Numerical Computation of Galois Groups

Jonathan D. Hauenstein · Jose Israel Rodriguez · Frank Sottile

Received: 28 May 2016 / Revised: 29 April 2017 / Accepted: 5 May 2017 / Published online: 14 June 2017
© SFoCM 2017

Abstract The Galois/monodromy group of a family of geometric problems or equations is a subtle invariant that encodes the structure of the solutions. 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 studies 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.

Communicated by J E Cremona.

Research of Hauenstein supported in part by NSF Grant ACI-1460032, Sloan Research Fellowship BR2014-110 TR14, and Army Young Investigator Program (YIP) W911NF-15-1-0219. Research of Rodriguez supported in part by NSF Grant DMS-1402545. Research of Sottile supported in part by NSF Grant DMS-1501370.

Jose Israel Rodriguez
JoIsRo@uchicago.edu
http://home.uchicago.edu/~joisro

Jonathan D. Hauenstein
hauenstein@nd.edu
http://www.nd.edu/~jhauenst

Frank Sottile
sottile@math.tamu.edu
http://www.math.tamu.edu/~sottile/

1 Department of Applied and Computational Mathematics and Statistics, University of Notre Dame, Notre Dame, IN 46556, USA
2 Department of Statistics, University of Chicago, Chicago, IL 60637, USA
3 Department of Mathematics, Texas A & M University, College Station, TX 77843, USA
Keywords  Galois group · Monodromy · Fiber product · Homotopy continuation · Numerical algebraic geometry · Polynomial system

Mathematics Subject Classification 65H10 · 65H20 · 14Q15

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 \( f : V \to U \) 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 \([16,22]\). When \( U \) is rational, \( f : V \to U \) 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. In \([27]\) several Schubert problems were shown to have Galois group the full symmetric group by computing monodromy permutations along random loops in the base \( U \). This method computes an increasing sequence of subgroups, which can determine the Galois group only when it is the full symmetric group. In all other cases, it lacks a stopping criterion.

We offer two additional numerical methods to study Galois groups. For the first, we suppose that \( U \) is a rational variety. Then, the branch locus of the map \( f : V \to U \) is a hypersurface \( B \subset U \). Numerical algebraic geometry represents \( B \) by a projective line \( \ell \) in \( U \) meeting \( B \) transversally in finitely many points \( W = B \cap \ell \), called a witness set. Restricting \( V \) to \( \ell \) gives a curve \( C \) mapping to \( \ell \) whose monodromy group equals that of \( f : V \to U \). This group is generated by permutations coming from loops in \( \ell \) encircling each point of \( W \). See also \([13,30]\), which discuss computing monodromy of curves.

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 \( s = k-1 \), where \( k \) is the degree of the branched cover, this computes the Galois group. Partial information obtained for \( s < k-1 \) is often 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 \( C \to \mathbb{C}_t \) is four-to-one for \( t \notin B = \{0,4\} \). The fiber above the point \( t = 3 \) is \( \{-\sqrt{3}, -1, 1, \sqrt{3}\} \) (Fig. 1). Following these points along a loop in \( \mathbb{C}_t \) based on \( t = 3 \) 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.

The fiber product \(C \times_{C_t} C\) 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 irreducible components. One is the diagonal defined by \(x - y\) and \(x^4 - 4x^2 + t\). The off-diagonal has two components, which implies that the Galois group \(G\) action 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 \(G\) acting on ordered pairs of solutions (Fig. 1). This implies that \(G\) acts imprimitively as it fixes the partition \(\{-\sqrt{3}, \sqrt{3}\} \cup \{-1, 1\}\). Thus, \(G \subset S_4\) contains no 3-cycle, so \(G \subset D_4\). 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, \(G\) has an orbit of cardinality eight and so \(|G| \geq 8\), which implies that \(G = D_4\).

The systematic study of Galois groups of geometric problems and equations from applications is in its infancy. In nearly every known case [8, 16, 26–29, 33, 39, 41], the Galois group exhibits a striking dichotomy: either it 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 [29] to further investigate Galois groups, and we expect they will help to develop Galois groups as a tool to study geometric problems, including those from applications.

We sketch background in Sect. 2, including permutation groups, Galois groups, fundamental groups, fiber products, homotopy continuation, and witness sets. In Sect. 3, we discuss the method of computing monodromy by determining the branch locus, illustrating this on the classical problem of 27 lines on a cubic surface. In Sect. 4, we discuss using fiber products to obtain information about the Galois group, illustrating this with the monodromy action on the 27 lines. We further illustrate these methods using three examples from applications in Sect. 5, and we give concluding remarks in Sect. 6.
2 Galois Groups and Numerical Algebraic Geometry

We sketch 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 \( G \) be a subgroup of the symmetric group \( S_k \) on \( k \) letters. Then, \( G \) acts faithfully on \( \mathbb{C}^k := \{1, \ldots, c \} \). Write \( g(i) \) for the image of \( i \in [k] \) under \( g \in G \). The action is transitive if for any \( i, j \in [k] \) there is an element \( g \in G \) with \( g(i) = j \).

The group \( G \) has an induced action on \( s \)-tuples, \( [k]^s \). The action is \( s \)-transitive if for any two \( s \)-tuples \( (i_1, \ldots, i_s) \) and \( (j_1, \ldots, j_s) \) of distinct elements, there is a \( g \in G \) with \( g(i_r) = j_r \) for \( r = 1, \ldots, s \). The 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 [10, Section 4] and summarized in the following proposition, which follows from the O’Nan-Scott Theorem [34] and the classification of finite simple groups.

**Proposition 2.1** (Thm. 4.11 [10]) 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 [10] list the \( 2 \)-transitive permutation groups.

Suppose that \( G \) is transitive on \([k]\). A block is a subset \( B \) of \([k]\) such that for every \( g \in G \) either \( gB = B \) or \( gB \cap B = \emptyset \). The orbits of a block form a \( G \)-invariant partition of \([k]\) into blocks. The group \( G \) 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 [10, Section 4.9].

Each \( G \)-orbit \( O \subset [k]^2 \) determines a graph \( \Gamma_O \) with vertex set \([k]\)—its edges are the pairs in \( O \). 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 [10, Section 1.11]).

**Proposition 2.2** (Higman’s Theorem [23]) A transitive group \( G \) is primitive if and only if for each nondiagonal orbit \( O \subset [k]^2 \), the graph \( \Gamma_O \) 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 \( G \)-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. 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

Suppose that $f : V \to U$ is a dominant map ($f(V) = U$) between irreducible complex algebraic varieties of the same dimension. The function field $\mathbb{C}(V)$ of $V$ is a finite extension of $f^*\mathbb{C}(U)$, the pullback of the function field of $U$. The degree of this extension is the cardinality $k$ of a general fiber of $f$. The Galois group $\mathcal{G}(V \to U)$ of $f : V \to U$ is the Galois group of the Galois closure of $\mathbb{C}(V)$ over $f^*\mathbb{C}(U)$.

This is also a monodromy group. A map $f : V \to U$ as in the previous paragraph is a branched cover. Its branch locus $B$ is the set of points $u \in U$ such that $f^{-1}(u)$ does not consist of $k$ reduced points. Then, $f : f^{-1}(U \setminus B) \to U \setminus B$ 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 $\mathcal{G}(V \to U)$. Hermite [22] realized that Galois and monodromy groups coincide and Harris [16] 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 [41, Section 3.5]). For each $2 \leq s \leq k$ let $V_s^U$ be the $s$-fold fiber product,

$$V_s^U := V \times_U V \times_U \cdots \times_U V.$$

We also write $f$ for the map $V_s^U \to U$. The fiber of $V_s^U$ over a point $u \in U$ is $(f^{-1}(u))^s$, the set of $s$-tuples of points in $f^{-1}(u)$. Over $U \setminus B$, $V_s^U$ is a covering space of degree $k^s$. This is decomposable, and among its components are those lying in the big diagonal $\Delta$, where some coordinates of the $s$-tuples coincide. Define $V^{(s)}$ to be the closure in $V_s^U$ 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 $f^{-1}(u)$.

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

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

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

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

The function field of any component of $V^{(k)}$ is the Galois closure of $\mathbb{C}(V)$ over $f^*\mathbb{C}(U)$, and $V^{(k)}$ is the geometric counterpart of the usual construction of a Galois
closure by adjoining successive roots of an irreducible polynomial. By Proposition 2.4, $G = G(V \to U)$ is determined by any irreducible component of $V^{(k)}$. In fact $V^{(k-1)}$ suffices as $V^{(k)} \simeq V^{(k-1)}$. Other properties of $G$ as a permutation group are encoded in fiber products.

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

**Proof** This is essentially Lemma 1 of [39].

2.3 Fundamental Groups of Complements

Let $B \subset \mathbb{P}^n$ be a hypersurface and $\ell \subset \mathbb{P}^n$ be a line that meets $B$ transversally. Zariski [42] showed that the map of fundamental groups

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

is a surjection. Here, $\iota$ is the inclusion $\ell \setminus B \hookrightarrow \mathbb{P}^n \setminus B$. (See also [11, Prop. 3.3.1].)

Suppose that $B \cap \ell = \{b_1, \ldots, b_d\}$ and let $p \in \ell \setminus B$ be the base point. For each $i = 1, \ldots, d$, let $D_i$ be a closed disk in $\ell \simeq \mathbb{C}P^1$ centered at $b_i$ with $D_i \cap B = \{b_i\}$. Choose any path in $\ell \setminus B$ from $p$ to the boundary $\partial D_i$ of $D_i$ and let $\gamma_i$ be the loop based on $p$ that follows that path, traverses the boundary of $D_i$ once anticlockwise, and then returns to $p$ along the chosen path. Any loop in $\ell \setminus B$ based on $p$ that is homotopy-equivalent to $\gamma_i$ (for some choice of path from $p$ to $\partial D_i$) 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 $B \cap \ell$.

**Proposition 2.6** Let $B \subset \mathbb{P}^n$ be a hypersurface. If $\ell \subset \mathbb{P}^n$ is any line that meets $B$ transversally, then any set of based loops in $\ell$ encircling each point in $B \cap \ell$ generates the fundamental group of the complement, $\pi_1(\mathbb{P}^n \setminus B)$.

2.4 Homotopy Continuation and Monodromy

A homotopy $H$ is a polynomial map $H : \mathbb{C}^n \times \mathbb{C}_t \to \mathbb{C}^n$ that defines a curve $C \subset H^{-1}(0)$ which maps dominantly to $\mathbb{C}_t$. Write $f : C \to \mathbb{C}_t$ for this map. We assume that the inverse image 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 for $t \neq 0$. Given a point $(x, 1)$ of $C$, standard predictor-corrector methods construct a sequence of points $(x_i, t_i)$ where $x_0 = x$ and $1 = t_0 > t_1 > \cdots > t_s = 0$ on the arc containing $(x, 1)$. This computation of the points in $f^{-1}(0)$ from points of $f^{-1}(1)$ is called numerical homotopy continuation. It may be used to solve systems of polynomial equations.

When $U$ is rational, a branched cover $f : V \to U$ gives homotopy paths. Given a map $g : \mathbb{C}_t \to U$ 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 $\mathbb{C}_t$. Equations for $V$ give 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 $\gamma \subset \mathbb{C}^r$ (or in $U$) that does not meet the branch locus. When $\gamma \subset U \setminus B$ is a loop based on 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 $U \setminus B$.

2.5 Numerical Algebraic Geometry

Numerical algebraic geometry [6, 37] uses homotopy continuation to study algebraic varieties on a computer. Its fundamental data structure is a witness set, which is a geometric representation of a variety using linear sections [35, 36].

Let $F : \mathbb{C}^n \to \mathbb{C}^m$ be a polynomial map and suppose that $X$ is a component of $F^{-1}(0)$ of dimension $r$ and degree $d$. Let $\mathcal{L} : \mathbb{C}^n \to \mathbb{C}^r$ 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 $W = X \cap \mathcal{L}^{-1}(0)$. It often suffices to work with a witness superset. For example, if $X$ is a hypersurface, then $\mathcal{L}^{-1}(0)$ is a general line, $\ell$, and by Zariski’s Theorem (Proposition 2.6), the fundamental group of $\mathbb{C}^n \setminus V$ is generated by loops in $\ell$ encircling the points of $W$ and hence also by loops encircling points of $W'$.

Algorithms to compute witness sets for the image of an irreducible variety under a linear map $\pi$ are developed in [19]. Suppose that $F : \mathbb{C}^n \to \mathbb{C}^m$ is a polynomial map with $V \subset F^{-1}(0)$ a component of dimension $r$ as before. Let $U = \pi(V)$ be the closure of the image of $V$ under $\pi$. The witness set for the image $U$ is a quadruple $(F, \pi, \mathcal{L}, W)$ where $\pi : \mathbb{C}^n \to \mathbb{C}^p$ is given by $\pi(x) = Ax$ for a matrix $A \in \mathbb{C}^{p \times n}$, $\mathcal{L}$ is a special affine map adapted for the map $\pi$, and $W := V \cap \mathcal{L}^{-1}(0)$. The witness set $(F, \pi, \mathcal{L}, W)$ 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 $\mathcal{L}$. The map $\mathcal{L}$ is constructed so that the number of points in $\pi(W)$ is the degree 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 $w$. If we set $q = \dim U$, then this is done by defining $\mathcal{L}$ by the linear system $\begin{bmatrix} B_1 \\ B_2 \end{bmatrix} x = v$ where the rows of $B_1 \in \mathbb{C}^{q \times n}$ are general vectors in the row space of $A$, the rows of $B_2 \in \mathbb{C}^{(r-q) \times n}$ are general vectors in $\mathbb{C}^n$, and $v$ is a general vector of $\mathbb{C}^r$.

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 $F : \mathbb{C}^n \to \mathbb{C}^m$ be a polynomial map and suppose that $V = V_1 \cup \cdots \cup V_r$ is a union of components of $F^{-1}(0)$, all having dimension $r$, and that $\mathcal{L} : \mathbb{C}^n \to \mathbb{C}^r$ 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 $W$. Numerical
irreducible decomposition [37, Ch. 15] uses monodromy and a trace test to compute this witness set partition.

**Remark 2.7** Many problems are formulated in terms of homogeneous or multi-homogeneous equations whose solutions are subsets of (products of) projective space(s) $\mathbb{P}^n$. 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 $G := G(V \rightarrow U)$. Choose a regular value $p \in U \setminus B$ of $f$, so that $f^{-1}(p)$ consists of $k$ reduced points. Numerically following the points of $f^{-1}(p')$ as $p'$ varies along a sequence of loops in $U \setminus B$ based on $u$ computes a sequence $\sigma_1, \sigma_2, \ldots$ of monodromy permutations in $G \subseteq S_k$. If $G_i$ is the subgroup of $G$ generated by $\sigma_1, \ldots, \sigma_i$, then we have

$$G_1 \subseteq G_2 \subseteq \cdots \subseteq G \subseteq S_k.$$

This was used in [27] to show that $G = S_k$ by computing enough monodromy permutations so that $G_i = S_k$ for some $i$. When the Galois group is *deficient* in that $G \subsetneq S_k$, then this method cannot compute $G$, for it cannot determine whether it has computed generators of $G$. We explain how a witness set for the branch locus $B$ enables us to compute generators for $G$.

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 $k$ with branch locus $B \subset \mathbb{P}^n$. 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 $p \in \ell \setminus B$ and, for each point $w$ of $W$, choose a loop $\gamma_w$ based on $p$ encircling $w$ as in Sect. 2.3. Let $\sigma_w \in S_k$ be the monodromy permutation obtained by lifting $\gamma_w$ to $V$.

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

\[ \subseteq \subseteq \subseteq \]  

\[ \subseteq \subseteq \subseteq \]
Proof By Proposition 2.3, lifting-based loops in \( \mathbb{P}^n \setminus B \) to permutations in \( S_k \) gives a surjective homomorphism \( \pi_1(\mathbb{P}^n \setminus B) \to \mathcal{G} \). 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 \( B \). 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 \( C^n \) with \( B \subset C^n \), then \( \ell \subset C^n \) is a complex line, \( \ell \simeq \mathbb{C} \). If \( B \cap \ell \) is \( d \) distinct points where \( d = \deg B \), then the statement of Theorem 3.1 still holds, as \( B \cap \ell = B \cap \ell \).

Lifts of loops encircling the points of a witness superset for \( B \cap \ell \) 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 \( \ell \) meets \( B' \) transversally 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 to determine the Galois group \( \mathcal{G} \) of a branched cover \( f : V \to U \) when \( U \) is rational. Suppose that \( V \subset \mathbb{P}^m \times \mathbb{P}^n \) is irreducible of dimension \( n \) and that the map \( f : V \to \mathbb{P}^n \) 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 \( f : V \to \mathbb{P}^n \).
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 \( f : V \to \mathbb{P}^n \).

The branch point algorithm is a random algorithm whose correctness follows from Theorem 3.1 and Corollary 3.2. There is a nonempty Zariski open set in the Grassmannian of lines in \( \mathbb{P}^n \) consisting of lines \( \ell \) that meet \( B \) transversally, so that in step (1), \( B \cap \ell \) is a witness set. We discuss the steps (1) and (3) in Sects. 3.1.1 and 3.1.2.

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 \( f : V \to \mathbb{P}^n \) 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 \( F : \mathbb{C}^{m+1} \times \mathbb{C}^{n+1} \to \mathbb{C}' \) is a system of \( r \geq m \) polynomials that are separately homogeneous in each set of variables \( x \) and \( u \). Let

\[
\begin{pmatrix}
C^m & \mathbb{P}^m \\
\mathbb{C}^{m+1} & 0
\end{pmatrix}
\]
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 restrict \( f : V \rightarrow \mathbb{P}^n \) to a line \( \ell \hookrightarrow \mathbb{P}^n \), 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 \( \ell \).

Example 3.5 Consider the irreducible surface \( V \) in \( \mathbb{P}_1^{xy} \times \mathbb{P}_2^{uvw} \) 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 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 set of points of \( V \) where the Jacobian \( J_{xy} F = \left( \frac{\partial F}{\partial x} \frac{\partial F}{\partial y} \right) \) has rank less than \( m = 1 \). This is defined by the vanishing of the partial derivatives as \( 3F = x \frac{\partial F}{\partial x} + y \frac{\partial F}{\partial y} \). Eliminating \( x \) and \( y \) from the ideal of partial derivatives 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 Fig. 2.

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

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

Let \( C \subset \mathbb{P}_1^{xy} \times \mathbb{P}_1^{st} \) 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 $\ell_1 = \mathbb{P}^1_{st}$ and working in the affine chart where $s = 1$ yield

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

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 $\mathbb{P}^1_{xy} \times \mathbb{P}^1_{st}$ given by $7x + 3y = 58$ and $s = 1$ as well as the branch locus in the affine chart of $\mathbb{C}\mathbb{P}^1_{st}(= \ell_1)$ where $s = 1$. This chart for $\mathbb{P}^1_{xy}$ has parameterization $x = 4 + 9z$ and $y = 10 - 21z$ for $z \in \mathbb{C}$ and is also used in Fig. 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 the 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. Any reduction to a complete intersection will have the points of $B \cap \ell$ as solutions, and possible additional solutions, and will therefore compute a witness superset for $B \cap \ell$.

3.1.2 Computing Monodromy Permutations

Let $W \subset \ell$ be a witness superset 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 $G$. To compute these encircling loops, choose a general base point $p \in \ell \setminus W$ and work in an affine chart of $\ell$ that contains $p$ and $W$ which is identified with $\mathbb{C}$. The papers [13,30] present algorithms to compute encircling loops for any base point. Our software is more naive and simply requires that $p$ be generic.

Let $\epsilon > 0$ be any positive number smaller than the minimum distance between points of $W \cup \{p\}$. 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 anticlockwise,
\[ w + \epsilon \sim w + \epsilon \sqrt{-1} \sim w - \epsilon \sim w - \epsilon \sqrt{-1} \sim w + \epsilon , \]
gives a loop encircling the point \( w \). For loops based on \( p \), 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 \( w - \epsilon \sqrt{-1} \). For these to give based loops in \( \ell \setminus W \), it suffices that \( p \) avoid finitely many real lines spanned by pairs \( \{ w, v + \epsilon \sqrt{-1} \} \) and \( \{ w, v - \epsilon \sqrt{-1} \} \) for \( w, v \in V \). This is a dense open subset of \( \mathbb{C} \).

Avoiding the points of \( W \) may not be sufficient as path following near a branch point is ill-conditioned. This potential problem is alleviated in our software as it uses \texttt{Bertini}, whose path-tracking uses adaptive step size and adaptive multi-precision [5]. The path-tracking results can be certified, e.g., starting with the output of the \texttt{Bertini} computation via [17].

Observe that concatenating these loops in anticlockwise 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 (2) where \( p = 0.4 + 0.3\sqrt{-1} \).

![Diagram of loops encircling points](image)

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 \( V \rightarrow \mathbb{P}_w^2 \) is the full symmetric group.

### 3.1.3 Implementation Subtleties

Our computations are not directly on projective space, but rather in affine charts as explained in Remark 2.7, and not with general lines, but random specific lines. These choices may fail to be generic. For example, a line \( \ell \) may not meet the branch locus \( B \) transversally, or this may not be observed as the chosen affine chart on \( \ell \) omits a point of \( B \), or the affine chart containing \( V \) may omit a component of the critical point set. We illustrate these possibilities in the following three examples. In each of these cases and others, the branch point algorithm may only compute a proper subgroup of \( G \). Since a general line meets \( B \) transversally and general affine charts meet every component of the critical point set, random lines and charts will be sufficient to compute \( G \) in practice.

**Example 3.8** Recall the family \( V \rightarrow \mathbb{P}^2 \) of cubics in Example 3.5. The line \( \ell_2 \) 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 $\ell_2$. This is observed in Fig. 3 where we see that the line $\ell_2$ 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 $\ell_2$ 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.

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 $\ell_1$, this is the affine chart where $t - s = 1$, which omits the fourth point of $B \cap \ell_1$ of (1), $p$ in Fig. 3. Thus, only three of the four branch points are on this affine chart of $\ell_1$. Since $B$ has degree four, lifting loops encircling these three points gives permutations that generate $G$, 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 $\ell_3$ by $g:[s:t] \mapsto [s-t:3:s]$. 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 $G$, 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.

**Example 3.11** A choice of vertical affine chart may also be unfortunate. The affine chart on $\mathbb{P}^1_{xy}$ 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 $\ell$ does not contain the point $q$, this is sufficient to compute $G$, for the same reason as in Example 3.10.

If $V \subset \mathbb{P}^m \times \mathbb{P}^m$ 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 $G$. 

---

**Fig. 3** Branch locus and lines
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 Fig. 4), and these lines have a particular incidence structure (see Sect. 4.1). Jordan [26] studied the Galois action on the 27 lines, observing that the Galois group is a subgroup of the group of symmetries of that incidence structure. This is isomorphic to the Weyl group $E_6$, which has order 51,840. We formulate the Galois group as the monodromy of a map $f : V \to U$ and compute it with the Branch Point Algorithm.

There are 20 homogeneous cubic monomials in the four coordinates of $\mathbb{P}^3$. This identifies 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 has dimension 4. The incidence variety

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

has a map $f : V \to \mathbb{P}^{19}(=U)$. 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 Boole to be 32.

We summarize computations to determine a witness set for this branch locus. Let $G$ be a general cubic (variable coefficients) and consider the vectors $v = (1, 0, k_1, k_2)$ and $w = (0, 1, k_3, k_4)$, which span a general line in $\mathbb{P}^3$. This line lies on the cubic surface $\mathcal{V}(G)$ when the homogeneous cubic $G(rv + sw)$ (the cubic restricted to the line spanned by $v$ and $w$) is identically zero. That is, the coefficients $K_0, K_1, K_2, K_3$ of $r^3, r^2s, rs^2, \text{ and } s^3$ in $G(rv + sw)$ vanish. This defines the incidence variety $V$ in the space $\mathbb{P}^{19} \times \mathbb{C}_k^4$, as the vectors $v, w$ 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 $g : \mathbb{C}_t \to \ell \subset \mathbb{P}^{19}$ of a random line $\ell$ 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 $i = 0, \ldots, 3$. There

---

**Fig. 4** Cubic surface with 27 lines (courtesy of Oliver Labs)
are 192 critical points of the projection $C \to \mathbb{C}_t$, 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 [14] and Bertini [4]. This gave 22 distinct permutations, each a product of six 2-cycles and listed in Fig. 5. 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.

4 Fiber Products

Let $f : V \to U$ be a branched cover of degree $k$ with Galois/monodromy group $G$. As explained in Sect. 2.2, the action of $G$ 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 [38]. Suppose that $V \subset \mathbb{C}_x^m \times \mathbb{C}_y^n$ is an $n$-dimensional irreducible component of $F^{-1}(0)$ where $F : \mathbb{C}_x^m \times \mathbb{C}_y^n \to \mathbb{C}^m$ and we write $F(x, y)$ with $x \in \mathbb{C}^m$ and $y \in \mathbb{C}^n$. The fiber product $V_{C^n}^2 = V \times_{\mathbb{C}^n} V \to \mathbb{C}^n$ is the pullback of the product $V \times V \to \mathbb{C}^n \times \mathbb{C}^n$ along the diagonal $\Delta \subset \mathbb{C}^n \times \mathbb{C}^n$. Where $V$ equal to $F^{-1}(0)$, then $V_{C^n}^2$ equals $G^{-1}(0)$, where

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

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 $V_{C^n}^2 = (V \times V) \cap (\mathbb{C}^m \times \mathbb{C}^m \times \Delta)$.

In general, $V$ is a component of $F^{-1}(0)$ and $V_{C^n}^2$ is a union of some components of $G^{-1}(0)$. We may compute a witness set representation for $V_{C^n}^2$ using its description as the intersection of the product $(V \times V)$ with $\mathbb{C}^m \times \mathbb{C}^m \times \Delta$ as in Section 12.1 of [6]. Iterating this computes $V_{C^n}^s$, which has several irreducible components. Among these may be components that do not map dominantly to $\mathbb{C}^n$—these come from fibers of $V \to \mathbb{C}^n$ 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. The remaining components constitute $V^{(s)}$, whose fibers over points of $C^n \setminus B$ are $s$-tuples of distinct points.

In practice, we first restrict $V$ to a general line $\ell \subset C^n$, for then $V|_\ell$ is an irreducible curve $C$ that maps dominantly to $\ell$. It suffices to compute the fiber products $C_{s, \ell}$, 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 $\ell$. As $C^{(s)}$ is the union of components of $C^{(s-1)} \times _\ell C$ that lie outside the big diagonal, we may compute it 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 can simplify this computation (e.g., as used in Sect. 4.1). Also, equations for $V^{(s)}$ of $C^{(s)}$ may be computed symbolically as in the modules de Cauchy of [31].

We offer three algorithms based on fiber products that obtain information about the Galois/monodromy group $G$ of $f : V \to U$. Let $k$, $\ell$, 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 $G$)

1. Compute an irreducible component $X$ of $C^{(k-1)}$.
2. For any $(k-1)$-tuple $(x_1, \ldots, x_{k-1}) \in X$ lying over $p$, the Galois/monodromy group is

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

**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.

**Algorithm 4.2** (Orbit decomposition of $G$ on $s$-tuples and $s$-transitivity)

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

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

2. The action of $G$ 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

$$O_i := f^{-1}(p) \cap X_i \quad i = 1, \ldots, r.$$

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 $G$ for primitivity)

1. Compute an irreducible decomposition of $C^{(2)}$.
2. If $C^{(2)}$ is irreducible, then $G$ is $2$-transitive and primitive.
(3) Otherwise, Step 2 of Algorithm 4.2 decomposes \((f^{-1}(p))^2\) into \(\mathcal{G}\)-orbits.
(4) Then, \(\mathcal{G}\) is primitive if and only if for each nondiagonal \(\mathcal{G}\)-orbit \(\mathcal{O}\), the graph \(\Gamma_{\mathcal{O}}\) of Sect. 2.1 is connected.

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

Remark 4.4 Algorithm 4.1 to compute \(\mathcal{G}\) using fiber products may be infeasible in practice: even if \(C \subset \mathbb{P}^1 \times \ell\), then \(C^{(k-1)} \subset (\mathbb{P}^1)^{k-1} \times \ell\) is a curve in a \(k\)-dimensional space. Such a formulation would have also have a very high degree, as the map \(C^{(k-1)} \to \ell\) has degree \(k!\), and when restricted to an irreducible component has degree \(|\mathcal{G}|\). For the computation in Sect. 5.1, \(k = 26\) and \(|\mathcal{G}| = 2^{13} \times 13! \approx 5 \times 10^{13}\).

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 Sect. 1.

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 [15, pp. 480–489].

Let \(p_1, \ldots, p_6\) be six points in \(\mathbb{P}^2\) not lying on a conic and with no three collinear. The space of cubics vanishing at \(p_1, \ldots, p_6\) is four-dimensional and gives a rational map \(\mathbb{P}^2 \dashrightarrow \mathbb{P}^3\) whose image is a cubic surface \(S\) that is isomorphic to \(\mathbb{P}^2\) blown up at the six points \(p_1, \ldots, p_6\). That is, \(S\) contains six lines \(\widehat{p}_1, \ldots, \widehat{p}_6\) and has a map \(\pi : S \to \mathbb{P}^2\) 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 \(\pi\), 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 \(i = 1, \ldots, 6\).
- 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 \(\{p_1, \ldots, p_6\} \setminus \{p_i\}\) for \(i = 1, \ldots, 6\).

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 \(\lambda\) on \(S\) is disjoint from 16 others and meets the remaining ten. With these ten, \(\lambda\) forms five triangles—the plane \(\Pi\) containing any two lines \(\lambda, \mu\) on \(S\) that meet will contain a third line \(v\) on \(S\) as \(\Pi \cap S\) is a plane cubic curve containing \(\lambda\) and \(\mu\).

We explain this in detail for the lines \(\widehat{p}_1, \ell_{12}, \text{and } \widehat{C}_1\).

- 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 \(\ell_{ij}\) 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 \(\ell_{1i}\) for \(2 \leq i \leq 6\), as \(p_1\) lies on these conics \(C_i\) and lines \(\ell_{1i}\).
The line $\ell_{12}$ 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, $\ell_{1i}$ and $\ell_{2i}$, this is because $\ell_{12}$ meets the lines $\ell_{1i}$ and $\ell_{2i}$ 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 $\ell_{12}$ meets both $\widehat{p}_1$ and $\widehat{p}_2$. It also meets $\ell_{1j}$ for $2 \leq i < j \leq 6$, as well as $\widehat{C}_1$, and $\widehat{C}_2$, because $\ell_{12}$ meets the underlying lines and conics at points outside of $p_1, \ldots, p_6$. See Fig. 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 $p_2, \ldots, p_6$ and no other points. As we have seen, $\widehat{C}_1$ meets $\widehat{\ell}_{1i}$ for $2 \leq i \leq 6$.

We describe the decomposition of $V^{(2)}$ and $V^{(3)}$. Let $V^{[2]}$ be the closure in $V^2_{\mathbb{P}^{19}}$ 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 $(\lambda, \mu)$ of lines $\lambda, \mu$ that lie on the cubic given by $p$. Then, $V^{[2]}$ has degree 729 over $\mathbb{P}^{19}$ with three irreducible components. We describe typical points $(\lambda, \mu)$ in the fibers of each.

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

However, $G$ is primitive, which may be seen using Algorithm 4.3 and Higman’s Theorem (Proposition 2.2). As $V$ is irreducible, $G$ is transitive. Since $D$ is irreducible, the 216 unordered pairs of disjoint lines form an orbit $D$ of $G$. The graph $\Gamma_D$ is connected. Indeed, the only nonneighbors 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 $\widehat{p}_j$, we have that $\Gamma_D$ 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, $\tau$. The typical point of $\tau$ 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, $\sigma$. The typical point of $\sigma$ 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 $\rho_i$ consisting of triples $(\lambda_1, \lambda_2, \lambda_3)$ of lines where the $i$th line does not meet the other two, but the last two do meet. Each has degree 2160 over $\mathbb{P}^{19}$ and $\mu_3$ is a component of $I \times_{\mathbb{P}^{19}} V$.

4. There are three components $\xi_i$ consisting of triples $(\lambda_1, \lambda_2, \lambda_3)$ of lines where the $i$th line meets the other two, but the last two do not meet. Each has degree 2160 over $\mathbb{P}^{19}$ and $\mu_3$ is a component of $D \times_{\mathbb{P}^{19}} V$.

5 Galois Groups in Applications

We present three problems from applications with 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 $x_1, \ldots, x_N \in \mathbb{R}^d$ having preferred pairwise distances $u_{ij} = u_{ji}$ for $1 \leq i, j \leq N$, that is, minimizing the potential

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

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 $\Psi_u$. This yields the system of cubic equations

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

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 [20, 21]).
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 $S_2 \wr S_{13}$, which has order $51, 011, 754, 393, 600 = 2^{13} \times 13!$.

The Branch Point Algorithm shows that the Galois group of this system is indeed equal to the wreath product $S_2 \wr S_{13}$. 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

Burmester [9] 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 [40] with the complete solution to all Alt–Burmester problems described in [7]. We compute the Galois group for four of the Alt–Burmester problems.

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 for the apex 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 [7] in using isotropic coordinates, the $M$-pose and $N$-position Alt–Burmester problem is described by the following parameters:

Fig. 7 A linkage, poses, positions, and a solution for 3 poses and 4 positions
positions: \((D_j, \overline{D}_j), \) for \(j = 1, \ldots, M+N\)
orientations: \((\Theta_j, \overline{\Theta}_j), \) for \(j = 1, \ldots, M\) with \(\Theta_j\overline{\Theta}_j = 1.\)

With variables \(G_1, G_2, z_1, z_2, G_1, G_2, \overline{z}_1, \overline{z}_2, \Theta_j, \overline{\Theta}_j\) for \(j = M+1, \ldots, M+N\), we consider

\[
L_{rj}L_{rj} - L_{r1}L_{r1} = 0, \quad \text{for } j = 2, \ldots, M+N \quad \text{and} \quad r = 1, 2
\]
\[
\Theta_j\overline{\Theta}_j - 1 = 0, \quad \text{for } j = 1, \ldots, M
\]

where

\[
L_{rj} := \Theta_jz_r + D_j - G_r \quad \text{and} \quad \overline{L}_{rj} = \overline{\Theta}_j\overline{z}_r + \overline{D}_j - \overline{G}_r.
\]

We first consider the case studied by Burmester, namely \(M = 5\) and \(N = 0\). Using modern terminology, Burmester noted that this system is a fiber product since the synthesis problem for four-bar linkages uncouples into two synthesis problems for 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 decompose into two components: 4 points on the diagonal \(\Delta\) and 12 disjoint pairs. The Branch Point Algorithm uses homotopy continuation to track a loop around each of 64 branch points. These loops yield the permutations listed in Fig. 8.

Cycles involving the first four solutions are in **boldface**, to highlight that these solutions are permuted among themselves while the other twelve solutions are permuted among 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 [7, 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 \(S_2 \wr S_{2m}\) 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...
and is thus the full wreath product $S_2 \wr S_{30}$. This Galois group is the largest it could be given the left-right symmetry.

For each case of $(M, N)$ equal to $(3, 4)$ and $(2, 6)$ we computed ten random permutations. This showed that the Galois groups of these problems are indeed equal to $S_2 \wr S_{201}$ and $S_2 \wr S_{1112}$ having order $2^{201} \times 201! \approx 5 \times 10^{437}$ and $2^{1112} \times 1112! \approx 10^{3241}$, respectively.

### 5.3 Algebraic Statistics

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 $u_0, \ldots, u_n$ 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 $\ell_u$ on the model $\mathcal{M}$ lies in $\mathbb{P}_p \times \mathbb{P}_u$. This is the Zariski closure of points $(p, u)$ where $p$ is a smooth point of $\mathcal{M}$ and a critical point of $\ell_u$. Then, $V$ is $n$-dimensional and irreducible, and its projection to $\mathbb{P}_u$ gives a branched cover whose degree is the maximum likelihood degree [24,25]. For an algebraic statistical model, we can ask for the Galois group of this maximum likelihood estimation (the branched cover $V \to \mathbb{P}^n$).

The model defined by the determinant

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

has maximum likelihood degree 6 and has a Galois group that is a proper subgroup of the full symmetric group $S_6$ [18]. 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 2–1 to a set of 12 branch points yielding a witness set for the branch point locus which is a component of the data discriminant.\(^1\)

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 [12]. Moreover, in [32, Section 5], it is shown that over a real data point, a typical

\(^{1}\) The defining polynomial of degree 12 was computed in [32, Ex. 6] and is available at the Web site https://sites.google.com/site/rootclassification/publications/DD.
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 [Algorithms 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 (1923), pp. 13–19.
2. B. Anderson and U. Helmke, Counting critical formations on a line, SIAM Journal on Control and Optimization, 52 (2014), pp. 219–242.
3. D. Bates, E. Gross, A. Leykin, and J. Rodriguez, Bertini for Macaulay2. arXiv:1603.05908, 2013.
4. D. Bates, J. Hauenstein, A. Sommese, and C. Wampler, Bertini: Software for numerical algebraic geometry. Available at http://bertini.nd.edu.
5. D. Bates, J. Hauenstein, A. Sommese, and C. Wampler, Adaptive multiprecision path tracking, SIAM J. Numer. Anal., 46 (2008), pp. 722–746.
6. D. Bates, J. Hauenstein, A. Sommese, and C. Wampler, Numerically solving polynomial systems with Bertini, vol. 25 of Software, Environments, and Tools, Society for Industrial and Applied Mathematics (SIAM), Philadelphia, PA, 2013.
7. D. Brake, J. Hauenstein, A. Murray, D. Myszka, and C. Wampler, The complete solution of Alt-Burmester synthesis problems for four-bar linkages, Journal of Mechanisms and Robotics, 8 (2016), p. 041018.
8. 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 (2015), pp. 4183–4206.
9. L. Burmester, Lehrbuch der Kinematic, Verlag Von Arthur Felix, Leipzig, Germany, 1886.
10. P. Cameron, Permutation groups, vol. 45 of London Mathematical Society Student Texts, Cambridge University Press, Cambridge, 1999.
11. A. Dimca, Singularities and topology of hypersurfaces, Universitext, Springer-Verlag, New York, 1992.
12. J. Draisma and J. I. Rodriguez, Maximum likelihood duality for determinantal varieties, International Mathematics Research Notices, 2014(2014), pp. 5648–5666.
13. A. Galligo and A. Poteaux, Computing monodromy via continuation methods on random Riemann surfaces, Theoret. Comput. Sci., 412 (2011), pp. 1492–1507.
14. D. Grayson and M. Stillman, Macaulay2, a software system for research in algebraic geometry. Available at http://www.math.uiuc.edu/Macaulay2/.
15. P. Griffiths and J. Harris, Principles of algebraic geometry, Wiley Classics Library, John Wiley & Sons, Inc., New York, 1994. Reprint of the 1978 original.
16. J. Harris, Galois groups of enumerative problems, Duke Math. J., 46 (1979), pp. 685–724.

\(^2\) http://home.uchicago.edu/~joisro/quickLinks/NCGG/.
17. J. Hauenstein, I. Haywood, and A. Liddell, Jr., An a posteriori certification algorithm for Newton homotopies, in ISSAC 2014—Proceedings of the 39th International Symposium on Symbolic and Algebraic Computation, ACM, New York, 2014, pp. 248–255.

18. J. Hauenstein, J. Rodriguez, and B. Sturmfels, Maximum likelihood for matrices with rank constraints, Journal of Algebraic Statistics, 5 (2014), pp. 18–38.

19. J. Hauenstein and A. Sommese, Witness sets of projections, Appl. Math. Comput., 217 (2010), pp. 3349–3354.

20. N. Hein, F. Sottile, and I. Zelenko, A congruence modulo four for real Schubert calculus with isotropic flags, Canadian Mathematical Bulletin, to appear.

21. N. Hein, F. Sottile, and I. Zelenko, A congruence modulo four in real Schubert calculus, J. Reine Angew. Math., 714 (2016), pp. 151–174.

22. C. Hermite, Sur les fonctions algébriques, CR Acad. Sci., 32 (1851), pp. 458–461.

23. A. Higman, Intersection matrices for finite permutation groups, J. Algebra, 6 (1967), pp. 22–42.

24. J. 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, New York, NY, USA, 2015, ACM, pp. 307–314.

25. J. Ruffo, Y. Sivan, E. Soprunova, and F. Sottile, Experimentation and conjectures in the real Schubert calculus for flag manifolds, Experiment. Math., 15 (2006), pp. 199–221.

26. A. Sommese and C. Wampler, Exceptional sets and fiber products, Found. Comput. Math., 8 (2008), pp. 171–196.

27. A. Sommese and C. Wampler, Exceptional sets and fiber products, Found. Comput. Math., 8 (2008), pp. 171–196.

28. A. Sommese and C. Wampler, Exceptional sets and fiber products, Found. Comput. Math., 8 (2008), pp. 171–196.

29. A. Sommese and C. Wampler, Exceptional sets and fiber products, Found. Comput. Math., 8 (2008), pp. 171–196.

30. A. Sommese and C. Wampler, Exceptional sets and fiber products, Found. Comput. Math., 8 (2008), pp. 171–196.

31. A. Sommese and C. Wampler, Exceptional sets and fiber products, Found. Comput. Math., 8 (2008), pp. 171–196.

32. A. Sommese and C. Wampler, Exceptional sets and fiber products, Found. Comput. Math., 8 (2008), pp. 171–196.