Computing Galois groups of Fano problems

Thomas Yahl
thomasjyahl@tamu.edu
Texas A&M University

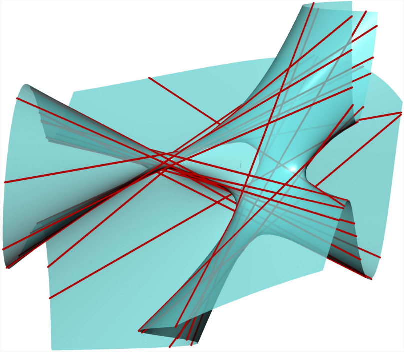
Ohio State University Algebraic Geometry Seminar

September 2022

arXiv:2209.07010

Lines in $\mathbb{P}^3$ on a cubic surface

- Cayley and Salmon showed there are 27 distinct lines that lie on a smooth cubic surface.
- Schläfli determined these lines lie in a "remarkable configuration"



Remark: In the image above, all 27 lines are real!

Fano problems

- The Grassmanian $\mathbb{G}(r, \mathbb{P}^n)$ is the space of r–planes in $\mathbb{P}^n$, a projective variety of dimension $(r+1)(n-r)$.
- The Fano scheme of X is the subscheme of the Grassmanian formed by the r–planes on X.
- Example: The Fano scheme of lines in $\mathbb{P}^3$ on a smooth cubic surface consists of 27 points in $\mathbb{G}(1, \mathbb{P}^3)$.

Fano problems

We consider Fano schemes where $X \subseteq \mathbb{P}^n$ is a complete intersection and classify them by their type.

- If $\operatorname{codim} X = s$, X is defined by homogeneous polynomials $F = (f_1, \ldots, f_s)$ of degrees $d_\bullet = (d_1, \ldots, d_s)$.
- The Fano scheme of r–planes on X has type $(r, n, d_\bullet)$.
- Example: The Fano scheme of lines in $\mathbb{P}^3$ on a cubic surface has type $(1, 3, (3))$.

We study the family of Fano schemes of a given type.

Fano problems

Write $\mathbb{C}^{(r,n,d_\bullet)}$ for the space of homogeneous polynomials $F = (f_1, \ldots, f_s)$ in $n+1$ variables of degrees $d_\bullet = (d_1, \ldots, d_s)$, parameterizing Fano schemes of type $(r, n, d_\bullet)$.

- For $F \in \mathbb{C}^{(r,n,d_\bullet)}$, write $\mathcal{V}_r(F)$ for the Fano scheme of r–planes on the zero set of F.
- A Fano scheme is general if it is determined by a general system $F \in \mathbb{C}^{(r,n,d_\bullet)}$.

Many properties of general Fano schemes are determined entirely by their type.

Fano problems

Note that $\ell \in \mathcal{V}_r(F)$ iff $F|_\ell = 0$. If $\ell \in \mathcal{V}_r(F)$ then..

- $f_i|_\ell = 0$
- $f_i|_\ell$ is a polynomial of degree d_i in r variables (after choosing coordinates).
- all $\binom{d_i+r}{r}$ coefficients vanish.

The <u>expected dimension</u> of a Fano scheme of type $(r, n, d_\bullet)$ is

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

Fano problems

Theorem (Debarre,Manivel)
A general Fano scheme of type $(r, n, d_\bullet)$ *has dimension* $\delta(r, n, d_\bullet)$ *if* $\delta(r, n, d_\bullet) \geq 0$ *and* $2r \leq n - s$*, and is empty otherwise.*

A Fano problem is a tuple $(r, n, d_\bullet)$ such that a general Fano scheme of type $(r, n, d_\bullet)$ is finite.

For a Fano problem $(r, n, d_\bullet)$, the general Fano scheme has a fixed cardinality called the degree of the Fano problem, $\deg(r, n, d_\bullet)$.

Examples

Debarre and Manivel give explicit formulas for this degree via techniques from intersection theory.

All Fano problems with less than 1000 solutions are listed below.

r	n	$d_\bullet$	$\deg(r, n, d_\bullet)$
1	4	$(2, 2)$	16
1	3	(3)	27
2	6	$(2, 2)$	64
3	8	$(2, 2)$	256
1	7	$(2, 2, 2, 2)$	512
1	6	$(2, 2, 3)$	720

Galois groups of Fano problems

There is an incidence correspondence.

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

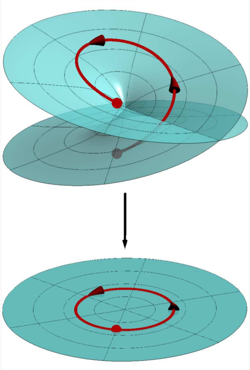
$$\begin{array}{ccc} & \Gamma & \\ {\scriptstyle \pi_{(r,n,d_\bullet)}} \swarrow & & \searrow \\ \mathbb{C}^{(r,n,d_\bullet)} & & \mathbb{G}(r,\mathbb{P}^n) \end{array}$$

- Γ is a smooth, irreducible variety of dimension $\dim \mathbb{C}^{(r,n,d_\bullet)}$.
- For $F \in \mathbb{C}^{(r,n,d_\bullet)}$ the fiber $\pi^{-1}_{(r,n,d_\bullet)}(F)$ is the Fano scheme $\mathcal{V}_r(F)$.
- $\pi_{(r,n,d_\bullet)}$ is a smooth covering space over a Zariski open set U.

Galois groups of Fano problems

The Galois group $\mathcal{G}_{(r,n,d_\bullet)}$, of the Fano problem $(r, n, d_\bullet)$ is the monodromy group of $\pi_{(r,n,d_\bullet)}$.

- The monodromy group of $\pi_{(r,n,d_\bullet)}$ is defined by lifting loops in U based at a fixed point $F \in U$.
- The monodromy group is defined up to isomorphism.



Galois groups of Fano problems

Question: Why are these called Galois groups?

Answer: Jordan first defined them algebraically!

- $\pi_{(r,n,d_\bullet)}$ is dominant and induces a reverse inclusion of function fields.
- $\mathcal{G}_{(r,n,d_\bullet)}$ is isomorphic to the Galois group $\mathrm{Gal}_{\mathbb{C}(\mathbb{C}^{(r,n,d_\bullet)})}(\overline{\mathbb{C}(\Gamma)})$.

$$\Gamma \longrightarrow \mathbb{C}^{(r,n,d_\bullet)}$$

$$\mathbb{C}(\mathbb{C}^{(r,n,d_\bullet)}) \hookrightarrow \mathbb{C}(\Gamma)$$

Equivalence of these definitions was shown by Harris, but the result traces back to Hermite.

Galois groups of Fano problems

A complete classification of Galois groups of Fano problems is close!

- $\mathcal{G}_{(1,3,(3))} = E_6$ [Jordan],[Harris].
- $\mathcal{G}_{(1,n,(2n-3))}$ is the symmetric group for $n \geq 4$ [Harris].
- $\mathcal{G}_{(r,2r+2,(2,2))} = D_{2r+3}$ for $r \geq 1$ [Hashimoto,Kadets].
- If $(r, n, d_\bullet)$ is a Fano problem not equal to $(1, 3, (3))$ or $(r, 2r + 2, (2, 2))$ for $r \geq 1$, then $\mathcal{G}_{(r,n,d_\bullet)}$ contains the alternating group [Hashimoto,Kadets].

Galois groups of Fano problems

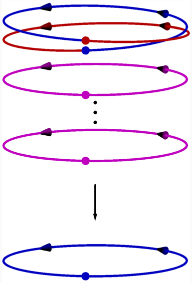
Goal: Prove that for Fano problems not equal to $(1, 3, (3))$ or $(r, 2r + 2, (2, 2))$ for $r \geq 1$, the Galois group is the symmetric group.

Plan: Extend Harris' method of proof by using computational tools.

Using Harris' method

To show $\mathcal{G}_{(1,n,(2n-3))}$ contains a simple transposition, Harris exhibited $F \in \mathbb{C}^{(1,n,(2n-3))}$ such that:

1. $\mathcal{V}_r(F)$ contains a unique double point.
2. $\mathcal{V}_r(F)$ contains $\deg(1,n,(2n-3)) - 2$ smooth points.



More specific plan: Find such systems for other Fano problems using computational tools.

Using Harris' method

We prescribe a subscheme of $\mathcal{V}_r(F)$ to choose $F \in \mathbb{C}^{(r,n,d_\bullet)}$.

- Fix $\ell \in \mathbb{G}(r, \mathbb{P}^n)$ to lie in $\mathcal{V}_r(F)$.
- Fix a tangent vector at $\ell \in \mathcal{V}_r(F)$, $v \in T_\ell \mathcal{V}_r(F)$.

Choose $F \in \mathbb{C}^{(r,n,d_\bullet)}$ general satisfying these conditions.

How do we check Harris' conditions?

Using Harris' method

Choose your favorite coordinates on $\mathbb{G}(r, \mathbb{P}^n)$ to describe $\mathcal{V}_r(F)$ as the zeros of a square polynomial system.

- Use symbolic computation to verify $\ell \in \mathcal{V}_r(F)$ is an isolated point of multiplicity 2.
- Use numerical certification to isolate $\deg(r, n, d_\bullet) - 2$ other points of $\mathcal{V}_r(F)$.

Note: By isolating $\deg(r, n, d_\bullet) - 2$ points of $\mathcal{V}_r(F)$ other than ℓ, the other points are necessarily smooth!

Using Harris' method

A point $x \in \mathbb{C}^m$ is a simple double zero of a square polynomial system G if $G(x) = 0$, $\ker DG(x) = \langle v \rangle$ for $v \neq 0$, and

$$D^2 G(x)(v, v) \notin \operatorname{im} DG(x).$$

By work of Shub, simple double zeros are isolated zeros of multiplicity 2.

Note: We can choose $F \in \mathbb{C}^{(r,n,d_\bullet)}$ (and hence G) to have complex rational coefficients. The above can be checked symbolically.

Using Harris' method

Smale defined quantities $\alpha(G, x)$, $\beta(G, x)$, and $\gamma(G, x)$ to a square system G and a point $x \in \mathbb{C}^m$.

Theorem (Smale et al.)
If G and x are such that

$$\alpha(G, x) < \frac{13 - 3\sqrt{17}}{4},$$

then x converges under iterations of the Newton operator to a solution ξ of G. Further, $||x - \xi|| \leq 2\beta(G, x)$.

- `alphaCertified` will verify these inequalities for you!

Using Harris' method

The Krawczyk operator $K_{G,x,Y}$ acts on the space of complex intervals, given a square system G, $x \in \mathbb{C}^m$, and $Y \in \mathrm{GL}_m(\mathbb{C})$.

Theorem (Krawczyk)
If G, x, Y, and I are such that

$$K_{G,x,Y}(I) \subseteq I,$$

then I contains a zero of G.

- `HomotopyContinuation.jl` can find such complex intervals!

Results

Theorem (Y.)
The Fano problems not equal to $(1, 3, (3))$ or $(r, 2r + 2, (2, 2))$ for $r \geq 1$ and with less than 75,000 solutions have Galois group equal to the symmetric group.

- This determines the Galois group of 12 Fano problems which were previously unknown.

Data and code verifying this result is available at:

`github.com/tjyahl/FanoGaloisGroups`

Results

Timings are reported for verifying the simple double point and certifying the remaining solutions is given below. (`alphaCertified`,`HomotopyContinuation.jl`)

r	n	$d_\bullet$	$\deg(r, n, d_\bullet)$	`alCer` (h)	`HomCo` (s)
1	7	$(2, 2, 2, 2)$	512	2.66	.61
1	6	$(2, 2, 3)$	720	2.88	.87
2	8	$(2, 2, 2)$	1024	27.32	1.57
1	5	(3,3)	1053	2.69	.32
1	5	(2,4)	1280	6.09	.73
1	10	(2,2,2,2,2,2)	20480	-	15.44
1	9	(2,2,2,2,3)	27648	-	25.97
2	10	(2,2,2,2)	32768	-	36.67

Moving forward

There is more to do!

- (In progress) Generate and verify data for larger Fano problems. Current bottlenecks are memory and time!
- Turn this into a proof for ALL Fano problems not equal to $(1, 3, (3))$ or $(r, 2r + 2, (2, 2))$ for $r \geq 1$.
- Explore using numerical certification to prove more about Galois groups and beyond.

Thank you all for your time!

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

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

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

References ii

S. Hashimoto and B. Kadets.
38406501359372282063949 and all that: Monodromy of Fano problems.
International Mathematics Research Notices, 2020.
rnaa275, arxiv:2002.04580.

J. Hauenstein and F. Sottile.
Algorithm 921: alphaCertified: Certifying solutions to polynomial systems.
ACM Trans. Math. Softw., 38(4):28, 2012.

C. Jordan.
Traité des Substitutions et des Équations algébriques.
Gauthier-Villars, Paris, 1870.

[1, 2, 3, 4, 5, 6]

r	n	$d_\bullet$	$\deg(r, n, d_\bullet)$	alCer (h)	HomCo (s)
1	7	$(2, 2, 2, 2)$	512	2.66	.61
1	6	$(2, 2, 3)$	720	2.88	.87
2	8	$(2, 2, 2)$	1024	27.32	1.57
1	5	(3,3)	1053	2.69	.32
1	5	(2,4)	1280	6.09	.73
1	10	(2,2,2,2,2,2)	20480	-	15.44
1	9	(2,2,2,2,3)	27648	-	25.97
2	10	(2,2,2,2)	32768	-	36.67
1	8	(2,2,3,3)	37584	-	38.23
1	8	(2,2,2,4)	47104	-	111.88
1	7	(3,3,3)	51759	-	42.86
1	7	(2,3,4)	64512	-	125.63