## Galois Groups of Purely Lacunary Polynomial Systems

Thomas Yahl tyahl@wisc.edu University of Wisconsin - Madison

Workshop on Computational Geometry, BIRS June 2024

An enumerative problem consists of:

- A parameter space  $\mathcal{P}$ .
- A solution space  $\mathcal{S}$ .
- An incidence space  $\mathcal{I} \subseteq \mathcal{P} \times \mathcal{S}$ .

We will assume each of these spaces are algebraic varieties.

When an enumerative problem has finitely many smooth solutions for general parameters, the projection

$$\mathcal{I} \subseteq \mathcal{P} imes \mathcal{S} \ \pi \downarrow \mathcal{P}$$

restricts to a covering space over a Zariski open set.

The <u>Galois group</u> of an enumerative problem is monodromy group of the projection  $\pi : \mathcal{I} \to \mathcal{P}$ .

 Elements are permutations of a general fiber obtained by lifting based loops.

• By ordering the fiber, the Galois group is a subgroup of the symmetric group.



"Why Galois Groups?"

- The Galois group of an enumerative problem controls the ability to symbolically compute solutions in radicals.
- Partial knowledge of the Galois group can be used to reduce computation.
- Galois groups have been useful for analyzing problems in applications.
- They were objects of interest to Galois, Jordan, Hermite, Harris, and others.

We'll consider Galois groups of sparse polynomial systems.

- ('18) Esterov studied Galois groups of sparse systems to determine which sparse systems were solvable by radicals.
- ('20) Brysiewicz, Rodriguez, Sottile, and Y. wrote software exploiting Galois groups of sparse systems for solving.
- ('22) Brysiewicz and Burr utilized Galois groups of sparse systems in creating a sparse trace test.

Sparse polynomial systems are polynomial systems whose monomial structure has been predetermined.

- A (Laurent) monomial with exponent vector  $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}^n$  is  $x^{\alpha} = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ .
- A (Laurent) polynomial f of support  $\mathcal{A} \subseteq \mathbb{Z}^n$  has the form  $f(x) = \sum_{\alpha \in \mathcal{A}} c_{\alpha} x^{\alpha}, \ c_{\alpha} \in \mathbb{C}.$
- A sparse system of support  $\mathcal{A}_{\bullet} = (\mathcal{A}_1, \dots, \mathcal{A}_n)$  is a system

$$F = (f_1, \ldots, f_n)$$

where  $f_i$  has support  $A_i$  for each  $i = 1, \ldots, n$ .

**Example:** Consider the supports  $\mathcal{B}_{\bullet} = (\mathcal{B}_1, \mathcal{B}_2)$  depicted below.



A system F of support  $\mathcal{B}_{\bullet}$  has the form

$$F(x,y) = \begin{pmatrix} c_1 + c_2 x y^2 + c_3 x^2 y^2 \\ c_4 x + c_5 x y + c_6 y^2 \end{pmatrix}.$$

The number of zeros of a general system of support  $\mathcal{A}_{\bullet}$  is determined by the polyhedral structure of the supports.

The <u>mixed volume</u>  $MV(\mathcal{C}_1, \ldots, \mathcal{C}_n)$  of a set of convex bodies  $\mathcal{C}_1, \ldots, \mathcal{C}_n \subseteq \mathbb{R}^n$  is a measure of the size of the these sets.

• We write  $MV(\mathcal{A}_{\bullet}) = MV(conv(\mathcal{A}_1), \dots, conv(\mathcal{A}_n))$ 

**Theorem (Bernstein, Kushnirenko, Khovanskii)** A sparse polynomial system F of support  $A_{\bullet}$  has at most  $MV(A_{\bullet})$ smooth, isolated zeros in  $(\mathbb{C}^{\times})^n$ , and this bound is attained for a general system of support  $A_{\bullet}$ .

## **Sparse Polynomial Systems**



Thus, for a general choice of coefficients  $c_1, \ldots, c_6 \in \mathbb{C}$ , the system

$$c_1 + c_2 x y^2 + c_3 x^2 y^2 = 0$$
  
$$c_4 x + c_5 x y + c_6 y^2 = 0$$

has 6 smooth, isolated zeros in  $(\mathbb{C}^{\times})^2$ .

Given supports  $\mathcal{A}_{\bullet}$ , we have:

- A parameter space  $\mathcal{P}_{\mathcal{A}_{\bullet}} = \mathbb{C}^{\sum_{i} |\mathcal{A}_{i}|}$ .
- A solution space  $\mathcal{S} = (\mathbb{C}^{\times})^n$ .
- An incidence correspondence

$$\mathcal{I}_{\mathcal{A}_{\bullet}} = \{ (F, x) \in \mathcal{P}_{\mathcal{A}_{\bullet}} \times \mathcal{S} : F(x) = 0 \}$$
$$\begin{array}{c} \pi \downarrow \\ \mathcal{P}_{\mathcal{A}_{\bullet}} \end{array}$$

 By the BKK theorem, π restricts to a MV(A<sub>•</sub>)-sheeted covering space over a Zariski open set.

The <u>Galois group</u>  $\mathcal{G}_{\mathcal{A}_{\bullet}}$  of the family of sparse polynomial systems of support  $\mathcal{A}_{\bullet}$  is the Galois group of this enumerative problem.

Galois groups can be approximated using numerical homotopy continuation software such as NAG4M2, Bertini, and HomotopyContinuation.jl.

**Example:** Consider our running example support  $\mathcal{B}_{\bullet}$ . A system of support  $\mathcal{B}_{\bullet}$  has the form

$$F(x,y) = \begin{pmatrix} c_1 + c_2 x y^2 + c_3 x^2 y^2 \\ c_4 x + c_5 x y + c_6 y^2 \end{pmatrix} = 0.$$

Tracking the zeros of a base system along various loops in  $\mathcal{P}_{\mathcal{B}_{\bullet}}$  yields permutations which generate the symmetric group  $\mathcal{S}_{6}$ .

**Open Problem:** The inverse Galois problem for sparse polynomial systems: what are the groups that appear as the Galois group of a sparse polynomial system?

**Open Problem:** Given a sparse polynomial system, determine its Galois group.

- Esterov determined the supports  $\mathcal{A}_{\bullet}$  for which the Galois group  $\mathcal{G}_{\mathcal{A}_{\bullet}}$  is the symmetric group.
- Esterov's result relies on two special classes of supports.

**Open Problem:** The inverse Galois problem for sparse polynomial systems: what are the groups that appear as the Galois group of a sparse polynomial system?

**Open Problem:** Given a sparse polynomial system, determine its Galois group.

- Esterov determined the supports  $\mathcal{A}_{\bullet}$  for which the Galois group  $\mathcal{G}_{\mathcal{A}_{\bullet}}$  is the symmetric group.
- Esterov's result relies on two special classes of supports.

 $\mathcal{A}_{\bullet}$  is <u>lacunary</u> if every system  $F \in \mathcal{P}_{\mathcal{A}_{\bullet}}$  has been precomposed with a non-invertible surjective monomial map  $\phi : (\mathbb{C}^{\times})^n \to (\mathbb{C}^{\times})^n$ .

• This notion generalizes systems of the form  $f(x^3) = 0$ .

 $\mathcal{A}_{\bullet}$  is <u>triangular</u> if every sparse system F of support  $\mathcal{A}_{\bullet}$  has a proper, nontrivial subsystem.

• This notion generalizes systems of the form f(x, y) = g(y) = 0.

## Theorem (Esterov)

If  $\mathcal{A}_{\bullet}$  is not lacunary and not triangular, then the Galois group  $\mathcal{G}_{\mathcal{A}_{\bullet}}$  is the symmetric group.

The standard argument:

- A small loop around the discriminant lifts to a simple transposition in  $\mathcal{G}_{\mathcal{A}_{\bullet}}$ .
- The Galois group  $\mathcal{G}_{\mathcal{A}_{\bullet}}$  is 2-transitive.

We will examine the Galois group  $\mathcal{G}_{\mathcal{A}_\bullet}$  when  $\mathcal{A}_\bullet$  is lacunary.

## Theorem (Esterov)

If  $\mathcal{A}_{\bullet}$  is not lacunary and not triangular, then the Galois group  $\mathcal{G}_{\mathcal{A}_{\bullet}}$  is the symmetric group.

The standard argument:

- A small loop around the discriminant lifts to a simple transposition in  $\mathcal{G}_{\mathcal{A}_{\bullet}}$ .
- The Galois group  $\mathcal{G}_{\mathcal{A}_{\bullet}}$  is 2-transitive.

We will examine the Galois group  $\mathcal{G}_{\mathcal{A}_{\bullet}}$  when  $\mathcal{A}_{\bullet}$  is lacunary.

If  $\mathcal{A}_{\bullet}$  is lacunary, there is a support  $\mathcal{B}_{\bullet}$  and monomial map  $\phi : (\mathbb{C}^{\times})^n \to (\mathbb{C}^{\times})^n$  such that for every  $F \in \mathcal{P}_{\mathcal{A}_{\bullet}}$ ,

 $F = G \circ \phi$ 

for  $G \in \mathcal{P}_{\mathcal{B}_{\bullet}}$  with the same coefficients.

- The support  $\mathcal{B}_{\bullet}$  is a <u>reduced support</u> for  $\mathcal{A}_{\bullet}$ . (We will always assume  $MV(\mathcal{B}_{\bullet}) > 1$ .)
- The kernel K = ker φ is a finite group which acts on the zeros of F by coordinate-wise multiplication.

## Galois Groups of Sparse Polynomial Systems

Fix a general base system  $F \in \mathcal{P}_{\mathcal{A}_{\bullet}}$ .

• The zeros of F are partitioned into  $\mathcal{K}$ -orbits.



- The number of orbits is equal to m = MV(𝔅) and the size of each orbit is |𝔅|.
- The action of  $\mathcal{G}_{\mathcal{A}_\bullet}$  commutes with the action of  $\mathcal K$  and preserves these orbits.

That is,  $\mathcal{G}_{\mathcal{A}_{\bullet}}$  is imprimitive and the orbits form <u>blocks</u> of imprimitivity.

The wreath product  $\mathcal{K} \wr \mathcal{S}_m$  consists of permutations that permute these blocks and in each block act by an element of  $\mathcal{K}$ .



• The Galois group  $\mathcal{G}_{\mathcal{A}_{\bullet}}$  is a subgroup of the wreath product  $\mathcal{K} \wr \mathcal{S}_m$ .

One may *expect* that the Galois group  $\mathcal{G}_{\mathcal{A}_{\bullet}}$  is equal to the wreath product  $\mathcal{K} \wr \mathcal{S}_m$ , but this is not necessarily the case!

**Example:** Consider the lacunary support  $\mathcal{A}_{\bullet}$ . The support  $\mathcal{B}_{\bullet}$  is a reduced support via the monomial map  $\phi(x, y) = (x^2, y)$ .



- The kernel K = ker φ = {(1,1), (-1,1)} partitions the zeros of a system F ∈ P<sub>A</sub>, into 6 orbits of size 2.
- The Galois group G<sub>A<sub>•</sub></sub> is a proper subgroup of the wreath product K ≥ S<sub>6</sub> of index 2.

The support  $\mathcal{A}_{\bullet}$  is purely lacunary if it is lacunary and not triangular.

Equivalently, A<sub>•</sub> is purely lacunary if there is a reduced support
B<sub>•</sub> where G<sub>B<sub>•</sub></sub> is a symmetric group.

**Example:** The support  $\mathcal{A}_{\bullet}$  below is purely lacunary-our example support  $\mathcal{B}_{\bullet}$  is a reduced support, where  $\mathcal{G}_{\mathcal{B}_{\bullet}} = \mathcal{S}_{6}$ .



For purely lacunary supports  $\mathcal{A}_{\bullet}$ , there is an extension of the standard argument to determine  $\mathcal{G}_{\mathcal{A}_{\bullet}}$ .

- What happens if we lift a small loop around the discriminant?
  - $\circ\,$  A system in the discriminant now has many singular zeros.
  - $\circ~$  Lifting a small loop does  $\underline{not}$  produce a simple transposition.
- What is the analogue of 2-transitivity?
  - $\circ~\mathcal{G}_{\mathcal{A}_{\bullet}}$  is imprimitive and thus  $\underline{not}$  2-transitive.

## Proposition

Let  $\mathcal{A}_{\bullet}$  be purely lacunary with reduced support  $\mathcal{B}_{\bullet}$  such that  $\mathcal{G}_{\mathcal{B}_{\bullet}}$  is a symmetric group. A small loop around the  $(\mathcal{B}_{\bullet}$ -)discriminant lifts to a simple permutation <u>of blocks</u> in  $\mathcal{G}_{\mathcal{A}_{\bullet}}$ .



A general system F ∈ P<sub>A<sub>•</sub></sub> in the (B<sub>•</sub>-)discriminant has |K| singular zeros of multiplicity 2.

An imprimitive group  $\mathcal{G}$  acting on a set S is <u>k-block-transitive</u> if for every  $s_1, \ldots, s_k \in S$  from distinct blocks and  $t_1, \ldots, t_k \in S$  from distinct blocks, there exists  $g \in \mathcal{G}$  such that  $g \cdot s_i = t_i$  for all  $i = 1, \ldots, k$ .



- 1-block-transitivity is equivalent to transitivity.
- 2-block-transitivity is strictly weaker than 2-transitivity.

### Proposition

If  $\mathcal{A}_{\bullet}$  is purely lacunary, then  $\mathcal{G}_{\mathcal{A}_{\bullet}}$  is 2-block-transitive with respect to the blocks induced by its reduced support.

- (Block-)Transitivity properties of G<sub>A<sub>•</sub></sub> are encoded in fiber powers of the projection π : I<sub>A<sub>•</sub></sub> → P<sub>A<sub>•</sub></sub>.
- The result above follows by showing irreducibility of a certain component of the fiber square of the projection  $\pi : \mathcal{I}_{\mathcal{A}_{\bullet}} \to \mathcal{P}_{\mathcal{A}_{\bullet}}$ .

Any element of K ≥ S<sub>m</sub> can be represented in the form
 (k<sub>1</sub>,..., k<sub>m</sub>, σ) ∈ K ≥ S<sub>m</sub> for k<sub>1</sub>,..., k<sub>m</sub> ∈ K and σ ∈ S<sub>m</sub>.

Define the map  $\Sigma : \mathcal{K} \wr \mathcal{S}_m \to \mathcal{K}$  by

$$\Sigma((k_1,\ldots,k_m,\sigma))=\prod_{i=1}^m k_i.$$

#### Proposition

If  $\mathcal{G}$  is an imprimitive group which is 2-block-transitive and contains a simple transposition of blocks, then ker  $\Sigma \subseteq \mathcal{G}$ .

- Do all groups of this form appear as Galois groups of purely lacunary sparse systems?
  - The conjecture is, no.
  - $\circ~$  The condition  $[\mathcal{H}:\mathcal{K}]\mid \mathsf{MV}(\mathcal{B}_{\bullet})$  seems to be necessary.
- Given  $\mathcal{A}_{\bullet}$ , can we determine the subgroup  $\mathcal{H} \subseteq \mathcal{K}$ ?
  - $\circ\,$  Yes, there is a geometric realization of the map  $\Sigma!$
  - $\circ~{\cal H}$  is the group of units that preserve a certain variety.

- Do all groups of this form appear as Galois groups of purely lacunary sparse systems?
  - The conjecture is, no.
  - $\circ~$  The condition  $[\mathcal{H}:\mathcal{K}]\mid \mathsf{MV}(\mathcal{B}_{\bullet})$  seems to be necessary.
- Given  $\mathcal{A}_{\bullet}$ , can we determine the subgroup  $\mathcal{H} \subseteq \mathcal{K}$ ?
  - $\circ~$  Yes, there is a geometric realization of the map  $\Sigma!$
  - $\circ~{\cal H}$  is the group of units that preserve a certain variety.

- Do all groups of this form appear as Galois groups of purely lacunary sparse systems?
  - The conjecture is, no.
  - $\circ~$  The condition  $[\mathcal{H}:\mathcal{K}]\mid \mathsf{MV}(\mathcal{B}_{\bullet})$  seems to be necessary.
- Given  $\mathcal{A}_{\bullet}$ , can we determine the subgroup  $\mathcal{H} \subseteq \mathcal{K}$ ?
  - $\circ~$  Yes, there is a geometric realization of the map  $\Sigma!$
  - $\circ~{\cal H}$  is the group of units that preserve a certain variety.

- Do all groups of this form appear as Galois groups of purely lacunary sparse systems?
  - The conjecture is, no.
  - $\circ~$  The condition  $[\mathcal{H}:\mathcal{K}]\mid \mathsf{MV}(\mathcal{B}_{\bullet})$  seems to be necessary.
- Given  $\mathcal{A}_{\bullet}$ , can we determine the subgroup  $\mathcal{H} \subseteq \mathcal{K}$ ?

• Yes, there is a geometric realization of the map  $\Sigma$ ! •  $\mathcal{H}$  is the group of units that preserve a certain variety

- Do all groups of this form appear as Galois groups of purely lacunary sparse systems?
  - The conjecture is, no.
  - $\circ~$  The condition  $[\mathcal{H}:\mathcal{K}]\mid \mathsf{MV}(\mathcal{B}_{\bullet})$  seems to be necessary.
- Given  $\mathcal{A}_{\bullet}$ , can we determine the subgroup  $\mathcal{H} \subseteq \mathcal{K}$ ?
  - $\circ~$  Yes, there is a geometric realization of the map  $\Sigma!$
  - $\circ~\mathcal{H}$  is the group of units that preserve a certain variety.

Let  $\mathcal{J}_{\mathcal{A}_{\bullet}}$  be any irreducible component of the variety

$$\{(F, x_1, \dots, x_{\mathsf{MV}(\mathcal{A}_{\bullet})}) \in \mathcal{P}_{\mathcal{A}_{\bullet}} \times \mathcal{S}^{\mathsf{MV}(\mathcal{A}_{\bullet})} : F(x_i) = 0 \text{ for } \forall i\}$$

that projects dominantly to  $\mathcal{P}_{\mathcal{A}_{\bullet}}$  and is not contained in the diagonal.

A <u>deck transformation</u> of J<sub>A<sub>●</sub></sub> → P<sub>A<sub>●</sub></sub> is a birational automorphism of J<sub>A<sub>●</sub></sub> fixing the fibers of J<sub>A<sub>●</sub></sub> → P<sub>A<sub>●</sub></sub>.

#### Proposition

The Galois group  $\mathcal{G}_{\mathcal{A}_{\bullet}}$  is equal to the group of deck transformations of  $\mathcal{J}_{\mathcal{A}_{\bullet}} \to \mathcal{P}_{\mathcal{A}_{\bullet}}$ , as groups of permutations of the zeros of a general system  $F \in \mathcal{P}_{\mathcal{A}_{\bullet}}$ .

For each block  $B_1, \ldots, B_m$ , let  $j_i$  be such that the  $j_i$ -th zero of the base system F lies in  $B_i$ .

Consider the map  $\Pi:\mathcal{J}_{\mathcal{A}_\bullet}\to\mathcal{P}_{\mathcal{A}_\bullet}\times\mathcal{S}$  defined by

$$\Pi(F, x_1, \ldots, x_{\mathsf{MV}(\mathcal{A}_{\bullet})}) = \left(F, \prod_{i=1}^m x_{j_i}\right).$$

#### Proposition

The kernel ker  $\Sigma \subseteq \mathcal{G}_{\mathcal{A}_{\bullet}}$  is equal to the subgroup of deck transformations of  $\mathcal{J}_{\mathcal{A}_{\bullet}} \to \text{Im } \Pi$ .

#### Corollary

The Galois group  $\mathcal{G}_{\mathcal{A}_{\bullet}}$  is equal to  $\Sigma^{-1}(\mathcal{H})$  where  $\mathcal{H} \subseteq \mathcal{K}$  is group of deck transformations of Im  $\Pi \to \mathcal{P}_{\mathcal{A}_{\bullet}}$ .

We can write down equations for  $\mbox{Im}\,\Pi!$ 

- Recall given  $F \in \mathcal{P}_{\mathcal{A}_{\bullet}}$ , there is  $G \in \mathcal{P}_{\mathcal{B}_{\bullet}}$  such that  $F = G \circ \phi$ .
- The product of the zeros of G is a rational function in the coefficients of F, p(F).

The variety Im  $\Pi\subseteq \mathcal{P}_{\mathcal{A}_\bullet}\times \mathcal{S}$  is a dominant, irreducible component of the variety defined by

$$\phi(x)-p(F)=0.$$

## **E**xamples

**Example:** Consider the set of supports  $\mathcal{A}_{\bullet}$  obtained by scaling the first coordinate of our example supports  $\mathcal{B}_{\bullet}$ . The coefficients of each monomial appears next to the corresponding point below.



The variety Im  $\Pi$  is an irreducible component of the variety defined by

$$c_3^2 c_5^2 x^2 - c_1^2 c_4^2 = 0$$
  
$$c_3 c_4^2 y - c_1 c_5^2 = 0.$$

**Example:** This variety has two components that map dominantly to  $\mathcal{P}_{\mathcal{A}_{\bullet}}$ , defined by the systems below.

$$c_{3}c_{5}x - c_{1}c_{4} = 0 \qquad c_{3}c_{5}x + c_{1}c_{4} = 0$$
  
$$c_{3}c_{4}^{2}y - c_{1}c_{5}^{2} = 0 \qquad c_{3}c_{4}^{2}y - c_{1}c_{5}^{2} = 0$$

Both varieties have trivial group of deck transformations so that  $\mathcal{G}_{\mathcal{A}_{\bullet}} = \Sigma^{-1}(\{e\}) = \ker \Sigma$ , which has index 2 in the expected wreath product.

## **E**xamples

The variety  $\text{Im }\Pi$  is the only dominant, irreducible component of the variety defined by

$$c_3^2 c_5^2 x^3 - c_1^2 c_4^2 = 0$$
  
$$c_3 c_4^2 y - c_1 c_5^2 = 0,$$

and  $\mathcal{K} = \{(1, 1), (\omega, 1), (\omega^2, 1)\}$  acts on it. Thus,  $\mathcal{G}_{\mathcal{A}_{\bullet}}$  is the expected wreath product.

- Can this structure be exploited to reduce computation?
- Is there a conjecture for the "purely triangular" case?
- Is there any hope to determine the Galois group for systems which are both lacunary and triangular?

# Thank you for your attention!

Other Events:

- Macaulay2 Workshop Madison 2025. June 30-July 4, 2025.
- SIAM-AG 2025 Madison. June 7-11, 2025.