Galois Groups, Decomposable Branched Covers, and Applications to Sparse Polynomial Systems

Thomas Yahl
thomasjyahl@math.tamu.edu

Texas A&M University

October 2019

Joint with Taylor Brysiewicz, Jose Rodriguez, and Frank Sottile

Decomposable Branched Covers

A branched cover is a dominant map of complex irreducible varieties of the same dimension $\pi : X \to Y$ that restricts to a covering space $\pi : \pi^{-1}(U) \to U$ for an open set $U \subseteq Y$.

Example: The map $\pi : \mathbb{C} \to \mathbb{C}$ defined by $\pi(z) = z^3$ is a branched cover. It restricts to a covering space $\pi : \mathbb{C}^\times \to \mathbb{C}^\times$.

A branched cover $\pi : X \to Y$ is decomposable if the corresponding covering space $\pi : \pi^{-1}(U) \to U$ factors as a composition of two nontrivial covering spaces.

$$\pi : \pi^{-1}(U) \to Z \to U$$

Goal: Decompose branched covers as much as possible to compute fibres.

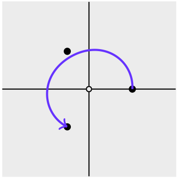
Galois Groups of Branched Covers

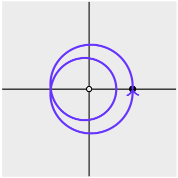
The Galois group of a branched cover $\pi : X \to Y$ is the monodromy group of (any of) its respective covering space(s).

The Galois group of a branched cover acts on the fibres of the covering space by the monodromy action.

Example: The Galois group of the previous example, $\pi : \mathbb{C} \to \mathbb{C}$ is $\mathbb{Z}/3\mathbb{Z}$.

$$\pi : \quad \mathbb{C} \longrightarrow \mathbb{C}$$

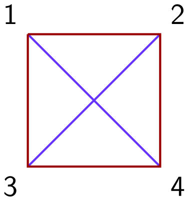




Imprimitive Groups

A group G acting on a set S is imprimitive if there is a nontrivial partition of S that is preserved by the action of G.

Example: Let $G = D_4$ be the symmetry group of the square acting on the vertices. The diagonals are preserved, so the partition $\{1,4\},\{2,3\}$ is preserved.



Proposition: The Galois group of a branched cover acts imprimitively on fibres if and only if the branched cover is decomposable.

Applications to Sparse Polynomial Systems

A (Laurent) monomial is an expression of the form $x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ for $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}^n$.

A finite set $A \subseteq \mathbb{Z}^n$ determines a family of sparse polynomials $f = \sum_{\alpha \in A} c_\alpha x^\alpha$ which is denoted $\mathbb{C}^A$.

A tuple of finite sets $A_\bullet = (A_1, \ldots, A_n)$ determines a family of sparse polynomial systems $F = (f_1, \ldots, f_n) \in \mathbb{C}^{A_1} \times \cdots \mathbb{C}^{A_n}$ denoted by $\mathbb{C}^{A_\bullet}$.

Theorem: (Bernstein-Kushnirenko) The number of solutions in $(\mathbb{C}^\times)^n$ of a generic polynomial system in $\mathbb{C}^{A_\bullet}$ is given by the mixed volume $\mathrm{MV}(\mathrm{conv}(A_1), \ldots, \mathrm{conv}(A_n))$.

Applications to Sparse Polynomial Systems

The incidence variety of the family of equations $\mathbb{C}^{A_\bullet}$ is the variety

$$X_{A_\bullet} = \{(F, x) \in \mathbb{C}^{A_\bullet} \times (\mathbb{C}^\times)^n : F(x) = 0\}.$$

The Bernstein-Kushnirenko theorem shows the projection $\pi : X_{A_\bullet} \to \mathbb{C}^{A_\bullet}$ is a branched cover and tells us the degree!

The solutions to a system $F \in \mathbb{C}^{A_\bullet}$ can be identified with the fibre $\pi^{-1}(F)$. Decompose to compute fibres!

There are two instances when this branched cover naturally decomposes:

(1) The family of equations is Lacunary. Example: $f(x^2) = 0$.

(2) The family of equations is Triangular. Example: $f(x, y) = g(y) = 0$.

Theorem: (Esterov) The Galois group of the branched cover is imprimitive only if either (1) or (2) holds. Otherwise the Galois group is symmetric.

Recursive Algorithm for Solving

Given a polynomial system $F \in \mathbb{C}^{A_\bullet}$ ...

(1) If the family of equations is lacunary:
   a. Change coordinates so that the system has the form $\widetilde{F} \circ \Phi$.
   b. Recursively compute solutions $y_1, \ldots, y_m$ to $\widetilde{F}$.
   c. Solve the binomial equations $\Phi(x) = y_i$.

(2) If the family of equations is triangular:
   a. Change coordinates so that the system contains a square subsystem $\widetilde{F}$ in $x_1, \ldots, x_k$.
   b. Recursively compute solutions $y_1, \ldots, y_m$ to $\widetilde{F}$.
   c. Compute solutions $(x_{k+1}, \ldots, x_n)$ to $F(y_i, x_{k+1}, \ldots, x_n)$ and piece together solutions to F.

(3) If the family of equations is neither lacunary nor triangular:
   a. Just use your other favorite solver!