COMPUTATIONAL ASPECTS OF GALOIS GROUPS IN ENUMERATIVE GEOMETRY

A Dissertation

by

THOMAS J. YAHL

Submitted to the Graduate and Professional School of
Texas A&M University
in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

Chair of Committee,	Frank Sottile
Committee Members,	Anne Shiu
	Peter Kuchment
	Timothy Davis
Head of Department,	Sarah Witherspoon

August 2023

Major Subject: Mathematics

ABSTRACT

To an enumerative problem, one may associate a Galois group which encodes symmetries of the solutions to the problem. Galois groups of enumerative problems were first defined and studied by Jordan who considered them in the context of several classical enumerative problems. Recently, Galois groups of enumerative problems have been exploited for fast and efficient solving of polynomial systems. As such, determining Galois groups of enumerative problems and understanding how they may be used in numerical computations is of great importance.

We detail the mathematical background needed to define Galois groups of enumerative problems and then describe tools from numerical and computational algebraic geometry used to compute and exploit Galois groups. We then give the algebraic definition of the Galois group originally used by Jordan, as well as a geometric definition. We prove these definitions are equivalent and explore Galois groups for two classes of enumerative problems, sparse polynomial systems and Fano problems.

A sparse polynomial system is a polynomial systems such that the monomials appearing in each polynomial have been chosen *a priori*. Esterov observed two classes of sparse polynomial systems whose Galois group is an imprimitive permutation group and determined that the Galois group is the symmetric group for all other sparse polynomial systems. In special cases, there are results which determine the Galois group when it is imprimitive, though the answer is not known in general. We detail a computational method used to decompose systems into simpler systems when the Galois group is imprimitive. This approach has shown to increase speed and accuracy in solving polynomial systems when the Galois group is imprimitive.

Fano problems, problems of enumerating linear spaces on a variety, were among those enumerative problems considered by Jordan in his study of Galois theory. Recently, Galois groups of Fano problems were nearly classified by Hashimoto and Kadets. All Galois groups of Fano problems which are unknown are either the alternating group or the symmetric group. We present a computational technique which may be used to prove the existence of a transposition in the Galois

group. This method was recently used to prove that several Galois groups of Fano problems are symmetric groups, which was previously unknown.

ACKNOWLEDGMENTS

I would like to show my deepest appreciation for those friends, family, instructors, and more who have continually pushed me to grow and learn. I've been graced by constant support from each of you, and I hope that one day I can provide the same for others.

CONTRIBUTORS AND FUNDING SOURCES

Contributors

This work was supported by a thesis committee consisting of Dr. Frank Sottile, Dr. Peter Kuchment, and Dr. Anne Shiu of the Department of Mathematics, and Dr. Tim Davis of the Department of Computer Science.

The proof of equivalent definitions of the Galois group in Chapter IV is from joint work with Frank Sottile. Chapter V is a summary of work done with Taylor Brysiewicz, Jose Israel Rodriguez, and Frank Sottile from a 2021 article in Numerical Algorithms and a 2021 article in the Journal of Software for Algebra and Geometry. All other work conducted for the dissertation was completed by the student independently.

Supported in part by grant 636314 from the Simons Foundation.

NOTATIONS

$\Bbbk$	A field of characteristic zero
$\mathbb{K}$	An algebraically closed field of characteristic zero
$\mathbb{K}^\times$	The multiplicative group of nonzero elements of $\mathbb{K}$
$\mathbb{C}$	The field of complex numbers
$\mathbb{K}^n$	The space of n–tuples of elements of $\mathbb{K}$
$\mathbb{P}^n$	Projective space of dimension n
$\Bbbk[x_1, \ldots, x_n]$	The polynomial ring with $\Bbbk$ valued coefficients and indeterminants $x_1, \ldots, x_n$
$\langle F \rangle$	The ideal generated by F
$\mathcal{V}(I)$	The variety defined by the ideal I
$\mathcal{I}(X)$	The defining ideal of the variety X
$\mathfrak{m}_x$	The defining ideal of the point x
$\mathbb{K}[X]$	The coordinate ring of the variety X
$\mathbb{K}(X)$	The function field of the variety X
$DF(x)$	The Jacobian of F evaluated at x
$D^2F(x)$	The Hessian of F evaluated at x
$\ker A$	The kernel of A
$\operatorname{rank} A$	The rank of A
T_xX	The tangent space of X at x
$\operatorname{sm}(X)$	The smooth locus of X
$\dim X$	The dimension of X
$\mu_I(x)$	The multiplicity of x as a zero of the ideal I

$\mathbb{P}X$	The projectivization of the affine cone X
CY	The affine cone over the projective variety Y
$\mathbb{A}_i^n$	The affine chart for $\mathbb{P}^n$ indexed by i
$\mathbb{G}(r, \mathbb{P}^n)$	The Grassmanian variety of r–planes in $\mathbb{P}^n$
$\mathbb{S}(r+1, n+1)$	The Stiefel manifold of full rank $(n+1) \times (r+1)$ matrices
Id_n	The $n \times n$ identity matrix
$\mathbf{GL}(m)$	The $m \times m$ invertible matrices
$[n]$	The set $\{1, \ldots, n\}$
$\binom{[n]}{k}$	The set of cardinality k subsets of $[n]$
$p_I(A)$	The determinant of the submatrix of A consisting of rows indexed by I
$\overline{X}$	The closure of X
π^*	The pullback of the map π
$[\mathbb{F} : \Bbbk]$	The index of $\Bbbk$ in $\mathbb{F}$
$\deg \pi$	The degree of π
$\pi : X \dashrightarrow Y$	A rational map from X to Y
$H(x, t)$	A homotopy with variable x and parameter t
$[a, b]$	The real closed interval of x such that $a \leq x \leq b$
$\mathrm{re}(z)$	The real part of z
$\mathrm{im}(z)$	The imaginary part of z
$\mathbb{IC}$	The space of one–dimensional complex intervals
$\mathbb{IC}^n$	The space of n–dimensional complex intervals
$\square F$	An interval enclosure of F
$K_{x,Y}$	The Krawczyk operator with parameters x and Y
$\mathcal{M}_\pi$	The monodromy group of π
S_d	The symmetric group on $[d]$

X_Y^d	The d–fold fiber product of a map $X \to Y$
Δ	The set of tuples with a repeated coordinate
$X_Y^{(d)}$	The closure $\overline{X_Y^d \setminus \Delta}$
$\mathcal{G}(\mathbb{L}/\Bbbk)$	The Galois group of the field extension $\mathbb{L}/\Bbbk$
$\mathbb{F}^H$	The elements of $\mathbb{F}$ fixed by the group H
$\mathbb{C}[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]$	The Laurent polynomial ring in the indeterminants $x_1, \ldots, x_n$
$\mathcal{A}_\bullet$	A set of supports
$\lvert\mathcal{A}_\bullet\rvert$	The sum of the cardinalities of each $\mathcal{A}_i$
$\mathrm{conv}(\mathcal{A})$	The convex hull of the set $\mathcal{A}$
$\mathrm{MV}(\mathcal{A}_\bullet)$	The mixed volume of the convex hulls $\mathrm{conv}(\mathcal{A}_1), \ldots, \mathrm{conv}(\mathcal{A}_n)$
$\mathrm{sat}(L)$	The saturation of L
$\mathcal{V}_r(X)$	The Fano scheme of r–planes on X

TABLE OF CONTENTS

Page

LIST OF FIGURES

FIGURE Page

LIST OF TABLES

TABLE Page

1. INTRODUCTION

Problems of counting or describing geometric objects in special position relative to other fixed objects are known as enumerative problems—Enumerative geometry is the study of these problems and the various techniques used to solve them. Enumerative problems arise in many applications, such as in designing mechanical arms with prescribed motion, reconstructing a scene from images, and determining stable or oscillatory distributions of chemicals in a reaction. The structure of these problems and the ability to compute their solutions is vital to these applications.

The Galois group of an enumerative problem encodes the structure and symmetries of the problem. These groups were first defined by Jordan in his seminal work on Galois theory, "Traité des substitutions et des équations algébriques" [1]. In this work, Jordan studied the Galois groups of several classical enumerative problems using known results concerning the solutions of these problems. The reverse is more common: generally the Galois group of an enumerative problem is studied to obtain information about the problem and its solutions. Indeed, information about the Galois group can be used to answer questions such as “Can all remaining solutions be computed in rational functions of a number of known solutions?” and “Can the solutions be computed exactly via radicals?”

While initially defined through algebraic means, a modern geometric view of the Galois group of an enumerative problem was given by Harris [2] and traces back further to Hermite [3]. In this description, the Galois group is given as the monodromy group of a map between spaces given as the zeros of a polynomial system. Such spaces are called varieties and are a primary object in algebraic geometry, which invites the use of its tools and techniques. Information about the Galois group can often then be inferred from properties of these varieties. For instance, transitivity and higher transitivity of the Galois group of an enumerative problem can be determined from the irreducibility of certain varieties associated to the problem. We discuss the necessary background in algebraic geometry to study Galois groups of enumerative problems in Chapter 2.

As varieties are determined by polynomial systems, they can be encoded and represented in a

computer by these systems. Further, points on a variety are solutions to these systems and can be approximated by numerical coordinates. Methods of studying varieties through this lens comprise the area of computational algebraic geometry. Symbolic methods from computational algebraic geometry produce exact results and formal proofs at the cost of time and large computational needs. In contrast, numerical methods from computational algebraic geometry are often fast and efficient, but rarely constitute a formal proof. In Chapter 3, we describe several tools and techniques from computational algebraic geometry that we use for studying Galois groups of enumerative problems.

A sparse polynomial system is a polynomial system such that the monomials appearing in each polynomial have been chosen a priori. The problem of describing the zeros of a sparse polynomial system is an enumerative problem we consider in depth. These systems have been well studied, a tight upper bound for their number of solutions was determined by Bernstein, Kushnirenko, and Khovanskii [4, 5]. Later, Huber and Sturmfels gave an algorithm for solving these systems and showed it to be optimal in a precise sense [6]. Recently, Esterov classified the Galois group for a large class of sparse polynomial systems and has made progress in determining the Galois group in other cases [7, 8]. In Chapter 4, we explore what is known about Galois groups of sparse polynomial systems, pose a conjecture on the groups that appear as the Galois group for a special class of sparse polynomial systems, and describe a method of solving these systems by exploiting their Galois groups as in [9, 10].

The classical problem of enumerating the lines on a cubic surface is one of the first instances of a Fano problem. More generally, a Fano problem consists of enumerating the linear spaces of a fixed dimension on a variety. For a general complete intersection, Debarre and Manivel derived formulas for the dimension and degree of the variety of linear spaces lying on the complete intersection. This setting encompases all Fano problems we consider, including classical cases. Galois groups of these Fano problems were among the first Galois groups ever considered, as Jordan considered the Galois group of the problem of lines on a cubic surface [1]. Figure 1.1 was generated using the graphics language `Asymptote` [11] and illustrates the lines on a cubic surface. Harris generalized Jordan's result by computing the Galois groups for a family of Fano problems [2].

Recently, Hashimoto and Kadets determined the Galois group for another family of Fano problems and then very nearly classified Galois groups of Fano problems [12]. In Chapter 5 we show how numerical algebraic geometry has been used to prove results about Galois groups of Fano problems, furthering this near classification.

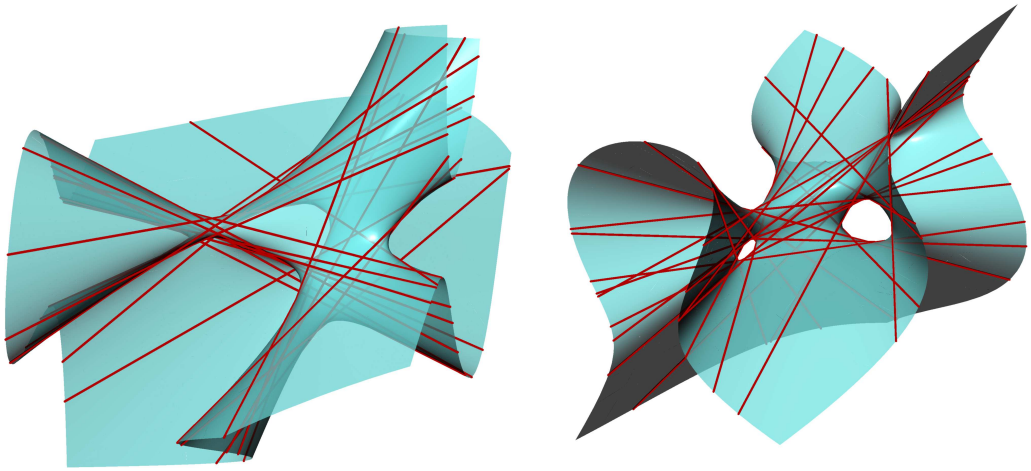

Figure 1.1: Two views of the 27 lines on a cubic surface

2. ALGEBRAIC GEOMETRY

2.1 Affine Varieties

Algebraic geometry may be described as the study of zeros of polynomial systems, called varieties. Varieties contained in an ambient space, such as affine space $\mathbb{K}^n$ and projective space $\mathbb{P}^n$, are called affine varieties and projective varieties respectively. Throughout, we assume the field of definition $\mathbb{K}$ of our polynomials and their zeros is an algebraically closed field of characteristic zero. More comprehensive accounts of algebraic geometry may be found in [13, 14, 15].

2.1.1 Ideals and Varieties

A *polynomial* is an element of the ring $\mathbb{K}[x_1, \ldots, x_n]$ generated by the coordinate functions $x_1, \ldots, x_n$ on $\mathbb{K}^n$, and a *system* of k polynomials is a k–tuple $F = (f_1, \ldots, f_k)$ of polynomials. A *zero* of the system $F = (f_1, \ldots, f_k)$ is a point $x \in \mathbb{K}^n$ such that $f_i(x) = 0$ for $i = 1, \ldots, k$. We write $\langle F \rangle = \langle f_1, \ldots, f_k \rangle \subseteq \mathbb{K}[x_1, \ldots, x_n]$ for the ideal generated by the system F. Every element of $\langle F \rangle$ is a linear combination over $\mathbb{K}[x_1, \ldots, x_n]$ of the polynomials $f_1, \ldots, f_k$, so that a zero of the system F is a zero of every polynomial $f \in \langle F \rangle$. Conversely, as $f_i \in \langle F \rangle$ for each $i = 1, \ldots, k$, if $x \in \mathbb{K}^n$ is a zero of every polynomial $f \in \langle F \rangle$, then it is a zero of the system F.

Definition 1. Given an ideal $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$, the set

$$\mathcal{V}(I) = \{x \in \mathbb{K}^n : f(x) = 0 \text{ for all } f \in I\}$$

is the *affine variety* defined by I.

Given a polynomial system F, we write $\mathcal{V}(F)$ for the affine variety $\mathcal{V}(\langle F \rangle)$, which is the set of zeros of F. Any variety $X = \mathcal{V}(I)$ is the zero set of a polynomial system. Indeed, by Hilbert's basis theorem, the ideal $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ is finitely–generated and $X = \mathcal{V}(I)$ is the set of zeros of any polynomial system F such that $I = \langle F \rangle$.

If there is a inclusion of ideals $I \subseteq J$, then there is a reverse inclusion of affine varieties

$\mathcal{V}(J) \subseteq \mathcal{V}(I)$. Given an inclusion of varieties $Y \subseteq X$, we say that Y is a *subvariety* of X. There are many ideals which define the same affine variety—for instance, in $\mathbb{A}^2$, the ideals $\langle x, y\rangle$ and $\langle x^2, xy, y^2\rangle$ both define the origin.

There is a unique ideal which represents an affine variety X. The *defining ideal* $\mathcal{I}(X)$ of an affine variety $X \subseteq \mathbb{K}^n$ is the ideal

$$\mathcal{I}(X) = \{f \in \mathbb{K}[x_1, \ldots, x_n] : f(x) = 0 \text{ for all } x \in X\}.$$

The defining ideal of a variety has the property that $\mathcal{V}(\mathcal{I}(X)) = X$, but the inclusion $I \subseteq \mathcal{I}(\mathcal{V}(I))$ may be proper. Indeed, the defining ideal of a variety is a radical ideal, as $f^m \in \mathcal{I}(X)$ implies $f \in \mathcal{I}(X)$. Recall the radical of an ideal I is the intersection of all prime ideals that contain I. The relationship between the functions $\mathcal{V}$ and $\mathcal{I}$ is given by Hilbert's Nullstellensatz.

Theorem 2 (Hilbert)**.** *The functions $\mathcal{V}$ and $\mathcal{I}$ are inverse bijections between the set of radical ideals of $\mathbb{K}[x_1, \ldots, x_n]$ and the set of affine varieties in $\mathbb{K}^n$. Further, for any ideal I, $\mathcal{I}(\mathcal{V}(I))$ is equal to the radical of I.*

From Theorem 2, the defining ideal of a point $x \in \mathbb{K}^n$ is a maximal ideal $\mathfrak{m}_x$ and conversely. As a proper ideal $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ is contained in some maximal ideal $\mathfrak{m}_x$, the variety $\mathcal{V}(I)$ necessarily contains the point $x \in \mathcal{V}(\mathfrak{m}_x) \subseteq \mathcal{V}(I)$. Thus, every proper ideal of $\mathbb{K}[x_1, \ldots, x_n]$ defines a nonempty variety in $\mathbb{K}^n$.

For arbitrary ideals $I, J \subseteq \mathbb{K}[x_1, \ldots, x_n]$, the function $\mathcal{V}$ satisfies $\mathcal{V}(I) \cup \mathcal{V}(J) = \mathcal{V}(I \cap J)$ and $\mathcal{V}(I) \cap \mathcal{V}(J) = \mathcal{V}(I + J)$. It follows that finite unions and arbitrary intersections of affine varieties are affine varieties. As such, affine varieties form the closed sets of a topology on $\mathbb{K}^n$ called the Zariski topology. An affine variety inherits this topology as a subspace of affine space.

Definition 3. The *Zariski topology* on an affine variety $X \subseteq \mathbb{K}^n$ is the topology whose closed sets are the subvarieties of X.

A polynomial $f \in \mathbb{K}[x_1, \ldots, x_n]$ is a function on $\mathbb{K}^n$ and its restriction $f : X \to \mathbb{K}$ to an affine variety X is a *regular function* on X. The set of regular functions on X forms a ring under

pointwise addition and multiplication called the *coordinate ring* $\mathbb{K}[X]$ of X. If a polynomial $f \in \mathbb{K}[x_1, \ldots, x_n]$ restricts to the zero function on X, it is an element of the defining ideal $f \in \mathcal{I}(X)$. It follows that the coordinate ring of an affine variety X may be represented by the quotient $\mathbb{K}[X] = \mathbb{K}[x_1, \ldots, x_n]/\mathcal{I}(X)$.

Coordinate rings allow us to speak of subvarieties of an affine variety $X \subseteq \mathbb{K}^n$ more generally. An ideal of the coordinate ring $\mathbb{K}[X] = \mathbb{K}[x_1, \ldots, x_n]/\mathcal{I}(X)$ corresponds to a unique ideal $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ containing $\mathcal{I}(X)$, and the variety of this ideal $\mathcal{V}(I) \subseteq \mathcal{V}(\mathcal{I}(X)) = X$ is a subvariety of X. Conversely, the defining ideal of any subvariety $Y \subseteq X$ contains $\mathcal{I}(X)$ and so corresponds to an ideal of the coordinate ring $\mathbb{K}[X]$.

2.1.2 Irreducibility

Often one would like to decompose a variety into simpler varieties. Irreducible varieties are varieties that can not be decomposed and serve as building blocks for such a decomposition.

Definition 4. An affine variety X is *irreducible* if it cannot be written as a union of two proper subvarieties. A variety which is not irreducible is *reducible*.

By taking complements, an affine variety is irreducible if every pair of nonempty Zariski open sets intersects nontrivially—equivalently, if every nonempty Zariski open set is dense in the Zariski topology. Irreducibility of an affine variety can be interpreted algebraically—an affine variety X is irreducible if and only if its defining ideal $\mathcal{I}(X)$ is prime. This implies the coordinate ring of an irreducible affine variety is an integral domain. The *function field* $\mathbb{K}(X)$ of an irreducible affine variety is the fraction field of its coordinate ring and its elements are called *rational functions*. A rational function is represented (non–uniquely) by quotients of regular functions f/g where $g \in \mathbb{K}[X]$ is nonzero.

Recall that an intersection of ideals corresponds to a union of varieties, $\mathcal{V}(I \cap J) = \mathcal{V}(I) \cup \mathcal{V}(J)$. Given a variety $X \subseteq \mathbb{K}^n$, its defining ideal $\mathcal{I}(X) \subseteq \mathbb{K}[x_1, \ldots, x_n]$ is radical and equal to the intersection of all prime ideals containing $\mathcal{I}(X)$. By considering the varieties defined by these prime ideals, we obtain an expression for X as a union of irreducible subvarieties. Results from

commutative algebra for Noetherian rings imply that this union is finite [13, 16].

Theorem 5. *An affine variety X can be decomposed into a finite union of irreducible varieties $X = Y_1 \cup \cdots \cup Y_k$ such that none of these varieties are contained within one another. Futher, this decomposition is unique up to a reordering of the varieties $Y_1, \ldots, Y_k$.*

The varieties $Y_1, \ldots, Y_k$ in Theorem 5 are called the *irreducible components* of X. An *isolated point* is an irreducible component of a variety consisting of a single point.

2.1.3 Smoothness and Dimension

Recall an affine variety $X \subseteq \mathbb{K}^n$ is defined by a system of m polynomials $F = (f_1, \ldots, f_m)$ such that $\mathcal{I}(X) = \langle F \rangle$. The Jacobian $DF(x_0) : \mathbb{K}^n \to \mathbb{K}^m$ of F at a point $x_0 \in X$ is the linear map represented by the matrix whose entries are the partial derivatives of the polynomials $f_1, \ldots, f_m$ evaluated at x_0.

Definition 6. Let X be a variety and F be a polynomial system such that $\mathcal{I}(X) = \langle F \rangle$. The *Zariski tangent space* $T_{x_0}X$ of an affine variety X at a point $x_0 \in X$ is defined by

$$T_{x_0}X = \{x \in \mathbb{K}^n : DF(x_0)(x - x_0) = 0\}.$$

The tangent space $T_{x_0}X$ of X at a point $x_0 \in X$ is independent of choice of system F used in Definition 6. Indeed, if F vanishes on X and G is a system such that $\langle G \rangle \subseteq \langle F \rangle$, expressing the polynomials of G as combinations of the polynomials of F and differentiating gives an inclusion $\ker DF(x_0) \subseteq \ker DG(x_0)$. If the systems F and G both vanish on X and generate the same ideal, then there is an equality $\ker DF(x_0) = \ker DG(x_0)$. As $T_{x_0}X$ is a translation of the kernel $\ker DF(x_0)$ by x_0, any system F satisfying $\mathcal{I}(X) = \langle F \rangle$ produces the same tangent space. We note that as a translated vector space, a tangent space has a dimension $\dim T_{x_0}X = \dim \ker DF(x_0)$.

Fix an irreducible variety $X \subseteq \mathbb{K}^n$ and a system F such that $\mathcal{I}(X) = \langle F \rangle$. Among the points $x \in X$, there is a maximal rank r of the Jacobian $DF(x)$ and this maximal rank is attained. A point $x \in X$ is *smooth* if $\operatorname{rank} DF(x) = r$ and the *smooth locus* $\operatorname{sm}(X)$ of X is the set of smooth

points. If $x \in X$ is not a smooth point, then $\operatorname{rank} DF(x) < r$ and the $r \times r$ minors of $DF(x)$ vanish. As the smooth locus is nonempty, the $r \times r$ minors of $DF(x)$ determine a proper subvariety of X and $\operatorname{sm}(X)$ is a Zariski open set. We say X is *smooth* if every point is smooth, $X = \operatorname{sm}(X)$.

Definition 7. The *dimension* $\dim X$ of an irreducible variety X is the dimension of the tangent space at a smooth point, $\dim X = \dim T_x X$ for $x \in \operatorname{sm}(X)$. The dimension of a reducible variety is the maximum dimension of its irreducible components.

There are many equivalent definitions of dimension. Several of these definitions and proof of their equivalences can be found in [13, 16]. The most useful equivalence for our purposes comes from the following result.

Theorem 8. *For an irreducible affine variety X, the dimension of X is equal to the transcendence degree of the function field $\mathbb{K}(X)$.*

2.2 Projective Varieties

A polynomial $f \in \mathbb{K}[x_0, \ldots, x_n]$ is homogeneous of degree d if $f(\lambda x) = \lambda^d f(x)$ for all $\lambda \in \mathbb{K}^\times$, and an ideal generated by homogeneous polynomials is a homogeneous ideal. Projective varieties are zero sets of homogeneous ideals in projective space. While much of the theory is analogous to that of affine varieties, there are differences that we highlight.

2.2.1 Ideals and Varieties

The projective space $\mathbb{P}^n$ is the set of one–dimensional linear subspaces in $\mathbb{K}^{n+1}$. Each one–dimensional linear subspace is the span of a point $x \in \mathbb{K}^{n+1} \setminus \{0\}$, and two points $x, y \in \mathbb{K}^{n+1} \setminus \{0\}$ span the same one–dimensional linear subspace exactly when there is a nonzero $\lambda \in \mathbb{K}^\times$ such that $y = \lambda x$. Thus, we consider $\mathbb{P}^n$ as the set of orbits of $\mathbb{K}^{n+1} \setminus \{0\}$ under the $\mathbb{K}^\times$–action of scalar multiplication. Write $[x] \in \mathbb{P}^n$ for the orbit of the point $x \in \mathbb{K}^{n+1} \setminus \{0\}$.

Given a homogeneous ideal $I \subseteq \mathbb{K}[x_0, \ldots, x_n]$, its zero set $\mathcal{V}(I) \subseteq \mathbb{K}^{n+1}$ is invariant under scalar multiplication—such a set is called an *affine cone*. Conversely, let $f \in \mathbb{K}[x_0, \ldots, x_n]$ be a polynomial that vanishes on an affine cone X. If we write f as a sum $f = f_0 + \ldots + f_d$ where each

f_i is a homogeneous polynomial of degree i, then each f_i vanishes on X. Thus, the defining ideal of an affine cone is generated by homogeneous polynomials and is a homogeneous ideal. Given an affine cone $X \subseteq \mathbb{K}^{n+1}$, the set $X \cap (\mathbb{K}^{n+1} \setminus \{0\})$ is a union of $\mathbb{K}^\times$–orbits which defines a set $\mathbb{P}X \subseteq \mathbb{P}^n$ called the *projectivization* of X.

Definition 9. A *projective variety* is the projectivization of an affine cone.

Given a projective variety $Y \subseteq \mathbb{P}^n$, the *affine cone over* Y is the Zariski closure

$$CY = \overline{\{x \in \mathbb{K}^{n+1} \setminus \{0\} : [x] \in Y\}}.$$

The functions $Y \to CY$ sending a projective variety in $\mathbb{P}^n$ to its affine cone in $\mathbb{K}^{n+1}$ and $X \to \mathbb{P}X$ sending an affine cone in $\mathbb{K}^{n+1}$ to its projectivization in $\mathbb{P}^n$ are inverse bijections.

The defining ideal $\mathcal{I}(Y)$ of a projective variety Y is defined to be the defining ideal $\mathcal{I}(CY)$ of its affine cone CY, which is a homogeneous radical ideal. Analagous to the affine setting, there is correspondence between homogeneous radical ideals of $\mathbb{K}[x_0, \ldots, x_n]$ and projective varieties in $\mathbb{P}^n$. However, the correspondence is not bijective—the homogeneous radical ideals $\langle x_0, \ldots, x_n \rangle$ and $\langle 1 \rangle$ both define the empty projective variety.

Theorem 10. *The functions $\mathbb{P}\mathcal{V}$ and $\mathcal{I}$ are inclusion reversing bijections between the sets of homogeneous radical ideals of $\mathbb{K}[x_0, \ldots, x_n]$ not equal to the ideal $\langle x_0, \ldots, x_n \rangle$ and the set of projective varieties contained in $\mathbb{P}^n$.*

Finite unions and arbitrary intersections of projective varieties are projective varieties, so we define the Zariski topology on $\mathbb{P}^n$ to be the topology whose closed sets are projective varieties. The Zariski topology on a projective variety $Y \subseteq \mathbb{P}^n$ is the inherited topology whose closed sets are the subvarieties of Y.

2.2.2 Affine Charts

We give another view of projective varieties through local coordinates. Consider the Zariski open sets $\mathbb{A}^n_i = \{[x_0, \ldots, x_n] \in \mathbb{P}^n : x_i \neq 0\}$, which cover $\mathbb{P}^n$. Every point $[x_0, \ldots, x_n] \in \mathbb{A}^n_i$

is represented by a unique point $(x_0/x_i, \ldots, x_n/x_i) \in \mathbb{K}^{n+1} \setminus \{0\}$, where the i-th coordinate is equal to 1. Thus the map $\phi_i : \mathbb{A}_i^n \to \mathbb{K}^n$ sending $[x_0, \ldots, x_n]$ to $(x_0/x_i, \ldots, \widehat{1}_i, \ldots, x_n/x_i) \in \mathbb{K}^n$ (removing the 1 in the i-th coordinate) is a bijection. The open sets and maps $(\mathbb{A}_i^n, \phi_i)_{i=0,\ldots,n}$ are *affine charts* for $\mathbb{P}^n$ and provide it with a system of local coordinates.

The Zariski topology on $\mathbb{P}^n$ is a gluing of the Zariski topology in these affine charts. That is, a subset $Y \subseteq \mathbb{P}^n$ is a projective variety if and only if the sets $\phi_i(Y \cap \mathbb{A}_i^n) \subseteq \mathbb{K}^n$ are affine varieties for $i = 0, \ldots, n$. For a projective variety $Y \subseteq \mathbb{P}^n$ defined by a system of homogeneous polynomials $F(x_0, \ldots, x_n)$, the affine variety $\phi_i(Y \cap \mathbb{A}_i^n)$ is the zero set of the system

$$\widetilde{F}(x_0, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n) = F(x_0, \ldots, 1_i, \ldots, x_n)$$

defined by setting the i-th coordinate equal to 1 in each polynomial of F. Conversely, if $Y \subseteq \mathbb{P}^n$ is such that the sets $\phi_i(Y \cap \mathbb{A}_i^n)$ are affine varieties for every $i = 0, \ldots, n$, then Y is a projective variety and is defined by a homogeneous ideal.

2.2.3 Irreducibility, Smoothness, & Dimension

As with affine varieties, if there is an inclusion $Y \subseteq X$, we say Y is a subvariety of X. An irreducible projective variety $Y \subseteq \mathbb{P}^n$ is one that cannot be written as a union of two proper subvarieties—equivalently, one whose affine cone is irreducible, or whose defining ideal $\mathcal{I}(Y) = \mathcal{I}(CY)$ is prime.

Given a projective variety Y, we may decompose the affine cone CY into irreducible components. The projectivizations of the irreducible components of CY give an irreducible decomposition for Y. Thus, a projective variety Y may be uniquely decomposed into a union or irreducible projective varieties and this decomposition is unique up to a reordering of the varieties. Again, we say the varieties in such a decomposition are the irreducible components of Y.

For a projective variety Y, its affine cone CY has a tangent space which we use to define the tangent space of the projective variety X.

Definition 11. The *Zariski tangent space* $T_{[x]}Y$ of a projective variety Y at a point $[x] \in Y$ is the

projectivization of the tangent space $T_x CY$ of the affine cone CY at any representative $x \in CY$ of the orbit $[x] \in \mathbb{P}^n$.

The dimension of a projective variety $Y \subseteq \mathbb{P}^n$ is defined to be $\dim Y = \dim CY - 1$. Thus the dimension of a tangent space is defined and we say a point $[x] \in Y$ is smooth if $\dim T_{[x]} Y = \dim Y$. The affine variety $\phi_i(Y \cap \mathbb{A}_i^n)$ may be identified with a subvariety of CY of dimension $\dim CY - 1$ so that the dimension is preserved by taking local coordinates. It follows that a point $[x] \in Y \cap \mathbb{A}_i^n$ is smooth if and only if $\phi_i([x]) \in \phi_i(Y \cap \mathbb{A}_i^n)$ is smooth. The smooth locus of a projective variety Y is the Zariski open set $\mathrm{sm}(Y)$ consisting of smooth points and Y is smooth if $\mathrm{sm}(Y) = Y$.

2.3 Grassmanian Varieties

An *r–plane* in $\mathbb{P}^n$ is a projective variety ℓ whose affine cone $C\ell \subseteq \mathbb{A}^{n+1}$ is an $(r+1)$–dimensional linear subspace. Grassmanian varieties are projective varieties which parameterize the r–planes in $\mathbb{P}^n$. There are several connections of Grassmanian varieties to representation theory, combinatorics, and intersection theory. We discuss definitions and various properties of Grassmanian varieties, including local coordinate charts, dimension, and smoothness. We begin with the definition of the central object of this section.

Definition 12. The *Grassmanian* $\mathbb{G}(r, \mathbb{P}^n)$ is the space of r–planes in $\mathbb{P}^n$.

We study r–planes in $\mathbb{P}^n$ by considering their affine cones. For $r \leq n$, the *Stiefel manifold* $\mathbb{S}(r+1, n+1)$ is the space of complex full rank $(n+1) \times (r+1)$ matrices. We write Id_m for the $m \times m$ identity matrix and $\mathrm{GL}(m) = \mathbb{S}(m, m)$ for the space of $m \times m$ invertible matrices. The space of $(n+1) \times (r+1)$ matrices forms an affine $(n+1)(r+1)$–dimensional affine space and the Stiefel manifold is the Zariski open set consisting of matrices with some nonzero maximal minor.

The column span of an element of $\mathbb{S}(r+1, n+1)$ is an $(r+1)$–dimensional linear subspace of $\mathbb{A}^{n+1}$. As all $(r+1)$–dimensional linear subspaces occur this way, the Stiefel manifold $\mathbb{S}(r+1, n+1)$ parameterizes $(r+1)$–dimensional linear subspaces of $\mathbb{A}^{n+1}$ (equivalently, r–planes in $\mathbb{P}^n$)—however, this is an overparameterization. Indeed, for any matrix $A \in \mathbb{S}(r+1, n+1)$ and

$B \in \mathrm{GL}(r+1)$, $AB \in \mathbb{S}(r+1, n+1)$ has the same column span as A. Conversely, if two matrices have the same column span, the columns of these matrices form bases for this linear subspace and there is a change of coordinates between these bases represented by an element of $\mathrm{GL}(r+1)$. That is, there is a bijection between the Grassmanian $\mathbb{G}(r, \mathbb{P}^n)$ and the orbits of $\mathrm{GL}(r+1)$ acting on $\mathbb{S}(r+1, n+1)$ by multiplication on the right. An r–plane $\ell \in \mathbb{G}(r, \mathbb{P}^n)$ is represented (not uniquely) by an element of $\mathbb{S}(r+1, n+1)$ whose entries we call *Stiefel coordinates* for ℓ.

2.3.1 Plücker Coordinates

We describe another set of coordinates on $\mathbb{G}(r, \mathbb{P}^n)$. Write $\binom{[n+1]}{r+1}$ for the set of subsets of $\{0, \ldots, n\}$ of cardinality $r+1$. For a subset $I \in \binom{[n+1]}{r+1}$ and $A \in \mathbb{S}(r+1, n+1)$, let $p_I(A)$ be the determinant of the submatrix of A consisting of rows indexed by I. The set $\{p_I(A) : I \in \binom{[n+1]}{r+1}\}$ is the set of maximal minors of the matrix A. For an r–plane $\ell \in \mathbb{G}(r, \mathbb{P}^n)$ with Stiefel coordinates $A \in \mathbb{S}(r+1, n+1)$, the tuple $(p_I(A))_{I \in \binom{[n+1]}{r+1}}$ are called *Plücker coordinates* for ℓ.

Consider an r–plane $\ell \in \mathbb{G}(r, \mathbb{P}^n)$ with Stiefel coordinates $A \in \mathbb{S}(r+1, n+1)$. Any other Stiefel coordinates for ℓ have the form $AB \in \mathbb{S}(r+1, n+1)$ for $B \in \mathrm{GL}(r+1)$, and for any $I \in \binom{[n+1]}{r+1}$ we have $p_I(AB) = \det(B) p_I(A)$. That is, the Plücker coordinates of an r–plane are unique up to scale and define a point in $\mathbb{P}^{\binom{n+1}{r+1}-1}$. The *Plücker embedding* of $\mathbb{G}(r, \mathbb{P}^n)$ is the map $p : \mathbb{G}(r, \mathbb{P}^n) \to \mathbb{P}^{\binom{n+1}{r+1}-1}$ sending $\ell \in \mathbb{G}(r, \mathbb{P}^n)$ to its Plücker coordinates in projective space. We show that this map is an injection and that the image is a projective variety, justifying the statement that $\mathbb{G}(r, \mathbb{P}^n)$ is a projective variety.

We demonstrate that the image of the Plücker embedding is a projective variety by showing that in each affine chart $U_I = \mathbb{A}_I^{\binom{n+1}{r+1}-1}$ of $\mathbb{P}^{\binom{n+1}{r+1}-1}$ indexed by $I \in \binom{[n+1]}{r+1}$, the image $p(\mathbb{G}(r, \mathbb{P}^n))$ defines an affine variety in local coordinates. By permuting the coordinates, we may assume that $I = \{0, \ldots, r\}$. For $\ell \in p(\mathbb{G}(r, \mathbb{P}^n)) \cap U_I$, Stiefel coordinates $A \in \mathbb{S}(r+1, n+1)$ representing ℓ are such that the $(r+1) \times (r+1)$ principal submatrix of A is invertible. Multiplying by the inverse

of this submatrix matrix, we obtain Stiefel coordinates for ℓ of the form

$$\widetilde{A} = \left(\begin{array}{c} \mathrm{Id}_{r+1} \\ \hline A' \end{array} \right).$$

Up to sign, the entries of A' are Plücker coordinates of ℓ in local coordinates, and all Plücker coordinates are polynomials in these entries. The set $p(\mathbb{G}(r, \mathbb{P}^n)) \cap U_I$ is then the graph of a polynomial function over the affine space of entries of A'. The graph of a polynomial function over a variety is a variety so that $p(\mathbb{G}(r, \mathbb{P}^n)) \cap U_I$ defines an affine variety in local coordinates. Hence, the image $p(\mathbb{G}(r, \mathbb{P}^n))$ is a projective variety.

We note that the analysis above also shows the Plücker embedding is injective. Indeed, given $\ell \in \mathbb{G}(r, \mathbb{P}^n)$ with Stiefel coordinates $A \in \mathbb{S}(r+1, n+1)$, there is some $I \in \binom{[n+1]}{r+1}$ such that $p_I(A) \neq 0$. By reordering coordinates, we may assume $I = \{0, \ldots, r\}$ and choose Stiefel coordinates for ℓ of the form $\widetilde{A}$ as above. Up to sign, the entries of the matrix A' are the Plücker coordinates of ℓ in local coordinates on U_I showing that Stiefel coordinates of ℓ may be recovered from the Plücker coordinates of ℓ. For any other point $\ell' \in \mathbb{G}(r, \mathbb{P}^n)$ such that $p(\ell') = p(\ell)$, $\widetilde{A}$ provides Stiefel coordinates for ℓ' as well, showing that the Plücker embedding is injective.

Identifying $\mathbb{G}(r, \mathbb{P}^n)$ with its image under the Plücker embedding, this shows $\mathbb{G}(r, \mathbb{P}^n)$ is a projective variety. The defining ideal $\mathcal{I}(\mathbb{G}(r, \mathbb{P}^n))$ has been well–studied and is generated by quadratics. These quadratics have combinatorial descriptions, which we do not require or include. More about this ideal and its combinatorial properties can be found in [17].

For each $I \in \binom{[n+1]}{r+1}$ the Grassmanian in local coordinates $p(\mathbb{G}(r, \mathbb{P}^n)) \cap U_I$ is isomorphic to an $(r+1)(n-r)$–dimensional affine space. From these local considerations, we arrive at the following result.

Theorem 13. *The Grassmanian $\mathbb{G}(r, \mathbb{P}^n)$ is a smooth projective variety of dimension $(r+1)(n-r)$.*

2.4 Quasi–Projective Varieties

Quasi–projective varieties are Zariski open subsets of projective varieties. All varieties we consider are quasi–projective and in later sections we omit the quantifier quasi–projective and refer to them simply as varieties.

Definition 14. A *quasi–projective variety* is a Zariski open subset of a projective variety.

The closure of a quasi–projective variety $X \subseteq \mathbb{P}^n$ is a projective variety $\overline{X} \subseteq \mathbb{P}^n$ which determines many properties of X. For example, the Zariski topology on X is the induced Zariski topology as a subset of $\overline{X}$. This means that a subvariety of a quasi–projective variety X has the form $X \cap Y$ where $Y \subseteq \mathbb{P}^n$ is a projective variety. Further, as X is a dense open subset of $\overline{X}$, X is irreducible if and only if $\overline{X}$ is irreducible. Smoothness of a point of a quasi–projective variety is also determined from its closure—a point x of a quasi–projective variety $X \subseteq \mathbb{P}^n$ is smooth if it is a smooth point of its closure $\overline{X} \subseteq \mathbb{P}^n$. We then have the notions of the smooth locus and a smooth quasi–projective variety. Last, the dimension of a quasi–projective variety is equal to that of its closure, $\dim X = \dim \overline{X}$.

Fix a quasi–projective variety $X \subseteq \mathbb{P}^n$. Given homogeneous polynomials $f, g \in \mathbb{K}[x_0, \ldots, x_n]$ of the same degree with $g \notin \mathcal{I}(\overline{X})$, the quotient f/g is a well–defined function on the Zariski open set of X where g is nonzero. A function h is *regular* at a point $[x] \in X$ if there is a Zariski neighborhood $U \subseteq X$ of $[x]$ for which h is defined and agrees with a function of the form f/g where $f, g \in \mathbb{K}[x_0, \ldots, x_n]$ are homogeneous polynomials of the same degree and $g \notin \mathcal{I}(\overline{X})$. A function on is regular on X if it is regular at every point of X and rational on X if it is regular on a Zariski open subset of X. The regular functions on a quasi–projective variety X form a ring $\mathbb{K}[X]$ called the *coordinate ring of* X. Theorem 2 may be used to show this notion agrees with our notion of the coordinate ring for an affine variety. On an irreducible quasi–projective variety X, the rational functions form a field $\mathbb{K}(X)$ called the *function field* of X.

We briefly describe products of quasi–projective varieties. Consider the product of projective

spaces $\mathbb{P}^n \times \mathbb{P}^m$. The image of the Segre embedding $\sigma_{n,m} : \mathbb{P}^n \times \mathbb{P}^m \to \mathbb{P}^{(n+1)(m+1)-1}$ defined by

$$\sigma_{n,m}([x_0, \ldots, x_n], [y_0, \ldots, y_m]) = [x_i y_j]_{\substack{i=0,\ldots,n \\ j=0,\ldots,m}}$$

is a projective variety known as a Segre variety [13]. As the Segre embedding is a bijection, we consider $\mathbb{P}^n \times \mathbb{P}^m$ as a projective variety by identifying it with the Segre variety $\operatorname{im} \sigma_{n,m} \subseteq \mathbb{P}^{(n+1)(m+1)-1}$. Given projective varieties $X \subseteq \mathbb{P}^n$ and $Y \subseteq \mathbb{P}^m$, their product $X \times Y$ is defined to be the image $\sigma_{n,m}(X \times Y)$ under the Segre embedding, which is a projective variety. Similarly, given quasi–projective varieties $X \subseteq \mathbb{P}^n$ and $Y \subseteq \mathbb{P}^m$, their product $X \times Y$ is the image $\sigma_{n,m}(X \times Y)$, which is a Zariski open subset of the projective variety $\sigma_{n,m}(\overline{X} \times \overline{Y})$.

2.5 Maps

With the notion of a regular function understood, we define maps between varieties. For a quasi–projective variety X, a map $f : X \to \mathbb{K}^m$ is regular if each of the m coordinate functions is regular. We extend this definition of a regular map to define regular and rational maps of quasi–projective varieties.

Definition 15. Let X and Y be quasi–projective varieties with $Y \subseteq \mathbb{P}^m$. A map $\pi : X \to Y$ is *regular at* $x \in X$ if there is an affine chart $(\mathbb{A}_i^m, \phi_i)$ of $\mathbb{P}^m$ and a Zariski open set $U \subseteq X$ containing x for which $\pi(U) \subseteq \mathbb{A}_i^m$ and the composition

$$U \xrightarrow{\pi} \mathbb{A}_i^m \xrightarrow{\phi_i} \mathbb{K}^m$$

is a regular map. A map $\pi : X \to Y$ is a *regular map* if it is regular at every point of X.

A regular map $\pi : X \to Y$ with a regular inverse is an *isomorphism* and we say the varieties X and Y are isomorphic.

If $\pi : X \to Y$ is a regular map and $f : Y \to \mathbb{K}$ is a regular function, then the composition $f \circ \pi$ is a regular function on X. That is, precomposing regular functions with π gives a map of coordinate rings $\pi^* : \mathbb{K}[Y] \to \mathbb{K}[X]$ called the *pullback* by π. We note an important property of

pullbacks. The closure of a regular map $\pi : X \to Y$ is dense in Y exactly when the pullback $\pi^* : \mathbb{K}[Y] \to \mathbb{K}[X]$ is injective. A regular map π satisfying either of these properties is said to be *dominant*.

Consider a regular map of affine varieties $\pi : X \to Y$. For a subvariety $Z = \mathcal{V}(f_1, \ldots, f_k) \subseteq Y$ defined by $f_1, \ldots, f_k \in \mathbb{K}[Y]$, the preimage of Z is the subvariety $\pi^{-1}(Z) = \mathcal{V}(f_1 \circ \pi, \ldots, f_k \circ \pi) \subseteq X$. That is, regular maps of affine varieties are continuous in the Zariski topology. As maps of quasi–projective varieties are locally described by regular maps of affine varieties restricted to open sets, it follows that regular maps of quasi–projective varieties are continuous in the Zariski topology.

For general $y \in Y$, the dimension of the fiber $\pi^{-1}(y)$ can be determined [13].

Theorem 16. *If $\pi : X \to Y$ is a dominant regular map of irreducible varieties with $\dim X = n$ and $\dim Y = m$, then $n \geq m$ and*

- *for every $y \in Y$, $\dim \pi^{-1}(y) \geq n - m$;*
- *there is a nonempty Zariski open set $U \subseteq Y$ such that $\dim \pi^{-1}(y) = n - m$ for $y \in U$.*

Since the preimage of a variety is a variety, the closure of the image $\overline{\pi(X)}$ of an irreducible variety X under a regular map $\pi : X \to Y$ is also irreducible. The Stiefel manifold $\mathbb{S}(r+1, n+1)$ is irreducible as it is a Zariski open subset of affine space, and the map $\pi : \mathbb{S}(r+1, n+1) \to \mathbb{G}(r, \mathbb{P}^n)$ is regular and surjective. Thus the Grassmanian $\mathbb{G}(r, \mathbb{P}^n)$ is irreducible. Further, Theorem 16 allows us to again compute the dimension of $\mathbb{G}(r, \mathbb{P}^n)$. As a fiber of $\mathbb{S}(r+1, n+1) \to \mathbb{G}(r, \mathbb{P}^n)$ is isomorphic to $\mathrm{GL}(r+1)$, we have that

$$\begin{aligned} \dim \mathbb{G}(r, \mathbb{P}^n) &= \dim \mathbb{S}(r+1, n+1) - \dim \mathrm{GL}(r+1) \\ &= (r+1)(n+1) - (r+1)^2 \\ &= (r+1)(n-r). \end{aligned}$$

We provide a useful criterion for determining whether a variety is irreducible

Proposition 17. *Let $\pi : X \to Y$ be a dominant map of varieties and Y be irreducible. If there is an open cover $Y = \cup_i U_i$ of Y by Zariski open sets $U_i \subseteq Y$ such that $\pi^{-1}(U_i) \subseteq X$ is irreducible for all i, then X is irreducible.*

Proof. Note that some irreducible component $Z \subseteq X$ necessarily maps dominantly to Y. Then for each i, we must have $\pi^{-1}(U_i) \subseteq Z$. Indeed, as the image $\pi(Z)$ is dense in Y, it intersects U_i nontrivially and hence $\pi^{-1}(U_i) \cap Z$ is nonempty. As the preimage $\pi^{-1}(U_i) \subseteq X$ is irreducible, it follows that $\pi^{-1}(U_i) \subseteq Z$. Thus, for a point $x \in X$, $\pi(x) \in U_i$ for some i and

$$x \in \pi^{-1}(\pi(x)) \subseteq \pi^{-1}(U_i) \subseteq Z.$$

Therefore, $X = Z$ and X is irreducible. □

The image of a variety under a regular map need not be a variety. However, there is a general statement that can be made about the image of a regular map. The following can be proved by considering integral extensions of rings, as is done in [13].

Theorem 18. *If $\pi : X \to Y$ is a regular map, the image $\pi(X)$ contains a Zariski open subset of the closure $\overline{\pi(X)} \subseteq Y$.*

2.5.1 Branched Covers

We define an important class of dominant maps.

Definition 19. A *branched cover* $\pi : X \to Y$ is a dominant map of irreducible varieties X and Y of the same dimension.

If X and Y are irreducible varieties and $\pi : X \to Y$ is a dominant map, the pullback π^* is injective and extends to a map of function fields $\pi^* : \mathbb{K}(Y) \to \mathbb{K}(X)$. Thus, we consider $\mathbb{K}(X)$ as a field extension of $\mathbb{K}(Y)$, written $\mathbb{K}(X)/\mathbb{K}(Y)$. For a branched cover $\pi : X \to Y$, the extension $\mathbb{K}(X)/\mathbb{K}(Y)$ is finite as these fields have the same transcendence degree.

Definition 20. The *degree* $\deg \pi$ of a branched cover $\pi : X \to Y$ is the degree of the field extension $\mathbb{K}(X)/\mathbb{K}(Y)$.

The following is an immediate consequence of this definition.

Proposition 21. *If $\pi : X \to Y$ and $\lambda : Y \to Z$ are branched covers, then $\lambda \circ \pi : X \to Z$ is a branched cover and* $\deg(\lambda \circ \pi) = (\deg \lambda)(\deg \pi)$.

A branched cover $\pi : X \to Y$ is *nontrivial* if $\deg \pi > 1$. For a branched cover $\pi : X \to Y$, a general fiber is zero–dimensional and the degree $\deg \pi$ is the cardinality of a general fiber. Indeed, consider a branched cover $\pi : X \to Y$. By the primitive element theorem, the function field $\mathbb{K}(X)$ is a simple extension of $\mathbb{K}(Y)$—there is an element $\alpha \in \mathbb{K}(X)$ such that $\mathbb{K}(X) = \mathbb{K}(Y)(\alpha)$, which we may assume to be a regular function by restricting to an open subset of X. As α is algebraic over $\mathbb{K}(Y)$, it satisfies an irreducible polynomial $g \in \mathbb{K}(Y)[t]$ of degree $\deg \pi$. There is a Zariski open set $U \subseteq Y$ for which the coefficients of g are regular functions and the discriminant of g is nonzero. For $y \in V$, evaluating g at y gives a polynomial $g_y(t) \in \mathbb{K}[t]$ with $\deg \pi$ distinct zeros since $\mathbb{K}$ is algebraically closed. The function α is a bijection between the points $x \in \pi^{-1}(y)$ and the $\deg \pi$ zeros of g_y. Thus, we've proved the following theorem.

Theorem 22. *If $\pi : X \to Y$ is a branched cover, there is a Zariski open set $U \subseteq Y$ such that for each $y \in U$ the fiber $\pi^{-1}(y)$ consists of* $\deg \pi$ *distinct points.*

We will require a generalization of Theorem 22 to include points of a fiber counted with multiplicity. We briefly describe how we assign multiplicity to an isolated point of the fiber $x \in \pi^{-1}(y)$ for a branched cover $\pi : X \to Y$ and a point $y \in Y$.

Given a point $x \in X$, a pair (f, U) is a germ of X at x if $U \subseteq X$ is a Zariski open set, $x \in U$, and $f : U \to \mathbb{K}$ is a regular function. Two germs are equivalent $(f, U) \sim (g, V)$ if the functions f and g agree on the intersection $U \cap V$, and the operations of addition and multiplication for germs are defined pointwise. Write $\mathcal{O}_{X,x}$ for the ring of germs of X at x. This ring is a local ring—$\mathcal{O}_{X,x}$ has a unique maximal ideal $\mathfrak{m}_x = \{(f, U) \in \mathcal{O}_{X,x} : f(x) = 0\}$.

If $\pi : X \to Y$ is a branched cover and $x \in \pi^{-1}(y)$, then there is a pullback on germs $\pi^* : \mathcal{O}_{Y,y} \to \mathcal{O}_{X,x}$ defined by precomposing with the branched cover π, $\pi^*(f, U) = (f \circ \pi, \pi^{-1}(U))$. If $\mathfrak{m}_y \subseteq \mathcal{O}_{Y,y}$ is the unique maximal ideal of $\mathcal{O}_{Y,y}$, let $\pi^*\mathfrak{m}_y \subseteq \mathcal{O}_{X,x}$ be the ideal generated by the

image of $\mathfrak{m}_y$ under π^*. If x is an isolated point of the fiber $\pi^{-1}(y)$, then the quotient $\mathcal{O}_{X,x}/\pi^*\mathfrak{m}_y$ is a finite–dimensional $\mathbb{K}$–vector space.

Definition 23. Let $\pi : X \to Y$ be a branched cover, $y \in Y$, and $x \in \pi^{-1}(y)$ be an isolated point. The *multiplicity* $\mu(x)$ of x is the dimension of the quotient $\mathcal{O}_{X,x}/\pi^*\mathfrak{m}_y$ as a $\mathbb{K}$–vector space.

An isolated point of the fiber $x \in \pi^{-1}(y)$ has multiplicity one exactly when there are local coordinates around x such that the Jacobian $D\pi(x)$ has rank $\dim X$. A point $x \in \pi^{-1}(y)$ is a *smooth point* of the fiber if it has multiplicity one and a *double point* of the fiber if it has multiplicity two.

Let $X \subseteq \mathbb{K}^n$ be an affine variety defined by a system F of m polynomials and $x \in X$ be an isolated point. Then we may consider F as a regular map $F : \mathbb{K}^n \to \mathbb{K}^m$ and $x \in X$ as an isolated point of the fiber $F^{-1}(0)$. As the ring of germs $\mathcal{O}_{\mathbb{K}^n,x}$ is the localization $\mathbb{K}[x_1, \ldots, x_n]_{\mathfrak{m}_x}$ at the maximal ideal $\mathfrak{m}_x$, it follows that the multiplicity of x may be expressed as

$$\mu_F(x) = \dim \left(\mathbb{K}[x_1, \ldots, x_n]/\langle F\rangle\right)_{\mathfrak{m}_x}.$$

In more generality, this multiplicity depends only on the ideal $\langle F\rangle$. If a variety $X = \mathcal{V}(I)$ is defined by an ideal I which is not necessarily radical, we may assign a multiplicity $\mu_I(x)$ to an isolated point of X.

We can now state the more general version of Theorem 22. A proof is given in [13, 15, 18].

Theorem 24. *Let $\pi : X \to Y$ be a branched cover and $y \in Y$.*

1. *The fiber $\pi^{-1}(y)$ contains at most $\deg \pi$ isolated points counting multiplicity.*
2. *There is a Zariski open set $U \subseteq Y$ for which the fiber $\pi^{-1}(y)$ is finite and consists of $\deg \pi$ points counting multiplicity.*

If $\pi : X \to Y$ is a branched cover, Theorem 24 shows there is a Zariski open set $U \subseteq Y$ for which the fiber $\pi^{-1}(y)$ consists of $\deg \pi$ smooth points.

2.5.2 Rational Maps

We now turn our attention to rational maps.

Definition 25. Let X and Y be irreducible varieties. A *rational map* $\pi : X \dashrightarrow Y$ is a regular map $\pi : U \to Y$ defined on a Zariski open set $U \subseteq X$.

Two rational maps are equal if they agree on a Zariski open set. As with regular maps, a rational map $\pi : X \dashrightarrow Y$ is dominant if its image is dense in Y. A dominant rational map $\pi : X \dashrightarrow Y$ defined on a Zariski open set $U \subseteq X$ defines a pullback of function fields $\pi^* : \mathbb{K}(Y) \to \mathbb{K}(U) = \mathbb{K}(X)$. That is, precomposing a rational function $f : Y \dashrightarrow \mathbb{K}$ with $\pi : X \dashrightarrow Y$ over the locus where they are defined gives a rational function $f \circ \pi : X \dashrightarrow Y$, and this determines a map of fields $\pi^* : \mathbb{K}(Y) \to \mathbb{K}(X)$.

If $\pi : X \dashrightarrow Y$ is a rational map and there exists $\psi : Y \dashrightarrow X$ such that the compositions $\psi \circ \pi : X \dashrightarrow X$ and $\pi \circ \psi : Y \dashrightarrow Y$ are identity maps when they are defined, then we say π is *birational* or a *birational isomorphism*, and X and Y are *birational*. In this case, the pullback $\pi^* : \mathbb{K}(Y) \to \mathbb{K}(X)$ is an isomorphism of fields. By an application of Theorem 18, we have the following.

Theorem 26. *If $\pi : X \dashrightarrow Y$ is a birational map, then there are Zariski open sets $U \subseteq X$ and $V \subseteq Y$ such that π is regular on U, $\pi(U) \subseteq V$, and $\pi : U \to V$ is an isomorphism.*

We show that if X and Y are irreducible varieties such that their function fields $\mathbb{K}(X)$ and $\mathbb{K}(Y)$ are isomorphic, then X and Y are birational. We note that by restricting to coordinate charts, we assume $X \subseteq \mathbb{K}^n$ and $Y \subseteq \mathbb{K}^m$. Denote the coordinate functions on $\mathbb{K}^n$ and $\mathbb{K}^m$ by $x_1, \ldots, x_n$ and $y_1, \ldots, y_m$ respectively. If $\pi : X \dashrightarrow X$ is a rational function such that $\pi^* : \mathbb{K}(X) \to \mathbb{K}(X)$ is the identity map, then $\pi^*(x_i) = x_i$ for each $i = 1, \ldots, n$ so that $\pi : X \dashrightarrow X$ is the identity map restricted to the Zariski open set that π is defined. From this, it suffices to show that for any map of fields $\theta : \mathbb{K}(Y) \to \mathbb{K}(X)$, there is a rational map $\pi : X \dashrightarrow Y$ such that $\theta = \pi^*$. Given a map of fields $\theta : \mathbb{K}(Y) \to \mathbb{K}(X)$, the rational map $\pi : X \dashrightarrow Y$ defined by $\pi(x) = (\theta(y_1)(x), \ldots, \theta(y_m)(x))$ satisfies $\theta = \pi^*$.

Proposition 27. *Irreducible varieties X and Y are birational if and only if their function fields $\mathbb{K}(X)$ and $\mathbb{K}(Y)$ are isomorphic.*

Combining Theorem 26 and Theorem 27, we see that if two irreducible varieties have isomorphic function fields, then they contain isomorphic Zariski open sets.

2.6 Topological Considerations

We consider complex varieties, those varieties defined over $\mathbb{K} = \mathbb{C}$. Recall the Euclidean topology on $\mathbb{C}^n$ is generated by open balls determined by the Euclidean distance function. As subspaces of $\mathbb{C}^n$, an affine variety inherits a Euclidean topology. Similarly, projective space $\mathbb{P}^n$ and projective varieties inherit a Euclidean topology by gluing the Euclidean topology on the affine charts. As subsets of projective spaces, quasi–projective varieties also inherit a Euclidean topology. We require a number of topological results related to the Euclidean topology on quasi–projective varieties which involve some level of interplay between the Zariski and Euclidean topologies on a variety. Proofs of these and similar results may be found in texts such as [13, 15, 18]. We start with the following fundamental result.

Theorem 28. *A Zariski open set of an irreducible variety is open, dense, connected, and path–connected in the Euclidean topology.*

As the smooth locus of a variety is a Zariski open set, it follows that the smooth locus of an irreducible variety is path–connected in the Euclidean topology. There is a converse which provides a criterion for determining whether a variety is irreducible.

Theorem 29. *A variety is irreducible if and only if its smooth locus is path–connected.*

There is more that can be said on the matter. The following result is an application of commutative algebra [16, 13].

Theorem 30. *A smooth point of a variety belongs to a unique irreducible component.*

Thus, a path contained in the smooth locus of a variety is contained in a single component. It follows that the path–connected components of the smooth locus of a variety are in bijection with its irreducible components.

Let X be a smooth, irreducible variety. In local coordinates, X is defined by a polynomial system F and the Jacobian DF has constant rank. Thus, by the implicit function theorem, X is an analytic manifold. In particular, around every point $x \in X$ there are analytic coordinate charts—for every $x \in X$, there is a Euclidean neighborhood $U \subseteq X$ of x that is homeomorphic with $\mathbb{C}^n$ and regular functions on U pull back to analytic functions on $\mathbb{C}^n$. By virtue of this, a proper subvariety $Z \subseteq X$ cannot contain a Euclidean open subset of X [19]. In addition, X is locally path–connected so that a subset $U \subseteq X$ is connected if and only if it is path–connected. We abuse notation and write $\mathcal{V}(f)$ for the zeros of an analytic function f.

Lemma 31. *If X is a smooth, irreducible variety and $U \subseteq X$ is a connected, Euclidean open set, then the complement $U \setminus Z$ of a proper subvariety $Z \subseteq X$ is connected.*

Proof. By working in local coordinates on X, we assume that $X \subseteq \mathbb{C}^m$. Further, given $f \in \mathcal{I}(Z)$, one has $Z \subseteq \mathcal{V}(f)$. Thus, without loss of generality, we may assume that Z is of the form $Z = \mathcal{V}(f)$. For a final reduction, it suffices to consider the case that U is an analytic coordinate chart. Indeed, for any two points $x, y \in U \setminus Z$ there is a path $\gamma : [0,1] \to U$ such that $\gamma(0) = x$ and $\gamma(1) = y$. By choosing analytic coordinate charts around points along γ, this path is contained in a connected union of analytic coordinate charts. If the complement of Z in each of these analytic coordinate charts is path–connected, then their union is as well.

Let U be an analytic coordinate chart and recall that $Z = \mathcal{V}(f)$. By pulling back f to an analytic function $\widetilde{f}$ on $\mathbb{C}^n$, the set $U \setminus Z$ is homeomorphic to the complement $\mathbb{C}^n \setminus \mathcal{V}(\widetilde{f})$. For $x, y \in \mathbb{C}^n \setminus \mathcal{V}(\widetilde{f})$, let $\ell(t) = (1-t)x + ty$ for $t \in \mathbb{C}$ be the line between x and y. The analytic function $\widetilde{f}(\ell(t))$ has finitely many zeros for $|t - 1/2| \leq 1/2$ since otherwise it is identically zero which implies that Z is not a proper subvariety of X. Thus, there is a path from $t = 0$ to $t = 1$ avoiding the zeros of $\widetilde{f}(\ell(t))$. Composing this path with ℓ gives a path from x to y contained in $\mathbb{C}^n \setminus \mathcal{V}(\widetilde{f})$. Thus, $\mathbb{C}^n \setminus \mathcal{V}(\widetilde{f})$ and $U \setminus Z$ are path–connected. □

In [18], Lemma 31 is used to prove that branched covers of smooth varieties are locally open maps in the following sense.

Theorem 32. *If $\pi : X \to Y$ is a branched cover of smooth varieties and $x \in X$ is an isolated point of the fiber $\pi^{-1}(\pi(x))$, then for every Euclidean neighborhood $U \subseteq X$ of x, the image $\pi(U)$ contains a Euclidean neighborhood of $\pi(x)$.*

3. COMPUTATIONAL ALGEBRAIC GEOMETRY

The correspondence between ideals and affine varieties allows one to represent an affine variety by a polynomial system, which may be encoded by finite data. Computers then allow one to study varieties via these data. Computational and numerical algebraic geometry is the collection of tools and techniques used for studying varieties and polynomial systems systematically in this way. The list of methods provided here is not comprehensive—the areas of computational and numerical algebraic geometry are active areas of research for which new methods are frequently developed. We present methods relevant to our study of Galois groups of enumerative problems.

3.1 Rational Univariant Representation

We first consider a symbolic method of reducing the study of polynomial systems and multivariate ideals to that of a univariate polynomial. We work over a field $\Bbbk$ of characteristic zero with algebraic closure $\mathbb{K}$. If $\Bbbk$ is a computable field such as $\mathbb{Q}$,$\mathbb{Q}(i)$, or $\mathbb{Q}(x)$, the operations below can be carried out with exact arithmetic.

Fix an ideal $I \subseteq \Bbbk[x_1, \ldots, x_n]$ such that the variety $\mathcal{V}(I) \subseteq \mathbb{K}^n$ is zero–dimensional. The quotient $\Bbbk[x_1, \ldots, x_n]/I$ is a finite–dimensional $\Bbbk$–vector space whose dimension is the cardinality of $\mathcal{V}(I)$ with each point $p \in \mathcal{V}(I)$ counted with its multiplicity $\mu_I(p)$. Indeed, multiplication by an element $f \in \Bbbk[x_1, \ldots, x_n]$ determines a linear map of $\Bbbk$–vector spaces $m_f : \Bbbk[x_1, \ldots, x_n]/I \to \Bbbk[x_1, \ldots, x_n]/I$ and the structure of this map is given by Stickelberger's theorem [20].

Theorem 33 (Stickelberger)**.** *The eigenvalues of the linear map m_f are the values $f(p) \in \mathbb{K}$ for $p \in \mathcal{V}(I)$. Each eigenvalue $\xi \in \mathbb{K}$ has multiplicity equal to $\sum_{p \in f^{-1}(\xi) \cap \mathcal{V}(I)} \mu_I(p)$.*

Note that after a choice of basis for $\Bbbk[x_1, \ldots, x_n]/I$, the linear map m_f may be represented by a $\Bbbk$–valued matrix, allowing for the computation of quantities such as the determinant, trace, and characteristic polynomial χ_f. A consequence of Stickelberger's theorem is that these quantities are also readily computed from the points of $\mathcal{V}(I)$ and their multiplicities. Further, when f separates the points of $\mathcal{V}(I)$, each point $p \in \mathcal{V}(I)$ corresponds to a unique zero $f(p) \in \mathcal{V}(\chi_f)$ of the same

multiplicity $\mu_I(p)$. Thus, we may enumerate the points of a variety and their multiplicities by studying zeros of univariate polynomials.

Consider f as a map $\mathcal{V}(I) \to \mathcal{V}(\chi_f)$. The pullback $f^* : \mathbb{K}[\mathcal{V}(\chi_f)] \to \mathbb{K}[\mathcal{V}(I)]$ is an injective linear map of vector spaces of the same dimension and so is an isomorphism. In particular, f^* is surjective and the coordinate functions $x_1, \ldots, x_n$ on $\mathcal{V}(I)$ are polynomial functions in f. Further, there is a regular map $\phi : \mathcal{V}(\chi_g) \to \mathcal{V}(I)$ that is inverse to f. When this occurs, the triple (f, χ_f, ϕ) is a *rational univariate representation* of I. Algorithms for computing linear forms f separating points of a zero-dimensional variety and the resulting rational univariate representation are given in [21] and have been implemented in [22].

3.1.1 Example

We demonstrate the use of the rational univariate representation for studying the variety $X \subseteq \mathbb{C}^2$ defined by the ideal

$$I = \langle x^2y - 2y + 1, xy^2 + 3x^2 - y + 1 \rangle \subseteq \mathbb{Q}[x, y].$$

We use the `Macaulay2` software package `RealRoots.m2` to compute a rational univariate representation of this ideal. After inputting the data of the ideal, the command `rationalUnivariateRepresentation` computes a separating linear form f for the variety X, the characteristic polynomial χ_f given by `ch`, and the rational map ϕ given by `ph`.

```
i1 : R = QQ[x,y]

i2 : I = ideal(x^2*y-2*y+1,x*y^2+3*x^2-y+1)

i3 : (f,ch,ph) = rationalUnivariateRepresentation(I)

i4 : f

o4 = x + y

i5 : ch

      6   1 5   37 4   127 3   154 2   169    19
```

```
o5 = Z  - -Z  - --Z  + ---Z  - ---Z  + ---Z - --
          2       6       3        3        6       3
```

One may study the points of X and their multiplicities by computing the zeros of the univariate polynomial `ch`. For example, `ch` is square–free, so all points of X are smooth.

```
i6 : ch' = diff(Z,ch)

i7 : gcd(ch,ch')

o7 = 1
```

Since `ch` is a polynomial of degree six with no multiple zeros, X consists of six smooth points.

3.2 Numerical Homotopy Continuation

In applications, one often wants numerical approximations to zeros of a polynomial system. For square systems, those with the same number of polynomials as variables, numerical methods such as Newton's method may be used to obtain approximate zeros. Numerical homotopy continuation is an example of such a numerical method and it produces numerical zeros of a polynomial system from known zeros of a given polynomial system. We assume throughout that our polynomials and points are defined over the complex numbers $\Bbbk = \mathbb{C}$.

We begin with some notation and terminology. A *start system* is a square polynomial system G such that numerical approximations for isolated smooth zeros of G are known, and a *target system* is a square polynomial system F whose zeros we would like to compute. A *homotopy* $H(x,t)$ between a start system G and a target system F is a system in the additional variable t such that $H(x,0) = G$ and $H(x,1) = F$. A homotopy H is a family of square polynomial systems that is parameterized by t and interpolates between the start system G and the target system F.

Given a smooth isolated zero of the start system $x_0 \in \mathcal{V}(G)$, the Jacobian $DH(x_0,0) = DG(x_0)$ has full rank and $(x_0,0)$ is a smooth point of a one–dimensional component of $\mathcal{V}(H)$. By the implicit function theorem, this component is locally described by a function of t. Treating

the variables x as functions of t and differentiating yields the Davidenko differential equation

$$\left(\frac{\partial}{\partial x}H(x,t)\right)\left(\frac{d}{dt}x(t)\right)+\frac{\partial}{\partial t}H(x,t)=0,\ x(0)=x_0,$$

which locally describes the component [23]. We say that x_0 gets tracked to $x(1)$ by solving this initial–value problem along a path from $t=0$ to $t=1$. Thus we may obtain zeros of the target system, as the value $x(1)$ is a zero of $H(x,1)=F(x)$. Typically, this initial–value problem is solved by alternatingly taking incremental steps towards $t=1$ through a *predictor* such as Euler's method or Runge–Kutta methods and then applying a *corrector* such as the Newton operator. More on solving initial–value problems through predictor–corrector methods can be found in [24, 25]. The process of tracking zeros is illustrated in Figure 3.1.

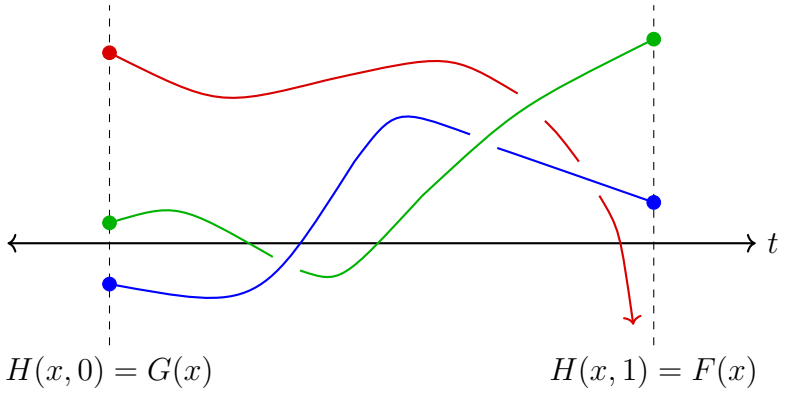

Figure 3.1: An illustration of a homotopy

If $x_1 \in \mathcal{V}(F)$ is a zero of the target system that lies in the smooth locus of $\mathcal{V}(H)$, the coordinates of x_1 may be obtained by solving an initial–value problem determined by the Davidenko equations. When x_1 is a singular point of $\mathcal{V}(H)$, solutions to such an initial–value problem may be computed for values near $t=1$ and various limiting methods may be used to approximate x_1. For a sufficient choice of start system, all isolated zeros of F are obtained in this way. While methods of numerical homotopy continuation may be applied to more general analytic systems, this feature is not shared

with them. There are various implementations of numerical homotopy continuation methods such as `HomotopyContinuation.jl`, `bertini`, and `NAG4M2` [26, 27, 28].

3.2.1 Example

We demonstrate how numerical homotopy continuation may be used to compute the zeros of the polynomial system

$$F(x,y) = \begin{pmatrix} x^2y^2 - 3x^2y + 2y^2 - 1 \\ xy^2 + 3x^2 - y + 1 \end{pmatrix}.$$

From the rational univariate representation of the ideal $\langle F \rangle$ calculated in Example 3.1.1, there are six smooth zeros of F. Thus we choose our start system G to have six zeros which are easily computed,

$$G = \begin{pmatrix} x^3 - 1 \\ y^2 - 1 \end{pmatrix}.$$

We use the `Macaulay2` software package `NumericalAlgebraicGeometry.m2` to track the zeros of G to zeros of F. The `track` method uses the straight–line homotopy

$$H(x,t) = (1-t)G(x) + \gamma t F(x),$$

where γ is a complex number.

```
i1 : R = QQ[x,y]

i2 : F = {x^2*y-2*y+1,x*y^2+3*x^2-y+1}

i3 : G = {x^3-1,y^2-1}

i4 : solns = track(G,F,startSolns,gamma=>random(CC))
```

We check that the track command obtained six zeros of F and we show they are distinct by

examining their coordinates.

```
i5 : #solns

o5 = 6

i6 : netList solns

     +-----------------------------------------+
o6 = |{-1.54216, -2.64371}                     |
     +-----------------------------------------+
     |{-1.19144, 1.72271}                      |
     +-----------------------------------------+
     |{-.0378421-.424283*ii, .458914+.0067642*ii}|
     +-----------------------------------------+
     |{-.0378421+.424283*ii, .458914-.0067642*ii}|
     +-----------------------------------------+
     |{1.40464-.163245*ii, .251588-2.15112*ii}   |
     +-----------------------------------------+
     |{1.40464+.163245*ii, .251588+2.15112*ii}   |
     +-----------------------------------------+
```

3.3 Numerical Certification

Once approximate zeros of a polynomial system are obtained, one would like some guarantee that the approximation lies close to a zero of the system. We detail one flavor of numerical certification which offers such guarantees. These methods are based on interval arithmetic, which we briefly develop.

We remark that given real intervals A and B, their setwise sum, difference, and product are again real intervals. A (one–dimensional) complex interval is a set of the form $A + Bi = \{x + yi : x \in A, y \in B\}$ for two real intervals A and B, and we denote the set of complex intervals by $\mathbb{IC}$. We identify a single complex number $x \in \mathbb{C}$ by the complex interval $[\mathrm{re}(x), \mathrm{re}(x)] + [\mathrm{im}(x), \mathrm{im}(x)]i$. The setwise sum and difference of complex intervals is again a complex interval, however the setwise product need not be. For real intervals A, B, C, D, we define the product of

two complex intervals $A + Bi$ and $C + Di$ to be the complex interval

$$(A + Bi)(C + Di) = (AC - BD) + (AD + BC)i.$$

That is, given $I, J \in \mathbb{IC}$, the product IJ is defined to be the smallest complex interval that contains the setwise product. In particular, there is an inclusion $\{xy : x \in I, y \in J\} \subseteq IJ$. We note that complex intervals do not satisfy a distributive law—for complex intervals $I, J, K \in \mathbb{IC}$, there is an inclusion $I(J + K) \subseteq IJ + IK$, but equality may not hold.

An n–dimensional complex interval is the Cartesian product of n one–dimensional complex intervals, $I = I_1 \times \cdots \times I_n$. The set of all n–dimensional complex intervals is the space $\mathbb{IC}^n$ with addition, subtraction, and multiplication each defined componentwise. Using these operations, we also define scalar multiplication by an element $I \in \mathbb{IC}$ and multiplication of $\mathbb{IC}$–valued matrices.

Given a complex interval $I \in \mathbb{IC}^n$ and a polynomial system F, we would like to bound the set of possible outputs $\{F(x) : x \in I\}$ by a complex interval. Using arithmetic of complex intervals as above, we may evaluate the expression $F(I) \in \mathbb{IC}^n$ to obtain a bounding interval. As equivalent algebraic expressions for F may provide different bounding intervals, we define an interval enclosure to be a map $\square F : \mathbb{IC}^n \to \mathbb{IC}^n$ that provides a choice of bounding complex interval $\{F(x) : x \in I\} \subseteq \square F(I)$.

We would now like to utilize interval arithmetic to isolate zeros of a square polynomial system F in n variables. Given a point $x \in \mathbb{C}^n$, an invertible matrix $Y \in \mathrm{GL}(n)$, and interval enclosures $\square F$ and $\square JF$ of the system F and its Jacobian JF respectively, the *Krawczyk operator* $K_{x,Y}$ acts on the set of n–dimensional complex intervals by

$$K_{x,Y}(I) = x - Y \cdot \square F(x) + (\mathrm{Id}_n - Y \cdot \square JF(I))(I - x).$$

There are different heuristics for the parameters x and Y, but typically one takes x to be an approximate zero of F and Y to be the inverse of the Jacobian $JF(x)$ at x. With these choices, the Krawczyk evaluated at a point x is the classical Newton operator. As such, the Krawczyk operator

is a generalization of the Newton operator for interval arithmetic [29]. The relationship between the Krawczyk operator and the zeros of F is given by the following.

Theorem 34. *Let F be a system of n polynomials in n variables. If $x \in \mathbb{C}^n$, $Y \in \mathrm{GL}(n)$, and $I \in \mathbb{IC}^n$ are such that $K_{x,Y}(I) \subseteq I$, then I contains a zero of F.*

The first proofs of this result were given for real intervals by Moore and for complex intervals by Rump [30, 31]. While we do not require them, there are variants of this fundamental result used in practice that allow one to prove that a complex interval I contains a unique zero of F. The use of interval enclosures allows one to verify the hypothesis of Theorem 34 using floating point arithmetic. There are softwares such as `HomotopyContinuation.jl` which implement these methods to isolate zeros of polynomial systems with interval arithmetic [29].

3.3.1 Example

Consider the system

$$F(x,y) = \begin{pmatrix} x^2y^2 - 3x^2y + 2y^2 - 1 \\ xy^2 + 3x^2 - y + 1 \end{pmatrix}.$$

We use the software package `HomotopyContinuation.jl` in `julia` to certify the approximate zeros obtained in Example 3.2.1. In particular, they converge under Newton's method to zeros of the system F.

```
julia> @polyvar x y

julia> F = [x^2*y-2*y+1,x*y^2+3*x^2-y+1]

julia> solns = ...

julia> certify(F,solns)
CertificationResult
===================
• 6 solution candidates given
• 6 certified solution intervals (2 real, 4 complex)
• 6 distinct certified solution intervals (2 real, 4 complex)
```

Thus, the software was able to find six disjoint complex intervals, each containing a zero of F. Further, we can check that our approximate zeros lie in these intervals, which verifies our approximations are accurate.

4. GALOIS THEORY IN ENUMERATIVE GEOMETRY

4.1 The Galois Group of an Enumerative Problem

The Galois group of an enumerative problem reflects the intrinsic structure and symmetry of the problem. We provide both a geometric definition and an algebraic definition for the Galois group and prove their equivalence. We assume throughout that our field of definition is the complex numbers $\Bbbk = \mathbb{C}$.

4.1.1 Geometric Monodromy Groups

We begin with an important property of a branched cover $\pi : X \to Y$ of degree d. By Theorem 22, there is a Zariski open set $U \subseteq Y$ such that for $y \in U$, the fiber $\pi^{-1}(y)$ consists of d distinct points. By restricting π, we assume that $U \subseteq \mathrm{sm}(Y)$. For each point $y \in U$ and a point of the fiber $x \in \pi^{-1}(y)$, in local coordinates the Jacobian at $D\pi(x)$ has full rank. By the implicit function theorem, π is a local diffeomorphism of Euclidean neighborhoods of x and y. Thus, the restriction $\pi : \pi^{-1}(U) \to U$ is a degree d covering space of smooth varieties.

Definition 35. The *Étale locus* of a branched cover $\pi : X \to Y$ is the maximal Zariski open set $U \subseteq Y$ for which the restriction $\pi : \pi^{-1}(U) \to U$ is a covering space of smooth varieties.

Recall that a covering space $\pi : X \to Y$ satisfies the homotopy lifting property—if Z is any space and $H : [0,1] \times Z \to Y$ is a continuous map, any continuous map $\widetilde{H}_0 : Z \to X$ lifting $H|_{\{0\}\times Z}$ extends to a unique map $\widetilde{H} : [0,1] \times Z \to X$. In particular, if $\gamma : [0,1] \to Y$ is a path starting at $y \in Y$ and $x \in \pi^{-1}(y)$ is a point of the fiber, then there is a lifted path $\widetilde{\gamma}_x : [0,1] \to X$ which starts at x.

Given a covering space $\pi : X \to Y$, a loop $\gamma : [0,1] \to Y$ based at $y \in Y$ satisfies $\gamma(0) = \gamma(1) = y$ and determines a permutation of the fiber $\pi^{-1}(y)$. Indeed, for every point of the fiber $x \in \pi^{-1}(y)$, there is a lifted path $\widetilde{\gamma}_x : [0,1] \to X$ starting at x and ending at $\widetilde{\gamma}_x(1) \in \pi^{-1}(y)$. The assignment $x \to \widetilde{\gamma}_x(1)$ is a permutation of $\pi^{-1}(y)$, as the reverse loop $\gamma'(t) = \gamma(1-t)$ determines the inverse assignment. We remark that by the homotopy lifting property, if γ_1 and γ_2 are two loops

based at y which are homotopic through a family of loops based at y, then their lifts determine same permutation of $\pi^{-1}(y)$. The *monodromy group* $\mathcal{M}_{\pi,y}$ of the covering space $\pi : X \to Y$ based at $y \in Y$ is the subgroup of the permutation group of the fiber $\pi^{-1}(y)$ obtained from lifting loops in Y based at y. More on monodromy groups of covering spaces can be found in [32, 33].

Definition 36. The *monodromy group* $\mathcal{M}_{\pi,y}$ of a branched cover $\pi : X \to Y$ based at $y \in Y$ is the monodromy group of its restriction $\pi : \pi^{-1}(U) \to U$ to the Étale locus $U \subseteq Y$ of π.

As Y is irreducible, the Étale locus $U \subseteq Y$ is path–connected and a different choice of base point yields an isomorphic monodromy group. Indeed, for $y, y' \in U$, there is a path $\ell : [0,1] \to U$ starting at y and ending at y' with reverse path $\ell'(t) = \ell(1-t)$. Given a loop γ based at y, concatenating the paths ℓ', γ, and ℓ gives a loop based at y'. This gives rise to an isomorphism of monodromy groups $\mathcal{M}_{\pi,y}$ with $\mathcal{M}_{\pi,y'}$. As the monodromy group $\mathcal{M}_{\pi,y}$ is determined up to isomorphism by the choice of base point, we may omit it and write $\mathcal{M}_\pi$ for the monodromy group of π.

By ordering the fiber $x_1, \ldots, x_d \in \pi^{-1}(y)$, we consider the monodromy group of π based at y as a subgroup of the symmetric group $\mathcal{M}_{\pi,y} \subseteq S_d$. A different ordering of the fiber produces a conjugate subgroup of $\mathcal{M}_\pi$ in S_d. We describe an alternative view of the monodromy group based on work of Vakil [34].

Fix a degree d branched cover $\pi : X \to Y$. Define the *d–fold fiber product*

$$X_Y^d = \{(x_1, \ldots, x_d) \in \underbrace{X \times \cdots \times X}_{d \text{ copies}} : \pi(x_1) = \cdots = \pi(x_d)\}.$$

Some irreducible components of X_Y^d will lie in the *big diagonal* Δ, which consists of d–tuples $(x_1, \ldots, x_d) \in X_Y^d$ having a repeated coordinate $x_i = x_j$ for some $i \neq j$. If $U \subseteq Y$ is the Étale locus of π, let

$$X_Y^{(d)} = \overline{\pi_d^{-1}(U) \setminus \Delta}.$$

There is a map $\pi_d : X_Y^{(d)} \to Y$ defined by projecting $X_Y^{(d)}$ to any of the d copies of X and composing with $\pi : X \to Y$. For $y \in U$, the fiber $\pi_d^{-1}(y)$ consists of the d–tuples of distinct points of the fiber $\pi^{-1}(y)$.

Fix $y \in U$ with fiber $\pi^{-1}(y) = \{x_1, \ldots, x_d\}$. As $\pi : \pi^{-1}(U) \to U$ is a covering space, there is a Euclidean neighborhood $V \subseteq Y$ of y such that for each $x_i \in \pi^{-1}(y)$, there is a Euclidean neighborhood $W_i \subseteq X$ and a diffeomorphism $\phi_i : V \to W_i$ such that $\pi \circ \phi_i$ is the identity on V. Then the map $\phi : V \to X_Y^{(d)}$ defined by $\phi(z) = (\phi_1(z), \ldots, \phi_d(z))$ is a homeomorphism onto its image with inverse π_d. Thus, $\phi(V)$ is a Euclidean neighborhood of $(x_1, \ldots, x_d)$ homoeomorphic to V. By permuting the points x_i and the maps ϕ_i, such a neighborhood exists for every point of the fiber $\pi_d^{-1}(y)$. Therefore, $\pi_d : \pi_d^{-1}(U) \to U$ is a covering space. It follows that for every irreducible component $X' \subseteq X_Y^{(d)}$, the restriction $\pi_d : X' \to Y$ is a branched cover. In particular, every irreducible component maps dominantly to Y and has dimension $\dim Y$.

The symmetric group S_d acts freely on $X_Y^{(d)}$—a permutation $\sigma \in S_d$ determines a regular map $\varphi_\sigma : X_Y^{(d)} \to X_Y^{(d)}$ by permuting the d copies of X. Each map φ_σ is an isomorphism with inverse $\varphi_\sigma^{-1} = \varphi_{\sigma^{-1}}$ and maps irreducible components of $X_Y^{(d)}$ to one another.

Proposition 37. *If $\pi : X \to Y$ is a branched cover and $X' \subseteq X_Y^{(d)}$ is any irreducible component, then the monodromy group $\mathcal{M}_\pi$ is isomorphic to the group*

$$\{\sigma \in S_d : \varphi_\sigma(X') \subseteq X'\}$$

of permutations in S_d which perserve X'.

Proof. Let $U \subseteq Y$ be the Étale locus of π, $y \in U$, and order a fiber $\pi^{-1}(y) = \{x_1, \ldots, x_d\}$. The monodromy group of π based at y is then identified with a subgroup of the symmetric group $\mathcal{M}_{\pi,y} \subseteq S_d$.

Given $\sigma \in \mathcal{M}_{\pi,y}$, there is a loop $\gamma : [0,1] \to U$ based at y with lifts $\widetilde{\gamma}_i : [0,1] \to \pi^{-1}(U)$ starting at x_i and ending at $x_{\sigma(i)}$. The path $\widetilde{\gamma} : [0,1] \to \pi_d^{-1}(U)$ defined by $\widetilde{\gamma}(t) = (\widetilde{\gamma}_1(t), \ldots, \widetilde{\gamma}_d(t))$ is a lift of γ starting at $(x_1, \ldots, x_d)$ and ending at $(x_{\sigma(1)}, \ldots, x_{\sigma(d)})$. Thus $(x_1, \ldots, x_d)$ and $(x_{\sigma(1)}, \ldots, x_{\sigma(d)})$

belong to the same component of $X_Y^{(d)}$. By permuting the points $x_1, \ldots, x_d$, the map φ_σ maps each component of $X_Y^{(d)}$ into itself.

Conversely, if $(x_1, \ldots, x_d)$ and $(x_{\sigma(1)}, \ldots, x_{\sigma(d)}) \in \pi_d^{-1}(y)$ lie in the same component $X' \subseteq X_Y^{(d)}$, then there is a path $\gamma : [0,1] \to \pi_d^{-1}(U) \cap X'$ connecting them. The loop $\pi_d \circ \gamma : [0,1] \to Y$ is based at y and its lifts to X are paths starting at x_i and ending at $x_{\sigma(i)}$ for each $i = 1, \ldots, d$ so that $\sigma \in \mathcal{M}_{\pi,y}$. □

By Proposition 37, if $\pi : X \to Y$ is a branched cover and $U \subseteq Y$ is any Zariski open set, the restriction $\pi : \pi^{-1}(U) \to U$ has the same monodromy group as π. Thus, in Definition 36 we may take U to be any Zariski open set such that $\pi : \pi^{-1}(U) \to U$ is a covering space.

We also have the following corollary.

Corollary 38. *If $\pi : X \to Y$ is a branched cover and $X' \subseteq X_Y^{(d)}$ is any irreducible component, then*

$$|\mathcal{M}_\pi| = \deg \pi_d|_{X'}.$$

Proof. Order a fiber $\pi^{-1}(y)$ so that we may consider $\mathcal{M}_{\pi,y} \subseteq S_d$ and fix a point $x \in \pi_d^{-1}(y)$ lying in the irreducible component X'. A permutation $\sigma \in \mathcal{M}_{\pi,y}$ is determined by the image $\varphi_\sigma(x) \in X'$ and there are $\deg \pi_d|_{X'}$ many such possible images as $\varphi_\sigma(X') \subseteq X'$. Thus $|\mathcal{M}_\pi| \leq \deg \pi_d|_{X'}$. Conversely, for every point $x' \in (\pi_d|_{X'})^{-1}(y)$ there is a permutation $\sigma \in S_d$ such that $\varphi_\sigma(x) = x'$. As φ_σ then necessarily fixes X', it follows that $\sigma \in \mathcal{M}_\pi$ and $|\mathcal{M}_\pi| \geq \deg \pi_d|_{X'}$. □

4.1.2 Algebraic Galois Groups

We briefly review some terminology. An algebraic extension $\mathbb{F}/\Bbbk$ of fields is *normal* if every univariate polynomial $f \in \Bbbk[x]$ that has a zero in $\mathbb{F}$ splits into linear factors over $\mathbb{F}$. The field generated by the zeros of a univariate polynomial $f \in \Bbbk[x]$ is a normal extension of $\Bbbk$ called the splitting field of f. For a finite extension $\mathbb{F}/\Bbbk$, there is a finite extension $\overline{\mathbb{F}}/\Bbbk$ of minimal degree containing $\mathbb{F}$ that is a normal extension. The field $\overline{\mathbb{F}}$ is a normal closure of $\mathbb{F}$ over $\Bbbk$ and is unique

up to isomorphism. If $\mathbb{F}/\Bbbk$ is normal, then $\mathbb{F}/\mathbb{L}$ is normal for every intermediate field $\Bbbk \subseteq \mathbb{L} \subseteq \mathbb{F}$.

Given a normal extension $\mathbb{F}/\Bbbk$, its Galois group $G = \mathcal{G}(\mathbb{F}/\Bbbk)$ is the group of automorphisms of the field $\mathbb{F}$ that fix all elements of $\Bbbk$. An intermediate field $\Bbbk \subseteq \mathbb{L} \subseteq \mathbb{F}$ determines a subgroup $\mathcal{G}(\mathbb{F}/\mathbb{L}) \subseteq G$ of automorphisms of $\mathbb{F}$ fixing $\mathbb{L}$, and all subgroups of G are of this form. More precisely, given a subgroup $H \subseteq G$, the set of elements of $\mathbb{F}$ fixed by all elements of H forms a field $\mathbb{F}^H$ with the property that $H = \mathcal{G}(\mathbb{F}/\mathbb{F}^H)$. More preciesly, these operations are related by the fundamental theorem of Galois theory. A proof and related material can be found in [35].

Theorem 39. *Let $\mathbb{F}/\Bbbk$ be a normal extension with Galois group $G = \mathcal{G}(\mathbb{F}/\Bbbk)$. The operations $\mathbb{L} \to \mathcal{G}(\mathbb{F}/\mathbb{L})$ sending an intermediate field $\Bbbk \subseteq \mathbb{L} \subseteq \mathbb{F}$ to a subgroup of G and $H \to \mathbb{F}^H$ sending a subgroup $H \subseteq G$ to an intermediate field of $\mathbb{F}/\Bbbk$ are inclusion reversing bijections. In addition, the following hold.*

1. *The order of a subgroup $\mathcal{G}(\mathbb{F}/\mathbb{L})$ is equal to the degree of the extension $\mathbb{F}/\mathbb{L}$.*
2. *An intermediate field $\Bbbk \subseteq \mathbb{L} \subseteq \mathbb{F}$ is normal over $\Bbbk$ if and only if the subgroup $\mathcal{G}(\mathbb{F}/\mathbb{L})$ is normal in G. In this case, the Galois group $\mathcal{G}(\mathbb{L}/\Bbbk)$ is isomorphic to the quotient $G/\mathcal{G}(\mathbb{F}/\mathbb{L})$.*

Recall that the pullback of a branched cover $\pi : X \to Y$ determines a reverse inclusion of function fields $\pi^* : \mathbb{C}(Y) \to \mathbb{C}(X)$ which enables us to consider $\mathbb{C}(X)$ as an extension of $\mathbb{C}(Y)$. As X and Y have the same dimension, $\mathbb{C}(X)$ and $\mathbb{C}(Y)$ have the same transcendence degree and $\mathbb{C}(X)/\mathbb{C}(Y)$ is a finite extension. We define the Galois group of a branched cover.

Definition 40. The *Galois group* $\mathcal{G}_\pi$ of a branched cover $\pi : X \to Y$ is the Galois group of the normal closure of the extension $\mathbb{C}(X)/\mathbb{C}(Y)$. That is, $\mathcal{G}_\pi = \mathcal{G}(\overline{\mathbb{C}(X)}/\mathbb{C}(Y))$.

We show that the Galois group $\mathcal{G}_\pi$ of a degree d branched cover $\pi : X \to Y$ may be understood geometrically. First, we replace $\pi : X \to Y$ with a branched cover whose Galois group is more easily understood. By the primitive element theorem, we may write $\mathbb{C}(X) = \mathbb{C}(Y)(\alpha)$ where $\alpha \in \mathbb{C}(X)$ is a zero of an irreducible polynomial $f \in \mathbb{C}(Y)[x]$ of degree d. By restricting to a Zariski open set $U \subseteq Y$ for which the coefficients of f are regular, we may consider $f(y, x) \in \mathbb{C}[U][x]$ as

a regular function on $U \times \mathbb{C}$ where x is the coordinate function $U \times \mathbb{C} \to \mathbb{C}$. As $f \in \mathbb{C}[U][x]$ is irreducible, the variety $\widetilde{X} = \mathcal{V}(f) \subseteq U \times \mathbb{C}$ is irreducible.

Consider the projection $\widetilde{\pi} : \widetilde{X} \to Y$ defined by $(y, x) \mapsto y$. On the Zariski open set where the lead coefficient of f and the discriminant of f are nonzero, a fiber $\widetilde{\pi}^{-1}(y_0)$ consists of d smooth points which are zeros of the polynomial $f(y_0, x) = 0$. It follows that $\widetilde{\pi} : \widetilde{X} \to Y$ is a degree d branched cover. As the function field of $\widetilde{X}$ may be expressed as $\mathbb{C}(\widetilde{X}) = \mathbb{C}(Y)(x)$ where x satisfies $f(x) = 0$, there is an isomorphism of fields the $\mathbb{C}(X)$ and $\mathbb{C}(\widetilde{X})$ which is the identity on $\mathbb{C}(Y)$. Thus the Galois groups $\mathcal{G}_\pi$ and $\mathcal{G}_{\widetilde{\pi}}$ are isomorphic and we focus on the branched cover $\widetilde{\pi} : \widetilde{X} \to Y$.

The d–fold fiber product $\widetilde{X}_Y^d$ is isomorphic to the variety $\mathcal{V}(f(y, x_1), \ldots, f(y, x_d)) \subseteq U \times \mathbb{C}^d$ where $x_1, \ldots, x_d$ are the coordinates on $\mathbb{C}^d$. If $X' \subseteq \widetilde{X}_Y^{(d)}$ is any irreducible component, its function field is generated by the rational functions on Y and the coordinate functions $x_1, \ldots, x_d$, $\mathbb{C}(X') = \mathbb{C}(Y)(x_1, \ldots, x_d)$. As X' is not contained in the big diagonal Δ, the coordinate functions $x_1, \ldots, x_d$ are distinct roots of $f \in \mathbb{C}(Y)[x]$. That is, $\mathbb{C}(X')$ is the splitting field of f over $\mathbb{C}(Y)$ and hence, $\mathbb{C}(X')$ is the normal closure of $\mathbb{C}(\widetilde{X})$.

As an element $\mu \in \mathcal{G}_{\widetilde{\pi}}$ is an isomorphism of the function field $\mathbb{C}(X')$ with itself preserving the subfield $\mathbb{C}(Y)$, μ is the pullback of a birational automorphism $\phi : X' \to X'$ that preserves the fibers of the map $\pi_d : X' \to Y$. Conversely, the pullback of any such birational automorphism is an element of $\mathcal{G}_{\widetilde{\pi}}$.

Proposition 41. *If $\pi : X \to Y$ is a branched cover and $X' \subseteq X_Y^{(d)}$ is any irreducible component, then the Galois group $\mathcal{G}_\pi$ is isomorphic to the set of birational automorphisms of X' that preserve the fibers of the restriction $\pi_d : X' \to Y$.*

4.1.3 Equivalence of Monodromy Group and Galois Group

To a degree d branched cover $\pi : X \to Y$ we've associated two groups, the monodromy group $\mathcal{M}_\pi$ and the Galois group $\mathcal{G}_\pi$—we show that they are isomorphic. A proof was given by Harris, though the idea traces back to Hermite [2, 3]. We present a modern proof from [36].

Theorem 42. *The monodromy group $\mathcal{M}_\pi$ and the Galois group $\mathcal{G}_\pi$ of a branched cover $\pi : X \to Y$ are isomorphic.*

Proof. Let $\pi : X \to Y$ be a branched cover, $\pi_d : X' \to Y$ be the restriction of π_d to an irreducible component $X' \subseteq X_Y^{(d)}$, and consider $\mathcal{G}_\pi$ under the identification from Proposition 41. By Proposition 37, we may consider $\mathcal{M}_\pi \subseteq \mathcal{G}_\pi$. The result then follows from the fundamental theorem of Galois theory, Theorem 39, as

$$|\mathcal{G}_\pi| = [\mathbb{C}(X') : \mathbb{C}(Y)] = \deg \pi_d|_{X'} = |\mathcal{M}_\pi|.$$

□

We follow tradition and refer to either of these groups as *the Galois group*. Recall that given a degree d branched cover $\pi : X \to Y$, the Galois group may be considered a subgroup of the symmetric group S_d. We remark on terminology. If $\mathcal{G}_\pi = S_d$, we say that the Galois group is *fully symmetric* or simply *symmetric*. If $\mathcal{G}_\pi \subset S_d$ is a proper subgroup, we say that the Galois group is *enriched*. For many problems, it is known that the Galois group contains the alternating group $A_d \subseteq \mathcal{G}_\pi$. Such a Galois group is said to be *at least alternating*.

4.2 Decomposable Branched Covers

We remark on a structure which guarantees that a branched cover has an enriched Galois group.

Definition 43. A branched cover $\pi : X \to Y$ is *decomposable* if there exists a Zariski open set $U \subseteq Y$ and a variety Z such that π factors as a composition of nontrivial branched covers

$$\pi^{-1}(U) \xrightarrow{\theta} Z \xrightarrow{\psi} U.$$

Recall that a group $G \subseteq S_n$ is imprimitive if it is transitive and there is a nontrivial partition of $[n]$ which is preserved by G. Equivalently, G is imprimitive if for every $i \in [n]$, the stabilizer of i in G is not a maximal proper subgroup. As noted in [37], the Galois group of a decomposable branched cover is imprimitive and conversely.

Theorem 44. *A branched cover $\pi : X \to Y$ is decomposable if and only if its Galois group $\mathcal{G}_\pi$ is imprimitive.*

Proof. Let $\pi : X \to Y$ be decomposable with $U \subseteq Y$ a Zariski open set and Z a variety such that π factors as a composition of $\theta : \pi^{-1}(U) \to Z$ and $\psi : Z \to U$. For a general point $y \in U$ with fiber $\psi^{-1}(y) = \{z_1, \ldots, z_k\}$, the set of fibers $\theta^{-1}(z_1), \ldots, \theta^{-1}(z_k)$ is a partition of $\pi^{-1}(y)$. Further, if $\gamma : [0,1] \to U$ is a loop based at y, for a fixed i, there is a lift $\gamma' : [0,1] \to Z$ starting at z_i and ending at z_j. By uniqueness of liftings, any lift $\gamma'' : [0,1] \to \pi^{-1}(U)$ of γ starting at a point $x \in \theta^{-1}(z_i)$ is a lift of γ'. In particular, $\gamma''(1) \in \theta^{-1}(z_j)$. That is, the action of the Galois group $\mathcal{G}_\pi$ preserves the partition $\theta^{-1}(z_1), \ldots, \theta^{-1}(z_k)$. Since the branched covers θ and ψ are nontrivial, this partition is nontrivial and the Galois group $\mathcal{G}_\pi$ is imprimitive.

If the Galois group $\mathcal{G}_\pi$ of the branched cover $\pi : X \to Y$ is imprimitive, we write $\mathbb{C}(X) = \mathbb{C}(Y)(\alpha)$ by the primitive element theorem where α is a root of an irreducible polynomial $f \in \mathbb{C}(Y)[t]$. The Galois group $\mathcal{G}_\pi$ is the Galois group of the polynomial f over $\mathbb{C}(Y)$. In particular, $\mathcal{G}_\pi$ acts on the roots of f and the stabilizer of α is a group whose fixed field is the field $\mathbb{C}(X)$. Since $\mathcal{G}_\pi$ is imprimitive, this stabilizer is not a maximal subgroup and any larger subugroup corresponds to a proper subfield $\mathbb{C}(Y) \subseteq \mathbb{L} \subseteq \mathbb{C}(X)$. Let Z be any irreducible variety whose function field is isomorphic to $\mathbb{L}$. Then the inclusion of fields $\mathbb{C}(Z) \to \mathbb{C}(X)$ and $\mathbb{C}(Y) \to \mathbb{C}(Z)$ are pullbacks of rational maps $\theta : X \to Z$ and $\psi : Z \to Y$ whose composition is the map $\pi : X \to Y$ when defined. By Theorem 18, there is a Zariski open set such that π factors as a composition of branched covers $\pi^{-1}(U) \to Z \to U$. As the inclusions $\mathbb{C}(Z) \subseteq \mathbb{C}(X)$ and $\mathbb{C}(Y) \subseteq \mathbb{C}(Z)$ are proper, these branched covers are nontrivial and hence, $\pi : X \to Y$ is decomposable. □

5. SPARSE POLYNOMIAL SYSTEMS

5.1 Sparse Polynomial Systems and Supports

Let $\mathbb{C}^\times = \mathbb{C} \setminus \{0\}$ be the multiplicative group of nonzero complex numbers and $(\mathbb{C}^\times)^n$ be the n–dimensional algebraic torus. A vector $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}^n$ determines a (Laurent) monomial with *exponent vector* α,

$$x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n},$$

which is a character, or multiplicative map, $x^\alpha : (\mathbb{C}^\times)^n \to \mathbb{C}$. A (Laurent) polynomial is a finite linear combination of monomials. The ring of Laurent polynomials $\mathbb{C}[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]$ is the ring of regular functions on $(\mathbb{C}^\times)^n$.

Given finite set $\mathcal{A} \subseteq \mathbb{Z}^n$, we consider polynomials $f \in \mathbb{C}[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]$ such that the exponent vector of each term lies in $\mathcal{A}$. Such a polynomial is said to have *support* $\mathcal{A}$ and we denote the vector space of these polynomials by $\mathbb{C}^{\mathcal{A}}$. The set of monomials $\{x^\alpha \in \mathbb{C}[x_1^{\pm 1}, \ldots, x_n^{\pm 1}] : \alpha \in \mathcal{A}\}$ is a basis for $\mathbb{C}^{\mathcal{A}}$ so that the dimension of $\mathbb{C}^{\mathcal{A}}$ is the cardinality of $\mathcal{A}$, $\dim \mathbb{C}^{\mathcal{A}} = |\mathcal{A}|$.

Given a set of supports $\mathcal{A}_\bullet = (\mathcal{A}_1, \ldots, \mathcal{A}_n)$, we form the space $\mathbb{C}^{\mathcal{A}_\bullet} = \mathbb{C}^{\mathcal{A}_1} \times \cdots \times \mathbb{C}^{\mathcal{A}_n}$ of *sparse polynomial systems* of support $\mathcal{A}_\bullet$, whose elements $F = (f_1, \ldots, f_n) \in \mathbb{C}^{\mathcal{A}_\bullet}$ are square systems of n polynomials in n variables such that each f_i has support $\mathcal{A}_i$. The space $\mathbb{C}^{\mathcal{A}_\bullet}$ is a vector space of dimension

$$\dim \mathbb{C}^{\mathcal{A}_\bullet} = |\mathcal{A}_\bullet| = |\mathcal{A}_1| + \cdots + |\mathcal{A}_n|.$$

As a polynomial $f \in \mathbb{C}^{\mathcal{A}}$ is a regular function on the n–dimensional algebraic torus $(\mathbb{C}^\times)^n$, the zero set of a sparse polynomial system $F \in \mathbb{C}^{\mathcal{A}_\bullet}$ define a subvariety $\mathcal{V}(F) \subseteq (\mathbb{C}^\times)^n$.

Fix a finite set $\mathcal{A} \subseteq \mathbb{Z}^n$ and a polynomial $f \in \mathbb{C}^{\mathcal{A}}$. As a monomial x^α is an invertible function, multiplication by x^α does not change the variety defined by f, $\mathcal{V}(x^\alpha f) = \mathcal{V}(f)$. The support of the

polynomial $x^\alpha f$ is a translate of $\mathcal{A}$ by $\alpha \in \mathbb{Z}^n$. Therefore, we may independently translate each support $\mathcal{A}_1, \ldots, \mathcal{A}_n$ and assume without loss of generality that each $\mathcal{A}_i$ contains the origin.

5.1.1 The Bernstein–Kushnirenko–Khovanskii Theorem

It was shown by Bernstein, Kushnirenko, and Khovanskii that the number of zeros of a sparse polynomial system $F \in \mathbb{C}^{\mathcal{A}_\bullet}$ depends on the polyhedral geometry of the set of supports $\mathcal{A}_\bullet$ [4, 5]. Given a finite set $\mathcal{A} \subseteq \mathbb{R}^n$, we denote its convex hull by $\mathrm{conv}(\mathcal{A})$. Given two sets C_1 and C_2 in $\mathbb{R}^n$, their Minkowski sum is their pointwise sum

$$C_1 + C_2 = \{x + y \in \mathbb{R}^n : x \in C_1, y \in C_2\}$$

and for $\lambda \geq 0$, the set $\lambda C_1 = \{\lambda x : x \in C_1\}$ is a scalar multiple of C_1.

We denote the Euclidean volume of a compact set $C \subseteq \mathbb{R}^n$ by $\mathrm{vol}(C)$. A classical result of Minkowski states that given compact convex bodies $C_1, \ldots, C_n \subseteq \mathbb{R}^n$ and non–negative indeterminants $t_1, \ldots, t_n$, the volume form $\mathrm{vol}(t_1 C_1 + \cdots + t_n C_n)$ is a homogeneous polynomial of degree n in $t_1, \ldots, t_n$. A proof is provided in [38], which deduces the general result from the special case that $C_1, \ldots, C_n$ are polytopes.

Definition 45. The *mixed volume* $\mathrm{MV}(C_1, \ldots, C_n)$ of compact convex bodies $C_1, \ldots, C_n \subseteq \mathbb{R}^n$ is the coefficient of the product $t_1 \cdots t_n$ in the volume form $\mathrm{vol}(t_1 C_1 + \cdots + t_n C_n)$.

We note three properties of the mixed volume which follow from this definition. Let $C_1, \ldots, C_n$ be convex bodies. First, the mixed volume is symmetric—for any permutation $\sigma \in S_n$, one has

$$\mathrm{MV}(C_1, \ldots, C_n) = \mathrm{MV}(C_{\sigma(1)}, \ldots, C_{\sigma(n)}).$$

The mixed volume is also multilinear in the sense that for a convex body C_1' and $\lambda \geq 0$,

$$\mathrm{MV}(C_1 + \lambda C_1', C_2, \ldots, C_n) = \mathrm{MV}(C_1, C_2, \ldots, C_n) + \lambda\, \mathrm{MV}(C_1', C_2, \ldots, C_n).$$

Last, we have that $\mathrm{MV}(C_1, \ldots, C_n) \geq 0$ and is normalized by $\mathrm{MV}(C, \ldots, C) = n! \operatorname{vol}(C)$. The polarization formula for the mixed volume

$$\mathrm{MV}(C_1, \ldots, C_n) = \sum_{i=1}^{k} \sum_{1 \leq i_1 < \cdots < i_k \leq n} (-1)^i \operatorname{vol}(C_{i_1} + \cdots + C_{i_k})$$

follows from these properties. Consequently, the mixed volume is determined by these properties. Given a set of supports $\mathcal{A}_\bullet$, we write $\mathrm{MV}(\mathcal{A}_\bullet)$ for the mixed volume of the convex hulls $\operatorname{conv}(\mathcal{A}_1), \ldots, \operatorname{conv}(\mathcal{A}_n)$. Bernstein showed that the function sending a set of supports $\mathcal{A}_\bullet$ to the number of zeros to a general system $F \in \mathbb{C}^{\mathcal{A}}$ satisfies these same properties and deduced the following.

Theorem 46 (Bernstein, Kushnirenko, Khovanskii)**.** *Given a set of supports $\mathcal{A}_\bullet = (\mathcal{A}_1, \ldots, \mathcal{A}_n)$, the mixed volume $\mathrm{MV}(\mathcal{A}_\bullet)$ is an upper bound on the number of isolated zeros of a system $F \in \mathbb{C}^{\mathcal{A}_\bullet}$ counting multiplicity. Further, there is a Zariski open set $U \subseteq \mathbb{C}^{\mathcal{A}_\bullet}$ for which a system $F \in U$ has $\mathrm{MV}(\mathcal{A}_\bullet)$ distinct zeros.*

5.1.2 Monomial Changes of Coordinates

We detail some terminology regarding maps and changing coordinates. The set of characters $\hom((\mathbb{C}^\times)^n, \mathbb{C}^\times)$ on $(\mathbb{C}^\times)^n$ forms a group under pointwise multiplication and we identify it with $\mathbb{Z}^n$ by sending a monomial x^α to its exponent vector α. By evaluation of a character at an element of $(\mathbb{C}^\times)^n$, we identify the dual of the character group $\hom(\mathbb{Z}^n, \mathbb{C}^\times) = (\mathbb{C}^\times)^n$.

A *monomial map* is a homomorphism $\varphi : (\mathbb{C}^\times)^n \to (\mathbb{C}^\times)^m$, or equivalently, a regular map whose m coordinate functions are monomials,

$$\varphi(x) = (x^{\alpha_1}, \ldots, x^{\alpha_m}),\ \alpha_1, \ldots, \alpha_m \in \mathbb{Z}^n.$$

The pullback $\varphi^* : \mathbb{C}[y_1^{\pm 1}, \ldots, y_m^{\pm 1}] \to \mathbb{C}[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]$ restricts to a homomorphism on the multiplicative group of monomials and hence determines a linear map of characters $\phi : \mathbb{Z}^m \to \mathbb{Z}^n$. If the m coordinate functions of φ are x^{α_i}, then ϕ is represented by the matrix $A = [\alpha_1 | \cdots | \alpha_m]$

whose columns are vectors $\alpha_i \in \mathbb{Z}^n$. The map φ may be recovered as the dual map of ϕ

$$(\mathbb{C}^\times)^n = \hom(\mathbb{Z}^n, \mathbb{C}^\times) \to \hom(\mathbb{Z}^m, \mathbb{C}^\times) = (\mathbb{C}^\times)^m.$$

If $\mathcal{A} \subseteq \mathbb{Z}^m$ is a finite set and $f \in \mathbb{C}^{\mathcal{A}}$, a monomial map $\varphi : (\mathbb{C}^\times)^n \to (\mathbb{C}^\times)^m$ determines a polynomial $f(\varphi(y))$ of support $\phi(\mathcal{A}) \subseteq \mathbb{Z}^n$.

By a change of coordinates on $(\mathbb{C}^\times)^n$, we mean an invertible monomial map $\varphi : (\mathbb{C}^\times)^n \to (\mathbb{C}^\times)^n$. If $\phi : \mathbb{Z}^n \to \mathbb{Z}^n$ is the linear map induced by the pullback φ^*, then ϕ is an isomorphism. That is, if $\alpha_1, \ldots, \alpha_n \in \mathbb{Z}^n$, the monomial map $\varphi(x) = (x^{\alpha_1}, \ldots, x^{\alpha_n})$ is a change of coordinates exactly when $\alpha_1, \ldots, \alpha_n$ span $\mathbb{Z}^n$.

If $\mathcal{A}_\bullet = (\mathcal{A}_1, \ldots, \mathcal{A}_n)$ is a set of supports and $\varphi : (\mathbb{C}^\times)^n \to (\mathbb{C}^\times)^n$ is a change of coordinates, then the set of supports $\mathcal{B}_\bullet = (\phi(\mathcal{A}_1), \ldots, \phi(\mathcal{A}_n))$ has the same mixed volume $\mathrm{MV}(\mathcal{A}_\bullet) = \mathrm{MV}(\mathcal{B}_\bullet)$. Indeed, if $F \in \mathbb{C}^{\mathcal{A}_\bullet}$ has $\mathrm{MV}(\mathcal{A}_\bullet)$ many zeros, then $F(\varphi(x)) \in \mathbb{C}^{\mathcal{B}_\bullet}$ has $\mathrm{MV}(\mathcal{A}_\bullet)$ many zeros as well so that $\mathrm{MV}(\mathcal{A}_\bullet) \leq \mathrm{MV}(\mathcal{B}_\bullet)$. Similarly, since φ is invertible, $\mathrm{MV}(\mathcal{B}_\bullet) \leq \mathrm{MV}(\mathcal{A}_\bullet)$ and equality holds.

5.2 Galois Groups of Sparse Polynomial Systems

Given a set of supports $\mathcal{A}_\bullet = (\mathcal{A}_1, \ldots, \mathcal{A}_n)$, we define the *incidence variety*

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

We determine properties of the incidence variety $\Gamma_{\mathcal{A}_\bullet}$ by showing it is isomorphic to the product $\mathbb{C}^{|\mathcal{A}_\bullet|-n} \times (\mathbb{C}^\times)^n$. In more technical terms, we show $\Gamma_{\mathcal{A}_\bullet}$ is isomorphic to the trivial rank $|\mathcal{A}_\bullet| - n$ vector bundle over $(\mathbb{C}^\times)^n$.

The condition that a system $F = (f_1, \ldots, f_n) \in \mathbb{C}^{\mathcal{A}_\bullet}$ vanishes at $(1, \ldots, 1) \in (\mathbb{C}^\times)^n$ amounts to the n linearly independent conditions $f_i(1, \ldots, 1) = 0$ for $i = 1, \ldots, n$. Thus, the space of systems $F \in \mathbb{C}^{\mathcal{A}_\bullet}$ the vanish at $(1, \ldots, 1) \in (\mathbb{C}^\times)^n$ is a vector space of dimension $N = |\mathcal{A}_\bullet| - n$ which we identify with $\mathbb{C}^N$ via a choice of basis. Then the map $\varphi : \mathbb{C}^N \times (\mathbb{C}^\times)^n \to \Gamma_{\mathcal{A}_\bullet}$ defined

by $\varphi(F(t), x) = (F(t/x), x)$ is an isomorphism as multiplication by x is invertible. As a result, $\Gamma_{\mathcal{A}_\bullet}$ is isomorphic to $\mathbb{C}^N \times (\mathbb{C}^\times)^n$ and hence is a smooth, irreducible variety of dimension

$$\dim \Gamma_{\mathcal{A}_\bullet} = N + n = |\mathcal{A}_\bullet|.$$

As a subset of the product $\Gamma_{\mathcal{A}_\bullet} \subseteq \mathbb{C}^{\mathcal{A}_\bullet} \times (\mathbb{C}^\times)^n$, there is a projection $\pi_{\mathcal{A}_\bullet} : \Gamma_{\mathcal{A}_\bullet} \to \mathbb{C}^{\mathcal{A}_\bullet}$. For a system $F \in \mathbb{C}^{\mathcal{A}_\bullet}$, we identify the fiber $\pi^{-1}_{\mathcal{A}_\bullet}(F)$ with the zeros of F. By Theorem 46, the cardinality of a general fiber $\pi^{-1}_{\mathcal{A}_\bullet}(F)$ for $F \in \mathbb{C}^{\mathcal{A}_\bullet}$ is the mixed volume $\mathrm{MV}(\mathcal{A}_\bullet)$. It follows that $\pi_{\mathcal{A}_\bullet} : \Gamma_{\mathcal{A}_\bullet} \to \mathbb{C}^{\mathcal{A}_\bullet}$ is a degree $\mathrm{MV}(\mathcal{A}_\bullet)$ branched cover when $\mathrm{MV}(\mathcal{A}_\bullet) > 0$. Therefore, we assume that our set of supports $\mathcal{A}_\bullet$ satisfies $\mathrm{MV}(\mathcal{A}_\bullet) > 0$, or equivalently, that a general system $F \in \mathbb{C}^{\mathcal{A}_\bullet}$ has a zero.

Definition 47. The *Galois group* $\mathcal{G}_{\mathcal{A}_\bullet}$ of the family of sparse polynomial systems of support $\mathcal{A}_\bullet$ is the Galois group of the branched cover $\pi_{\mathcal{A}_\bullet} : \Gamma_{\mathcal{A}_\bullet} \to \mathbb{C}^{\mathcal{A}_\bullet}$.

Galois groups of sparse polynomial systems were first studied by Esterov to determine those sparse polynomial systems whose zeros could be computed via radicals. Esterov showed that there are two properties of the set of supports that imply the Galois group is enriched and that all other sparse polynomial systems have fully symmetric Galois group [8]. For a set of supports with either of these properties, the branched cover $\pi_{\mathcal{A}_\bullet} : \Gamma_{\mathcal{A}_\bullet} \to \mathbb{C}^{\mathcal{A}_\bullet}$ is decomposable and the Galois group $\mathcal{G}_{\mathcal{A}_\bullet}$ is imprimitive.

We identify these properties of a set of supports $\mathcal{A}_\bullet = (\mathcal{A}_1, \ldots, \mathcal{A}_n)$ algebraically. Recall our assumption that $0 \in \mathcal{A}_i$ for all i. Given a subset $I \subseteq [n]$, we write $\mathcal{A}_I = (\mathcal{A}_i)_{i \in I}$ and define the free abelian group spanned by the supports $\mathcal{A}_I$,

$$\mathbb{Z}\mathcal{A}_I = \langle \alpha \in \mathbb{Z}^n : \alpha \in \mathcal{A}_i \text{ for some } i \in I \rangle.$$

We write $\mathbb{Z}\mathcal{A}_\bullet = \mathbb{Z}\mathcal{A}_{[n]}$. As each set $\mathcal{A}_i$ is finite, for every subset $I \subseteq [n]$ we have an explicit generating set for $\mathbb{Z}\mathcal{A}_I$. Computer algebra systems may be used to study these groups and compute,

for instance, their ranks.

5.2.1 Lacunary Supports

Definition 48. A set of supports $\mathcal{A}_\bullet$ is *lacunary* if $1 < [\mathbb{Z}^n : \mathbb{Z}\mathcal{A}_\bullet] < \mathrm{MV}(\mathcal{A}_\bullet)$.

If a set of supports $\mathcal{A}_\bullet$ is lacunary, then $\operatorname{rank} \mathbb{Z}\mathcal{A}_\bullet = n$, but $\mathbb{Z}\mathcal{A}_\bullet \subseteq \mathbb{Z}^n$ is a proper subgroup. When this occurs, there is an injective linear map $\phi : \mathbb{Z}^n \to \mathbb{Z}^n$ whose image is $\mathbb{Z}\mathcal{A}_\bullet$. As each support lies in its image $\mathcal{A}_i \subseteq \operatorname{im} \phi$, we define a new set of supports $\mathcal{B}_\bullet = (\phi^{-1}(\mathcal{A}_1), \ldots, \phi^{-1}(\mathcal{A}_n))$ called the *reduced support* of $\mathcal{A}_\bullet$.

As ϕ^{-1} is a bijection between the supports $\mathcal{A}_i$ and $\mathcal{B}_i$, there is an isomorphism $\iota : \mathbb{C}^{\mathcal{A}_\bullet} \to \mathbb{C}^{\mathcal{B}_\bullet}$ defined by sending $f_i = \sum_{\alpha \in \mathcal{A}_i} c_\alpha x^\alpha \in \mathbb{C}^{\mathcal{A}_i}$ to $\iota(f_i) = \sum_{\alpha \in \mathcal{A}_i} c_\alpha x^{\phi^{-1}(\alpha)} \in \mathbb{C}^{\mathcal{B}_i}$. In addition, the linear map $\phi : \mathbb{Z}^n \to \mathbb{Z}^n$ determines a monomial map $\varphi : (\mathbb{C}^\times)^n \to (\mathbb{C}^\times)^n$ such that for every polynomial $F \in \mathbb{C}^{\mathcal{A}_\bullet}$, there is an equality $F(x) = \iota(F)(\varphi(x))$. We say that $\iota(F) \in \mathbb{C}^{\mathcal{B}_\bullet}$ is the *reduced system* of F.

Theorem 49. *If $\mathcal{A}_\bullet$ is a lacunary set of supports, then the branched cover $\pi_{\mathcal{A}_\bullet} : \Gamma_{\mathcal{A}_\bullet} \to \mathbb{C}^{\mathcal{A}_\bullet}$ is decomposable.*

Proof. The monomial map $\varphi : (\mathbb{C}^\times)^n \to (\mathbb{C}^\times)^n$ determines a map of incidence varieties $\theta : \Gamma_{\mathcal{A}_\bullet} \to \Gamma_{\mathcal{B}_\bullet}$ defined by $\theta(F, x) = (\iota(F), \varphi(x))$. The map θ is a degree $[\mathbb{Z}^n : \mathbb{Z}\mathcal{A}_\bullet] > 1$ branched cover as $\varphi : (\mathbb{C}^\times)^n \to (\mathbb{C}^\times)^n$ is a degree $[\mathbb{Z}^n : \mathbb{Z}\mathcal{A}_\bullet]$ covering space. By the composition $\pi_{\mathcal{A}_\bullet} = \theta \circ \pi_{\mathcal{B}_\bullet} \circ \iota$ there is an equality $\deg \pi_{\mathcal{A}_\bullet} = (\deg \theta)(\deg \pi_{\mathcal{B}_\bullet})$. Since

$$\deg \theta = [\mathbb{Z}^n : \mathbb{Z}\mathcal{A}_\bullet] < \mathrm{MV}(\mathcal{A}_\bullet) = \deg \pi_{\mathcal{A}_\bullet},$$

it follows that $\deg \pi_{\mathcal{B}_\bullet} > 1$ and $\pi_{\mathcal{B}_\bullet}$ is a nontrivial branched cover. Thus, π factors as the composition of nontrivial branched covers θ and $\pi_{\mathcal{B}_\bullet}$,

$$\Gamma_{\mathcal{A}_\bullet} \xrightarrow{\theta} \Gamma_{\mathcal{B}_\bullet} \xrightarrow{\pi_{\mathcal{B}_\bullet}} \mathbb{C}^{\mathcal{B}_\bullet} \xrightarrow{\sim} \mathbb{C}^{\mathcal{A}_\bullet}. \qquad \square$$

By Theorem 44, if $\mathcal{A}_\bullet$ is lacunary, then the Galois group $\mathcal{G}_\pi$ is imprimitive. A nontrivial

partition that $\mathcal{G}_\pi$ preserves can be observed directly. Indeed, the group $\ker \varphi = \hom(\mathbb{Z}^n/\mathbb{Z}\mathcal{A}_\bullet, \mathbb{C}^\times)$ acts on the zeros $\mathcal{V}(F)$ of a system $F \in \mathbb{C}^{\mathcal{A}_\bullet}$ by component–wise multiplication and partitions $\mathcal{V}(F)$ into orbits. As $1 < [\mathbb{Z}^n : \mathbb{Z}\mathcal{A}_I] < \mathrm{MV}(\mathcal{A}_\bullet)$, this partition is nontrivial and it is preserved by the Galois group $\mathcal{G}_\pi$.

5.2.2 Triangular Supports

We now define the second family of sparse polynomial systems described by Esterov. Given a subgroup $L \subseteq \mathbb{Z}^n$, its saturation is the subgroup $\mathrm{sat}(L) = \{\alpha \in \mathbb{Z}^n : k\alpha \in L \text{ for some } k \in \mathbb{Z}_{>0}\}$. If $I \subseteq [n]$ is such that $\mathrm{rank}\ \mathbb{Z}\mathcal{A}_I = |I|$, there is a free abelian group $\mathbb{Z}^I$ and an isomorphism $\mathbb{Z}^I \to \mathrm{sat}(\mathbb{Z}\mathcal{A}_I)$ so that for each $i \in I$ we may consider $\mathcal{A}_i \subseteq \mathbb{Z}^I$. Considering $\mathbb{Z}^I$ as the space of characters on a torus $(\mathbb{C}^\times)^I$, we may consider a system $F \in \mathbb{C}^{\mathcal{A}_I}$ as a sparse polynomial system on $(\mathbb{C}^\times)^I$. We write $\mathrm{MV}(\mathcal{A}_I)$ for the mixed volume of the polytopes $\{\mathrm{conv}(\mathcal{A}_i)\}_{i\in I}$ in $\mathbb{R}^I = \mathbb{Z}^I \otimes \mathbb{R}$, which is the number of zeros of a general system $F \in \mathbb{C}^{\mathcal{A}_I}$ in $(\mathbb{C}^\times)^I$. As a different embedding results in a change of coordinates on $(\mathbb{C}^\times)^I$, the mixed volume $\mathrm{MV}(\mathcal{A}_I)$ is independent of the choice of isomorphism $\mathbb{Z}^I \to \mathrm{sat}(\mathbb{Z}\mathcal{A}_I)$.

Definition 50. A set of supports $\mathcal{A}_\bullet$ is *triangular* if there exists a subset $I \subseteq [n]$ for which $\mathrm{rank}\ \mathbb{Z}\mathcal{A}_I = |I|$ and $1 < \mathrm{MV}(\mathcal{A}_I) < \mathrm{MV}(\mathcal{A}_\bullet)$.

The set $I \subseteq [n]$ in Definition 50 may not be unique. If $\mathcal{A}_\bullet$ is triangular and $I \subseteq [n]$ is a subset such that $\mathrm{rank}\ \mathbb{Z}\mathcal{A}_I = |I|$ and $1 < \mathrm{MV}(\mathcal{A}_I) < \mathrm{MV}(\mathcal{A}_\bullet)$, we say the set I is a *witness for triangularity* for $\mathcal{A}_\bullet$. Let $\mathcal{A}_\bullet$ be a triangular set of supports witnessed by $I \subseteq [n]$ and write $J = [n] \setminus I$ for the complement of I. The saturation $\mathrm{sat}(\mathbb{Z}\mathcal{A}_I)$ is complemented in $\mathbb{Z}^n$—as the quotient $L = \mathbb{Z}^n/\mathrm{sat}(\mathbb{Z}\mathcal{A}_I)$ is a free abelian group, the exact sequence

$$0 \to \mathrm{sat}(\mathbb{Z}\mathcal{A}_I) \to \mathbb{Z}^n \to L \to 0$$

splits so that we may regard L as a subgroup of $\mathbb{Z}^n$ and write $\mathbb{Z}^n = \mathrm{sat}(\mathbb{Z}\mathcal{A}_I) \oplus L$. Via isomorphisms with free abelian groups $\mathbb{Z}^I \to \mathrm{sat}(\mathbb{Z}\mathcal{A}_I)$ and $\mathbb{Z}^J \to L$, we identify $\mathrm{sat}(\mathbb{Z}\mathcal{A}_I)$ and L with

the set of characters on respective tori $(\mathbb{C}^\times)^I$ and $(\mathbb{C}^\times)^J$. The isomorphism

$$\phi : \mathbb{Z}^n = \mathbb{Z}^I \oplus \mathbb{Z}^J \to \mathrm{sat}(\mathbb{Z}\mathcal{A}_I) \oplus L = \mathbb{Z}^n,$$

determines a change of coordinates $\varphi : (\mathbb{C}^\times)^n \to (\mathbb{C}^\times)^n = (\mathbb{C}^\times)^I \times (\mathbb{C}^\times)^J$ and we write $(x, y) \in (\mathbb{C}^\times)^I \times (\mathbb{C}^\times)^J$ for the splitting of coordinates in the image. Consider the new set of supports $\mathcal{B}_\bullet = (\phi^{-1}(\mathcal{A}_1), \ldots, \phi^{-1}(\mathcal{A}_n))$ and the corresponding map $\iota : \mathbb{C}^{\mathcal{A}_\bullet} \to \mathbb{C}^{\mathcal{B}_\bullet}$. As $\mathcal{B}_i = \phi^{-1}(\mathcal{A}_i) \subseteq \mathbb{Z}^I \oplus \{0\}$ for $i \in I$, we may consider a system $F \in \mathbb{C}^{\mathcal{B}_I}$ as a sparse polynomial system on $(\mathbb{C}^\times)^I$. A system $F \in \mathbb{C}^{\mathcal{B}_\bullet}$ has the form $F(x, y) = (F_I(x), F_J(x, y))$ where $F_I(x) \in \mathbb{C}^{\mathcal{B}_I}$ is a sparse polynomial system on $(\mathbb{C}^\times)^I$ and $F_J \in \mathbb{C}^{\mathcal{B}_J}$. We say that $F_I \in \mathbb{C}^{\mathcal{B}_I}$ is a *subsystem* of F. Thus, given a system $F \in \mathbb{C}^{\mathcal{A}_\bullet}$, the system $\iota(F)(x) = F(\varphi^{-1}(x)) \in \mathbb{C}^{\mathcal{B}_\bullet}$ has a subsystem.

Theorem 51. *If $\mathcal{A}_\bullet$ is a triangular set of supports, then the branched cover $\pi_{\mathcal{A}_\bullet} : \Gamma_{\mathcal{A}_\bullet} \to \mathbb{C}^{\mathcal{A}_\bullet}$ is decomposable.*

Proof. From our change of coordinates, it suffices to show that $\pi_{\Gamma_{\mathcal{B}_\bullet}}$ is decomposable. By considering systems $F_I(x) \in \mathbb{C}^{\mathcal{B}_I}$ as sparse polynomial systems on $(\mathbb{C}^\times)^I$, we define the variety

$$\Lambda_{\mathcal{B}_\bullet} = \{((F_I, F_J), x) \in \mathbb{C}^{\mathcal{B}_\bullet} \times (\mathbb{C}^\times)^I : F_I(x) = 0\}.$$

The projection $(\mathbb{C}^\times)^n \to (\mathbb{C}^\times)^I$ then determines a map $\theta : \Gamma_{\mathcal{B}_\bullet} \to \Lambda_{\mathcal{B}_\bullet}$ defined by $\theta(F, (x, y)) = (F, x)$. Similarly, by identifying $\Lambda_{\mathcal{B}_\bullet}$ with $\Gamma_{\mathcal{B}_I} \times \mathbb{C}^{\mathcal{B}_J}$, the branched cover $\pi_{\mathcal{B}_\bullet} : \Gamma_{\mathcal{B}_I} \to \mathbb{C}^{\mathcal{B}_I}$ determines a map

$$\psi : \Lambda_{\mathcal{B}_\bullet} = \Gamma_{\mathcal{B}_I} \times \mathbb{C}^{\mathcal{B}_J} \to \mathbb{C}^{\mathcal{B}_I} \times \mathbb{C}^{\mathcal{B}_J} = \mathbb{C}^{\mathcal{B}_\bullet}$$

of degree $\mathrm{MV}(\mathcal{B}_I)$. As their composition $\pi_{\mathcal{B}_\bullet} = \psi \circ \theta$ is dominant and the dimension of each variety is equal, it follows that θ is a branched cover as well. As $\deg \pi_{\mathcal{B}_\bullet} = (\deg \psi)(\deg \theta)$ and $1 < \mathrm{MV}(\mathcal{B}_I) < \mathrm{MV}(\mathcal{B}_\bullet)$, it follows that each of these branched covers is nontrivial and $\pi_{\mathcal{B}_\bullet}$ is decomposable. □

Again by Theorem 44, if $\mathcal{A}_\bullet$ is a triangular set of supports, then $\mathcal{G}_{\mathcal{A}_\bullet}$ is imprimitive.

5.2.3 Esterov's Theorem

We now state the result of Esterov on Galois groups of sparse polynomial systems.

Theorem 52 (Esterov)**.** *If $\mathcal{A}_\bullet$ is a set of supports which is neither lacunary nor triangular, then the Galois group $\mathcal{G}_{\mathcal{A}_\bullet}$ is fully symmetric.*

Esterov showed that if $\mathcal{A}_\bullet$ is neither lacunary nor triangular, then $\mathcal{G}_{\mathcal{A}_\bullet}$ is two–transitive and $\mathcal{G}_{\mathcal{A}_\bullet}$ contains a simple transposition. If the supports $\mathcal{A}_\bullet$ are lacunary or triangular, then the Galois group is a subgroup of a particular wreath product, but which subgroup is not known in general. There are partial results in determining the Galois group when the supports are lacunary and triangular [7, 39]. Esterov's theorem classifies those supports $\mathcal{A}_\bullet$ for which the branched cover $\pi_{\mathcal{A}_\bullet}$ is decomposable. By Theorem 49 and Theorem 51, if the set of supports $\mathcal{A}_\bullet$ is lacunary or triangular, then $\pi_{\mathcal{A}_\bullet}$ is decomposable. Conversely, if $\mathcal{A}_\bullet$ is not lacunary nor triangular, then the Galois group $\mathcal{G}_\pi$ is fully symmetric so that by Theorem 44, π is not decomposable.

5.3 Solving Sparse Polynomial Systems

We present methods of solving sparse polynomial systems from [9]. If $\mathcal{A}_\bullet$ is lacunary or triangular, we say that a system $F \in \mathbb{C}^{\mathcal{A}_\bullet}$ is *decomposable*. For such a system, the zeros are identified with the fiber $\pi^{-1}_{\mathcal{A}_\bullet}(F)$ and the branched cover $\pi_{\mathcal{A}_\bullet}$ decomposes by Theorem 49 and Theorem 51. As noted by Améndola and Rodriguez, the fiber $\pi^{-1}_{\mathcal{A}_\bullet}(F)$ may be computed "in stages" by iteratively decomposing $\pi_{\mathcal{A}_\bullet}$ and its factors. In addition, homotopy continuation methods may be used to further reduce computation [40].

Our primary tool in this section is the Smith normal form of a matrix. Recall that given an $n \times m$ integer matrix A, a Smith normal form is a matrix factorization of the form

$$A = PDQ,$$

where $P \in \mathrm{GL}(n)$ and $Q \in \mathrm{GL}(m)$ are invertible integer matrices and D is an $n \times m$ diagonal

integer matrix whose diagonal entries $d_1, \ldots, d_{\min\{n,m\}}$ satisfy $d_i \mid d_{i+1}$. For $1 \leq k \leq m$, write D_k for the $n \times k$ submatrix of D whose columns are the first k columns of D.

We proceed by demonstrating how fibers of the branched cover $\pi_{\mathcal{A}_\bullet} : \Gamma_{\mathcal{A}_\bullet} \to \mathbb{C}^{\mathcal{A}_\bullet}$ may be computed if $\mathcal{A}_\bullet$ is lacunary or triangular.

Lacunary case: Let $\mathcal{A}_\bullet$ be a lacunary set of supports and $F \in \mathbb{C}^{\mathcal{A}_\bullet}$. We express $\mathbb{Z}\mathcal{A}_\bullet$ as the image of a linear map represented by the $n \times m$ integer matrix A whose column vectors are the elements of the supports $\mathcal{A}_1, \ldots, \mathcal{A}_n$. As $\mathrm{MV}(\mathcal{A}_\bullet) > 0$, we have that $m > n$ and $\operatorname{rank} A = n$. Consider a Smith normal form $A = PDQ$ with $P \in \mathrm{GL}(n)$, $Q \in \mathrm{GL}(m)$ and D a diagonal $n \times m$ matrix with diagonal elements $d_1, \ldots, d_n \geq 1$. The matrix PD_n determines a linear map $\phi : \mathbb{Z}^n \to \mathbb{Z}^n$ whose image is $\mathbb{Z}\mathcal{A}_\bullet$.

The linear map ϕ determines a monomial map $\varphi : (\mathbb{C}^\times)^n \to (\mathbb{C}^\times)^n$, which is a composition $\varphi = \eta \circ \nu$ of a change of variables $\nu : (\mathbb{C}^\times)^n \to (\mathbb{C}^\times)^n$ corresponding to P and a surjective monomial map $\eta : (\mathbb{C}^\times)^n \to (\mathbb{C}^\times)^n$ determined by D_n. The monomial map η has the form

$$\eta(x_1, \ldots, x_n) = (x_1^{d_1}, \ldots, x_n^{d_n}).$$

Thus, given $y = (y_1, \ldots, y_n) \in (\mathbb{C}^\times)^n$, the fiber $\varphi^{-1}(y)$ of the monomial map φ may be computed by extracting the d_i–th roots of y_i for $i = 1, \ldots, n$ and then changing coordinates by ν^{-1}. More precisely, if $|z|$ and $\arg(z)$ denote the modulus and argument of $z \in \mathbb{C}$ respectively, then

$$\varphi^{-1}(y) = \left\{ \nu^{-1}(|y_1| e^{\arg(y_1) + 2\pi i j_1/d_1}, \ldots, |y_n| e^{\arg(y_n) + 2\pi i j_n/d_n}) : 0 \leq j_k < d_k \text{ for } 1 \leq k \leq n \right\}.$$

The reduced support $\mathcal{B}_\bullet = (\phi^{-1}(\mathcal{A}_1), \ldots, \phi^{-1}(\mathcal{A}_n))$ may be computed explicitly via linear algebra. Define the map $\iota : \mathbb{C}^{\mathcal{A}_\bullet} \to \mathbb{C}^{\mathcal{B}_\bullet}$ as before. For $F \in \mathbb{C}^{\mathcal{A}_\bullet}$, there is an equality $F(x) = \iota(F)(\varphi(x))$ so that the variety $\mathcal{V}(F)$ may be expressed as

$$\mathcal{V}(F) = \varphi^{-1}(\mathcal{V}(\iota(F))).$$

Given a blackbox solver to compute the isolated zeros of the system $\iota(F)$, this leads to an algorithm for solving lacunary sparse polynomial systems.

Algorithm 53 (`SolveLacunary`)**.**

`Input`**:** *A system $F \in \mathbb{C}^{\mathcal{A}_\bullet}$ with a lacunary set of supports and a blackbox polynomial system solver* `SOLVE`$(-)$.

`Output`**:** *The isolated zeros of $\mathcal{V}(F)$.*

`Do`**:**

1. *Compute the Smith normal form $A = PDQ$ of the matrix A whose columns are elements of the supports $\mathcal{A}_1, \ldots, \mathcal{A}_n$.*
2. *Determine the monomial map $\varphi : (\mathbb{C}^\times)^n \to (\mathbb{C}^\times)^n$, the reduced support $\mathcal{B}_\bullet$, and the reduced system $\iota(F) \in \mathbb{C}^{\mathcal{B}_\bullet}$.*
3. *Compute the zeros of the reduced system via the blackbox solver,* `SOLVE`$(\iota(F))$.
4. *Compute the fiber $\varphi^{-1}(z)$ for each $z \in \mathcal{V}(\iota(F))$.*
5. *Return the union* $\displaystyle\bigcup_{z \in \mathcal{V}(\iota(F))} \varphi^{-1}(z)$.

This algorithm has the benefit that the reduced system $\iota(F) \in \mathbb{C}^{\mathcal{B}_\bullet}$ has fewer zeros than $F \in \mathbb{C}^{\mathcal{A}_\bullet}$ by a factor of $[\mathbb{Z}^n : \mathbb{Z}\mathcal{A}_\bullet]$. As a result, if the blackbox solver `SOLVE` utilizes numerical homotopy algorithms, fewer paths are tracked.

Triangular case: Let $\mathcal{A}_\bullet$ be a triangular set of supports witnessed by $I \subseteq [n]$, and let $J \subseteq [n]$ be the complement of I. By reordering the supports, we may assume without loss of generality that $I = \{1, \ldots, k\}$ and $J = \{k+1, \ldots, n\}$. Similar to the lacunary case, we express the saturation $\mathrm{sat}(\mathbb{Z}\mathcal{A}_I)$ as the image of a linear map represented by the $n \times m$ integer matrix A whose columns vectors are elements of the supports $\mathcal{A}_i$ for $i \in I$. If $A = PDQ$ is a Smith normal form of A, then $\mathbb{Z}\mathcal{A}_I$ is generated by the columns of PD_k and its saturation $\mathrm{sat}(\mathbb{Z}\mathcal{A}_I)$ is generated by the first k columns of P.

Write $e_1, \ldots, e_n$ for the standard basis in $\mathbb{Z}^n$. The matrix P determines a linear map $\phi : \mathbb{Z}^n \to \mathbb{Z}^n$ that restricts to an isomorphism $\mathbb{Z}^I = \langle e_1, \ldots, e_k \rangle \to \mathrm{sat}(\mathbb{Z}\mathcal{A}_I)$. Further, the complement $\mathbb{Z}^J = \langle e_{k+1}, \ldots, e_n \rangle$ maps to a complement of $\mathrm{sat}(\mathbb{Z}\mathcal{A}_I)$. The torus $(\mathbb{C}^\times)^I$, whose set of characters is $\mathbb{Z}^I$, is then identified with the image of the projection $(\mathbb{C}^\times)^n \to (\mathbb{C}^\times)^k$ onto the first k coordinates, and the torus $(\mathbb{C}^\times)^J$ is the image of the projection $(\mathbb{C}^\times)^n \to (\mathbb{C}^\times)^{n-k}$ onto the last $n-k$ coordinates. We write $(x, y) \in (\mathbb{C}^\times)^I \times (\mathbb{C}^\times)^J = (\mathbb{C}^\times)^n$ for this split of coordinates.

The new set of supports $\mathcal{B}_\bullet = (\phi^{-1}(\mathcal{A}_1), \ldots, \phi^{-1}(\mathcal{A}_n))$ are computed via linear algebra and are such that $\mathcal{B}_i = \phi^{-1}(\mathcal{A}_i) \subseteq \mathbb{Z}^I$ for $i \in I$. That is, the linear map ϕ determines an explicit change of coordinates for which a system of support $\mathcal{A}_\bullet$ has an apparent subsystem given by the polynomials indexed by I. Precisely, a system in $\mathbb{C}^{\mathcal{B}_\bullet}$ then has the form $(F_I(x), F_J(x, y))$ where $F_I \in \mathbb{C}^{\mathcal{B}_I}$, $F_J \in \mathbb{C}^{\mathcal{B}_J}$, and $F_I(x)$ is a subsystem.

Recall the decomposition $\pi_{\mathcal{B}_\bullet} = \psi \circ \theta$ where $\theta : \Gamma_{\mathcal{B}_\bullet} \to \Lambda_{\mathcal{B}_\bullet}$ is defined by $\theta((F_I, F_J), (x, y)) = ((F_I, F_J), x)$ and $\psi : \Lambda_{\mathcal{B}_\bullet} \to \mathbb{C}^{\mathcal{B}_\bullet}$ is the map $\psi((F_I, F_J), x) = (F_I, F_J)$. Given a system $(F_I, F_J) \in \mathbb{C}^{\mathcal{B}_\bullet}$, the fiber $\psi^{-1}(F_I, F_J)$ is identified with the variety $\mathcal{V}(F_I) \subseteq (\mathbb{C}^\times)^I$. Similarly, for each $x_0 \in \mathcal{V}(F_I)$, the fiber $\theta^{-1}((F_I, F_J), x_0)$ is identified with the zeros of the polynomial system $F_J(x_0, y)$ for $y \in (\mathbb{C}^\times)^J$. A system of this form is called a *residual system* and is a sparse polynomial system of support $\overline{\mathcal{B}}_J = (\overline{\mathcal{B}}_j)_{j \in J}$ where $\overline{\mathcal{B}}_j$ is the image of $\mathcal{B}_j$ under the projection $\mathbb{Z}^n \to \mathbb{Z}^J$ onto the last $n-k$ standard basis vectors. For a general system $(F_I, F_J) \in \mathbb{C}^{\mathcal{B}_\bullet}$, each residual system has $\mathrm{MV}(\overline{\mathcal{B}}_J)$ distinct isolated zeros.

We remark on a use of numerical homotopy continuation for efficient solving as described in [40]. Let $(F_I, F_J) \in \mathbb{C}^{\mathcal{B}_\bullet}$ be a system such that the subsystem F_I has $\mathrm{MV}(\mathcal{B}_I)$ distinct isolated zeros and for some $x_0 \in \mathcal{V}(F_I)$, the residual system $F_J(x_0, y)$ has $\mathrm{MV}(\overline{\mathcal{B}}_J)$ distinct isolated zeros. Then this residual system may be used as a start system for numerical homotopy algorithms to compute the isolated zeros of each residual system $F_J(x_i, y)$ for $x_i \in \mathcal{V}(F_I)$.

Algorithm 54 (`SolveTriangular`)**.**

`Input:` *A general system $F \in \mathbb{C}^{\mathcal{A}_\bullet}$ with a triangular set of supports witnessed by I and a blackbox polynomial system solver* `SOLVE`$(-)$.

`Output`: *The isolated zeros of* $\mathcal{V}(F)$.

`Do`:

1. *Compute the Smith normal form* $A = PDQ$ *of the matrix* A *whose columns are elements of the supports* $(\mathcal{A}_i)_{i\in I}$.

2. *Apply the change of coordinates determined by the linear map* $\phi : \mathbb{Z}^n \to \mathbb{Z}^n$ *to obtain a system* $(F_I, F_J) \in \mathbb{C}^{\mathcal{B}_\bullet}$.

3. *Compute the isolated zeros of the subsystem via the blackbox solver,* `SOLVE`(F_I).

4. *For a single point* $x_0 \in \mathcal{V}(F_I)$*, compute the zeros of the residual system* $F_J(x_0, y)$ *via the blackbox solver,* `SOLVE`$(F_J(x_0, y))$.

5. *Use numerical homotopy continuation to compute the zeros of each residual system* $F_J(x_i, y)$ *for* $x_i \in \mathcal{V}(F_I)$.

5. *Compute the union* $\bigcup_{x_i\in\mathcal{V}(F_I)} \{(x_i, y) \in (\mathbb{C}^\times)^n : y \in \mathcal{V}(F_J(x_i, y))\}$ *and invert the change of coordinates.*

6. *Return the computed points.*

Both `SolveLacunary` and `SolveTriangular` require the input of a blackbox polynomial system solver. In both cases, the systems that require solving are again sparse polynomial systems. This leads to a recursive algorithm for solving sparse polynomial systems by decomposing systems if possible at every step. After every iteration of this algorithm, the mixed volume of the involved systems decreases and thus eventually terminates. This, along with our discussions of the previous algorithms provide a proof of correctness.

Algorithm 55 (`SolveDecomposable`)**.**

`Input`: *A general system* $F \in \mathbb{C}^{\mathcal{A}_\bullet}$ *and a blackbox polynomial system solver* `SOLVE`$(-)$.

`Output`: *The isolated zeros of* $\mathcal{V}(F)$.

`Do`:

1. *If $\mathcal{A}_\bullet$ is lacunary, then return* `SolveLacunary`$(F,$ `SolveDecomposable`$)$.

2. *Else if there exists a witness for triangularity $I \subseteq [n]$, then return* `SolveTriangular`$(F,$ `SolveDecomposable`$)$.

3. *Else return* `SOLVE`(F).

The `Macaulay2` package `DecomposableSparseSystems.m2` contains an implementation of `SolveDecomposable` which by default uses the blackbox solver `phc` [10, 41]. A numerical experiment compared the algorithm `SolveDecomposable` to the solver `phc` itself through the `Macaulay2` package `PHCPack` which provides an interface for `phc` [42]. This experiment compared the timing and accuracy in solving sparse polynomial systems having a mixture of lacunary and triangular structures. More details on this experiment are described in [9]. We briefly describe how these systems were generated.

Let $\mathcal{A}_1 = \left(\begin{smallmatrix} 0 & 1 & 2 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{smallmatrix}\right)$, $\mathcal{A}_2 = \left(\begin{smallmatrix} 1 & 0 & 1 & 2 & 1 \\ 0 & 1 & 1 & 1 & 2 \end{smallmatrix}\right)$, $\mathcal{B}_1 = \left(\begin{smallmatrix} 0 & 2 & 0 & 2 \\ 0 & 0 & 1 & 3 \end{smallmatrix}\right)$, $\mathcal{B}_2 = \left(\begin{smallmatrix} 0 & 1 & 2 & 0 & 2 & 0 \\ 0 & 0 & 0 & 1 & 1 & 2 \end{smallmatrix}\right)$, and $\mathcal{C}$ be the vertices of the unit cube in $\mathbb{Z}^5$. The supports $\mathcal{A}_1$, $\mathcal{A}_2$, $\mathcal{B}_1$, and $\mathcal{B}_2$ are illustrated in Figure 5.1. Given two embeddings $\imath : \mathbb{Z}^2 \to \mathbb{Z}^5$ and $\jmath : \mathbb{Z}^2 \to \mathbb{Z}^5$ such that $\imath(\mathbb{Z}^2) \cap \jmath(\mathbb{Z}^2) = \{0\}$, consider the set of supports $\mathcal{A}(\imath, \jmath) = (\imath(\mathcal{A}_1), \imath(\mathcal{A}_2), \jmath(\mathcal{B}_1), \jmath(\mathcal{B}_2), \mathcal{C})$.

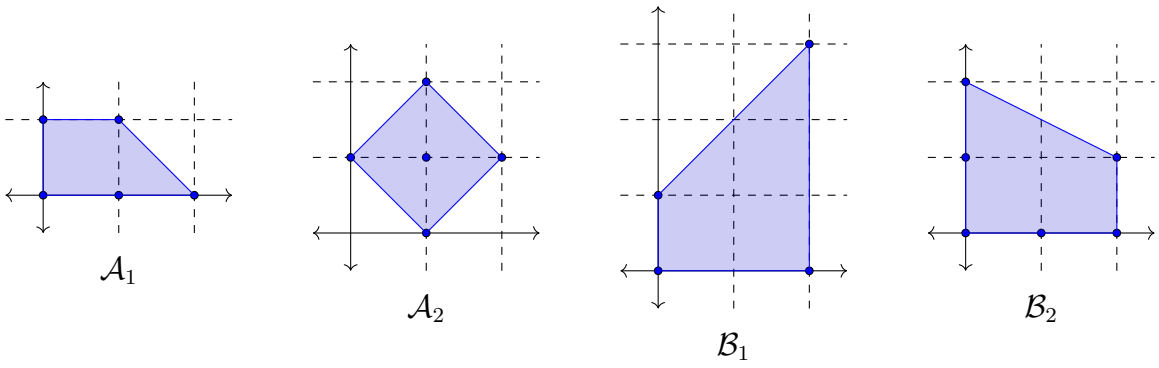

Figure 5.1: Supports for numerical experiment

For any embeddings $\imath$ and $\jmath$, the set of supports $\mathcal{A}(\imath, \jmath)$ is triangular. Indeed, there is a change of coordinates for which a system of support $\mathcal{A}(\imath, \jmath)$ has two subsystems witnessed by the sets $\{1, 2\}$

and $\{3, 4\}$ respectively. Further, these subsystems may be lacunary, depending on the embeddings $\imath$ and $\jmath$ respectively.

In total, the experiment generated over ten thousand instances of sparse polynomial systems having support $\mathcal{A}(\imath, \jmath)$ for various embeddings $\imath$ and $\jmath$. On average, Algorithm `SolveDecomposable` computed the zeros of the system faster and more reliably while including the overhead of recursively decomposing the systems. The results of this experiment are summarized in Figure 5.2.

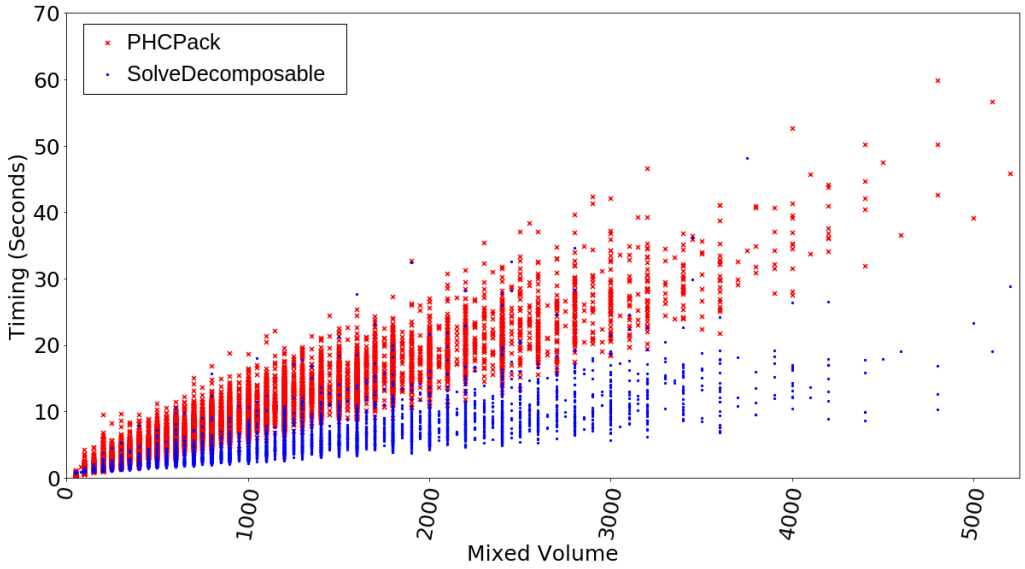

Figure 5.2: Scatter plot of timings for `SolveDecomposable` and `PHCPack`

6. FANO PROBLEMS

6.1 Fano Schemes

A Fano problem is the problem of enumerating linear spaces lying on a variety X. Given a variety $X \subseteq \mathbb{P}^n$, its *Fano scheme* $\mathcal{V}_r(X)$ of r–planes is the subvariety of $\mathbb{G}(r, \mathbb{P}^n)$ which consists of the r–planes that are contained in X.

We study Fano schemes of r–planes systematically when $X \subseteq \mathbb{P}^n$ is a complete intersection. Given a sequence $d_\bullet = (d_1, \ldots, d_s)$, we consider polynomial systems $F = (f_1, \ldots, f_s)$ where each f_i is a homogeneous polynomial in $n+1$ variables of degree d_i. The set of all such systems F is a vector space $\mathbb{C}^{(r,n,d_\bullet)}$ of dimension

$$\dim \mathbb{C}^{(r,n,d_\bullet)} = \sum_{i=1}^{s} \binom{n+d_i}{d}.$$

A *complete intersection* is the zero set $X = \mathcal{V}(F)$ of a system $F \in \mathbb{C}^{(r,,n,d_\bullet)}$ such that X is smooth and $\dim X = n - s$. By Bertini's Theorem [13], there is a Zariski open subset $U \subseteq \mathbb{C}^{(r,n,d_\bullet)}$ such that if $F \in U$, then the zero set $X = \mathcal{V}(F)$ is a complete intersection. By a *general* $F \in \mathbb{C}^{(r,n,d_\bullet)}$, we refer to a system in this Zariski open set $F \in U$.

Given a system $F = (f_1, \ldots, f_s) \in \mathbb{C}^{(r,n,d_\bullet)}$, we write $F|_\ell = (f_1|_\ell, \ldots, f_s|_\ell)$ for its component–wise restriction to the r–plane $\ell \in \mathbb{G}(r, \mathbb{P}^n)$. A Fano scheme of *type* $(r, n, d_\bullet)$ is a variety of the form

$$\mathcal{V}_r(X) = \{\ell \in \mathbb{G}(r, \mathbb{P}^n) : F|_\ell = 0\},$$

where $X = \mathcal{V}(F)$ and $F \in \mathbb{C}^{(r,n,d_\bullet)}$. A *general* Fano scheme of type $(r, n, d_\bullet)$ is a Fano scheme $\mathcal{V}_r(X)$ of a variety $X = \mathcal{V}(F)$ for general $F \in \mathbb{C}^{(r,n,d_\bullet)}$.

6.1.1 Dimension

We determine the expected dimension of a Fano scheme of a given type $(r, n, d_\bullet)$ by describing it as the vanishing of a section of a vector bundle, or more simply, as a polynomial system in local coordinates. Let $I = \{0, \ldots, r\}$ and consider the affine coordinate chart $U_I = \mathbb{A}_I^{\binom{n+1}{r+1}-1}$ of $\mathbb{G}(r, \mathbb{P}^n)$. An r–plane $\ell \in U_I$ has unique Stiefel coordinates of the form

$$A = \left(\frac{Id_{r+1}}{A'} \right),$$

where A' is a $(n-r) \times (r+1)$ matrix. The columns of A give a parameterization for ℓ and given a homogeneous polynomial $f \in \mathbb{C}[x_0, \ldots, x_n]$ of degree d, the restriction $f|_\ell$ is the substitution of this parameterization into f. In particular, $f|_\ell$ is a homogeneous polynomial in $r+1$ variables of degree d and the coefficients of $f|_\ell$ are polynomials in the entries of A'. Given $F \in \mathbb{C}^{(r,n,d_\bullet)}$ and $X = \mathcal{V}(F)$, the vanishing of the system $F|_\ell = 0$ is equivalent to the vanishing of the $\sum_{i=1}^s \binom{r+d_i}{r}$ coefficients of the polynomials $f_i|_\ell$. Thus, the Fano scheme $\mathcal{V}_r(X) \cap U_I$ is the zero set of a system of $\sum_{i=1}^s \binom{r+d_i}{r}$ polynomials in $(r+1)(n-r)$ variables, which are the entries of A'. This holds in any affine coordinate chart U_I for $I \in \binom{[n+1]}{r+1}$. The expected dimension of the Fano scheme $\mathcal{V}_r(X)$ is given by

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

Debarre and Manivel studied Fano schemes of complete intersections and showed that this expected dimension is the dimension for many Fano schemes [43].

Theorem 56 (Debarre, Manivel)**.** *If $\delta(r, n, d_\bullet) \geq 0$ and $2r \leq n - s$, then a general Fano scheme of type $(r, n, d_\bullet)$ is smooth and has dimension $\delta(r, n, d_\bullet)$. If $\delta(r, n, d_\bullet) < 0$ or $2r > n - s$, then a general Fano scheme is empty.*

6.1.2 Degree

We will be concerned with varieties that contain finitely many r–planes. A *Fano problem* is a tuple $(r, n, d_\bullet)$ for which $\delta(r, n, d_\bullet) = 0$ and $2r \leq n - s$. By Theorem 56, a general Fano scheme of this type will consist of finitely many r–planes.

Given a Fano problem $(r, n, d_\bullet)$, the cardinality of a general Fano scheme of type $(r, n, d_\bullet)$ is called the *degree* $\deg(r, n, d_\bullet)$ of the Fano problem. Debarre and Manivel calculated this degree explicitly by describing it as the Chern class of a vector bundle on $\mathbb{G}(r, \mathbb{P}^n)$. To state this result, we define the following polynomials. For a Fano problem $(r, n, d_\bullet)$, define

$$Q_{r,d_j}(x) = \prod_{\substack{a_i \in \mathbb{Z}_{\geq 0} \\ a_0 + \cdots + a_r = d_j}} (a_0 x_0 + \cdots + a_r x_r) \in \mathbb{Z}[x_0, \ldots, x_r].$$

The product of these polynomials is written $Q_{r,d_\bullet}(x) = Q_{r,d_1}(x) \cdots Q_{r,d_s}(x)$ and the Vandermonde polynomial is given by

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

Debarre and Manivel's result is stated as follows.

Theorem 57 (Debarre, Manivel)**.** *The degree of a Fano problem $(r, n, d_\bullet)$ is given by the coefficient of the monomial $x_0^n x_1^{n-1} \cdots x_r^{n-r}$ in the product $Q_{r,d_\bullet}(x)V(x)$.*

For the Fano problem $(r, n, d_\bullet)$, the quantity $\prod_i d_i^{r+1}$ divides the degree $\deg(r, n, d_\bullet)$ and provides a lower bound. This and other lower bounds may be used to enumerate Fano problems up to a given degree. Table 6.1 shows those Fano problems with degree less than 1200, for example.

6.2 Galois Groups of Fano Problems

Given a Fano problem $(r, n, d_\bullet)$, we define an incidence variety

$$\Gamma = \{(F, \ell) \in \mathbb{C}^{(r,n,d_\bullet)} \times \mathbb{G}(r, \mathbb{P}^n) : F|_\ell = 0\}.$$

r	n	$d_\bullet$	$\deg(r,n,d_\bullet)$	Galois Group
1	4	$(2,2)$	16	D_5
1	3	(3)	27	E_6
2	6	$(2,2)$	64	D_7
3	8	$(2,2)$	256	D_9
1	7	$(2,2,2,2)$	512	S_{512}
1	6	$(2,2,3)$	720	S_{720}
4	10	$(2,2)$	1024	D_{11}
2	8	$(2,2,2)$	1024	S_{1024}
1	5	$(3,3)$	1053	S_{1053}

Table 6.1: Fano problems of degree less than 1200

As a subset of the product $\Gamma \subseteq \mathbb{C}^{(r,n,d_\bullet)} \times \mathbb{G}(r,\mathbb{P}^n)$, there are projection maps $\pi_{(r,n,d_\bullet)} : \Gamma \to \mathbb{C}^{(r,n,d_\bullet)}$ and $\rho : \Gamma \to \mathbb{G}(r,\mathbb{P}^n)$. By studying the map ρ, we show that Γ is a smooth, irreducible variety and compute its dimension.

Let $I \in \binom{[n+1]}{r+1}$ and consider the affine coordinate chart $U_I = \mathbb{A}_I^{\binom{n+1}{r+1}-1}$ of the Grassmanian $\mathbb{G}(r,\mathbb{P}^n)$. We show that the Zariski open set $V_I = \rho^{-1}(U_I)$ is isomorphic to $\mathbb{C}^N \times U_I$, where $N = \sum_{i=1}^{s} \binom{n+d_i}{n} - \binom{r+d_i}{r}$. By a linear change of coordinates on $\mathbb{P}^n$, we may assume that $I = \{0,\ldots,r\}$. A point of U_I has a unique set of Stiefel coordinates of the form

$$\left(\begin{array}{c} Id_{r+1} \\ \hline A \end{array}\right),$$

where A is a $(n-r)\times(r+1)$ matrix. Then there is a linear change of coordinates $\phi_\ell : \mathbb{P}^n \to \mathbb{P}^n$ represented by the matrix

$$\left(\begin{array}{c|c} Id_{r+1} & 0 \\ \hline A & Id_{n-r} \end{array}\right)^{-1},$$

which maps ℓ to the coordinate r–plane $\vartheta \in \mathbb{G}(r,\mathbb{P}^n)$ defined by $x_{r+1} = \cdots = x_n = 0$. The

set of homogeneous polynomials of degree d that vanish on ϑ is a vector space of dimension $\binom{n+d}{n} - \binom{r+d}{r}$ so that the space of systems $F \in \mathbb{C}^{(r,n,d_\bullet)}$ that vanish on ϑ is a vector space of dimension N that we identify with $\mathbb{C}^N$ by a choice of basis. Thus, there is a map $\varphi : \mathbb{C}^N \times U_I \to V_I$ defined by $\varphi(F, \ell) = (\widetilde{F}, \ell)$, where $\widetilde{F}$ is the system obtained by changing coordinates by ϕ_ℓ. As the change of coordinates ϕ_ℓ is invertible, φ is an isomorphism.

The Zariski open sets U_I for $I \in \binom{[n+1]}{r+1}$ form an open cover of the Grassmanian $\mathbb{G}(r, \mathbb{P}^n)$ and their preimages $V_I = \rho^{-1}(U_I)$ are irreducible. By Theorem 17, Γ is irreducible. It follows that Γ is a smooth, irreducible variety of dimension

$$\begin{aligned}\dim \Gamma &= (r+1)(n-r) + \sum_{i=1}^{s} \tbinom{n+d_i}{n} - \tbinom{r+d_i}{r} \\ &= \sum_{i=1}^{s} \tbinom{n+d_i}{n} = \dim \mathbb{C}^{(r,n,d_\bullet)}.\end{aligned}$$

The fibers of the projection $\pi_{(r,n,d_\bullet)} : \Gamma \to \mathbb{C}^{(r,n,d_\bullet)}$ are identified with Fano schemes of type $(r, n, d_\bullet)$. As Γ is a smooth, irreducible variety of dimension $\dim \Gamma = \dim \mathbb{C}^{(r,n,d_\bullet)}$, Theorem 56 implies $\pi_{(r,n,d_\bullet)}$ is a degree $\deg(r, n, d_\bullet)$ branched cover.

Definition 58. The *Galois group* $\mathcal{G}_{(r,n,d_\bullet)}$ of the Fano problem $(r, n, d_\bullet)$ is the Galois group of the branched cover $\pi_{(r,n,d_\bullet)} : \Gamma \to \mathbb{C}^{(r,n,d_\bullet)}$.

6.2.1 Known Results

Galois groups of Fano problems were among those Galois groups studied by Jordan, in the first written work on Galois theory [1]. Jordan studied the Galois group of the lines on a cubic surface, which is the Fano problem $(1, 3, (3))$. Jordan showed that the Galois group is a subgroup of the Weyl group $W(E_6)$ by using classically known results concerning these lines. Galois groups of Fano problems were left largely untouched until Harris generalized Jordan's result by considering the algebraic Galois groups Jordan defined as geometric monodromy groups. Harris showed Jordan's inclusion is an equality $\mathcal{G}_{(1,3,(3))} = W(E_6)$ and proved the following generalization.

Theorem 59 (Harris)**.** *For $n \geq 4$, the Galois group $\mathcal{G}_{(1,n,(2n-3))}$ of the Fano problem of lines in $\mathbb{P}^n$*

on a hypersurface of degree $2n-3$ *is fully symmetric.*

Harris' arguement was similar to that of Esterov—Harris showed these Galois groups are two–transitive and that they contain a transposition. To show these Galois groups contain a simple transposition, Harris utilized the following.

Proposition 60 (Harris)**.** *If* $\pi : X \to Y$ *is a degree* d *branched cover of smooth varieties and there exists* $y \in Y$ *is such that the fiber* $\pi^{-1}(y)$ *consists of* $d-2$ *smooth points* $x_1, \ldots, x_{d-2} \subseteq X$ *and a unique double point* $x_{d-1} \in X$*, then the Galois group* $\mathcal{G}_\pi$ *contains a simple transposition.*

Proof. As $x_1, \ldots, x_{d-2}$ are smooth points of the fiber, there are Euclidean neighborhoods $V_1, \ldots, V_{d-2}$ which map diffeomorphically by π to a neighborhood $U \subseteq Y$ of y by the implicit function theorem. By shrinking these neighborhoods if necessary, we may assume they are disjoint from one another and that there is a Euclidean neighborhood V_{d-1} of x_{d-1} disjoint from each V_i. By Theorem 32, the image $\pi(V_{d-1})$ contains a Euclidean neighborhood of y which we may take to be U. That is, we may assume that $\pi^{-1}(U)$ consists of $d-1$ connected components each contained in the disjoint neighborhoods $V_1, \ldots, V_{d-1}$ of $x_1, \ldots, x_{d-1}$.

If $W \subseteq Y$ is a Zariski open set such that the restriction $\pi : \pi^{-1}(W) \to W$ is a covering space, then $W \cap U$ is nonempty and we fix $\widetilde{y} \in W \cap U$. The fiber $\pi^{-1}(\widetilde{y}) = \{\widetilde{x}_1, \ldots, \widetilde{x}_d\}$ consists of d points and by reordering we assume that $\widetilde{x}_i \in V_i$ for $i = 1, \ldots, d-2$ and $\widetilde{x}_{d-1}, \widetilde{x}_d \in V_{n-1}$.

By Lemma 31, $V_{n-1} \cap \pi^{-1}(W)$ is path–connected and there exists a path $\widetilde{\gamma} : [0,1] \to V_{n-1} \cap \pi^{-1}(W)$ starting at x_{d-1} and ending at x_d. Consider the lifts of the projected path $\gamma : [0,1] \to U \cap W$, which is a loop based at $\widetilde{y}$. For $i = 1, \ldots, d-2$, the lift starting at x_i lies entirely in V_i and so necessarily ends at x_i. As the lift $\widetilde{\gamma} : [0,1] \to V_{n-1} \cap \pi^{-1}(W)$ starts at x_{d-1} and ends at x_d, The loop γ generates a simple transposition of the fiber $\pi^{-1}(\widetilde{y})$.

□

Recently, Hashimoto and Kadets nearly classified Galois groups of all Fano problems. They began by identifying a special family of Fano problems, each having an enriched Galois group. It was then shown by an iterative method that the Galois groups of many Fano problems are at least

two–transitive. A classification of highly transitive permutation groups by Jordan then shows that many Galois groups contain the alternating group.

Theorem 61 (Hashimoto, Kadets)**.**

1. *The Galois group $\mathcal{G}_{(r,2r+2,(2,2))}$ is the Weyl group $W(D_{2r+3})$ for $r \geq 1$.*

2. *If $(r, n, d_\bullet)$ is not equal to $(1, 3, (3))$ or $(r, 2r + 2, (2, 2))$ for $r \geq 1$, then the Galois group $\mathcal{G}_{(r,n,d_\bullet)}$ is at least alternating.*

6.3 Computing Galois Groups of Fano Problems

By Theorem 61, a complete classification of Galois groups of Fano problems rests on determining the Galois groups of those Fano problems $(r, n, d_\bullet)$ not equal to $(1, 3, (3))$ or $(r, 2r + 2, (2, 2))$ for $r \geq 1$. In [44], a numerical method utilizing Proposition 60 was used to prove that several Galois groups of Fano problems which are at least alternating are in fact fully symmetric. We present the method used in that article and its results.

Given a Fano problem $(r, n, d_\bullet)$, we wish to construct a system $F \in \mathbb{C}^{(r,n,d_\bullet)}$ so that the Fano scheme $\mathcal{V}_r(X)$ of the variety $X = \mathcal{V}(F)$ contains $\deg(r, n, d_\bullet) - 2$ smooth points and a unique double point. To accomplish this, let $I = \{0, \ldots, r\}$ and describe $V_r(X)$ in local coordinates on U_I by a system $\widetilde{F}$ of $\sum_{i=1}^{s} \binom{r+d_i}{r} = (r + 1)(n - r)$ polynomials in $(r + 1)(n - r)$ variables. We would like $\widetilde{F}$ to have $\deg(r, n, d_\bullet) - 2$ smooth zeros and a unique double zero.

The linear space of systems $F \in \mathbb{C}^{(r,n,d_\bullet)}$ which vanish on an r–plane $\ell \in \mathbb{G}(r, \mathbb{P}^n)$ may be determined explicitly. Indeed, representing ℓ in coordinates on U_I as the point x_ℓ, it is the locus of systems F for which $\widetilde{F}(x_\ell) = 0$. The condition that $\widetilde{F}(x_\ell) = 0$ is a linear condition on the coefficients of $\widetilde{F}$, which is a linear condition on the coefficients of F, $\mathbb{C}^{(r,n,d_\bullet)}$. The condition that a vector $v \in \mathbb{C}^{(r+1)(n-r)}$ lie in the tangent space $v \in T_\ell \mathcal{V}_r(X)$ is also a linear condition on $\mathbb{C}^{(r,n,d_\bullet)}$ as it is the locus of systems for which $\widetilde{F}$ satisfies $D\widetilde{F}(x_\ell)v = 0$, which is linear in the coefficients of $\widetilde{F}$. Further, if ℓ and v have been chosen to have complex rational coefficients, that is, $\mathbb{Q}(i)$–valued coefficients, then these linear constraints may be obtained symbolically. That is, there is a linear space of systems $F \in \mathbb{C}^{(r,n,d_\bullet)}$, whose coefficients we may take to be $\mathbb{Q}(i)$–valued, such that

if $X = \mathcal{V}(F)$, then $\ell \in \mathcal{V}_r(X)$ and $v \in T_\ell \mathcal{V}_r(X)$. We show how one might verify whether such a system $F \in \mathbb{C}^{(r,n,d_\bullet)}$ has $\deg(r, n, d_\bullet) - 2$ smooth zeros and a unique double zero. We will utilize the following theorem from [45].

Theorem 62 (Dedieu, Shub)**.** *If G is a square system of m polynomials in m variables and $x \in \mathbb{C}^m$ is a point such that $G(x) = 0$, $\ker DG(x) = \langle u \rangle$ for $u \neq 0$, and*

$$D^2G(x)(u, u) \notin \text{im } DG(x),$$

then x is a zero of G of multiplicity two.

By choosing $F \in \mathbb{C}^{(r,n,d_\bullet)}$, $\ell \in \mathbb{G}(r, \mathbb{P}^n)$, and $v \in T_\ell \mathcal{V}_r(X)$ with $\mathbb{Q}(i)$–valued coefficients and coordinates as above, we may use Theorem 62 to use symbolic computation to verify whether x_ℓ is a double zero of $\widetilde{F}$.

Using numerical homotopy continuation, one may obtain approximate zeros of the system $\widetilde{F}$. Further, methods of numerical certification may be used to compute bounding complex intervals of zeros of $\widetilde{F}$ from these approximate zeros. It can be checked that these bounding complex intervals are disjoint from one another and from x_ℓ. If there are $\deg(r, n, d_\bullet) - 2$ many such bounding complex intervals, we are done. Indeed, each bounding complex interval must contain at least one zero of $\widetilde{F}$ and x_ℓ has multiplicity two. Thus, each complex interval contains a unique zero of $\widetilde{F}$ and there are $\deg(r, n, d_\bullet)$ points counting multiplicity.

For those Fano problems $(r, n, d_\bullet)$ with $\deg(r, n, d_\bullet) < 75,000$ whose Galois group is at least alternating, this process was used to compute a system $F \in \mathbb{C}^{(r,n,d_\bullet)}$ contains $\deg(r, n, d_\bullet) - 2$ smooth points and a unique double point. These systems and code verifying the structure of these systems is available at [46].

Theorem 63. *If $(r, n, d_\bullet)$ is a Fano problem with $\deg(r, n, d_\bullet) < 75,000$ and at least alternating Galois group, then the Galois group is fully symmetric.*

Table 6.2 provides a list of those Fano problems covered by the statement of Theorem 63.

r	n	$d_\bullet$	$\deg(r, n, d_\bullet)$
1	7	$(2, 2, 2, 2)$	512
1	6	$(2, 2, 3)$	720
2	8	$(2, 2, 2)$	1024
1	5	(3,3)	1053
1	5	(2,4)	1280
1	10	(2,2,2,2,2,2)	20480
1	9	(2,2,2,2,3)	27648
2	10	(2,2,2,2)	32768
1	8	(2,2,3,3)	37584
1	8	(2,2,2,4)	47104
1	7	(3,3,3)	51759
1	7	(2,3,4)	64512

Table 6.2: Fano Problems with newly computed Galois group

REFERENCES

[1] C. Jordan, *Traité des Substitutions et des Équations algébriques*. Gauthier-Villars, Paris, 1870.

[2] J. Harris, "Galois groups of enumerative problems," *Duke Math. Journal*, vol. 46, no. 4, pp. 685–724, 1979.

[3] C. Hermite, "Sur les fonctions algébriques," *CR Acad. Sci.(Paris)*, vol. 32, pp. 458–461, 1851.

[4] D. N. Bernstein, "The number of roots of a system of equations," *Funkcional. Anal. i Priložen.*, vol. 9, no. 3, pp. 1–4, 1975.

[5] A. G. Kušnirenko, "Newton polyhedra and Bezout's theorem," *Funkcional. Anal. i Priložen.*, vol. 10, no. 3, pp. 82–83, 1976.

[6] B. Huber and B. Sturmfels, "A polyhedral method for solving sparse polynomial systems," *Math. Comp.*, vol. 64, no. 212, pp. 1541–1555, 1995.

[7] A. Esterov and L. Lang, "Sparse polynomial equations and other enumerative problems whose Galois groups are wreath products," *Selecta Math. (N.S.)*, vol. 28, no. 2, pp. Paper No. 22, 35, 2022.

[8] A. Esterov, "Galois theory for general systems of polynomial equations," *Compos. Math.*, vol. 155, no. 2, pp. 229–245, 2019.

[9] T. Brysiewicz, J. I. Rodriguez, F. Sottile, and T. Yahl, "Solving decomposable sparse systems," *Numer. Algorithms*, vol. 88, no. 1, pp. 453–474, 2021.

[10] T. Brysiewicz, J. I. Rodriguez, F. Sottile, and T. Yahl, "Decomposable sparse polynomial systems," *J. Softw. Algebra Geom.*, vol. 11, no. 1, pp. 53–59, 2021.

[11] J. Bowman and A. Hammerlindl, "Asymptote: a vector graphics language," vol. 29, no. 2, pp. 288–294, 2008.

[12] S. Hashimoto and B. Kadets, "38406501359372282063949 and all that: Monodromy of Fano problems," *International Mathematics Research Notices*, 2020.

[13] I. R. Shafarevich, *Basic algebraic geometry. 1*. third ed.

[14] D. Perrin, *Algebraic geometry*. Universitext, Springer-Verlag London, Ltd., London; EDP Sciences, Les Ulis, 2008. Translated from the 1995 French original by Catriona Maclean.

[15] R. Hartshorne, *Algebraic geometry*. Graduate Texts in Mathematics, No. 52, Springer-Verlag, New York-Heidelberg, 1977.

[16] M. F. Atiyah and I. G. Macdonald, *Introduction to commutative algebra*. Addison-Wesley Series in Mathematics, Westview Press, Boulder, CO, economy ed., 2016. For the 1969 original see [MR0242802].

[17] W. Fulton, *Young tableaux*, vol. 35 of *London Mathematical Society Student Texts*.

[18] D. Mumford, *Algebraic geometry. I*. Classics in Mathematics, Springer-Verlag, Berlin, 1995. Complex projective varieties, Reprint of the 1976 edition.

[19] R. C. Gunning and H. Rossi, *Analytic functions of several complex variables*. AMS Chelsea Publishing, Providence, RI, 2009. Reprint of the 1965 original.

[20] L. Gonzalez-Vega, F. Rouillier, and M.-F. Roy, "Symbolic recipes for polynomial system solving," in *Some tapas of computer algebra*, vol. 4 of *Algorithms Comput. Math.*, pp. 34–65, Springer, Berlin, 1999.

[21] F. Rouillier, "Solving zero-dimensional systems through the rational univariate representation," *Appl. Algebra Engrg. Comm. Comput.*, vol. 9, no. 5, pp. 433–461, 1999.

[22] J. Lopez, F. Sottile, and T. Yahl, "Real solutions to systems of polynomial equations in Macaulay2," 2022. `arXiv:2208.05576`.

[23] D. F. Davidenko, "On a new method of numerical solution of systems of nonlinear equations," *Doklady Akad. Nauk SSSR (N.S.)*, vol. 88, pp. 601–602, 1953.

[24] A. J. Sommese and C. W. Wampler, II, *The numerical solution of systems of polynomials*.

[25] A. Morgan, *Solving polynomial systems using continuation for engineering and scientific problems*, vol. 57 of *Classics in Applied Mathematics*.

[26] A. Leykin, "Numerical algebraic geometry," *J. Softw. Algebra Geom.*, vol. 3, pp. 5–10, 2011.

[27] P. Breiding and S. Timme, "HomotopyContinuation.jl: A Package for Homotopy Continuation in Julia," in *International Congress on Mathematical Software*, pp. 458–465, Springer, 2018.

[28] D. Bates, J. Hauenstein, A. Sommese, and C. Wampler, "Bertini: Software for numerical algebraic geometry," Available at `http://www.nd.edu/~sommese/bertini`.

[29] P. Breiding, K. Rose, and S. Timme, "Certifying zeros of polynomial systems using interval arithmetic," 2020. `arXiv:2011.05000`.

[30] R. E. Moore, "A test for existence of solutions to nonlinear systems," *SIAM J. Numer. Anal.*, vol. 14, no. 4, pp. 611–615, 1977.

[31] S. M. Rump, "Solving algebraic problems with high accuracy," in *Parallel and large-scale computers: performance, architecture, applications (Montreal, Que., 1982)*, IMACS Trans. Sci. Comput., II, pp. 299–300, IMACS, New Brunswick, NJ, 1983.

[32] J. R. Munkres, *Topology: a first course*. Prentice-Hall, Inc., Englewood Cliffs, N.J., 1975.

[33] A. Hatcher, *Algebraic topology*. Cambridge University Press, Cambridge, 2002.

[34] R. Vakil, "Schubert induction," *Ann. of Math. (2)*, vol. 164, no. 2, pp. 489–512, 2006.

[35] T. W. Hungerford, *Algebra*, vol. 73 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, 1980. Reprint of the 1974 original.

[36] F. Sottile and T. Yahl, "Galois groups in enumerative geometry and applications," 2021. `arXiv:2108.07905`.

[37] G. P. Pirola and E. Schlesinger, "Monodromy of projective curves," *J. Algebraic Geom.*, vol. 14, no. 4, pp. 623–642, 2005.

[38] G. Ewald, *Combinatorial convexity and algebraic geometry*, vol. 168 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1996.

[39] A. Esterov and L. Lang, "Permuting the roots of univariate polynomials whose coefficients depend on parameters," 2022. arxiv:2204.14235.

[40] C. Améndola and J. I. Rodriguez, "Solving parameterized polynomial systems with decomposable projections," 2016. arXiv:1612.08807.

[41] J. Verschelde, "Algorithm 795: PHCpack: A general-purpose solver for polynomial systems by homotopy continuation," *ACM Trans. Math. Softw.*, vol. 25, no. 2, pp. 251–276, 1999. Available at http://www.math.uic.edu/~jan.

[42] E. Gross, S. Petrović, and J. Verschelde, "Interfacing with PHCpack," *J. Softw. Algebra Geom.*, vol. 5, pp. 20–25, 2013.

[43] O. Debarre and L. Manivel, "Sur la variété des espaces linéaires contenus dans une intersection complète," *Mathematische Annalen*, vol. 312, pp. 549–574, 1998.

[44] T. Yahl, "Computing Galois groups of Fano problems," *J. Symbolic Comput.*, vol. 119, pp. 81—-89, 2023.

[45] J.-P. Dedieu and M. Shub, "On simple double zeros and badly conditioned zeros of analytic functions of n variables," *Math. Comp.*, vol. 70, no. 233, pp. 319–327, 2001.

[46] T. Yahl, "Data and tools for computing Galois groups of Fano problems," 2022. https://github.com/tjyahl/FanoGaloisGroups.