RESEARCH STATEMENT

THOMAS YAHL

Abstract. The Galois group of a problem reflects intrinsic structure of the problem as well as the complexity of computing its solutions. We consider problems coming from enumerative geometry, of finding geometric objects having specified incidences with other fixed objects. The aim of this project is two-fold. First, to develop new methods of solving the resulting algebraic systems by exploiting structure in their Galois groups. Second, to progress current work in computing and classifying Galois groups of specific problems. We use computational tools to both gain insight and obtain new results, developing new techniques in the course of study.

Overview

Enumerative geometry is the study and description of all objects having specified incidences with other fixed objects, such as the set of lines bitangent to a planar quartic curve. Applications of enumerative geometry are ubiquitous and appear in areas such as computer vision, robotics, and mathematical physics. Often one needs approximate solutions to these problems, which may be represented as solutions to polynomial equations and computed with polynomial system solvers. These problems may be poorly conditioned or have large or nearly infinite solutions, both of which are problematic for current solvers. Often geometric structures are present that may be used to reduce computation in these cases. It is a difficult and important problem to create algorithms and specialized solvers to solve these problems by means of these structures.

The complexity of computing solutions of an enumerative problem is determined by its Galois group, which is itself a reflection of intrinsic structures of the problem. Even partial knowledge of the Galois group of an enumerative problem may be exploited to reduce computation for solvers. For instance, Galois groups have been used for fast and effective solving in [4, 6, 7]. The problem of determining Galois groups of enumerative problems is valuable for continuing to create better and more efficient solvers for these problems, as well as for a more complete understanding of these problems and their structure.

The goal of this project is confront the problems described above as follows:

1. *Develop new and improved methods of computing solutions to polynomial systems by exploiting geometric structure.*
2. *Determine Galois groups of enumerative problems, in particular, for the classes of Sparse polynomial systems and Fano problems.*

Preliminary progress on these problems has been successful. The articles [4, 3, 8] address solving sparse polynomial systems through the use of numerical algebraic geometry, toric geometry, and Galois theory. In addition, the article [17] computes several Galois groups of Fano problems, each of which were previously unknown. Finally, through collaboration with undergraduate students, data was generated to estimate Galois groups of sparse polynomial systems. This led to a conjecture for those groups which appear as the Galois group of a sparse polynomial system.

Past Work and Background

Galois groups of enumerative problems. A problem in enumerative geometry can loosely be described as follows:

1. Fix some geometric objects (points, conics, etc.). Let P parameterize these objects.
2. Choose some other geometric objects desired to be incident in some way with the fixed objects. Let S be the set of these objects.
3. Choose specified incidences (tangency, containment, etc.) for the objects in S relative to fixed objects from P.
4. Describe the set of objects in S satisfying these incidences for a choice of fixed objects from P, called solutions.

To an enumerative problem parameterized by a space P and space of solutions S, the incidence variety Γ is the set of all pairs consisting of fixed objects from P with their solutions in S. As a subset of the product $\Gamma \subseteq P \times S$, there is a projection to the parameter space $\pi : \Gamma \to P$. This map contains the information of all problems in the family, along with their solutions. The spaces P, S and Γ are often algebraic varieties, allowing methods of algebraic geometry to study these problems.

A branched cover is a map of (complex) irreducible varieties of the same dimension, with dense image. These are so called as there is a maximal Zariski open set (dense, open, and path-connected) whereon the branched cover restricts to a covering space. As a covering space has a monodromy group defined by lifting directed loops in the base, branched covers also have well-defined monodromy groups. These monodromy groups are defined up to isomorphism by a choice of base point in P and act on the fiber over this base point. For all problems we consider, the map $\pi : \Gamma \to P$ is a branched cover.

Definition 1. The Galois group of an enumerative problem, or of the branched cover $\pi : \Gamma \to P$, is the monodromy group of π.

Traditionally we refer to these as Galois groups as Jordan first described them algebraically, as the Galois group of a certain extension of function fields [13]. The equivalence of these definitions was shown by Harris, but the idea traces back to Hermite [11, 12]. The article *Galois groups in enumerative geometry and applications* [16], being revised for publication as part of this project, summarizes the history and current state of Galois groups in enumerative geometry. Praised as "the first comprehensive survey on the emerging topic", it provides an entry point for early career researchers and details several modern results and applications.

Sparse polynomial systems. Sparse polynomial systems are those systems whose monomial structure has been determined a priori. Many systems arising in applications may be considered as sparse polynomial systems and this structure may be use to efficiently compute solutions. For instance, it has recently been shown that a celebrated algorithm for solving sparse polynomial systems is in a sense "optimal" for solving certain problems arising in economics and algebraic optimization [14, 2].

For a (Laurent) monomial $x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$, the vector $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}^n$ is called its exponent vector. Given a finite set of exponent vectors $\mathcal{A} \subseteq \mathbb{Z}^n$, one considers the set of polynomials whose only exponent vectors belong to $\mathcal{A}$. These polynomials are said to have support $\mathcal{A}$. A set of supports $\mathcal{A}_\bullet = (\mathcal{A}_1, \ldots, \mathcal{A}_n)$ then determines a family of sparse polynomial systems—those square polynomial systems $F = (f_1, \ldots, f_n)$ where f_i has support $\mathcal{A}_i$. Every square polynomial system can be considered as a sparse polynomial system by considering the monomials that appear in each polynomial. Families of sparse polynomial systems then give a convenient framework for solving a given polynomial system.

Galois groups of sparse polynomial systems. The set of sparse polynomial systems of support $\mathcal{A}_\bullet$ is parameterized by the space P consisting of lists of coefficients of the polynomials comprising these systems. We choose our solution space to be the algebraic torus $S = (\mathbb{C}^\times)^n$, where $\mathbb{C}^\times = \mathbb{C} \setminus \{0\}$ is the set of nonzero complex numbers. Those sparse polynomial systems of support $\mathcal{A}_\bullet$ may then be viewed as an enumerative problem with incidence variety Γ and a branched cover $\pi : \Gamma \to P$ as described above. The Galois group of the family of sparse polynomial systems of support $\mathcal{A}_\bullet$, or briefly, the Galois group associated to $\mathcal{A}_\bullet$, is the Galois group of this branched cover.

Esterov determined two combinatorial conditions on the set of supports $\mathcal{A}_\bullet$ for which its associated Galois group acts imprimitively and restricts it from being the symmetric group. We say the set of supports is lacunary or triangular if it satisfies these conditions respectively. Esterov was able to show that when the set of supports is neither lacunary nor triangular, the associated Galois group is the symmetric group [9]. If a set of supports is lacunary or triangular, Esterov's work shows the corresponding Galois group is a subgroup of an iterated wreath product. In many examples, the Galois group is strictly contained in this wreath product. In this case, the Galois group is not generally known but has been determined in some special cases [10].

Solving decomposable sparse polynomial systems. Many polynomial system solvers consider a polynomial system as a sparse polynomial system by considering the monomial structure of the system. While this monomial structure is often taken into account, other geometric structures such as the associated Galois group are not.

When the set of supports $\mathcal{A}_\bullet$ is lacunary or triangular, the branched cover $\pi : \Gamma \to P$ factors as a composition of nontrivial branched covers on a Zariski open set—such a branched cover is said to be decomposable. It is known that decomposability of a branched cover is equivalent to imprimitivity of its Galois group [15]. For sparse systems, this classifies decomposable branched covers as those that come from lacunary or triangular sets of supports, and each branched cover of the factorization cover comes from a simpler set of supports. Every branched cover can be decomposed into a finite composition of branched covers, as this classification gives a stopping criterion for such a decomposition.

The work [1] shows how decompositions may be used to reduce computation through the use of numerical homotopy continuation. Following this methodology, our work *Solving decomposable sparse polynomial systems* [4] describes a recursive algorithm for solving sparse polynomial systems based on recursively decomposing branched covers, solving the system in stages. In each stage of the algorithm, the polynomial systems needed to be solved either involve fewer variables or the polynomials are of smaller degree than the original system.

Software implementing this algorithm was written and its use was detailed in our work *Decomposable sparse polynomial systems* [3]. This implementation exploits the structure of the Galois group associated to a sparse family and outperforms some current software and as such is progress towards the goal of producing new techniques and algorithms for solving polynomial systems.

Fano problems. A Fano problem concerns enumerating r–planes on a variety $X \subseteq \mathbb{P}^n$ when there are finitely many, generalizing the classical problem of lines in $\mathbb{P}^3$ lying on a cubic surface. Jordan defined and studied the Galois group of the problem of lines on a cubic surface in the first treatise on Galois theory, initiating the study of Galois groups of Fano problems.

A variety $X \subseteq \mathbb{P}^n$ is determined by homogeneous polynomials $(f_1, \dots, f_s)$ in $n+1$ variables and of respective degrees $d_\bullet = (d_1, \dots, d_s)$. The space of all such tuples of polynomials is a space P parameterizing a family varieties. A general choice of parameters determines a smooth complete intersection $X \subseteq \mathbb{P}^n$ of codimension s. The space of r–planes in $\mathbb{P}^n$ is called a Grassmanian, and is the solution space S for Fano problems. We wish to describe the set of r–planes from S that lie on the variety determined by a general choice of parameters from P. When there are finitely many such r–planes, we call this a Fano problem.

A Fano problem is summarized by the combinatorial data $(r, n, d_\bullet)$ and we often refer to a Fano problem by this data. Debarre and Manivel precisely determined which data $(r, n, d_\bullet)$ determine a Fano problem [5]. Further, they gave a generically sharp upper bound on the number of solutions using techniques from intersection theory. A list of small Fano problems and their number of solutions is given in Table 1. Note the second row of the table lists the classical problem of lines in $\mathbb{P}^3$ on a cubic surface.

Table 1. Small Fano problems

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

Galois groups of Fano problems. A Fano problem $(r, n, d_\bullet)$ as described above is an enumerative problem determining an incidence variety Γ and branched cover $\pi : \Gamma \to P$. The Galois group of the Fano problem $(r, n, d_\bullet)$ is the Galois group of this branched cover.

Jordan studied the Galois group of lines in $\mathbb{P}^3$ on a cubic surface–the Fano problem $(1, 3, (3))$. He showed that this Galois group must preserve the incidence structure of the lines and so must be a subgroup of the Coxeter group E_6 [13]. Harris was able to show Jordan's inclusion to be an equality, and computed the Galois group for a generalization of this problem.

For $n \geq 4$, Harris studied the problem of lines in $\mathbb{P}^n$ on a hypersurface of degree $2n-3$ and showed that it's Galois group is equal to the symmetric group [11]. By showing these Galois groups are highly transitive, Harris demonstrated it was sufficient to show they contain a simple transposition. This simple transposition was the result of producing a single instance of parameters for which the corresponding fiber contains a unique double point, is otherwise smooth, and of the generic degree counting multiplicity. The local monodromy around such a system generates a simple transposition.

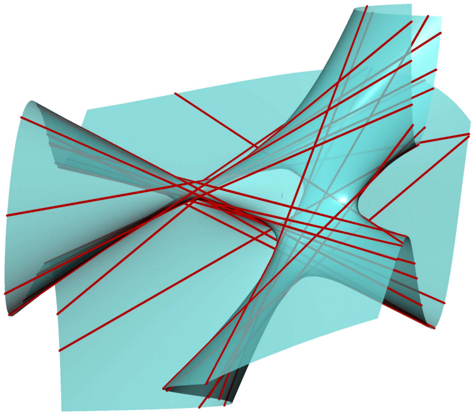

FIGURE 1. 27 lines on a smooth cubic surface

The remaining Fano problems were left untouched for over 40 years until Hashimoto and Kadets showed the problem of r–planes in $\mathbb{P}^{2r+2}$ on the intersection of two quadric hypersurfaces has Galois group equal to the Coxeter group D_{2r+3}. This constrained Galois group is again the result of there being incidences among these r–planes. In addition, Hashimoto and Kadets were able to show that with the exception of the Fano problems of lines on a cubic surface and r–planes on the intersection of two quadric hypersurfaces, the r–planes for a general instance of a Fano problem do not intersect. A consequence of this being that all other Galois groups of Fano problems are highly transitive and contain the alternating group. It is an open problem to classify the remaining Galois groups of Fano problems.

Future Work and Conjectures

Sparse polynomial systems. By Esterov's work, those Galois groups of sparse polynomial systems are unknown only in the case that $\mathcal{A}_\bullet$ is lacunary or triangular. As these are the systems for which the corresponding systems are decomposable, more detailed description of their Galois groups may lead to more specialized algorithms for solving them.

Problem 2. Completely describe the Galois groups of families of sparse polynomial systems when the support $\mathcal{A}_\bullet$ is lacunary or triangular.

Problem 3. Further utilize the Galois groups of families of sparse polynomial systems for solving systems of a given support.

We simplify the first of these problems by restricting the sets of supports we consider. A set of lacunary or triangular supports is simple if $\pi : \Gamma \to P$ factors nontrivially as the composition of exactly two branched covers, $\pi = \mu \circ \phi$.

For a simple set of supports $\mathcal{A}_\bullet$, the associated Galois group is necessarily a subgroup of a wreath product of the form $W = G \wr H$, where G and H are the Galois groups of the factors of the decomposition of π, ϕ and μ respectively. A consequence of Esterov's theorem is that G is either a finite abelian group or a symmetric group depending on whether $\mathcal{A}_\bullet$ is lacunary or triangular respectively, and H is a symmetric group.

By simulating monodromy via numerical path-lifting, one can better understand the Galois group for specific examples. This is the approach taken in [7] to determine whether certain problems in computer vision are decomposable. Collaborating with a group of undergraduate students, data was generated in this way for sparse polynomial systems with simple support $\mathcal{A}_\bullet$. By generating numerous examples and analyzing their Galois groups, a conjecture arose for the set of groups arising as the Galois group associated to a set of simple supports. This conjecture agrees with a recent result of Esterov [10].

Conjecture 4. Let $\mathcal{A}_\bullet$ be a simple set of supports.

1. If $\mathcal{A}_\bullet$ is lacunary, there is a map $\theta : W \to G$ from the expected wreath product $W = G \wr H$ to the finite abelian group G. The Galois group associated to $\mathcal{A}_\bullet$ is the preimage $\theta^{-1}(K)$ for some subgroup $K \subseteq G$.
2. If $\mathcal{A}_\bullet$ is triangular, the Galois group associated to $\mathcal{A}_\bullet$ is either the expected wreath product of symmetric groups $W = G \wr H$ or it is the product of symmetric groups $G \times H$.

Fano problems. A sentiment instituted by Jordan is that Galois groups of enumerative problems should be as large as their structure permits. The results of Hashimoto and Kadets suggests that the Fano problems of lines on a cubic surface or r–planes on the intersection of two quadrics are the only Fano problems with any intrinsic structure. As the remaining Galois groups at least contain the alternating group, we arrive at the following conjecture.

Conjecture 5. Galois groups of Fano problems are symmetric groups, with the exception of the Fano problems of lines on a cubic surface and r–planes on the intersection of two quadric hypersurfaces

Harris' work showing some Galois groups of Fano problems are equal to the symmetric group provides evidence for this. In the work *Computing Galois groups of finite Fano problems*, this project was able to extend Harris' argument to more Fano problems. The idea used to extend Harris' argument is novel, but the process of generating data for these Fano problems can be long and arduous.

Theorem 6. *The Galois group of a Fano problem with less than 75,000 solutions is the symmetric group, with the exception of the Fano problems of lines on a cubic surface and r–planes on the intersection of two quadric hypersurfaces.*

This result proves that 12 Galois groups of specific Fano problems are equal to the symmetric group, each of which were previously unknown. Data for these Fano problems and code verifying these parameters have the desired properties is given at [18]. This result is easily expanded by generating data for larger Fano problems. There are plans to generate this data on a large machine, pushing this result to its limit.

The proof of this result above also suggests a method of proof for the conjecture. In particular, this project proposes to show a general point of the discriminant of the parameter space of a Fano problem has a Fano scheme consisting of a single double point and is otherwise smooth. Similar methods were used by Esterov in his study of Galois groups of sparse polynomial systems.

References

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

[2] P. Breiding, F. Sottile, and J. Woodcock. Euclidean distance degree and mixed volume. *FoCM*, 2021.

[3] T. Brysiewicz, J. I. Rodriguez, F. Sottile, and T. Yahl. Decomposable sparse polynomial systems. *J. Softw. Algebra Geom.*, 11(1):53–59, 2021.

[4] T. Brysiewicz, J. I. Rodriguez, F. Sottile, and T. Yahl. Solving decomposable sparse systems. *Numer. Algorithms*, 88(1):453–474, 2021.

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

[6] T. Duff, C. Hill, A. Jensen, K. Lee, A. Leykin, and J. Sommars. Solving polynomial systems via homotopy continuation and monodromy. *IMA Journal of Numerical Analysis*, 39(3):1421–1446, 2019.

[7] T. Duff, V. Korotynskiy, T. Pajdla, and M. Regan. Galois/monodromy groups for decomposing minimal problems in 3D reconstruction, 2021. `arXiv:2105.04460`.

[8] T. Duff, S. Telen, E. Walker, and T. Yahl. Parameter homotopies in cox coordinates. 2020. `arXiv:2012.04255`.

[9] A. Esterov. Galois theory for general systems of polynomial equations. *Compos. Math.*, 155(2):229–245, 2019.

[10] A. Esterov. Permuting the roots of univariate polynomials whose coefficients depend on parameters. 2022. `arXiv:2204.14235`.

[11] J. Harris. Galois groups of enumerative problems. *Duke Math. Journal*, 46(4):685–724, 1979.

[12] C. Hermite. Sur les fonctions algébriques. *CR Acad. Sci.(Paris)*, 32:458–461, 1851.

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

[14] K. Lee and X. Tang.

[15] G. P. Pirola and E. Schlesinger. Monodromy of projective curves. *J. Algebraic Geom.*, 14(4):623–642, 2005.

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

[17] T. Yahl. Computing galois groups of finite fano problems. 2022. `arXiv:2209.07010`.

[18] T. Yahl. Data and tools for computing galois groups of fano problems, 2022. `https://github.com/tjyahl/FanoGaloisGroups`.

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

Email address: `thomasjyahl@math.tamu.edu`

URL: `https://tjyahl.github.io/`