

NUMERICAL COMPUTATION OF GALOIS GROUPS

JONATHAN D. HAUENSTEIN, JOSE ISRAEL RODRIGUEZ, AND FRANK SOTTILE

ABSTRACT. The Galois/monodromy group of a family of geometric problems or equations is a subtle invariant that encodes the structure of the solutions. Computing monodromy permutations using numerical algebraic geometry gives information about the group, but can only determine it when it is the full symmetric group. We give numerical methods to compute the Galois group and study it when it is not the full symmetric group. One algorithm computes generators while the other gives information on its structure as a permutation group. We illustrate these algorithms with examples using a `Macaulay2` package we are developing that relies upon `Bertini` to perform monodromy computations.

1. INTRODUCTION

Galois groups, which are a pillar of number theory and arithmetic geometry, encode the structure of field extensions. For example, the Galois group of the cyclotomic extension of \mathbb{Q} given by the polynomial $x^4 + x^3 + x^2 + x + 1$ is the cyclic group of order four, and not the full symmetric group. A finite extension \mathbb{L}/\mathbb{K} , where \mathbb{K} has transcendence degree n over \mathbb{C} , corresponds to a branched cover $f: V \rightarrow U$ of complex algebraic varieties of dimension n , with \mathbb{L} the function field of V and \mathbb{K} the function field of U . The Galois group of the Galois closure of \mathbb{L}/\mathbb{K} equals the monodromy group of the branched cover [14, 19]. When U is rational, $f: V \rightarrow U$ may be realized as a family of polynomial systems rationally parameterized by points of U . Applications of algebraic geometry and enumerative geometry are sources of such families. For these, internal structure such as numbers of real solutions and symmetry of the original problem are encoded in the Galois/monodromy group.

Computing monodromy is a fundamental operation in numerical algebraic geometry. Computing monodromy permutations along randomly chosen loops in the base U was used in [24] to show that several Schubert problems had Galois/monodromy group the full symmetric group. Leaving aside the defect of that computation—the continuation (and hence the monodromy permutations) was not certified—this method only computes an increasing sequence of subgroups of the Galois group, and thus only determines the Galois group when it is the full symmetric group. In all other cases, this method lacks a stopping criterion.

We offer two additional numerical methods to obtain certifiable information about Galois groups and investigate their efficacy. The first method is easiest to describe when U is a rational curve so that $\mathbb{K} = \mathbb{C}(t)$, the field of rational functions. Then V is an algebraic curve C equipped with a dominant map $f: C \rightarrow \mathbb{C}$ whose fiber at $t \in \mathbb{C}$ consists of solutions to a polynomial system that depends upon t . This is a degree k cover outside the branch locus B , which is a finite subset of \mathbb{C} . The monodromy group of $f: C \rightarrow \mathbb{C}$ is generated by permutations coming from loops encircling each branch point.

Research of Hauenstein supported in part by NSF grant ACI-1460032, Sloan Research Fellowship, and Army Young Investigator Program (YIP).

Research of Rodriguez supported in part by NSF grant DMS-1402545.

Research of Sottile supported in part by NSF grant DMS-1501370.

Our second method uses numerical irreducible decomposition of the s -fold fiber product to determine orbits of the monodromy group acting on s -tuples of distinct points in a fiber. When $s = k-1$, this computes the Galois group. The partial information obtained when $s < k-1$ may be sufficient to determine the Galois group.

We illustrate these methods. The irreducible polynomial $x^4 - 4x^2 + t$ over $\mathbb{C}(t)$ defines a curve C in $\mathbb{C}_x \times \mathbb{C}_t$ whose projection $C \rightarrow \mathbb{C}_t$ is four-to-one for $t \notin B = \{0, 4\}$. The fiber above the point $t = 3$ is $\{-\sqrt{3}, -1, 1, \sqrt{3}\}$. Following these points along a loop in \mathbb{C}_t based at $t = 3$ that encircles the branch point $t = 0$ gives the 2-cycle $(-1, 1)$. A loop encircling the branch point $t = 4$ gives the product of 2-cycles, $(-\sqrt{3}, -1)(1, \sqrt{3})$. These permutations generate the Galois group, which is isomorphic to the dihedral group D_4 and has order 8.

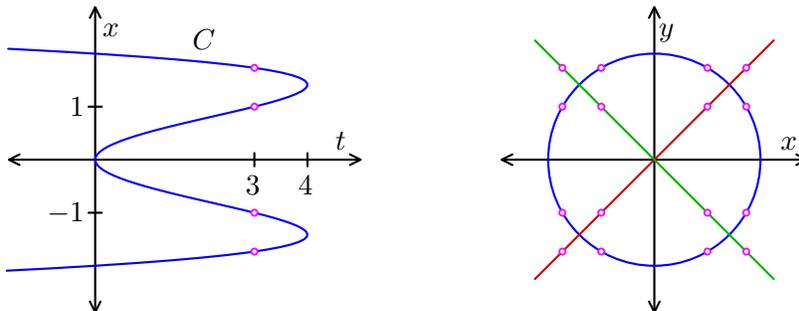


FIGURE 1. Curve C over \mathbb{C}_t and fiber of $C \times_{\mathbb{C}_t} C$ over $t = 3$.

The fiber product $C \times_{\mathbb{C}_t} C$ consists of triples (x, y, t) , where x and y lie in the fiber of C above t . It is defined in $\mathbb{C}_x \times \mathbb{C}_y \times \mathbb{C}_t$ by the polynomials $x^4 - 4x^2 + t$ and $y^4 - 4y^2 + t$. Since

$$(x^4 - 4x^2 + t) - (y^4 - 4y^2 + t) = (x - y)(x + y)(x^2 + y^2 - 4),$$

it has three components. One is the diagonal defined by $x - y$ and $x^4 - 4x^2 + t$. The off-diagonal consists of two irreducible components, which implies that the action of the Galois group \mathcal{G} is not two-transitive. One component is defined by $x + y$ and $x^4 - 4x^2 + t$. Its fiber over $t = 3$ consists of the four ordered pairs $(\pm\sqrt{3}, \mp\sqrt{3})$ and $(\pm 1, \mp 1)$, which is an orbit of \mathcal{G} acting on ordered pairs of solutions. This implies that \mathcal{G} acts imprimitively as it fixes the partition $\{-\sqrt{3}, \sqrt{3}\} \sqcup \{-1, 1\}$. Thus $\mathcal{G} \subset S_4$ contains no 3-cycle, so $\mathcal{G} \subset D_4$. The third component is defined by $x^2 + y^2 - 4$ and $x^4 - 4x^2 + t$ and its projection to \mathbb{C}_t has degree eight. Thus \mathcal{G} has an orbit of cardinality eight, which implies $|\mathcal{G}| \geq 8$, from which we can conclude that \mathcal{G} is indeed the dihedral group D_4 .

The systematic study of Galois groups of families of geometric problems and equations coming from applications is in its infancy. Nearly every case we know where the Galois group has been determined exhibits a striking dichotomy (e.g., [7, 14, 23, 24, 25, 26, 28, 34, 36]): either the group acts imprimitively, so that it fails to be 2-transitive, or it is at least $(k-2)$ -transitive in that it contains the alternating group (but is expected to be the full symmetric group). The methods we develop here are being used [26] to further investigate Galois groups and we expect they will help to develop Galois groups as a tool to study geometric problems, including those that arise in applications.

The paper is structured as follows. Section 2 introduces the background material including permutation groups, Galois groups, fundamental groups, fiber products, homotopy continuation, and witness sets. In Section 3, we discuss the method of computing monodromy by

determining the branch locus, illustrating this on the classical problem of determining the monodromy group of the 27 lines on a cubic surface. In Section 4, we discuss using fiber products to obtain information about the Galois group, illustrating this method with the monodromy action on the lines on a cubic surface. We further illustrate these methods using three examples from applications in Section 5, and we give concluding remarks in Section 6.

2. GALOIS GROUPS AND NUMERICAL ALGEBRAIC GEOMETRY

We describe some background, including permutation groups, Galois/monodromy groups, and fundamental groups of hypersurface complements from classical algebraic geometry, as well as the topics from numerical algebraic geometry of homotopy continuation, monodromy, witness sets, fiber products, and numerical irreducible decomposition.

2.1. Permutation groups. Let $\mathcal{G} \subset S_k$ be a subgroup of the symmetric group on k letters. Then \mathcal{G} has a faithful action on $[k] := \{1, \dots, k\}$. For $g \in \mathcal{G}$ and $i \in [k]$, write $g(i)$ for the image of i under g . We say that \mathcal{G} is *transitive* if for any $i, j \in [k]$ there is an element $g \in \mathcal{G}$ with $g(i) = j$. Every group is transitive on some set, e.g., on itself by left multiplication.

The group \mathcal{G} has an induced action on s -tuples, $[k]^s$. The action of \mathcal{G} is *s -transitive* if for any two s -tuples (i_1, \dots, i_s) and (j_1, \dots, j_s) each having distinct elements, there is a $g \in \mathcal{G}$ with $g(i_r) = j_r$ for $r = 1, \dots, s$. The full symmetric group S_k is k -transitive and its alternating subgroup A_k of even permutations is $(k-2)$ -transitive. There are few other highly transitive groups. This is explained in [9, § 4] and summarized in the following proposition, which follows from the O’Nan-Scott Theorem [29] and the classification of finite simple groups.

Proposition 2.1 (Thm. 4.11 [9]). *The only 6-transitive groups are the symmetric and alternating groups. The only 4-transitive groups are the symmetric and alternating groups, and the Mathieu groups M_{11} , M_{12} , M_{23} , and M_{24} . All 2-transitive permutation groups are known.*

Tables 7.3 and 7.4 in [9] list the 2-transitive permutation groups.

Suppose that \mathcal{G} is transitive on $[k]$. A *block* is a subset B of $[k]$ such that for every $g \in \mathcal{G}$ either $gB = B$ or $gB \cap B = \emptyset$. The orbits of a block form a \mathcal{G} -invariant partition of $[k]$ into blocks. The group \mathcal{G} is *primitive* if its only blocks are $[k]$ or singletons, otherwise it is *imprimitive*. Any 2-transitive permutation group is primitive, and primitive permutation groups that are not symmetric or alternating are rare—the set of k for which such a nontrivial primitive permutation group exists has density zero in the natural numbers [9, § 4.9].

Each \mathcal{G} -orbit $\mathcal{O} \subset [k]^2$ determines a graph $\Gamma_{\mathcal{O}}$ with vertex set $[k]$ —its edges are the pairs in \mathcal{O} . For the diagonal orbit $\{(a, a) \mid a \in [k]\}$, this graph is disconnected, consisting of k loops. Connectivity of all other orbits is equivalent to primitivity (see [9, § 1.11]).

Proposition 2.2 (Higman’s Theorem [20]). *A transitive group \mathcal{G} is primitive if and only if for each non-diagonal orbit $\mathcal{O} \subset [k]^2$, the graph $\Gamma_{\mathcal{O}}$ is connected.*

Imprimitive groups are subgroups of wreath products $S_a \text{ Wr } S_b$ with $ab = k$ and $a, b > 1$ where this decomposition comes from the blocks of a \mathcal{G} -invariant partition. The dihedral group D_4 of the symmetries of a square is isomorphic to $S_2 \text{ Wr } S_2$, with an imprimitive action on the vertices—it preserves the partition into diagonals. More generally, the dihedral group D_k of symmetries of a regular k -gon is imprimitive on the vertices whenever k is composite.

2.2. Galois and monodromy groups. A map $f: V \rightarrow U$ between irreducible complex algebraic varieties of the same dimension with $f(V)$ dense in U is a *dominant* map. When $f: V \rightarrow U$ is dominant, the function field $\mathbb{C}(V)$ of V is a finite extension of $f^*\mathbb{C}(U)$, the pullback of the function field of U . This extension has degree k , where k is the degree of f , which is the cardinality of a general fiber. The *Galois group* $\mathcal{G}(V \rightarrow U)$ of $f: V \rightarrow U$ is the Galois group of the Galois closure of $\mathbb{C}(V)$ over $f^*\mathbb{C}(U)$.

This algebraically defined Galois group is also a geometric monodromy group. A dominant map $f: V \rightarrow U$ of equidimensional varieties is a *branched cover*. The *branch locus* B of $f: V \rightarrow U$ is the set of points $u \in U$ such that $f^{-1}(u)$ does not consist of k reduced points. Then $f: f^{-1}(U \setminus B) \rightarrow U \setminus B$ is a degree k covering space. The group of deck transformations of this cover is a subgroup of the symmetric group S_k and is isomorphic to the Galois group $\mathcal{G}(V \rightarrow U)$, as permutation groups. Hermite [19] realized that Galois and monodromy groups coincide and Harris [14] gave a modern treatment. The following is elementary.

Proposition 2.3. *Let $u \in U \setminus B$. Following points in the fiber $f^{-1}(u)$ along lifts to V of loops in $U \setminus B$ gives a homomorphism from the fundamental group $\pi_1(U \setminus B)$ of $U \setminus B$ to the set of permutations of $f^{-1}(u)$ whose image is the Galois/monodromy group.*

There is a purely geometric construction of Galois groups using fiber products (explained in [36, § 3.5]). For each $2 \leq s \leq k$ let V_U^s be the s -fold fiber product,

$$V_U^s := \overbrace{V \times_U V \times_U \cdots \times_U V}^s.$$

We also write f for the map $V_U^s \rightarrow U$. The fiber of V_U^s over a point $u \in U$ is $(f^{-1}(u))^s$, the set of s -tuples of points in $f^{-1}(u)$. Over $U \setminus B$, V_U^s is a covering space of degree k^s . This is decomposable, and among its components are those lying in the big diagonal Δ , where some coordinates of the s -tuples coincide. We define $V^{(s)}$ to be the closure in V_U^s of $f^{-1}(U \setminus B) \setminus \Delta$. Then every irreducible component of $V^{(s)}$ maps dominantly to U and its fiber over a point $u \in U \setminus B$ consists of s -tuples of distinct points of $f^{-1}(u)$. This may be done iteratively as $V^{(s+1)}$ is the union of components of $V^{(s)} \times_U V$ lying outside of the big diagonal.

Suppose that $s = k$. Let $u \in U \setminus B$ and write the elements of $f^{-1}(u)$ in some order,

$$f^{-1}(u) = \{v_1, v_2, \dots, v_k\}.$$

The fiber of $V^{(k)}$ over u consists of the $k!$ distinct k -tuples $(v_{\sigma(1)}, \dots, v_{\sigma(k)})$ for σ in the symmetric group S_k .

Proposition 2.4. *The Galois group $\mathcal{G}(V \rightarrow U)$ is the subgroup of S_k consisting of all permutations σ such that $(v_{\sigma(1)}, \dots, v_{\sigma(k)})$ lies in the same component of $V^{(k)}$ as does (v_1, \dots, v_k) .*

The function field of any component of $V^{(k)}$ is the Galois closure of $\mathbb{C}(V)$ over $f^*\mathbb{C}(U)$, and the construction of $V^{(k)}$ is the geometric counterpart of the usual construction of a Galois closure by adjoining successive roots of an irreducible polynomial. Proposition 2.4 implies that we may read off the Galois group from any irreducible component of $V^{(k)}$. In fact $V^{(k-1)}$ will suffice as $V^{(k)} \simeq V^{(k-1)}$. (Knowing $k-1$ points from $\{v_1, \dots, v_k\}$ determines the k th.) Other properties of \mathcal{G} as a permutation group may be read off from these fiber products.

Proposition 2.5. *The irreducible components of $V^{(s)}$ correspond to orbits of \mathcal{G} acting on s -tuples of distinct points. In particular, \mathcal{G} is s -transitive if and only if $V^{(s)}$ is irreducible.*

Proof. This is essentially Lemma 1 of [34]. Let $u \in U \setminus B$ and suppose that $v := (v_1, \dots, v_s)$ and $v' := (v'_1, \dots, v'_s)$ are points in the fiber in V_U^s above u that lie in the same irreducible component X . Let σ be a path in $X \setminus f^{-1}(B)$ connecting v to v' . Then $f(\sigma) = \gamma$ is a loop in $U \setminus B$ based at u . Lifting γ to V gives a monodromy permutation $g \in \mathcal{G}$ with the property that $g(v_i) = v'_i$ for $i = 1, \dots, s$. Thus v and v' lie in the same orbit of \mathcal{G} acting on s -tuples of points of V in the fiber $f^{-1}(u)$.

Conversely, let $v_1, \dots, v_s \in V$ be points in a fiber above $u \in U \setminus B$ and let $g \in \mathcal{G}$. There is a loop $\gamma \subset U \setminus B$ that is based at U and whose lift to V gives the action of g on $f^{-1}(u)$. Lifting γ to V_U^s gives a path connecting the two points (v_1, \dots, v_s) and $(g(v_1), \dots, g(v_s))$ in the fiber above u , showing that they lie in the same component of V_U^s . Restricting to s -tuples of distinct points establishes the proposition. \square

2.3. Fundamental groups of complements. Classical algebraic geometers studied the fundamental group $\pi_1(\mathbb{P}^n \setminus B)$ of the complement of a hypersurface $B \subset \mathbb{P}^n$. Zariski [37] showed that if Π is a general two-dimensional linear subspace of \mathbb{P}^n , then the inclusion $\iota: \Pi \setminus B \rightarrow \mathbb{P}^n \setminus B$ induces an isomorphism of fundamental groups,

$$(1) \quad \iota_* : \pi_1(\Pi \setminus B) \xrightarrow{\sim} \pi_1(\mathbb{P}^n \setminus B).$$

(As the complement of B is connected, we omit base points in our notation.) Consequently, it suffices to study fundamental groups of complements of plane curves $C \subset \mathbb{P}^2$. Zariski also showed that if ℓ is a line meeting B in $d = \deg B$ distinct points, so that the intersection is transverse, then the natural map of fundamental groups

$$\iota_* : \pi_1(\ell \setminus B) \twoheadrightarrow \pi_1(\mathbb{P}^n \setminus B)$$

is a surjection. (See also [10, Prop. 3.3.1].)

We recall some facts about $\pi_1(\ell \setminus B)$. Suppose that $B \cap \ell = \{b_1, \dots, b_d\}$ and that $p \in \ell \setminus B$ is our base point. For each $i = 1, \dots, d$, let D_i be a closed disc in $\ell \simeq \mathbb{C}\mathbb{P}^1$ centered at b_i with $D_i \cap B = \{b_i\}$. Choose any path in $\ell \setminus B$ from p to the boundary ∂D_i of D_i and let γ_i be the loop based at p that follows that path, traverses the boundary of D_i once anti-clockwise, and then returns to p along the chosen path. Any loop in $\ell \setminus B$ based at p that is homotopy-equivalent to γ_i (for some choice of path from p to ∂D_i) is a (based) loop in $\ell \setminus B$ **encircling** b_i . The fundamental group $\pi_1(\ell \setminus B)$ is a free group freely generated by loops encircling any $d-1$ points of $B \cap \ell$. We record the consequence of Zariski's result that we will use.

Proposition 2.6. *Let $B \subset \mathbb{P}^n$ be a hypersurface. If $\ell \subset \mathbb{P}^n$ is any line that meets B in finitely many reduced points, then a set of based loops in ℓ encircling each of these points generate the fundamental group of the complement, $\pi_1(\mathbb{P}^n \setminus B)$.*

2.4. Homotopy continuation and monodromy. Numerical algebraic geometry [5, 32] uses numerical analysis to study algebraic varieties on a computer. We present its core algorithms of Newton refinement and continuation, and explain how they are used to compute monodromy. Let $F: \mathbb{C}^n \rightarrow \mathbb{C}^n$ be a polynomial map with $F^{-1}(0)$ consisting of finitely many reduced points. To any $x \in \mathbb{C}^n$ that is not a critical point of F so that the Jacobian matrix $JF(x)$ of F at x is nonsingular, we may apply a Newton step

$$N_F(x) := x - JF(x)^{-1} \cdot F(x).$$

If x is sufficiently close to a zero x^* of F , then $N_F(x)$ is closer still in that the sequence defined by $x_0 := x$ and $x_{i+1} := N_F(x_i)$ for $i \geq 0$ satisfies $\|x^* - x_i\| < 2^{1-2^i} \|x^* - x\|$.

A homotopy H is a polynomial map $H: \mathbb{C}^n \times \mathbb{C}_t \rightarrow \mathbb{C}^n$ that defines a curve $C \subset H^{-1}(0)$ which maps dominantly to \mathbb{C}_t . Write $f: C \rightarrow \mathbb{C}_t$ for this map. We assume that the inverse image $f^{-1}[0, 1]$ in C of the interval $[0, 1]$ is a collection of arcs connecting the points of C above $t = 1$ to points above $t = 0$ which are smooth at $t \neq 0$. Given a point $(x, 1)$ of C , standard predictor-corrector methods (e.g. Euler tangent prediction followed by Newton refinement) construct a sequence of points (x_i, t_i) where $x_0 = x$ and $1 = t_0 > t_1 > \dots > t_s = 0$ on the arc containing $(x, 1)$. This computation of the points in $f^{-1}(0)$ from points of $f^{-1}(1)$ by continuation along the arcs $f^{-1}[0, 1]$ is called *numerical homotopy continuation*. Numerical algebraic geometry uses homotopy continuation to solve systems of polynomial equations and to study algebraic varieties. While we will not describe methods to solve systems of equations, we will describe other methods of numerical algebraic geometry.

When U is rational, a branched cover $f: V \rightarrow U$ gives homotopy paths. Given a map $g: \mathbb{C}_t \rightarrow U$ whose image is not contained in the branch locus B of f , the pullback g^*V is a curve C with a dominant map to \mathbb{C}_t . Pulling back equations for V gives a homotopy for tracking points of C . We need not restrict to arcs lying over the interval $[0, 1]$, but may instead take any path $\gamma \subset \mathbb{C}_t$ (or in U) that does not meet the branch locus. When $\gamma \subset U \setminus B$ is a loop based at a point $u \in U \setminus B$, homotopy continuation along $f^{-1}(\gamma)$ starting at $f^{-1}(u)$ computes the monodromy permutation of $f^{-1}(u)$ given by the homotopy class of $g(\gamma)$ in $U \setminus B$. The observation that numerical homotopy continuation may compute monodromy is the *point de départ* of this paper.

2.5. Numerical algebraic geometry. Numerical algebraic geometry uses solving, path-tracking, and monodromy to study algebraic varieties on computer. For this, it relies on the fundamental data structure of a witness set, which is a geometric representation based on linear sections [30, 31].

Let $F: \mathbb{C}^n \rightarrow \mathbb{C}^m$ be a polynomial map and suppose that X is a component of $F^{-1}(0)$ of dimension r and degree d . Let $\mathcal{L}: \mathbb{C}^n \rightarrow \mathbb{C}^r$ be a general affine-linear map so that $\mathcal{L}^{-1}(0)$ is a general affine subspace of codimension r . By Bertini's Theorem, $W := X \cap \mathcal{L}^{-1}(0)$ consists of d distinct points, and we call the triple (F, \mathcal{L}, W) (or simply W) a *witness set* for X . If \mathcal{L} varies in a family $\{\mathcal{L}_t \mid t \in \mathbb{C}\}$, then $V \cap \mathcal{L}_t^{-1}(0)$ gives a homotopy which may be used to follow the points of W and sample points of X . This is used in many algorithms to manipulate X based on geometric constructions. A *witness superset* for X is a finite subset $W' \subset F^{-1}(0) \cap \mathcal{L}^{-1}(0)$ that contains $W = X \cap \mathcal{L}^{-1}(0)$. In many applications, it suffices to work with a witness superset. For example, if X is a hypersurface, then $\mathcal{L}^{-1}(0)$ is a general line, ℓ , and by Zariski's Theorem (Prop. 2.6), the fundamental group of $\mathbb{C}^n \setminus V$ is generated by loops in ℓ encircling the points of W , and hence also by loops encircling points of W' .

One algorithm is computing a witness set for the image of an irreducible variety under a linear map [16]. Suppose that $F: \mathbb{C}^n \rightarrow \mathbb{C}^m$ is a polynomial map with $V \subset F^{-1}(0)$ a component of dimension r as before, and that we have a linear map $\pi: \mathbb{C}^n \rightarrow \mathbb{C}^p$. Let $U = \overline{\pi(V)}$ be the closure of the image of V under π , which we suppose has dimension q and degree δ . To compute a witness set for U from one for V , we need an affine-linear map $\mathcal{L}: \mathbb{C}^n \rightarrow \mathbb{C}^r$ adapted to the map π .

Suppose that π is given by $\pi(x) = Ax$ for a matrix $A \in \mathbb{C}^{p \times n}$. Let B be a matrix $\begin{bmatrix} B_1 \\ B_2 \end{bmatrix}$ where the rows of $B_1 \in \mathbb{C}^{q \times n}$ are general vectors in the row space of A and the rows of $B_2 \in \mathbb{C}^{(r-q) \times n}$ are general vectors in \mathbb{C}^n . Then $B_1^{-1}(0)$ is the pullback of a general linear subspace of codimension q in \mathbb{C}^p . Choose a general vector $v \in \mathbb{C}^r$, define $\mathcal{L}(x) := Bx - v$, and set $W := V \cap \mathcal{L}^{-1}(0)$. The quadruple (F, π, \mathcal{L}, W) is a witness set for the image of

V under π . By the choice of B , the number of points in $\pi(W)$ is the degree δ of U , and for $u \in \pi(W)$, the number of points in $\pi^{-1}(u) \cap W$ is the degree of the fiber of V over w , which has dimension $r-q$. The witness set (F, π, \mathcal{L}, W) for the image U may be computed from any witness set (F, \mathcal{L}', W') for V by following the points of W' along a path connecting the general affine map \mathcal{L}' to the special affine map \mathcal{L} .

Numerical continuation may be used to sort points in a general affine section of a reducible variety V into witness sets of its components. Let $F: \mathbb{C}^n \rightarrow \mathbb{C}^m$ be a polynomial map and suppose that $V = V_1 \cup \dots \cup V_s$ is a union of components of $F^{-1}(0)$, all having dimension r , and that $\mathcal{L}: \mathbb{C}^n \rightarrow \mathbb{C}^r$ is a general affine linear map with $\mathcal{L}^{-1}(0)$ meeting V transversely in d points $W := V \cap \mathcal{L}^{-1}(0)$. The witness sets $W_i := V_i \cap \mathcal{L}^{-1}(0)$ for the components form the *witness set partition* of W that we seek.

Following points of W along a homotopy as \mathcal{L} varies, those from W_i remain on V_i . Consequently, if we compute monodromy by allowing \mathcal{L} to vary in a loop, the partition of W into orbits is finer than the witness set partition. Computing additional monodromy permutations may coarsen this orbit partition, but it will always refine the witness set partition.

Suppose that \mathcal{L}_t depends affine-linearly on t . The path of $w \in W$ under the corresponding homotopy will in general be a non-linear function of t . However if we follow all points in the witness set W_i for a component, then their sum in \mathbb{C}^n (the trace) is an affine-linear function of t . For general \mathcal{L}_t , the only subsets of W whose traces are linear in t are unions of the W_i . Thus we may test if a union of blocks in an orbit partition is a union of the W_i . These two methods, monodromy break up and the trace test, are combined in the algorithm of numerical irreducible decomposition [32, Ch. 15] to compute the witness set partition.

Remark 2.7. Oftentimes problems are naturally formulated in terms of homogeneous or multi-homogeneous equations whose solutions are subsets of (products of) projective spaces \mathbb{P}^n . That is, we have a polynomial map $F: \mathbb{C}^{n+1} \rightarrow \mathbb{C}^r$ and we want to study the projective variety given by $F^{-1}(0)$. Restricting F to any affine hyperplane not containing the origin of \mathbb{C}^{n+1} , we obtain the intersection of $F^{-1}(0)$ with an affine chart of \mathbb{P}^n . If the hyperplane is general, then the points of interest, including homotopy paths and monodromy loops, will lie in that affine chart, and no information is lost by this choice.

When discussing computation, we will refer to the affine chart given by the vanishing of an affine form, as well as referring to the chart via a parameterization of the corresponding affine hyperplane. When performing computations, our software works in random affine charts.

3. BRANCH POINT METHOD

Given a branched cover $f: V \rightarrow U$ of degree k with branch locus B such that U is rational, we have the following direct approach to computing its Galois group $\mathcal{G} := \mathcal{G}(V \rightarrow U)$. Choose a regular value $u \in U \setminus B$ of f , so that $f^{-1}(u)$ consists of k reduced points. Numerically following the points of $f^{-1}(u')$ as u' varies along a sequence of loops in $U \setminus B$ based at u computes a sequence $\sigma_1, \sigma_2, \dots$ of monodromy permutations in $\mathcal{G} \subseteq S_k$. If G_i is the subgroup of \mathcal{G} generated by $\sigma_1, \dots, \sigma_i$, then we have

$$G_1 \subseteq G_2 \subseteq \dots \subseteq \mathcal{G} \subseteq S_k.$$

This method was used in [24] (and elsewhere) to show that $\mathcal{G} = S_k$ by computing enough monodromy permutations so that $G_i = S_k$. When the Galois group is *deficient* in that $\mathcal{G} \subsetneq S_k$, then this method cannot compute \mathcal{G} , for it cannot determine if it has computed

generators of \mathcal{G} . The results described in Section 2 lead to an algorithm to compute a set of generators for \mathcal{G} and therefore determine \mathcal{G} .

As U is rational, we may replace it by \mathbb{P}^n where $n = \dim U$ and assume that $f: V \rightarrow \mathbb{P}^n$ is a branched cover of degree k . The branch locus $B \subset \mathbb{P}^n$ is the set of points $b \in \mathbb{P}^n$ where $f^{-1}(b)$ does not consist of k distinct (reduced) points. As V is irreducible, if $k > 1$, then B is a hypersurface. Suppose that B has degree d .

Let $\ell \subset \mathbb{P}^n$ be a projective line that meets B transversally in d points, so that $W = B \cap \ell$ is a witness set for B . By Bertini's Theorem, a general line in \mathbb{P}^n has this property. Let $u \in \ell \setminus B$ and, for each point b of $B \cap \ell$, choose a loop γ_b based at u encircling b as in Subsection 2.3. Let $\sigma_b \in S_k$ be the monodromy permutation obtained by lifting γ_b to V .

Theorem 3.1. *The Galois group $\mathcal{G}(V \rightarrow U)$ is generated by any $d-1$ of the monodromy permutations $\{\sigma_b \mid b \in B \cap \ell\}$.*

Proof. By Proposition 2.3, lifting based loops in $\mathbb{P}^n \setminus B$ to permutations in S_k gives a surjective homomorphism $\pi_1(\mathbb{P}^n \setminus B) \rightarrow \mathcal{G}$. By Zariski's Theorem (Proposition 2.6) the fundamental group of $\mathbb{P}^n \setminus B$ is generated by loops encircling any $d-1$ points of $\ell \cap B$, where $d = \deg B$. Therefore their lifts to monodromy permutations generate the Galois group \mathcal{G} . \square

It is not necessary to replace U by \mathbb{P}^n . If we instead use \mathbb{C}^n with $B \subset \mathbb{C}^n$, then $\ell \subset \mathbb{C}^n$ is a complex line, $\ell \simeq \mathbb{C}$. If $B \cap \ell$ is d distinct points where d is the degree of the closure \overline{B} in \mathbb{P}^n , then the statement of Theorem 3.1 still holds, as $B \cap \ell = \overline{B} \cap \ell$.

Lifts of loops encircling the points of a witness superset for $\ell \cap B$ will also generate \mathcal{G} .

Corollary 3.2. *Suppose that B' is a reducible hypersurface in \mathbb{P}^n that contains the hypersurface B and that ℓ meets B' in a witness superset $W = B' \cap \ell$ for B . Then lifts $\{\sigma_w \mid w \in W\}$ of loops $\{\gamma_w \mid w \in W\}$ encircling points of W generate \mathcal{G} .*

3.1. Branch point algorithm. Theorem 3.1 and Corollary 3.2 give a procedure for determining the Galois group \mathcal{G} of a branched cover $f: V \rightarrow U$ when U is rational. Suppose that $V \subset \mathbb{P}^m \times \mathbb{P}^n$ is irreducible of dimension n and that the map $f: V \rightarrow \mathbb{P}^n$ given by the projection to \mathbb{P}^n is dominant, so that $f: V \rightarrow \mathbb{P}^n$ is a branched cover.

Algorithm 3.3 (Branch Point Algorithm).

- (1) Compute a witness set $W = B \cap \ell$ (or a witness superset) for the branch locus B of $f: V \rightarrow \mathbb{P}^n$.
- (2) Fix a base point $p \in \ell \setminus B$ and compute the fiber $f^{-1}(p)$.
- (3) Compute monodromy permutations $\{\sigma_w \mid w \in W\}$ that are lifts of based loops in $\ell \setminus B$ encircling the points w of W .

The monodromy permutations $\{\sigma_w \mid w \in W\}$ generate the Galois group \mathcal{G} of $f: V \rightarrow \mathbb{P}^n$.

The correctness of the branch point algorithm follows from Theorem 3.1 and Corollary 3.2. We discuss the steps (1) and (3) in more detail.

3.1.1. Witness superset for the branch locus. Suppose that $V \subset \mathbb{P}^m \times \mathbb{P}^n$ is an irreducible variety of dimension n such that the projection $f: V \rightarrow \mathbb{P}^n$ is a branched cover with branch locus B . Since f is a proper map (its fibers are projective varieties), B is the set of critical values of f . These are images of the critical points CP , which are points of V where either V is singular or it is smooth and the differential of f does not have full rank.

We use x for the coordinates of the cone \mathbb{C}^{m+1} of \mathbb{P}^m and u for the cone \mathbb{C}^{n+1} over \mathbb{P}^n . Then $V = F^{-1}(0)$, where $F: \mathbb{C}_x^{m+1} \times \mathbb{C}_u^{n+1} \rightarrow \mathbb{C}^r$ is a system of $r \geq m$ polynomials that are

separately homogeneous in each set of variables x and u . Let $J_x F := (\partial F_i / \partial x_j)_{i=1, \dots, r}^{j=0, \dots, m}$ be the $r \times (m+1)$ -matrix of the *vertical partial derivatives* of F .

Proposition 3.4. *The critical points CP of the map $f: V \rightarrow \mathbb{P}^n$ are the points of V where $J_x F$ has rank less than m .*

To compute a witness set for the branch locus $B = f(CP)$ we will restrict $f: V \rightarrow \mathbb{P}^n$ to a line $g: \ell \hookrightarrow \mathbb{P}^n$, obtaining a curve $C := g^{-1}(V) \subset \mathbb{P}^m \times \ell$ equipped with the projection $f: C \rightarrow \ell$. We then compute the critical points on C of this map and their projection to ℓ .

Example 3.5. Consider the irreducible two-dimensional variety V in $\mathbb{P}_{xy}^1 \times \mathbb{P}_{uvw}^2$ defined by the vanishing of $F := ux^3 + vy^3 - wxy^2$. Write f for the projection of V to \mathbb{P}^2 , which is a

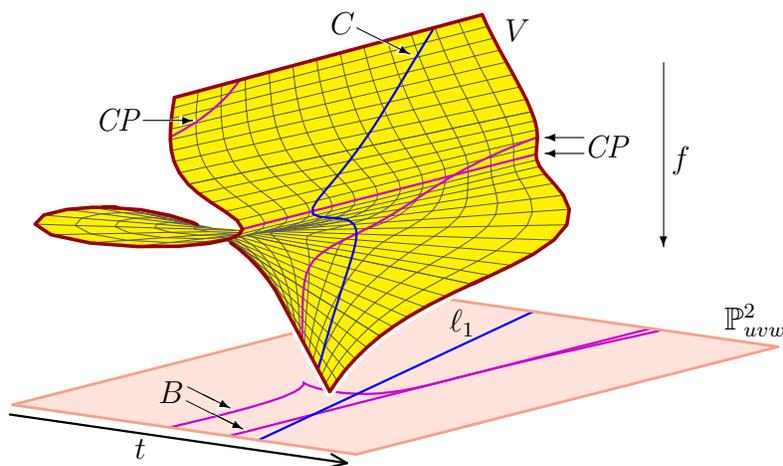


FIGURE 2. The surface $ux^3 + vy^3 - wxy^2 = 0$.

dominant map. This has degree three and in Example 3.7 we will see that the Galois group is the full symmetric group S_3 . Its critical point locus is the locus of points of V where the Jacobian $J_{xy} F = [\partial F / \partial x \ \partial F / \partial y]$ has rank less than $m = 1$. This is defined by the vanishing of the partial derivatives as $3F = x\partial F / \partial x + y\partial F / \partial y$. Eliminating x and y from the ideal these partial derivatives generate yields the polynomial $u(27uv^2 - 4w^3)$, which defines the branch locus B and shows that both B and CP are reducible. In fact, B consists of the line $u = 0$ and the cuspidal cubic $27uv^2 = 4w^3$. It is singular at the cusp $[1 : 0 : 0]$ of the cubic and the point $[0 : 1 : 0]$ where the two components meet. The cubic has its flex at this point and the line $u = 0$ is its tangent at that flex. The branch locus is also the discriminant of F , considered as a homogeneous cubic in x, y . We display V , CP , and B in Figure 2.

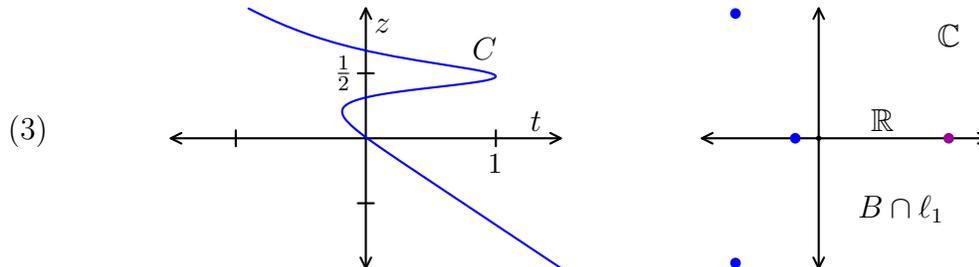
Consider the line $\ell_1 \subset \mathbb{P}^2$ which is the image of the map $g: \mathbb{P}^1 \hookrightarrow \mathbb{P}^2$ defined by

$$[s : t] \mapsto [s-t : 2s-3t : 5s+7t].$$

Let $C \subset \mathbb{P}_{xy}^1 \times \mathbb{P}_{st}^1$ be the curve $g^{-1}(V)$ defined by $G := (s-t)x^3 + (2s-3t)y^3 - (5s+7t)xy^2$. Its Jacobian with respect to the x and y variables is simply $g^{-1}(J_{xy} F)$, and so the critical points and branch locus are pullbacks of those of F along g . They are defined by the two partial derivatives $\partial G / \partial x$ and $\partial G / \partial y$. These equations of bidegree $(1, 2)$ have four common zeroes in $\mathbb{P}^1 \times \mathbb{P}^1$. Projecting to $\ell_1 = \mathbb{P}_{st}^1$ and working in the affine chart where $s = 1$ yield

$$(2) \quad -0.64366 + 0.95874\sqrt{-1}, \quad -0.18202, \quad -0.64366 - 0.95874\sqrt{-1}, \quad 1.$$

The first three points lie in the cubic component of B , while the last is in the line $u = 0$ (so that $s = t$). We display the curve C in the real affine chart on $\mathbb{P}_{xy}^1 \times \mathbb{P}_{st}^1$ given by $7x + 3y = 58$ and $s = 1$ as well as the branch locus in the affine chart of $\mathbb{C}\mathbb{P}_{st}^1 (= \ell_1)$ where $s = 1$. This chart for \mathbb{P}_{xy}^1 has parameterization $x = 4 + 9z$ and $y = 10 - 21z$ for $z \in \mathbb{C}$ and is also used in Figure 2, where the t -coordinate is as indicated.



Remark 3.6. In this example (and, in fact, whenever $V \subset \mathbb{P}^m \times \mathbb{P}^n$ is a hypersurface so that $m = 1$), the critical point locus CP is defined by both vertical partial derivatives, and is therefore a complete intersection. In general, CP is defined by the polynomial system F and the condition on the rank of the Jacobian, and is not a complete intersection. In numerical algebraic geometry, it is advantageous to work with complete intersections.

There are several methods to reformulate this system as a complete intersection. If $r > m$, then F may be replaced by a random subsystem of m polynomials. We could also require the vanishing of only a random linear combination of the maximal minors of the Jacobian matrix $J_x F$. Another is to add variables, parameterizing a vector in the null space of $J_x F$. That is, add the system $J_x F \cdot v = 0$ to F , where v spans a general line in \mathbb{C}^{m+1} , so that v lies in an affine chart \mathbb{C}^m of \mathbb{P}^m , and then project from $\mathbb{C}_v^m \times \mathbb{P}_x^m \times \mathbb{P}_y^n$ to \mathbb{P}_y^n and obtain a witness set for B . This also has the advantage that the new equations $J_x F \cdot v = 0$ have total degree equal to those of F and are linear in the entries of v .

These reductions to complete intersections will have not only the points of $B \cap \ell$ as solutions, but possible additional solutions, and will therefore compute a witness superset for $B \cap \ell$.

3.1.2. Computing monodromy permutations. Suppose that we have a witness superset $W \subset \ell$ for B , so that W contains the transverse intersection $B \cap \ell$. By Corollary 3.2, monodromy permutations lifting based loops encircling the points of W generate the Galois group \mathcal{G} . To compute these encircling loops, we choose a general (random) base point $p \in \ell \setminus W$ and work in an affine chart of ℓ that contains p and W and is identified with \mathbb{C} . After describing our construction of loops, we will state the condition for genericity.

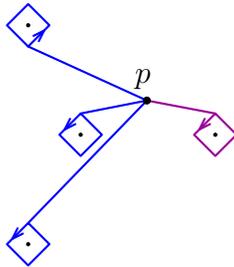
Let $\epsilon > 0$ be any positive number smaller than the minimum distance between points of W . For $w \in W$, the points $w \pm \epsilon$ and $w \pm \epsilon\sqrt{-1}$ are vertices of a square (diamond) centered at w that contains no other points of W . Traversing this anti-clockwise,

$$w + \epsilon \rightsquigarrow w + \epsilon\sqrt{-1} \rightsquigarrow w - \epsilon \rightsquigarrow w - \epsilon\sqrt{-1} \rightsquigarrow w + \epsilon,$$

gives a loop encircling the point w . To obtain loops based at p , we concatenate each square loop with a path from p to that loop as follows. If $w - p$ has negative imaginary part, then this is the straight line path from p to $w + \epsilon\sqrt{-1}$ and if $w - p$ has positive imaginary part, the path is from p to $w - \epsilon\sqrt{-1}$. Our assumption of genericity on the point p is that these chosen paths from p to the squares do not meet points of W , so that we obtain loops in $\ell \setminus W$.

Observe that concatenating these loops in anti-clockwise order of the paths from p gives a loop whose negative encircles the point at infinity.

Example 3.7. We show this collection of based loops encircling the points $W = B \cap \ell_1$ from the witness set on the right in (3) where $p = 0.4 + 0.3\sqrt{-1}$.



Starting from the rightmost point $1 \in W$ and proceeding clockwise, we obtain the permutations $(2, 3)$, $(1, 3)$, $(1, 2)$, and $(1, 3)$. These generate S_3 , showing that the Galois group of the cover $V \rightarrow \mathbb{P}^2_{uvw}$ is the full symmetric group.

3.1.3. *Implementation subtleties.* In our computations, we do not work directly on projective space, but rather in affine charts as explained in Remark 2.7, and not with general lines, but randomly chosen specific lines. We illustrate different ways that specific (unfortunate) choices of charts and lines may not give a witness set for the branch locus. While these are overcome in practice by working with affine charts and lines whose coefficients are randomly generated numbers in \mathbb{C} , it is important to point out the subtleties of nongeneric behavior with examples.

Example 3.8. Recall the family $V \rightarrow \mathbb{P}^2$ of cubics in Example 3.5. The line ℓ_2 given by the map $[s : t] \mapsto [t+s : t-s : 0] \subset \mathbb{P}^2$ which induces a curve C_2 that is not general because the projection $C_2 \rightarrow \ell_2$ does not have four distinct branch points. There are two critical points, each of multiplicity two, as two pairs of simple critical points came together over ℓ_2 . This is observed in Figure 3 where we see that the line ℓ_2 contains both singular points q and r of the branch locus, so $B \cap \ell_2$ consists of two points of multiplicity two. The line ℓ_2 does not intersect the branch locus B transversally, so Zariski’s Theorem (Proposition 2.6) does not hold. Also, $B \cap \ell_2$ is not a witness set for B . Lifts of loops encircling the points of $B \cap \ell_2$ generate the cyclic group of order three, rather than the full symmetric group.

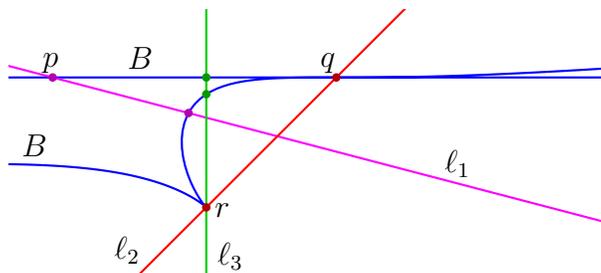


FIGURE 3. Branch locus and lines.

As $V \subset \mathbb{P}^1 \times \mathbb{P}^2$, we choose affine charts for both factors. If the charts are not generic, they may omit points of interest. We illustrate some possibilities.

Example 3.9. Consider the affine chart on \mathbb{P}^2 given by $u = 1$, excluding points on the one-dimensional component $u = 0$ of the branch locus B . On the line ℓ this is the affine chart

where $t - s = 1$, which omits the fourth point of $B \cap \ell_1$ of (2), (p in Figure 3). Thus only three of the four branch points are on this affine chart of ℓ_1 . Since B has degree four, lifting loops encircling these three points gives permutations that generate \mathcal{G} , by Theorem 3.1.

Example 3.10. Suppose now that $\ell_3 \subset \mathbb{P}^3$ has equation $v = w$. Then $B \cap \ell_3$ consists of three points, with the point $[1 : 0 : 0]$ at the cusp of B of multiplicity two. We may parameterize ℓ_3 by $g: [s : t] \mapsto [s-t : s : s]$. Then the affine chart given by $s = 1$ does not contain the singular point of $B \cap \ell_3$. Even though the intersection is transverse in this affine chart, the two permutations we obtain by lifting loops encircling these points do not generate \mathcal{G} , as Theorem 3.1 does not hold. The difference with Example 3.9 is that the branch point at infinity (not on our chosen chart) is singular in this case.

Example 3.11. A choice of vertical affine chart may also be unfortunate. The affine chart on \mathbb{P}_{xy}^1 where $y = 1$ does not meet the line component ($u = y = 0$) of the critical point locus CP . Computing a witness set for CP in this chart and projecting to compute a witness set $B \cap \ell$ for B will only give points in the cubic component of B . When ℓ does not contain the point q , this is sufficient to compute \mathcal{G} , for the same reason as in Example 3.10.

If V is not a hypersurface so that $m > 1$, then there may be more interesting components of CP not meeting a given vertical affine chart. This may result in the computed points of the witness set $B \cap \ell$ for B being insufficient to generate the Galois group \mathcal{G} .

3.1.4. *27 lines on a cubic surface.* A cubic surface S is a hypersurface in \mathbb{P}^3 defined by a homogeneous form of degree three. It is classical that a smooth cubic surface contains exactly 27 lines (see Figure 4), and these lines have a particular incidence structure (see Section 4.1). Jordan [23] studied the Galois action on the 27 lines. It turns out that the Galois group is the

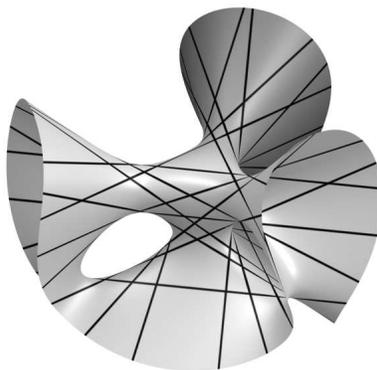


FIGURE 4. Cubic surface with 27 lines (courtesy of Oliver Labs).

group of symmetries of that incidence structure, which is isomorphic to the Weyl group E_6 , a group of order 51,840. We formulate this as a monodromy problem $f: V \rightarrow U$ and use the Branch Point Algorithm to compute and identify this monodromy group.

There are 20 homogeneous cubic monomials in the variables X, Y, Z, W for \mathbb{P}^3 , so we identify the space of cubics with $U = \mathbb{P}^{19}$. For $F \in \mathbb{P}^{19}$, let $\mathcal{V}(F)$ be the corresponding cubic surface. Let \mathbb{G} be the Grassmannian of lines in \mathbb{P}^3 , which is an algebraic manifold of dimension 4. Form the incidence variety

$$V := \{(F, \ell) \in \mathbb{P}^{19} \times \mathbb{G} \mid \ell \text{ lies on } \mathcal{V}(F)\},$$

which has a map $f: V \rightarrow \mathbb{P}^{19}(= U)$. Algebraic geometry tells us that the cubics with 27 lines are exactly the smooth cubics, and therefore the branch locus B is exactly the space of singular cubics. That is, B is given by the classical multivariate discriminant, whose degree was determined by G. Boole to be 32.

We summarize the computations associated with determining a witness set for this branch locus. Let G be a general cubic (variable coefficients) and consider the vectors $\mathbf{v} = (1, 0, k_1, k_2)$ and $\mathbf{w} = (0, 1, k_3, k_4)$, which span a general line in \mathbb{P}^3 . This line lies on the cubic surface $\mathcal{V}(G)$ when the homogeneous cubic $G(r\mathbf{v}+s\mathbf{w})$ (the cubic restricted to the line spanned by \mathbf{v} and \mathbf{w}) is identically zero. That is, when the coefficients K_0, K_1, K_2, K_3 of $r^3, r^2s, rs^2,$ and s^3 in $G(r\mathbf{v}+s\mathbf{w})$ vanish. This defines the incidence variety V in the space $\mathbb{P}^{19} \times \mathbb{C}_k^4$, as the vectors \mathbf{v}, \mathbf{w} and parameters k_i give an affine open chart of \mathbb{G} . These polynomials K_i are linear in the coefficients of G , which shows that the fiber of V above a point of \mathbb{G} is a linear subspace of \mathbb{P}^{19} . Since \mathbb{G} is irreducible, as are these fibers, we conclude that V is irreducible.

We choose an affine parameterization $g: \mathbb{C}_t \rightarrow \ell \subset \mathbb{P}^{19}$ of a random line ℓ in \mathbb{P}^{19} . Then $C := g^*(V)$ is a curve in $\mathbb{C}_t \times \mathbb{C}_k^4$ defined by $g^*(K_i)$ for $i = 0, \dots, 3$. There are 192 critical points of the projection $C \rightarrow \mathbb{C}_t$, which map six-to-one to 32 branch points. Since the branch locus B has degree 32, these branch points are $B \cap \ell$ and form a witness set for B .

Computing loops around the 32 branch points took less than 45 seconds using our implementation in `Bertini.m2` [3] using `Macaulay2` [12] and `Bertini` [4]. This gave 22 distinct permutations, each a product of six 2-cycles. These are listed in Figure 5, and they generate the Weyl group of E_6 of order 51,840 confirming that it is the Galois group of the problem of 27 lines on a cubic surface.

$$\begin{array}{ll}
 (1,3)(4,21)(7,27)(8,23)(9,10)(11,12), & (1,5)(2,11)(7,13)(8,15)(10,18)(20,21), \\
 (1,6)(4,13)(8,25)(10,19)(11,16)(20,27), & (1,7)(3,27)(5,13)(16,22)(19,24)(25,26), \\
 (1,8)(3,23)(5,15)(6,25)(14,22)(17,24), & (1,12)(3,11)(13,17)(15,19)(18,25)(20,22), \\
 (1,17)(2,27)(8,24)(10,26)(12,13)(16,21), & (1,18)(4,24)(5,10)(12,25)(14,27)(16,23), \\
 (1,19)(2,23)(6,10)(7,24)(12,15)(14,21), & (1,20)(5,21)(6,27)(9,24)(12,22)(23,26), \\
 (1,26)(4,15)(7,25)(10,17)(11,14)(20,23), & (2,6)(5,16)(8,9)(10,23)(13,22)(17,20), \\
 (2,7)(3,17)(4,16)(9,26)(11,13)(23,24), & (2,8)(3,19)(4,14)(6,9)(11,15)(24,27), \\
 (2,12)(3,5)(4,20)(9,18)(13,27)(15,23), & (2,14)(4,8)(5,26)(13,25)(17,18)(21,23), \\
 (2,18)(9,12)(10,11)(14,17)(16,19)(22,24), & (2,20)(4,12)(6,17)(11,21)(19,26)(24,25), \\
 (3,16)(4,17)(6,12)(8,18)(10,15)(22,27), & (3,18)(5,9)(7,14)(8,16)(11,25)(21,24), \\
 (3,26)(8,20)(9,17)(12,14)(15,21)(25,27), & (6,26)(7,8)(13,15)(14,16)(17,19)(23,27).
 \end{array}$$

FIGURE 5. Monodromy permutations.

4. FIBER PRODUCTS

Let $f: V \rightarrow U$ be a branched cover of degree k with Galois/monodromy group \mathcal{G} . As explained in Subsection 2.2, the action of \mathcal{G} on s -tuples of points in a fiber of f is given by the decomposition into irreducible components of iterated fiber products. We discuss the computation and decomposition of iterated fiber products using numerical algebraic geometry.

Computing fiber products in numerical algebraic geometry was first discussed in [33]. Suppose that $V \subset \mathbb{C}_x^m \times \mathbb{C}_y^n$ is an n -dimensional irreducible component of $F^{-1}(0)$ where

$F: \mathbb{C}_x^m \times \mathbb{C}_y^n \rightarrow \mathbb{C}^m$ and we write $F(x, y)$ with $x \in \mathbb{C}^m$ and $y \in \mathbb{C}^n$. There are several methods to compute (components of) iterated fiber products.

First, if $\mathbb{C}^n \simeq \Delta \subset \mathbb{C}^n \times \mathbb{C}^n$ is the diagonal, then $V_{\mathbb{C}^n}^2 = V \times_{\mathbb{C}^n} V \rightarrow \mathbb{C}^n$ is the pullback of the product $V \times V \rightarrow \mathbb{C}^n \times \mathbb{C}^n$ along the diagonal Δ . Were V equal to $F^{-1}(0)$, then $V_{\mathbb{C}^n}^2$ equals $G^{-1}(0)$, where

$$G : \mathbb{C}^m \times \mathbb{C}^m \times \mathbb{C}^n \longrightarrow \mathbb{C}^m \times \mathbb{C}^m$$

is given by $G(x^{(1)}, x^{(2)}, y) = (F(x^{(1)}, y), F(x^{(2)}, y))$ where $x^{(1)}$ lies in the first copy of \mathbb{C}^m and $x^{(2)}$ lies in the second. We also have $V_{\mathbb{C}^n}^2 = (V \times V) \cap (\mathbb{C}^m \times \mathbb{C}^m \times \Delta)$.

In general, V is a component of $F^{-1}(0)$ and $V_{\mathbb{C}^n}^2$ is a union of some components of $G^{-1}(0)$, and we may compute a witness set representation for $V_{\mathbb{C}^n}^2$ using its description as the intersection of the product $(V \times V)$ with $\mathbb{C}^m \times \mathbb{C}^m \times \Delta$ as in § 12.1 of [5]. Iterating this computes $V_{\mathbb{C}^n}^s$, which has several irreducible components. Among these may be components that do not map dominantly to \mathbb{C}^n —these come from fibers of $V \rightarrow \mathbb{C}^n$ of dimension at least one and thus will lie over a proper subvariety of the branch locus B as V is irreducible and B is a hypersurface. There will also be components lying in the big diagonal where some coordinates in the fiber are equal, with the remaining components constituting $V^{(s)}$, whose fibers over points of $\mathbb{C}^n \setminus B$ are s -tuples of distinct points.

In practice, we first restrict V to a general line $\ell \subset \mathbb{C}^n$, for then $V|_{\ell}$ will be an irreducible curve C that maps dominantly to ℓ . It suffices to compute the fiber products C_{ℓ}^s , decompose them into irreducible components, and discard those lying in the big diagonal to obtain $C^{(s)}$ which will be the restriction of $V^{(s)}$ to ℓ . As $C^{(s+1)}$ is the union of components of $C^{(s)} \times_{\ell} C$ that lie outside the big diagonal, we may compute $C^{(s)}$ iteratively: First compute $C^{(2)}$, then for each irreducible component D of $C^{(2)}$, decompose the fiber product $D \times_{\ell} C$, removing components in the big diagonal, and continue. Symmetry may also be used to simplify this computation (e.g., as used in Subsection 4.1).

We offer three algorithms based on computing fiber products that obtain information about the Galois/monodromy group \mathcal{G} of $f: V \rightarrow U$. Let k, ℓ , and C be as above. Let $p \in \ell \setminus B$ be a point whose fiber in C consists of k distinct points.

Algorithm 4.1 (Compute \mathcal{G}).

- (1) Compute an irreducible component X of $C^{(k-1)}$.
- (2) Fixing a $k-1$ -tuple $(x_1, \dots, x_{k-1}) \in X$ lying over p , let

$$\mathcal{G} = \{ \sigma \in S_k \mid (x_{\sigma(1)}, \dots, x_{\sigma(k-1)}) \text{ lies over } p \}.$$

- (3) Then \mathcal{G} is the Galois monodromy group.

Proof of correctness. Recall that $C^{(k-1)} \simeq C^{(k)}$ since knowing $k-1$ of the points in a fiber of C over a point $p \in \ell \setminus B$ determines the remaining point, and the same for V . Since X lies in a unique component of $V^{(k-1)}$, this follows by Proposition 2.4. \square

Algorithm 4.2 (Orbit decomposition of \mathcal{G} on s -tuples and s -transitivity).

- (1) Compute an irreducible decomposition of $C^{(s)}$,

$$C^{(s)} = X_1 \cup X_2 \cup \dots \cup X_r.$$

- (2) The action of \mathcal{G} on distinct s -tuples has r orbits, one for each irreducible component X_i . In the fiber $f^{-1}(p)$ of $C^{(s)}$ these orbits are

$$\mathcal{O}_i := f^{-1}(p) \cap X_i \quad i = 1, \dots, r.$$

- (3) If $r = 1$, so that $C^{(s)}$ is irreducible, then G acts s -transitively.

Proof of correctness. This follows by Proposition 2.5. □

Algorithm 4.3 (Test \mathcal{G} for primitivity).

- (1) Compute an irreducible decomposition of $C^{(2)}$.
- (2) If $C^{(2)}$ is irreducible, then \mathcal{G} is 2-transitive and primitive.
- (3) Otherwise, use Step 2 of Algorithm 4.2 to obtain the decomposition of $(f^{-1}(p))^2$ into \mathcal{G} -orbits, and construct the graphs $\Gamma_{\mathcal{O}}$ of Subsection 2.1.
- (4) Then \mathcal{G} is primitive if and only if all graphs $\Gamma_{\mathcal{O}}$ are connected when \mathcal{O} is not the diagonal.

Proof of correctness. This follows by Higman’s Theorem (Proposition 2.2). □

Remark 4.4. Algorithm 4.1 to compute \mathcal{G} using fiber products will be infeasible in practice: Even if we have $C \subset \mathbb{P}^1 \times \ell$, then $C^{(k-1)} \subset (\mathbb{P}^1)^{k-1} \times \ell$, a curve in a k -dimensional space. Such a formulation would have very high degree, as $C \subset \mathbb{P}^1 \times \ell$ would be defined by a polynomial of degree at least k . Worse than this possibly high dimension and degree of polynomials is that the degree of $C^{(k-1)} \rightarrow \ell$ will be $k!$ with each irreducible component having degree $|\mathcal{G}|$. For the computation in Subsection 5.1, $k = 26$ and $\mathcal{G} = 2^{13} \cdot 13! \approx 5 \times 10^{13}$.

Nevertheless, the interesting transitive permutation groups will fail to be s -transitive for $s \leq 5$ (Proposition 2.1), and interesting characteristics of that action may be discovered through studying $C^{(2)}$ using Algorithm 4.3, as shown in the Introduction.

4.1. Lines on a cubic surface. We briefly review the configuration of the 27 lines on a cubic surface, and what we expect from the decomposition of $V^{(s)}$ for $s = 2, 3$. This is classical and may be found in many sources such as [13, pp. 480–489].

Let p_1, \dots, p_6 be six points in \mathbb{P}^2 not lying on a conic and with no three collinear. The space of cubics vanishing at p_1, \dots, p_6 is four-dimensional and gives a rational map $\mathbb{P}^2 - \rightarrow \mathbb{P}^3$ whose image is a cubic surface S that is isomorphic to \mathbb{P}^2 blown up at the six points p_1, \dots, p_6 . That is, S contains six lines $\widehat{p}_1, \dots, \widehat{p}_6$ and has a map $\pi: S \rightarrow \mathbb{P}^2$ that sends the line \widehat{p}_i to p_i and is otherwise an isomorphism. The points of the line \widehat{p}_i correspond to tangent directions in \mathbb{P}^2 at p_i , and the *proper transform* of a line or curve in \mathbb{P}^2 is its inverse image under π , with its tangent directions at p_i (points in \widehat{p}_i) lying above p_i , for each i . This surface S contains 27 lines as follows.

- Six are the blow ups \widehat{p}_i of the points p_i for $i = 1, \dots, 6$.
- Fifteen ($= \binom{6}{2}$) are the proper transforms $\widehat{\ell}_{ij}$ of the lines through two points p_i and p_j for $1 \leq i < j \leq 6$.
- Six are the proper transforms \widehat{C}_i of the conics through five points $\{p_1, \dots, p_6\} \setminus \{p_i\}$ for $i = 1, \dots, 6$.

Figure 6 gives a configuration of six points in \mathbb{P}^2 , together with three of the lines and one of the conics they determine, showing some points of intersection.

Each line λ on S is disjoint from 16 others and meets the remaining ten. With these ten, λ forms five triangles—the plane Π containing any two lines λ, μ on S that meet will contain a third line ν on S as $\Pi \cap S$ is a plane cubic curve containing λ and μ .

We explain this in detail for the lines $\widehat{p}_1, \widehat{\ell}_{12}$, and \widehat{C}_1 .

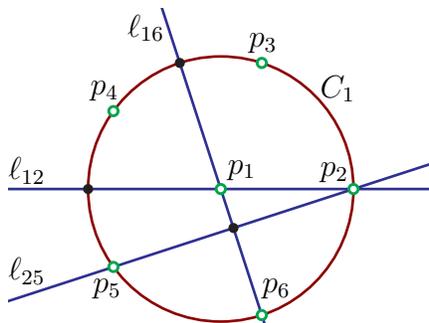


FIGURE 6. Six points, some lines, and a conic.

- The line \widehat{p}_1 is disjoint from \widehat{p}_i for $2 \leq i \leq 6$ as the points are distinct. It is disjoint from $\widehat{\ell}_{ij}$ for $2 \leq i < j \leq 6$, as no such line ℓ_{ij} meets p_1 , and it is disjoint from \widehat{C}_1 , as $p_1 \notin C_1$. The line \widehat{p}_1 does meet the lines \widehat{C}_i and $\widehat{\ell}_{1i}$ for $2 \leq i \leq 6$, as p_1 lies on these conics C_i and lines ℓ_{1i} .
- The line $\widehat{\ell}_{12}$ is disjoint from the lines \widehat{p}_i , $\widehat{\ell}_{1i}$, $\widehat{\ell}_{2i}$, and \widehat{C}_i , for $3 \leq i \leq 6$. We have seen this for the \widehat{p}_i . For the lines, $\widehat{\ell}_{1i}$ and $\widehat{\ell}_{2i}$, this is because ℓ_{12} meets the lines ℓ_{1i} and ℓ_{2i} at the points p_1 and p_2 , but it has a different slope at each point, and the same is true for the conic C_i . We have seen that $\widehat{\ell}_{12}$ meets both \widehat{p}_1 and \widehat{p}_2 . It also meets $\widehat{\ell}_{ij}$ for $2 \leq i < j \leq 6$, as well as \widehat{C}_1 , and \widehat{C}_2 , because ℓ_{12} meets the underlying lines and conics at points outside of p_1, \dots, p_6 . (See Figure 6.)
- Finally, the line \widehat{C}_1 is disjoint from \widehat{p}_1 , from $\widehat{\ell}_{ij}$ for $2 \leq i < j \leq 6$, and from \widehat{C}_i for $2 \leq i \leq 6$. The last is because C_1 meets each of those conics in four of the points p_2, \dots, p_6 and no other points. As we have seen, \widehat{C}_1 meets \widehat{p}_i and $\widehat{\ell}_{1i}$ for $2 \leq i \leq 6$.

We describe the decomposition of $V^{(2)}$ and $V^{(3)}$. Let $V^{[2]}$ be the closure in $V_{\mathbb{P}^{19}}^2$ of its restriction to $\mathbb{P}^{19} \setminus B$. Let $p \in \mathbb{P}^{19} \setminus B$. The fiber $f^{-1}(p)$ in $V^{[2]}$ consists of the $27^2 = 729$ pairs (λ, μ) of lines λ, μ that lie on the cubic given by p . The variety $V^{[2]}$ has degree 729 over \mathbb{P}^{19} and decomposes into three subvarieties. We describe typical points (λ, μ) in the fibers of each.

- (1) The diagonal Δ , whose points are pairs where $\lambda = \mu$. It has degree 27, is irreducible and isomorphic to V .
- (2) The set of disjoint pairs, D , whose points are pairs of disjoint lines (λ, μ) where $\lambda \cap \mu = \emptyset$. It has degree $27 \cdot 16 = 432$ over \mathbb{P}^{19} .
- (3) The set of incident pairs, I , whose points are pairs of incident lines (λ, μ) where $\lambda \cap \mu \neq \emptyset$. It has degree $27 \cdot 10 = 270$ over \mathbb{P}^{19} .

In particular, since $V^{(2)}$ decomposes into two components, which we verified using a numerical irreducible decomposition via Bertini [4], the action of \mathcal{G} fails to be 2-transitive.

However, \mathcal{G} is primitive, which may be seen using Algorithm 4.3 and Higman's Theorem (Proposition 2.2). As V is irreducible, \mathcal{G} is transitive. Since D is irreducible, the 216 unordered pairs of disjoint lines form an orbit \mathcal{D} of \mathcal{G} . The graph $\Gamma_{\mathcal{D}}$ is connected. Indeed, the only non-neighbors of \widehat{p}_1 are \widehat{C}_j and $\widehat{\ell}_{1j}$ for $2 \leq j \leq 6$. As \widehat{C}_j is disjoint from \widehat{C}_1 and $\widehat{\ell}_{1j}$ is disjoint from \widehat{p}_i for $i \neq 1, j$, and \widehat{p}_1 is disjoint from both \widehat{C}_1 and \widehat{p}_i , $\Gamma_{\mathcal{D}}$ is connected (and has diameter two). Similarly, as I is irreducible, the pairs of incident lines form a single orbit whose associated graph may be checked to have diameter two.

The decomposition of $V^{(3)}$ has eight components, which we verified using a numerical irreducible decomposition via Bertini [4]. These components have four different types up to the action of S_3 on triples.

- (1) Triangles, τ . The typical point of τ is a triangle, three distinct lines that meet each other. This has degree 270 over \mathbb{P}^{19} and is a component of $I \times_{\mathbb{P}^{19}} V$.
- (2) Mutually skew triples, σ . The typical point of σ is three lines, none of which meet each other. This has degree 4320 over \mathbb{P}^{19} , and is a component of $D \times_{\mathbb{P}^{19}} V$.
- (3) There are three components ρ_i consisting of triples $(\lambda_1, \lambda_2, \lambda_3)$ of lines where the i th line does not meet the other two, but those two meet. Each has degree 2160 over \mathbb{P}^{19} and μ_3 is a component of $I \times_{\mathbb{P}^{19}} V$.
- (4) There are three components ξ_i consisting of triples $(\lambda_1, \lambda_2, \lambda_3)$ of lines where the i th line meets the other two, but those two do not meet. Each has degree 2160 over \mathbb{P}^{19} and μ_3 is a component of $D \times_{\mathbb{P}^{19}} V$.

5. GALOIS GROUPS IN APPLICATIONS

We present three problems from applications that have interesting Galois groups, which we compute using our methods.

5.1. Formation shape control. Anderson and Helmke [2] consider a least-squares solution to a problem of placing agents at positions $x_1, \dots, x_N \in \mathbb{R}^d$ having preferred pairwise distances $u_{ij} = u_{ji}$ for $1 \leq i, j \leq N$, that is, minimizing the potential

$$\Psi_u := \sum_{i,j} (\|x_i - x_j\|^2 - u_{ij}^2)^2.$$

They specialize to points on a line $d = 1$ and eliminate translational ambiguity by setting $x_N = 0$. Then they relax the problem to finding the complex critical points of the gradient descent flow given by Ψ_u . This yields the system of cubic equations

$$0 = \sum_{j=1}^N ((x_i - x_j)^2 - u_{ij}^2)(x_i - x_j) \quad i = 1, \dots, N-1, \quad x_N = 0.$$

Thus when $N \geq 4$ there are at most 3^{N-1} isolated complex solutions for general u_{ij} , one of which is degenerate: $x_i = 0$ for all i with the agents collocated at the origin. When the u_{ij} are real, there are always at least $2N-1$ real critical formations. The symmetry $x_i \mapsto -x_i$ reflecting in the origin gives an involution acting freely on the nondegenerate solutions. This commutes with complex conjugation and implies that there is an additional congruence modulo four in the number of real solutions (compare to [17, 18]).

We compute the Galois group when $N = 4$. Anderson and Helmke show that the upper bound of 27 critical points is obtained for general u_{ij} , with 26 nondegenerate solutions having no two agents collocated. They also show that all possible numbers of real critical points (not including the origin), 6, 10, 14, 18, 22, 26 between $6 = 2N - 2$ and 26 that are congruent to 6 modulo four do indeed occur. The symmetry $x_i \mapsto -x_i$ implies that the Galois group preserves the partition of the solutions into the pairs $\{x_i, -x_i\}$, which implies that it is a subgroup of the wreath product $S_2 \text{Wr } S_{13}$, which has order $51,011,754,393,600 = 2^{13} \cdot 13!$.

The Branch Point Algorithm shows that the Galois group of this system is indeed equal to the wreath product $S_2 \text{Wr } S_{13}$. We found this by computing 144 critical points that map two-to-one to the 72 branch points. Taking loops around each of the 72 branch points can

be performed in under a minute using one processor on a laptop. Interestingly, while most critical points were simple in that their local monodromy was a 2-cycle, several were not.

5.2. Alt-Burmester 4-bar examples. In 1886, Burmester [8] considered the synthesis problem for planar four-bar linkages based on motion generation, specifying poses along a curve. Alt [1] proposed synthesis problems based on path generation, specifying positions along a curve. The synthesis problem consisting of some poses and some positions was called an Alt-Burmester problem in [35] with the complete solution to all Alt-Burmester problems described in [6]. We compute the Galois group for four of the Alt-Burmester problems having finitely many solutions.

Figure 7 illustrates these problems. A *four-bar linkage* is a quadrilateral with one side fixed and four rotating joints. A triangle is erected on the side opposite the fixed side, and a tool is mounted on the apex of the triangle with a particular orientation. A pose is a position

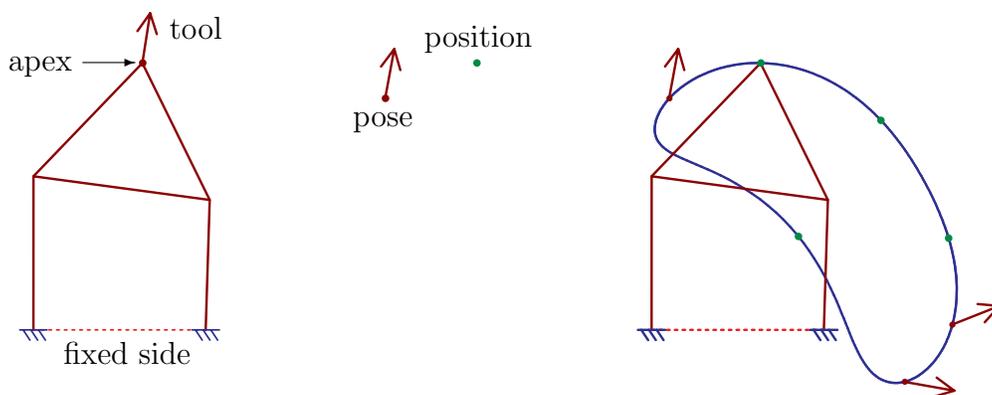


FIGURE 7. A linkage, poses, positions, and a solution for 3 poses and 4 positions.

together with an orientation for the tool. Specifying M poses and $N = 10 - 2M$ positions, there will generically be finitely many linkages that take on the given poses and whose apex can pass through the given positions in its motion.

Following [6] in isotropic coordinates, the M -pose and N -position Alt-Burmester problem is described by the following parameters:

$$\begin{aligned} \text{positions:} & \quad (D_j, \bar{D}_j), \text{ for } j = 1, \dots, M+N \\ \text{orientations:} & \quad (\Theta_j, \bar{\Theta}_j), \text{ for } j = 1, \dots, M \text{ with } \Theta_j \bar{\Theta}_j = 1. \end{aligned}$$

With variables $G_1, G_2, z_1, z_2, \bar{G}_1, \bar{G}_2, \bar{z}_1, \bar{z}_2, \Theta_j, \bar{\Theta}_j$ for $j = M+1, \dots, M+N$, we consider

$$\begin{aligned} L_{rj} \bar{L}_{rj} - L_{r1} \bar{L}_{r1} &= 0, \text{ for } j = 2, \dots, M+N \text{ and } r = 1, 2 \\ \Theta_j \bar{\Theta}_j - 1 &= 0, \text{ for } j = M+1, \dots, M+N \end{aligned}$$

where

$$L_{rj} := \Theta_j z_r + D_j - G_r \text{ and } \bar{L}_{rj} = \bar{\Theta}_j \bar{z}_r + \bar{D}_j - \bar{G}_r.$$

We first consider the classical case studied by Burmester, namely $M = 5$ and $N = 0$. As noted by Burmester, the system of 8 polynomials, using modern terminology, is a fiber product since the synthesis problem for four-bar linkages uncouples into two synthesis problems for so-called RR dyads (left- and right- halves of the linkage). Each RR dyad synthesis

problem has 4 solutions with Galois group S_4 . Thus, the polynomial system for the four-bar linkage synthesis problem has 16 solutions which decomposes into two components: 4 points on the diagonal Δ and 12 disjoint pairs. The Branch Point Algorithm uses homotopy continuation to track a loop around each of the 64 branch points. These loops yield the permutations listed in Figure 8. Cycles involving the first four solutions are in **boldface**, to help

(1,2,3,4) (5,8,13,15)(6,10,12,16)(7,9,11,14),	(3,4) (5,14)(6,15)(7,16)(8,9)(12,13),
(1,2,4,3) (5,16,8,11)(6,14,9,12)(7,15,10,13),	(2,3) (5,7)(8,10)(11,15)(12,14)(13,16),
(1,3,2,4) (5,9,15,12)(6,8,14,13)(7,10,16,11),	(1,3) (6,7)(8,15)(9,16)(10,14)(11,12),
(1,4,2,3) (5,12,15,9)(6,13,14,8)(7,11,16,10),	(1,2) (5,6)(8,12)(9,13)(10,11)(14,15),
(1,3)(2,4) (5,13)(6,12)(7,11)(8,15)(9,14)(10,16),	(2,4) (5,13)(6,11)(7,12)(9,10)(14,16),
(1,4)(2,3) (5,8)(6,9)(7,10)(11,16)(12,14)(13,15),	(1,4) (5,10)(6,9)(7,8)(11,13)(15,16),
(1,4,3) (5,14,10)(6,16,8)(7,15,9)(11,13,12),	(2,3,4) (5,12,16)(6,11,15)(7,13,14)(8,9,10),
(1,2,3) (5,7,6)(8,11,14)(9,13,16)(10,12,15),	(1,2,4) (5,9,11)(6,10,13)(7,8,12)(14,16,15),
(2,4,3) (5,16,12)(6,15,11)(7,14,13)(8,10,9),	(1,3,4) (5,10,14)(6,8,16)(7,9,15)(11,12,13),

FIGURE 8. Monodromy permutations for Burmester 5-0.

see that these solutions are permuted amongst themselves while the other twelve solutions are permuted amongst themselves. This shows that the Galois group of each component and of their union is also S_4 . For the off-diagonal component, it is the action of S_4 on ordered pairs of numbers $\{1, 2, 3, 4\}$.

The remaining three cases under consideration are $(M, N) = (4, 2), (3, 4), (2, 6)$ which have 60, 402, and 2224 isolated solutions, respectively [6, Table 1]. In each, the left-right symmetry of the mechanism ($r = 1, 2$ above) implies that the Galois group of a problem with $k = 2m$ solutions will be a subgroup of the group $S_2 \text{Wr } S_m$ of order $2^m m!$. We applied the Branch Point Algorithm first to the Alt-Burmester problem with $M = 4$ and $N = 2$. We tracked a loop around each of the 2094 branch points to compute generators of the Galois group, thereby showing the Galois group has order

$$284\,813\,089\,515\,958\,324\,736\,640\,819\,941\,867\,520\,000\,000 = 2^{30} \cdot 30!,$$

and is thus the full wreath product $S_2 \text{Wr } S_{30}$. This Galois group is the largest it could be given the left-right symmetry.

For each of the cases when (M, N) is $(3, 4)$ and $(2, 6)$ we computed ten random permutations, which was sufficient to show that the Galois groups of these problems are indeed equal to $S_2 \text{Wr } S_{201}$ and $S_2 \text{Wr } S_{1112}$ having order $2^{201} \cdot 201! \approx 5 \cdot 10^{437}$ and $2^{1112} \cdot 1112! \approx 10^{3241}$, respectively.

5.3. Algebraic statistics example. Maximum likelihood estimation on a discrete algebraic statistical model \mathcal{M} involves maximizing the likelihood function $\ell_u(p) := p_0^{u_0} p_1^{u_1} \cdots p_n^{u_n}$ for data consisting of positive integers u_0, \dots, u_n restricted to the model. The model \mathcal{M} is defined by polynomial equations in the probability simplex, which is the subset of \mathbb{R}^{n+1} where $p_0 + \cdots + p_n = 1$ and $p_i \geq 0$. We consider the Zariski closure of \mathcal{M} in \mathbb{P}^n (also written \mathcal{M}), as $p_0 + \cdots + p_n = 1$ defines an affine open subset of \mathbb{P}^n .

The variety V of critical points of ℓ_u on the model \mathcal{M} lies in $\mathbb{P}_p^n \times \mathbb{P}_u^n$. This is the Zariski closure of points (p, u) where p is a smooth point of \mathcal{M} and a critical point of ℓ_u . Then V is n -dimensional and irreducible, and its projection to \mathbb{P}_u^n gives a branched cover whose degree

is the *maximum likelihood degree* [21, 22]. For an algebraic statistical model, we can ask for the Galois group of this maximum likelihood estimation (the branched cover $V \rightarrow \mathbb{P}^n$).

The model defined by the determinant (4) has maximum likelihood degree 6, and has a Galois group that is a proper subgroup of the full symmetric group S_6 [15].

$$(4) \quad \det \begin{pmatrix} 2p_{11} & p_{12} & p_{13} \\ p_{21} & 2p_{22} & p_{23} \\ p_{13} & p_{23} & 2p_{33} \end{pmatrix} = 0.$$

Using the Branch Point Algorithm, we solve a system of equations to find 24 critical points of the projection (note the difference between critical points of the likelihood function and critical points of the projection). The critical points of the projection map 2 to 1 to a set of 12 branch points yielding a witness set for the branch point locus which is a component of the data discriminant¹. The Branch Point Algorithm finds the following generating set of the Galois group, which has order $4! = 24$ and is isomorphic to S_4 :

$$\{ (12)(34), (26)(45), (14)(23), (15)(36), (16)(35), (126)(345) \}.$$

The reason for the interesting Galois group is explained by maximum likelihood duality [11]. Moreover, in [27, § 5], it is shown that over a real data point, a typical fiber has either 2 or 6 real points. This further strengthens the notion that degenerate Galois groups can help identify the possibility of interesting real structures.

6. CONCLUSION

We have given algorithms to compute Galois groups. The main contributions are two numerical algorithms [Algorithm 3.3 and 4.2], that allow for practical computation of Galois groups. The first algorithm, the Branch Point Algorithm, has been implemented in `Macaulay2` building on monodromy computations performed by `Bertini` and is publicly available. Moreover, we have shown its effectiveness in examples ranging from enumerative geometry, kinematics, and statistics. The other algorithm uses fiber products to test for s -transitivity. This is practical as permutation groups that are not alternating or symmetric are at most 5-transitive (and $k \leq 24$). These two algorithms demonstrate that homotopy continuation can be used to compute Galois groups.

REFERENCES

- [1] H. Alt. Über die erzeugung gegebener ebener kurven mit hilfe des gelenkviereckes. *Zeitschrift für Angewandte Mathematik und Mechanik*, 3(1):13–19, 1923.
- [2] B.D.O. Anderson and U. Helmke. Counting critical formations on a line. *SIAM Journal on Control and Optimization*, 52(1):219–242, 2014.
- [3] D.J. Bates, E. Gross, A. Leykin, and J.I. Rodriguez. Bertini for Macaulay2. *preprint arXiv:1310.3297*, 2013.
- [4] D.J. Bates, J.D. Hauenstein, A.J. Sommese, and C.W. Wampler. Bertini: Software for numerical algebraic geometry. Available at <http://bertini.nd.edu>.
- [5] D.J. Bates, J.D. Hauenstein, A.J. Sommese, and C.W. Wampler. *Numerically solving polynomial systems with Bertini*, volume 25 of *Software, Environments, and Tools*. Society for Industrial and Applied Mathematics (SIAM), Philadelphia, PA, 2013.

¹ The defining polynomial of degree 12 was computed in [27, Ex. 6] and is available at the website <https://sites.google.com/site/rootclassification/publications/DD>.

- [6] D.A. Brake, J.D. Hauenstein, A.P. Murray, D.H. Myszka, and C.W. Wampler. The complete solution of Alt-Burmester synthesis problems for four-bar linkages. *Journal of Mechanisms and Robotics*, 8(4):041018, 2016.
- [7] C. Brooks, A. Martín del Campo, and F. Sottile. Galois groups of Schubert problems of lines are at least alternating. *Trans. Amer. Math. Soc.*, 367:4183–4206, 2015.
- [8] L. Burmester. *Lehrbuch der Kinematic*. Verlag Von Arthur Felix, Leipzig, Germany, 1886.
- [9] P.J. Cameron. *Permutation groups*, volume 45 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1999.
- [10] A. Dimca. *Singularities and topology of hypersurfaces*. Universitext. Springer-Verlag, New York, 1992.
- [11] J. Draisma and J. I. Rodriguez. Maximum likelihood duality for determinantal varieties. *International Mathematics Research Notices*, 2014(20):5648–5666, 2014.
- [12] D.R. Grayson and M.E. Stillman. Macaulay2, a software system for research in algebraic geometry. Available at <http://www.math.uiuc.edu/Macaulay2/>.
- [13] P. Griffiths and J. Harris. *Principles of algebraic geometry*. Wiley Classics Library. John Wiley & Sons, Inc., New York, 1994. Reprint of the 1978 original.
- [14] J. Harris. Galois groups of enumerative problems. *Duke Math. J.*, 46:685–724, 1979.
- [15] J.D. Hauenstein, J.I. Rodriguez, and B. Sturmfels. Maximum likelihood for matrices with rank constraints. *Journal of Algebraic Statistics*, 5:18–38, 2014.
- [16] J.D. Hauenstein and A.J. Sommese. Witness sets of projections. *Appl. Math. Comput.*, 217(7):3349–3354, 2010.
- [17] N. Hein, F. Sottile, and I. Zelenko. A congruence modulo four for real Schubert calculus with isotropic flags, 2016. *Canadian Mathematical Bulletin*, to appear.
- [18] N. Hein, F. Sottile, and I. Zelenko. A congruence modulo four in real schubert calculus, 2016. *Journal für die reine und angewandte Mathematik*, to appear.
- [19] C. Hermite. Sur les fonctions algébriques. *CR Acad. Sci.(Paris)*, 32:458–461, 1851.
- [20] D.G. Higman. Intersection matrices for finite permutation groups. *J. Algebra*, 6:22–42, 1967.
- [21] S. Hoşten, A. Khetan, and B. Sturmfels. Solving the likelihood equations. *Found. Comput. Math.*, 5(4):389–407, 2005.
- [22] J. Huh and B. Sturmfels. Likelihood geometry. In *Combinatorial algebraic geometry*, volume 2108 of *Lecture Notes in Math.*, pages 63–117. Springer, 2014.
- [23] C. Jordan. *Traité des Substitutions*. Gauthier-Villars, Paris, 1870.
- [24] A. Leykin and F. Sottile. Galois groups of Schubert problems via homotopy computation. *Math. Comp.*, 78(267):1749–1765, 2009.
- [25] A. Martín del Campo and F. Sottile. Experimentation in the Schubert calculus. [arXiv.org/1308.3284](https://arxiv.org/abs/1308.3284), 2016. to appear in *Schubert Calculus—Osaka 2012*, ed. by H.Naruse, T.Ikeda, M.Masuda, and T.Tanisaki, Advanced Studies in Pure Mathematics, Mathematical Society of Japan.
- [26] D.K. Molzahn, M. Niemerg, D. Mehta, and J.D. Hauenstein. Investigating the maximum number of real solutions to the power flow equations: Analysis of lossless four-bus systems. [arXiv/org:1603.05908](https://arxiv.org/abs/1603.05908), 2016.
- [27] J.I. Rodriguez and X. Tang. Data-discriminants of likelihood equations. In *Proceedings of the 2015 ACM on International Symposium on Symbolic and Algebraic Computation, ISSAC '15*, pages 307–314, New York, NY, USA, 2015. ACM.
- [28] J. Ruffo, Y. Sivan, E. Soprunova, and F. Sottile. Experimentation and conjectures in the real Schubert calculus for flag manifolds. *Experiment. Math.*, 15(2):199–221, 2006.
- [29] L.L. Scott. Representations in characteristic p . In *The Santa Cruz Conference on Finite Groups (Univ. California, Santa Cruz, Calif., 1979)*, volume 37 of *Proc. Sympos. Pure Math.*, pages 319–331. Amer. Math. Soc., Providence, R.I., 1980.
- [30] A.J. Sommese, J. Verschelde, and C.W. Wampler. Introduction to numerical algebraic geometry. In *Solving polynomial equations*, volume 14 of *Algorithms Comput. Math.*, pages 301–335. Springer, Berlin, 2005.
- [31] A.J. Sommese and C.W. Wampler. Numerical algebraic geometry. In *The mathematics of numerical analysis (Park City, UT, 1995)*, volume 32 of *Lectures in Appl. Math.*, pages 749–763. Amer. Math. Soc., Providence, RI, 1996.

- [32] A.J. Sommese and C.W. Wampler. *The numerical solution of systems of polynomials*. World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ, 2005.
- [33] A.J. Sommese and C.W. Wampler. Exceptional sets and fiber products. *Found. Comput. Math.*, 8(2):171–196, 2008.
- [34] F. Sottile and J. White. Double transitivity of Galois groups in Schubert calculus of Grassmannians. *Algebr. Geom.*, 2(4):422–445, 2015.
- [35] Y. Tong, D.H. Myszka, and A.P. Murray. Four-bar linkage synthesis for a combination of motion and path-point generation. *Proceedings of the ASME International Design Engineering Technical Conferences, DETC2013-12969*, 2013.
- [36] R. Vakil. Schubert induction. *Ann. of Math. (2)*, 164(2):489–512, 2006.
- [37] O. Zariski. A theorem on the Poincaré group of an algebraic hypersurface. *Annals of Mathematics*, 38(1):131–141, 1937.

DEPARTMENT OF APPLIED & COMPUTATIONAL MATHEMATICS & STATISTICS, UNIVERSITY OF NOTRE DAME, NOTRE DAME, IN 46556, USA

E-mail address: `hauenstein@nd.edu`

URL: `http://www.nd.edu/~jhauenst`

DEPARTMENT OF STATISTICS, UNIVERSITY OF CHICAGO, CHICAGO, IL 60637, USA

E-mail address: `JoIsRo@uchicago.edu`

URL: `http://home.uchicago.edu/~joisro`

DEPARTMENT OF MATHEMATICS, TEXAS A&M UNIVERSITY, COLLEGE STATION, TX 77843, USA

E-mail address: `sottile@math.tamu.edu`

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