degree of the minimal problem. As we have seen before, there is a Galois group for each minimal problem. When the Galois group is imprimitive, Proposition 3 implies that the branched cover is decomposable. If a decomposition (2) is known, then that may be exploited for solving.

One such problem with imprimitive Galois group is that of reconstructing five points given images from two cameras, which is illustrated in Figure 5. The branched cover corresponding to this minimal problem has degree 20. The imprimitivity may be understood by observing that the solutions come in pairs: Given one solution $([\mathbf{I} \mid \mathbf{0}], [\mathbf{R} \mid \mathbf{t}])$, a second is given by rotating the camera $[\mathbf{R} \mid \mathbf{t}]$ $180°$ around the line between the two cameras. (This also changes the inferred positions of the unknown points $\mathbf{x} \in \mathbb{R}^3$.) This is called a *twisted pair* in the literature, and we see that the Galois group preserves the resulting partition of the 20 solutions into ten twisted pairs, and is hence a subgroup of $S_2 \wr S_{10}$. In fact, the Galois group is even smaller, it is $(S_2 \wr S_{10}) \cap A_{20}$ [19], which is the Weyl group D_{10}. This imprimitivity implies the associated branch cover is decomposable and the system can be solved in stages. A decomposition for this problem is implicit in [65].

In [19], the minimal problems of degree at most 1000 with imprimitive Galois group were classified. Those were further studied using numerical algebraic geometry, which led to an understanding of their structure, and for each an explicit decomposition was found.

7.3. **Alt's Problem.** Polynomial systems arise in engineering when designing mechanisms with a desired range of motion. Robotic arm movements, for instance, may need to be able to reach several positions to perform specific tasks. These movements can be modeled by polynomial systems, from which they can be studied with the methods discussed. One such problem due to Alt [2] is the nine-point synthesis problem for four-bar linkages.

A *four-bar linkage* is a planar mechanism built from a quadrilateral (which may self-intersect) with rotating joints and fixed side lengths. One side of the quadrilateral is the *base* which is fixed in place, while the other sides move as allowed by freely rotating the joints. The side opposite the base is the *coupler bar*, and a triangle is erected on the coupler bar. In an actual mechanism, a tool is placed at the apex of the triangle and the mechanism is maneuvered to position the tool.

To understand this motion, consider the quadrilateral. Removing the coupler bar, the two bars that were incident to it may each rotate freely around their fixed points. The coupler bar imposes a distance constraint on the rotating bars, and there remains one degree of freedom. (The abstract curve of this motion has genus one.) In the resulting motion, the apex of the triangle traces the *coupler curve*.

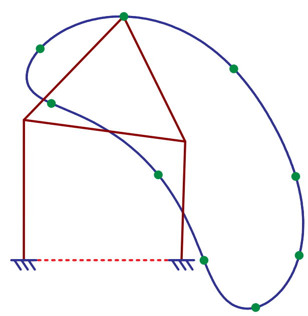


FIGURE 6. A four-bar mechanism and coupler curve.

The space of all mechanisms is nine-dimensional. Indeed, the two fixed points may be any points in $\mathbb{R}^2$, giving four dimensions (degrees of freedom). The lengths of each of the remaining five segments in the mechanism give five more, for a total of nine. That the coupler curve contains a given point in $\mathbb{R}^2$ is a single, simple condition on the space of four-bar mechanisms. Thus we expect there are only finitely many mechanisms whose coupler curve contains nine given general points. Alt [2] recognized this, and his nine-point synthesis problem asks for the mechanisms whose coupler curve contains a given nine points.

Identifying $\mathbb{R}^2$ with $\mathbb{C}$, we represent the bars as complex numbers. Complexifying gives a useful formulation of Alt's problem in *isotropic coordinates*—this is described in [60]. Solutions to these equations for nine general points were computed using homotopy continuation in [60], finding 8652 solutions.

In [36], this computation was repeated and a soft certificate was computed to certify that the 8652 computed solutions. While 8652 is almost surely the number of solutions, these computations only show that it is a lower bound, and a proof of the number 8652 remains elusive. Further evidence for the number 8652 was found in [34], but that result also only implies that 8652 is a lower bound.

In this formulation, solutions come in pairs due to relabeling—swapping labels of the bars incident to the base and to the apex of the triangle results in another solution and gives the same four-bar mechanism. Classically Roberts [68] and Chebyshev [15] (see [91] for a discussion) show that there are three mechanisms—called Robert's Cognates—with the same coupler curve. Consequently, the Galois group of this formulation of Alt's problem is imprimitive as it preserves the six solutions which give the same coupler curve. We also see that, assuming the number 8652 is correct, that there are 4326 four-bar mechanisms whose coupler curve contains nine given points, and 1442 distinct coupler curves.

Since label swapping may be done independently on each cognate, the Galois group G of the six solutions with given coupler curve is a subgroup of $\mathbb{Z}/2\mathbb{Z} \wr S_3 = (\mathbb{Z}/2\mathbb{Z})^3 \rtimes S_3$—this assumes that the cognates have symmetry S_3. Consequently, the Galois group of this formulation is a subgroup of $G \wr S_{1432}$. To the best of our knowledge, the Galois group of this problem has not been determined.

References

1. E. L. Allgower and K. Georg, Introduction to numerical continuation methods, Classics in Applied Mathematics, vol. 45, SIAM, 2003.
2. H. Alt, Über die erzeugung gegebener ebener kurven mit hilfe des gelenkviereckes, Zeitschrift für Angewandte Mathematik und Mechanik **3** (1923), no. 1, 13–19.
3. C. Améndola, J. Lindberg, and J. I. Rodriguez, Solving parameterized polynomial systems with decomposable projections, 2021, `arXiv:1612.08807`.
4. B. Banwait, F. Fité, and D. Loughran, Del Pezzo surfaces over finite fields and their Frobenius traces, Math. Proc. Cambridge Philos. Soc. **167** (2019), no. 1, 35–60.
5. D.J. Bates, J.D. Hauenstein, A.J. Sommese, and C.W. Wampler, Bertini: Software for numerical algebraic geometry, Available at `http://www.nd.edu/~sommese/bertini`.
6. C. Beltrán and A. Leykin, Certified numerical homotopy tracking, Exp. Math. **21** (2012), no. 1, 69–83.
7. ———, Robust certified numerical homotopy tracking, Found. Comput. Math. **13** (2013), no. 2, 253–295.
8. D. N. Bernstein, The number of roots of a system of equations, Funct. Anal. Appl. **9** (1975), 183–185.
9. P. Breiding, K. Rose, and S. Timme, Certifying zeros of polynomial systems using interval arithmetic, 2020, `arXiv:2011.05000`.
10. P. Breiding and S. Timme, HomotopyContinuation.jl: A Package for Homotopy Continuation in Julia, International Congress on Mathematical Software, Springer, 2018, pp. 458–465.
11. C.J. Brooks, A. Martín del Campo, and F. Sottile, Galois groups of Schubert problems of lines are at least alternating, Trans. Amer. Math. Soc. **367** (2015), no. 6, 4183–4206.
12. T. Brysiewicz, J. I. Rodriguez, F. Sottile, and T. Yahl, Solving decomposable sparse systems, Numerical Algorithms (2020).
13. ———, Decomposable sparse polynomial systems, Journal of Software for Algebra and Geometry (2021).
14. A. Cayley, On the triple tangent planes of surfaces of third order, The Cambridge and Dublin Mathematical Journal **4** (1849), 118–138.
15. P. Chebyshev, Les plus simple systémes de tiges articulées, Oeuvres de P.L. Tchebychef, Tome II (A. Markoff and N. Sonin, eds.), l'académie impériale des sciences, St. Petersburg, 1907, pp. 271–281.
16. O. Debarre and L. Manivel, Sur la variété des espaces linéaires contenus dans une intersection complète, Mathematische Annalen **312** (1998), 549–574.
17. W. Decker, G.-M. Greuel, G. Pfister, and H. Schönemann, Singular 4-0-3 — A computer algebra system for polynomial computations, `http://www.singular.uni-kl.de`, 2016.
18. H. D'Souza, On the monodromy group of everywhere tangent lines to the octic surface in $\mathbf{P}^3$, Proc. Amer. Math. Soc. **104** (1988), no. 4, 1010–1013.
19. T. Duff, V. Korotynskiy, T. Pajdla, and M. Regan, Galois/monodromy groups for decomposing minimal problems in 3D reconstruction, 2021, `arXiv:2105.04460`.

20. Timothy Duff, Kathlen Kohn, Anton Leykin, and Tomas Pajdla, Plmp – point-line minimal problems in complete multi-view visibility, Proceedings of the IEEE/CVF International Conference on Computer Vision (ICCV), October 2019.
21. T. Ekedahl, An effective version of Hilbert's irreducibility theorem, Séminaire de Théorie des Nombres, Paris 1988–1989, Progr. Math., vol. 91, Birkhäuser, Boston, MA, 1990, pp. 241–249.
22. A. Eremenko and A. Gabrielov, Rational functions with real critical points and the B. and M. Shapiro conjecture in real enumerative geometry, Ann. of Math. (2) **155** (2002), no. 1, 105–129.
23. A. Eremenko, A. Gabrielov, M. Shapiro, and A. Vainshtein, Rational functions and real Schubert calculus, Proc. Amer. Math. Soc. **134** (2006), no. 4, 949–957 (electronic).
24. A. Esterov, Galois theory for general systems of polynomial equations, Compos. Math. **155** (2019), no. 2, 229–245.
25. A. Esterov and L. Lang, Sparse polynomial equations and other enumerative problems whose Galois groups are wreath products, 2019, `arXiv:1812.07912`.
26. G. Ewald, Combinatorial convexity and algebraic geometry, Graduate Texts in Mathematics, vol. 168, Springer-Verlag, New York, 1996.
27. J.-C. Faugère, A new efficient algorithm for computing Gröbner bases without reduction to zero (F_5), Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation, ACM, New York, 2002, pp. 75–83.
28. Wm. Fulton, Young tableaux, Cambridge University Press, Cambridge, 1997.
29. The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.11.1, 2021.
30. D.R. Grayson and M.E. Stillman, Macaulay2, a software system for research in algebraic geometry, Available at `http://www.math.uiuc.edu/Macaulay2/`.
31. J. Harris, Galois groups of enumerative problems, Duke Math. Journal **46** (1979), no. 4, 685–724.
32. S. Hashimoto and B. Kadets, 38406501359372282063949 and all that: Monodromy of Fano problems, International Mathematics Research Notices (2020), rnaa275, `arxiv:2002.04580`.
33. A. Hatcher, Algebraic topology, Cambridge University Press, Cambridge, 2002.
34. J. Hauenstein and M. Helmer, Probabilistic saturations and Alt's problem, 2019, `arxiv:1908.06020`.
35. J.D. Hauenstein, J.I. Rodriguez, and F. Sottile, Numerical Computation of Galois Groups, Found. Comput. Math. **18** (2018), no. 4, 867–890.
36. J.D. Hauenstein and F. Sottile, Algorithm 921: alphaCertified: Certifying solutions to polynomial systems, ACM Trans. Math. Softw. **38** (2012), no. 4, 28.
37. N. Hein, C.J. Hillar, A. Martín del Campo, F. Sottile, and Z. Teitler, The monotone secant conjecture in the real Schubert calculus, Exp. Math. **24** (2015), no. 3, 261–269.
38. N. Hein, F. Sottile, and I. Zelenko, A congruence modulo four in real Schubert calculus, J. Reine Angew. Math. **714** (2016), 151–174.
39. C. Hermite, Sur les fonctions algébriques, CR Acad. Sci.(Paris) **32** (1851), 458–461.
40. D. Hilbert, Mathematical problems, Bull. Amer. Math. Soc. **8** (1902), no. 10, 437–479.
41. B. Huber, F. Sottile, and B. Sturmfels, Numerical Schubert calculus, Journal of Symbolic Computation **26** (1998), no. 6, 767–788.
42. B. Huber and B. Sturmfels, A polyhedral method for solving sparse polynomial systems, Math. Comp. **64** (1995), no. 212, 1541–1555.
43. C. Jordan, Traité des Substitutions et des Équations algébriques, Gauthier-Villars, Paris, 1870.
44. S.L. Kleiman, The transversality of a general translate, Compositio Math. **28** (1974), 287–297.
45. S.L. Kleiman and D. Laksov, Schubert calculus, Amer. Math. Monthly **79** (1972), 1061–1082.
46. R. Krawczyk, Newton-Algorithmen zur Bestimmung von Nullstellen mit Fehlerschranken, Computing (Arch. Elektron. Rechnen) **4** (1969), 187–201.
47. A. Kukelova, Algebraic methods in computer vision, Ph.D. thesis, Czech Technical University in Prague, 2013.
48. A.G. Kušnirenko, Newton polyhedra and Bezout's theorem, Funkcional. Anal. i Priložen. **10** (1976), no. 3, 82–83.
49. ———, Polyèdres de Newton et nombres de Milnor, Invent. Math. **32** (1976), no. 1, 1–31.

50. S. Lang, Algebra, Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York, 2002.
51. J. Levinson and K. Purbhoo, A topological proof of the Shapiro-Shapiro conjecture, 2019, `ArXiv.org/1907.11924`.
52. A. Leykin, Numerical Algebraic Geometry, The Journal of Software for Algebra and Geometry **3** (2011), 5–10, Available at `http://j-sag.org/volume3.html`.
53. A. Leykin, J.I. Rodriguez, and F. Sottile, Trace test, Arnold Mathematical Journal **4** (2018), no. 1, 113–125.
54. A. Leykin and F. Sottile, Galois groups of Schubert problems via homotopy computation, Math. Comp. **78** (2009), no. 267, 1749–1765.
55. T.Y. Li, T. Sauer, and J.A. Yorke, The cheater's homotopy: an efficient procedure for solving systems of polynomial equations, SIAM Journal on Numerical Analysis **26** (1989), no. 5, 1241–1251.
56. A. Martín del Campo and F. Sottile, Experimentation in the Schubert calculus, Schubert Calculus, Osaka 2012 (H. Naruse, T. Ikeda, M. Masuda, and T. Tanisaki, eds.), Advanced Studies in Pure Mathematics, vol. 71, Mathematical Society of Japan, 2016, pp. 295–336.
57. A. Martín del Campo, F. Sottile, and R. Williams, Classification of Schubert Galois groups in $Gr(4,9)$, `arXiv.org/1902.06809`, 2019.
58. A. Morgan, Solving polynomial systems using continuation for engineering and scientific problems, Classics in Applied Mathematics, vol. 57, SIAM, 2009.
59. A.P. Morgan and A.J. Sommese, Coefficient-parameter polynomial continuation, Appl. Math. Comput. **29** (1989), no. 2, part II, 123–160.
60. A.P. Morgan, A.J. Sommese, and C.W. Wampler, Complete solution of the nine-point path synthesis problem for four-bar linkages, ASME J. Mech. Des. **114** (1992), no. 1, 153–159.
61. E. Mukhin and V. Tarasov, Lower bounds for numbers of real solutions in problems of Schubert calculus, Acta Math. **217** (2016), no. 1, 177–193.
62. E. Mukhin, V. Tarasov, and A. Varchenko, The B. and M. Shapiro conjecture in real algebraic geometry and the Bethe ansatz, Ann. of Math. (2) **170** (2009), no. 2, 863–881.
63. ———, Schubert calculus and representations of the general linear group, J. Amer. Math. Soc. **22** (2009), no. 4, 909–940.
64. J.R. Munkres, Topology: a first course, Prentice-Hall, Inc., Englewood Cliffs, N.J., 1975.
65. D. Nistér, An efficient solution to the five-point relative pose problem, IEEE Transactions on Pattern Analysis and Machine Intelligence **26** (2004), no. 6, 756–770.
66. G.P. Pirola and E. Schlesinger, Monodromy of projective curves, J. Algebraic Geom. **14** (2005), no. 4, 623–642.
67. K. Purbhoo, Reality and transversality for Schubert calculus in $\mathrm{OG}(n, 2n+1)$, Math. Res. Lett. **17** (2010), no. 6, 1041–1046.
68. S. Roberts, On three-bar motion in plane space, Proceedings London Mathematical Society (1875), 14–23.
69. J. Ruffo, Y. Sivan, E. Soprunova, and F. Sottile, Experimentation and conjectures in the real Schubert calculus for flag manifolds, Experiment. Math. **15** (2006), no. 2, 199–221.
70. G. Salmon, On the triple tangent planes to a surface of third order, The Cambridge and Dublin Mathematical Journal **4** (1849), 252–260.
71. L. Schläfli, An attempt to determine the twenty-seven lines upon a surface of the third order and to divide such surfaces into species in reference to the reality of the lines upon the surface, Quarterly Journal of Math. **2** (1858), 55–65, 110–121.
72. H. Schubert, Kalkül der abzählenden Geometrie, Springer-Verlag, Berlin-New York, 1979, Reprint of the 1879 original, With an introduction by Steven L. Kleiman.
73. S. Smale, Newton's method estimates from data at one point, The merging of disciplines: new directions in pure, applied, and computational mathematics, Springer, New York, 1986, pp. 185–196.
74. A.J. Sommese, J. Verschelde, and C.W. Wampler, Numerical decomposition of the solution sets of polynomial systems into irreducible components, SIAM J. Numer. Anal. **38** (2001), no. 6, 2022–2046.

75. ———, Using monodromy to decompose solution sets of polynomial systems into irreducible components, Applications of algebraic geometry to coding theory, physics and computation (Eilat, 2001), NATO Sci. Ser. II Math. Phys. Chem., vol. 36, Kluwer Acad. Publ., Dordrecht, 2001, pp. 297–315.
76. ———, Symmetric functions applied to decomposing solution sets of polynomial systems, SIAM J. Numer. Anal. **40** (2002), no. 6, 2026–2046.
77. ———, Introduction to numerical algebraic geometry, Solving polynomial equations, Algorithms Comput. Math., vol. 14, Springer, Berlin, 2005, pp. 301–335.
78. A.J. Sommese and C.W. Wampler, Numerical algebraic geometry, The mathematics of numerical analysis (Park City, UT, 1995), Lectures in Appl. Math., vol. 32, Amer. Math. Soc., Providence, RI, 1996, pp. 749–763.
79. ———, The numerical solution of systems of polynomials arising in engineering and science, World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ, 2005.
80. F. Sottile, Real Schubert calculus: polynomial systems and a conjecture of Shapiro and Shapiro, Experiment. Math. **9** (2000), no. 2, 161–182.
81. ———, Real solutions to equations from geometry, University Lecture Series, vol. 57, American Mathematical Society, Providence, RI, 2011.
82. F. Sottile and J. White, Double transitivity of Galois groups in Schubert calculus of Grassmannians, Algebr. Geom. **2** (2015), no. 4, 422–445.
83. F. Sottile, J. White, and R. Williams, Galois groups in simple Schubert problems are at least alternating, in preparation.
84. F. Sottile, R. Williams, and L. Ying, Galois groups of composed Schubert problems, Facets of Algebraic Geometry: A Collection in Honor of William Fulton's 80th Birthday (P. Aluffi, D. Anderson, M. Hering, M. Mustaţă, and S & Payne, eds.), London Mathematical Society Lecture Note Series, Cambridge University Press, 2022, p. ????
85. R. Steffens and T. Theobald, Mixed volume techniques for embeddings of Laman graphs, Comput. Geom. **43** (2010), no. 2, 84–93.
86. P. Stevenhagen and H.W. Lenstra, Jr., Chebotarëv and his density theorem, Math. Intelligencer **18** (1996), no. 2, 26–37.
87. N. Tschebotareff, Die Bestimmung der Dichtigkeit einer Menge von Primzahlen, welche zu einer gegebenen Substitutionsklasse gehören, Math. Ann. **95** (1926), no. 1, 191–228.
88. R. Vakil, A geometric Littlewood-Richardson rule, Ann. of Math. (2) **164** (2006), no. 2, 371–421, Appendix A written with A. Knutson.
89. ———, Schubert induction, Ann. of Math. (2) **164** (2006), no. 2, 489–512.
90. J. Verschelde, Algorithm 795: PHCpack: A general-purpose solver for polynomial systems by homotopy continuation, ACM Transactions on Mathematical Software **25** (1999), no. 2, 251–276.
91. E. Verstraten, Cognate linkages the roberts–chebyshev theorem, Explorations in the History of Machines and Mechanisms (Dordrecht) (T. Koetsier and M. Ceccarelli, eds.), Springer Netherlands, 2012, pp. 505–519.
92. R. Williams, Restrictions on Galois groups of Schubert problems, Ph.D. thesis, Texas A&M Univeristy, 2017.
93. O. Zariski, A theorem on the Poincaré group of an algebraic hypersurface, Annals of Mathematics **38** (1937), no. 1, 131–141.

F. Sottile, Department of Mathematics, Texas A&M University, College Station, Texas 77843, USA

Email address: sottile@math.tamu.edu

URL: http://www.math.tamu.edu/~sottile

T. Yahl, Department of Mathematics, Texas A&M University, College Station, Texas 77843, USA

Email address: thomasjyahl@math.tamu.edu

URL: http://www.math.tamu.edu/~thomasjyahl