Solving decomposable sparse polynomial systems

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

Joint with Taylor Brysiewicz, Jose Rodriguez, and Frank Sottile.

Georgia Tech Algebra Seminar

September 2022

Introduction

We'd like to solve polynomial systems more efficiently.

- Every polynomial system may be considered as a "sparse polynomial system".
- Families of systems give rise to geometry.
- We exploit geometry for solving.

Sparse polynomial systems

A vector $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}^n$ is the exponent vector of the (Laurent) monomial

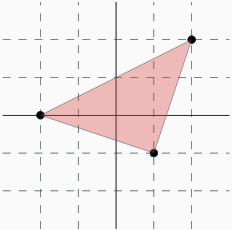
$$x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}.$$

A set $\mathcal{A} \subseteq \mathbb{Z}^n$ is the support of a polynomial f if the exponent vector of every term of f lies in $\mathcal{A}$.

Example: Let $\mathcal{A} \subseteq \mathbb{Z}^2$ be the point set $\longrightarrow$

A polynomial of support $\mathcal{A}$ has the form

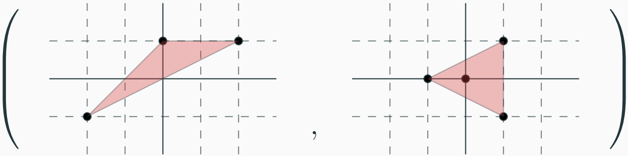
$$f = c_{(2,2)}x^2y^2 + c_{(1,-1)}xy^{-1} + c_{(-2,0)}x^{-2}.$$



Sparse polynomial systems

The set of sparse polynomial systems of support $\mathcal{A}_\bullet = (\mathcal{A}_1, \ldots, \mathcal{A}_n)$ (with $\mathcal{A}_i \subseteq \mathbb{Z}^n$) consists of systems $F = (f_1, \ldots, f_n)$ where f_i has support $\mathcal{A}_i$.

Example: Let $\mathcal{A}_\bullet = (\mathcal{A}_1, \mathcal{A}_2)$ be the set of supports below.



A sparse polynomial system of support $\mathcal{A}_\bullet$ has the form

$$F = \begin{pmatrix} c_{(2,1)}x^2y + c_{(0,1)}y + c_{(-2,-1)}x^{-2}y^{-1} \\ c_{(1,1)}xy + c_{(1,-1)}xy^{-1} + c_{(-1,0)}x^{-1} + c_{(0,0)} \end{pmatrix}.$$

Sparse polynomial systems

Write $\mathbb{C}^{\mathcal{A}_\bullet}$ for the space of sparse polynomial systems of support $\mathcal{A}_\bullet$.

- We care about solutions in the algebraic torus $(\mathbb{C}^\times)^n$.
- The zero set of $F \in \mathbb{C}^{\mathcal{A}_\bullet}$ is $\mathcal{V}(F) = \{x \in (\mathbb{C}^\times)^n : F(x) = 0\}$.

Goal: We want to compute numerical solutions to sparse polynomial systems (using some geometric structure).

Question: What is the number of solutions to a general system of support $\mathcal{A}_\bullet$?

Sparse polynomial systems

- For a subset $S \subseteq \mathbb{R}^n$, let $\mathrm{conv}(S)$ denote the convex hull.
- The mixed volume of convex bodies $C_1, \ldots, C_n \subseteq \mathbb{R}^n$ is the coefficient of $t_1 \cdots t_n$ in

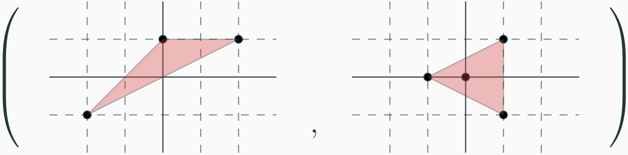
$$\mathrm{Vol}(t_1 C_1 + \cdots + t_n C_n).$$

- Write $\mathrm{MV}(\mathcal{A}_\bullet)$ for the mixed volume of the convex bodies $\mathrm{conv}(\mathcal{A}_1), \ldots, \mathrm{conv}(\mathcal{A}_n)$.

Theorem (Bernstein)
There are at most $MV(\mathcal{A}_\bullet)$ many isolated zeros of a system $F \in \mathbb{C}^{\mathcal{A}_\bullet}$. There is a Zariski open set of $\mathbb{C}^{\mathcal{A}_\bullet}$ where this bound is attained.

Sparse polynomial systems

Example: Recall the supports $\mathcal{A}_\bullet$ from before.



A sparse polynomial system of support $\mathcal{A}_\bullet$ has the form

$$F = \begin{pmatrix} c_{(2,1)}x^2y + c_{(0,1)}y + c_{(-2,-1)}x^{-2}y^{-1} \\ c_{(1,1)}xy + c_{(1,-1)}xy^{-1} + c_{(-1,0)}x^{-1} + c_{(0,0)} \end{pmatrix}.$$

`Macaulay2` helps to show that $\mathrm{MV}(\mathcal{A}_\bullet) = 10$.

Sparse polynomial systems

There is an incidence correspondence:

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

$$\begin{array}{ccc} & \Gamma & \\ {\scriptstyle \pi_{\mathcal{A}_\bullet}} \swarrow & & \searrow \\ \mathbb{C}^{\mathcal{A}_\bullet} & & (\mathbb{C}^\times)^n \end{array}$$

- Γ is a smooth, irreducible variety of dimension $\mathbb{C}^{\mathcal{A}_\bullet}$.
- The fiber $\pi_{\mathcal{A}_\bullet}^{-1}(F)$ is the zero set $\mathcal{V}(F)$.
- Over a Zariski open set, $\pi_{\mathcal{A}_\bullet}$ restricts to a smooth $\mathrm{MV}(\mathcal{A}_\bullet)$-to-1 covering space.

Such a map is a branched cover.

Decomposable branched covers

A branched cover $\pi : \Gamma \to P$ is decomposable if it factors through nontrivial branched covers over a Zariski open set,

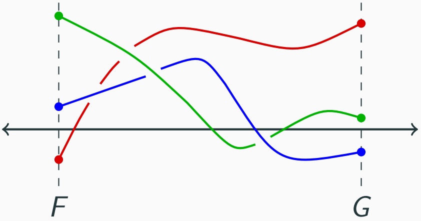
$$\pi : \Gamma \xrightarrow{\mu} \Lambda \xrightarrow{\phi} P.$$

- Fibers can be computed "in stages".
- Can be exploited by homotopy methods.

How do we exploit this structure?

Obligatory homotopy continuation slide

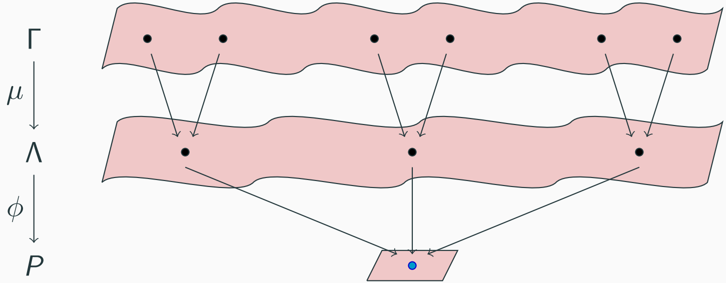
Uses numerical methods to “track” solutions from a “start system” F to a “target system” G.



- Allows us to numerically compute fibers, given a general fiber.

Decomposable branched covers

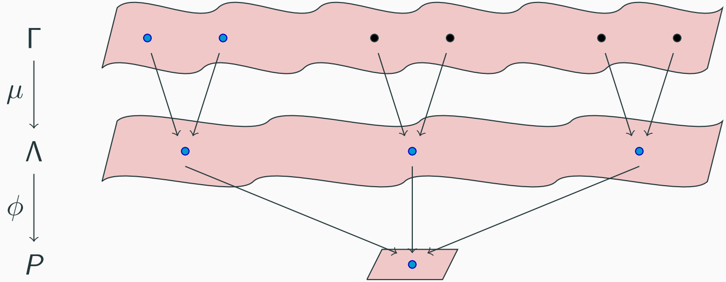
We exploit decomposability by computing only a partial fiber.



We use homotopy methods!

Decomposable branched covers

We exploit decomposability by computing only a partial fiber.

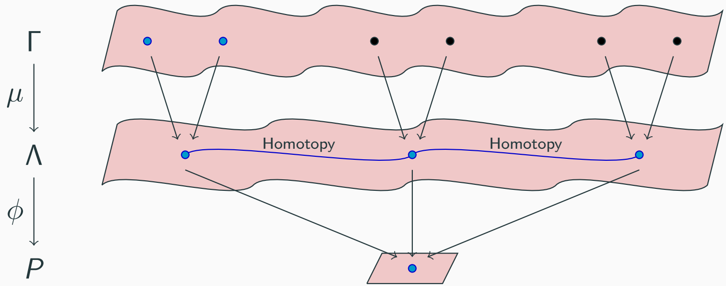


Other points of the fiber are recovered using homotopy continuation!

Now how to detect decomposability?

Decomposable branched covers

We exploit decomposability by computing only a partial fiber.



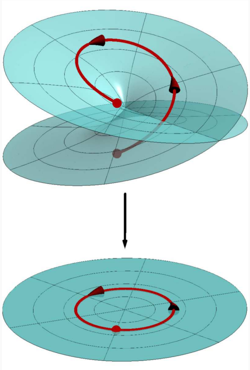
Other points of the fiber are recovered using homotopy continuation!

Now how to detect decomposability?

Decomposable branched covers

Let $\pi : \Gamma \to P$ be a branched cover.

- π has a well-defined monodromy group, defined by lifting based loops.
- The monodromy group is defined up to isomorphism.



Definition

The Galois group $\mathcal{G}_\pi$ of a branched cover $\pi : \Gamma \to P$ is its monodromy group.

Decomposable branched covers

Question: Why are these called Galois groups?

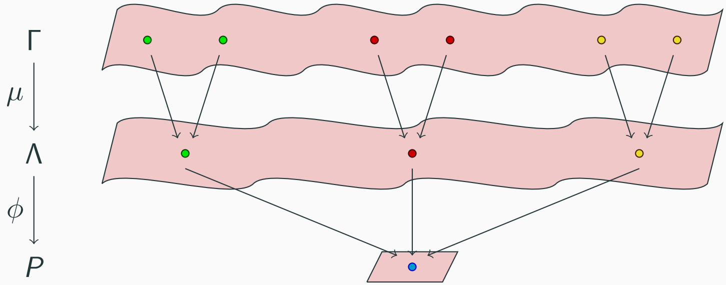
Answer: Jordan first defined them algebraically!

- A branched cover $\pi : \Gamma \to P$ induces a reverse inclusion of function fields.
- $\mathcal{G}_\pi$ is isomorphic to the Galois group $\mathrm{Gal}_{\mathbb{C}(P)}(\overline{\mathbb{C}(\Gamma)})$.

$$\begin{array}{ccc} \Gamma & \qquad & \mathbb{C}(\Gamma) \\ \downarrow & & \uparrow \\ P & & \mathbb{C}(P) \end{array}$$

Decomposable branched covers

Galois groups of decomposable branched covers are imprimitive.



If the monodromy group is based at $F \in P$, invariant blocks are given by fibers $\mu^{-1}(G)$ for $G \in \phi^{-1}(F)$.

Decomposable branched covers

Theorem (Pirola,Schlesinger)

A branched cover $\pi : \Gamma \to P$ is decomposable if and only if its Galois group $\mathcal{G}_\pi$ is imprimitive.

- We use this to detect decomposability!

How does this fit into the scope of sparse polynomial systems?

Galois groups of sparse polynomial systems

Let $\mathcal{G}_{\mathcal{A}_\bullet}$ be the Galois group of the branched cover $\pi_{\mathcal{A}_\bullet} : \Gamma \to \mathbb{C}^{\mathcal{A}_\bullet}$ corresponding to the set of supports $\mathcal{A}_\bullet$.

Esterov found 2 conditions for which $\mathcal{A}_\bullet$ is decomposable. Such $\mathcal{A}_\bullet$ and systems of support $\mathcal{A}_\bullet$ are called..

- Lacunary: similar to $f(x^3) = 0$.
- Triangular: similar to $f(x, y) = g(y) = 0$.

Galois groups of sparse polynomial systems

Given a subset $I \subseteq \{1, \ldots, n\}$, let

$$\mathbb{Z}\mathcal{A}_I = \{\alpha - \beta : \alpha, \beta \in \mathcal{A}_i \text{ for } i \in I\} \subseteq \mathbb{Z}^n$$

be the affine span of the set of supports.

Definition

The support $\mathcal{A}_\bullet$ is lacunary if $\mathbb{Z}\mathcal{A}_\bullet$ is a proper subgroup of full rank.

Example: Consider the sparse polynomials of support $\mathcal{A} = \{0, 2, 4\}$.

Those polynomials have the form $f = c_0 + c_2 x^2 + c_4 x^4$.

Galois groups of sparse polynomial systems

If $\mathcal{A}_\bullet$ is lacunary, there is a (monomial) change of coordinates such that every $F \in \mathbb{C}^{\mathcal{A}_\bullet}$ has the form

$$F(x_1, \ldots, x_n) = G(x_1^{\alpha_1}, \ldots, x_n^{\alpha_n}).$$

The system G is called the reduced system of F.

To solve lacunary systems, one..

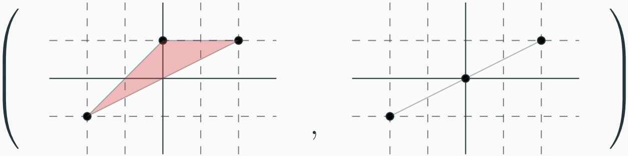
(0. Applies a monomial change of coordinates.)

1. Solve the reduced system G.
2. Extracts roots to obtain zeros of F.

Definition

The support $\mathcal{A}_\bullet$ is triangular if there is a nonempty proper subset $I \subseteq \{1, \ldots, n\}$ such that $\operatorname{rank} \mathbb{Z}\mathcal{A}_I = |I|$.

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



The subset $I = \{2\}$ shows this support is triangular. The second polynomial has the form

$$f_2 = c_{(2,1)}x^2y + c_{(0,0)} + c_{(-2,-1)}x^{-2}y^{-1}.$$

Galois groups of sparse polynomial systems

If $\mathcal{A}_\bullet$ is triangular, there is a (monomial) change of coordinates such that every $F \in \mathbb{C}^{\mathcal{A}_\bullet}$ has the form

$$F(x_1, \ldots, x_n) = (G(x_1, \ldots, x_k), H(x_1, \ldots, x_n)).$$

The system G is called a subsystem of F.

To solve triangular systems, one..

(0. Applies a monomial change of coordinates.)

1. Solve the subsystem G.
2. Subsitute a zero of G into H and solve the residual system.
3. Apply homotopy techniques to compute remaining solutions.

Galois groups of sparse polynomial systems

Theorem (Esterov)
If $\mathcal{A}_\bullet$ is lacunary or triangular, the Galois group $\mathcal{G}_{\mathcal{A}_\bullet}$ is imprimitive. Otherwise, $\mathcal{G}_{\mathcal{A}_\bullet}$ is the symmetric group.

- As a result, we understand which sparse polynomial systems are decomposable!
- The theorem above does not determine the Galois group when $\mathcal{A}_\bullet$ is lacunary or triangular. This is an open problem!

Solving sparse polynomial systems

We can take this one step further! Let $F \in \mathbb{C}^{\mathcal{A}_\bullet}$.

- If $\mathcal{A}_\bullet$ is lacunary, the reduced system G may be decomposable!
- If $\mathcal{A}_\bullet$ is triangular, the subsystem G and the residual system may be decomposable!

This leads to a recursive algorithm for solving sparse polynomial systems.

Solving sparse polynomial systems

`solveDecomposableSystem`

`Input:`

- General sparse system: $F \in \mathbb{C}^{\mathcal{A}_\bullet}$
- A blackbox solver: `solver`

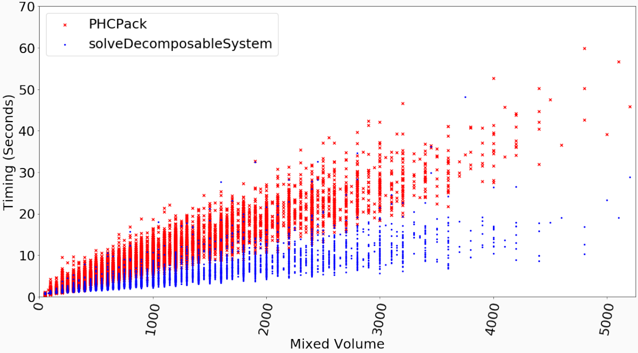
---

1. If $\mathcal{A}_\bullet$ is lacunary
   a. Use `solveDecomposableSystem` on the reduced system
   b. Extract roots
2. If $\mathcal{A}_\bullet$ is triangular
   a. Use `solveDecomposableSystem` on the subsystem
   b. Use `solveDecomposableSystem` on the residual system
   c. Use homotopy methods to recover all zeros
3. Else, use `solver` on F.

Solving sparse polynomial systems

Result: It works! And well!

We implemented and tested the method above against our choice of blackbox solver `PHCPack`. The generated systems of 5 polynomials were lacunary with 2 subsystems and varying numbers of solutions.



Solving sparse polynomial systems

We use decomposability for reducing computation in solving sparse polynomial systems. There is room for improvement!

- Decomposability corresponds to imprimitivity in the Galois group. How else can we use the Galois group?
- The Galois group isn't known in the case that $\mathcal{A}_\bullet$ is lacunary or triangular! There may be more to this story.
- How to use decomposability for other classes of systems?

Thank you all for your time!

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

D. N. Bernstein.
The number of roots of a system of equations.
Funkcional. Anal. i Priložen., 9(3):1–4, 1975.

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

References ii

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

A. P. Morgan.
Solving polynomial systems using continuation for engineering and scientific problems.
Prentice Hall, Inc., Englewood Cliffs, NJ, 1987.

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

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

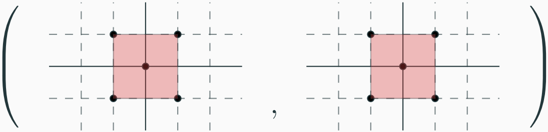
Solving sparse polynomial systems

If $\pi : \Gamma \xrightarrow{\mu} \Lambda \xrightarrow{\phi} P$ is a branched cover and $\mathcal{G}_\phi \subseteq S_d$, $\mathcal{G}_\pi$ is contained in the wreath product

$$\mathcal{G}_\mu \wr \mathcal{G}_\phi = (\mathcal{G}_\mu)^d \rtimes \mathcal{G}_\phi.$$

$\mathcal{G}_\pi$ may be a proper subgroup of this wreath product.

Example: Let $\mathcal{A}_\bullet = (\mathcal{A}_1, \mathcal{A}_2)$ be the set of supports below.



The expected wreath product is $\mathbb{Z}/2\mathbb{Z} \wr S_4$, but the Galois group is $\mathcal{G}_{\mathcal{A}_\bullet} = (\mathbb{Z}/2\mathbb{Z} \wr S_4) \cap A_8$.

Solving sparse polynomial systems

We say $\mathcal{A}_\bullet$ is simple if $\pi_{\mathcal{A}_\bullet}$ factors into nontrivial branched covers $\pi_{\mathcal{A}_\bullet} = \mu \circ \phi$ where neither μ nor ϕ is decomposable.

Conjecture
Assume $\mathcal{A}_\bullet$ is simple.

- If $\mathcal{A}_\bullet$ is lacunary, $\mathcal{G}_{\mathcal{A}_\bullet} \subseteq T \wr S_d = T^d \rtimes S_d$ where $T \simeq \mathbb{Z}^n/\mathbb{Z}\mathcal{A}_\bullet$ is a finite abelian group. There is a map $\theta : T \wr S_d \to T$ and $\mathcal{G}_{\mathcal{A}_\bullet} \simeq \theta^{-1}(H)$ for some subgroup $H \subseteq T$.
- If $\mathcal{A}_\bullet$ is triangular, $\mathcal{G}_{\mathcal{A}_\bullet} \subseteq S_k \wr S_d$ and either $\mathcal{G}_{\mathcal{A}_\bullet} = S_k \wr S_d$ or $\mathcal{G}_{\mathcal{A}_\bullet} = S_k \times S_d$.