SOLVING DECOMPOSABLE SPARSE SYSTEMS

TAYLOR BRYSIEWICZ, JOSE ISRAEL RODRIGUEZ, FRANK SOTTILE, AND THOMAS YAHL

ABSTRACT. Améndola et al. proposed a method for solving systems of polynomial equations lying in a family which exploits a recursive decomposition into smaller systems. A family of systems admits such a decomposition if and only if the corresponding Galois group is imprimitive. When the Galois group is imprimitive we consider the problem of computing an explicit decomposition. A consequence of Esterov's classification of sparse polynomial systems with imprimitive Galois groups is that this decomposition is obtained by inspection. This leads to a recursive algorithm to compute complex isolated solutions to decomposable sparse systems, which we present and give evidence for its efficiency.

INTRODUCTION

The Galois group of a univariate polynomial exposes its internal symmetry and controls its solvability by radicals. More generally, families of polynomial systems (and of geometric problems) have Galois groups [12] which expose their internal symmetry. We describe how to solve a polynomial system using numerical homotopy continuation [20, 25] by exploiting the structure of a family to which it belongs.

A family of polynomial systems (geometric problems) is represented as a branched cover of algebraic varieties $\pi\colon X \to Z$ where Z parameterizes the family and the fiber over $z \in Z$ consists of complex solutions to the corresponding instance. Removing the branch locus gives a covering space whose monodromy group is a Galois group [12] of a field extension. Pirola and Schlesinger [23] observed that the Galois group acts imprimitively if and only if after replacing Z by a Zariski open subset V, the branched cover factors as a composition

$$\pi^{-1}(V) \; \longrightarrow \; Y \; \longrightarrow \; V \tag{1}$$

of nontrivial branched covers, in which case π is decomposable.

Améndola et al. [1] explained how to use an explicit decomposition to compute fibers $\pi^{-1}(z)$ using monodromy [7]. They showed how several examples in the literature involve a decomposable branched cover. In particular, Robert's cognates in kinematics and label swapping in algebraic statistics are used to illustrate the utility of decomposability. Examples like these span several disciplines and serve as a primary motivation for our study. For these examples, the variety Y and intermediate maps were determined using invariant theory as there was a finite group acting as automorphisms of $\pi\colon X \to Z$. In general, it is nontrivial to determine a decomposition (1) of a branched cover $\pi\colon X \to Z$ with imprimitive Galois group, especially when the cover admits only the trivial automorphism.

Esterov [8] determined which systems of sparse polynomials have an imprimitive Galois group. One goal was to classify those which are solvable by radicals. He identified two simple structures which imply that the system is decomposable. In these cases, the decomposition is transparent. He also showed that the Galois group is full symmetric when neither structure occurs. We use Esterov's classification to give a recursive numerical homotopy continuation algorithm for solving decomposable sparse systems.

The first such structure is when a polynomial system is composed with a monomial map, such as $g(x^3) = 0$. To solve this, first solve $g(y) = 0$ and then extract third roots of each solution. The second structure is when the system is triangular, such as

$$f(x, y) \ = \ g(y) \ = \ 0 \,.$$

To solve this, first solve $g(y) = 0$ and then for each solution y^*, solve $f(x, y^*) = 0$. The goal of the paper is to recognize and exploit these structures for solving polynomial systems, where by *solve*, we mean, "Find all isolated solutions over the complex numbers with nonzero coordinates."

In general, Esterov's classification leads to a sequence of branched covers, each corresponding to a sparse system with symmetric monodromy or to a monomial map. Our algorithm identifies this structure and uses it to recursively solve a decomposable system. We give some examples which demonstrate that, despite its overhead, this algorithm is a significant improvement over a direct use of the polyhedral homotopy [15, 28].

Throughout this paper we assume each polynomial of a system is prescribed by a finite sum of terms, which consist of a monomial multiplied by a coefficient. We use the terminology *sparse polynomial system* when the monomials of each finite sum are known. A polynomial system presented as a straight-line program would not be considered sparse, although it could theoretically be translated into one. We develop algorithms for solving sparse polynomial systems, which is in comparison to the monodromy methods proposed in [1] where there is no sparsity requirement. Sparsity is important for us because we use the monomial support to identify triangular and lacunary structure.

We say *general sparse polynomial system*, when the coefficients appearing in the sparse system are general. By the Bernstein-Kushnirenko Theorem [3, 17], the number of complex isolated solutions to a general sparse system of equations depends only on the convex hulls of the exponent vectors of the monomials. When the system supported on the vertices is decomposable, we propose using it as a start system in a homotopy to solve the original system. This is similar in spirit to the Bézout or total degree homotopy [10].

In Section 1 we present some general background on Galois groups of branched covers and explain the relation between decompositions of the branched cover and imprimitivity of the Galois group, finishing with a discussion of how to obtain an explicit decomposition. We specialize to decomposable sparse systems in Section 2, where we explain Esterov's classification and describe how to compute the corresponding decompositions. We present our algorithms for solving sparse decomposable systems in Section 3, and give an application to furnish start systems for homotopies. Section 4 gives timings and information on the performance of our algorithm.

1. Branched covers, Galois groups, and decomposable projections

We sketch some mathematical background, first explaining how Galois groups arise from branched covers and the relationship between imprimitive Galois groups and decompositions of the branched cover. We then discuss how to compute a decomposition when the Galois group is imprimitive.

1.1. **Galois groups.** Let $\pi\colon X \to Z$ be a dominant map ($\pi(X)$ is dense in Z) of irreducible complex algebraic varieties of the same dimension. Such a map is a *branched cover*. There exists a number d and a nonempty Zariski open (in particular, dense, open, and path-connected) subset $U \subset Z$ such that for each $z \in U$, $\pi^{-1}(z)$ consists of d points. The branched cover is *trivial* when $d = 1$. We define two subgroups of the symmetric group S_d which are well-defined up to conjugacy.

We may further assume that the map $\pi^{-1}(U) \to U$ is a degree d covering space. This covering space has a monodromy group which acts on a fiber $\pi^{-1}(z)$ for $z \in U$ as follows [22, Ch. 13]. Given a loop γ in U based at z, the lifts of γ give d paths in X connecting points of $\pi^{-1}(z)$, and thus a permutation of $\pi^{-1}(z)$. The collection of all such monodromy permutations forms the *monodromy group* of π, which acts transitively because $\pi^{-1}(U)$ is connected as X is irreducible.

Second, as $\pi\colon X \to Z$ is dominant, the field $\mathbb{C}(Z)$ of rational functions on Z is a subfield of $\mathbb{C}(X)$, the field of rational functions on X. Since π has degree d, $\mathbb{C}(X)$ is a degree d extension of $\mathbb{C}(Z)$. If K is the Galois closure of $\mathbb{C}(X)/\mathbb{C}(Z)$, then the *Galois group G_π* of the branched cover $\pi\colon X \to Z$ is the Galois group of $K/\mathbb{C}(Z)$. Harris [12] gave a modern proof that the Galois group equals the monodromy group, but this idea goes back at least to Hermite [14].

We recall some terminology concerning permutation groups [29]. Suppose that $G \subset S_d$ is a permutation group acting transitively on the set $[d] := \{1, 2, \ldots, d\}$. A *block* of G is a subset $B \subset [d]$ such that for every $g \in G$, either $gB = B$ or $gB \cap B = \emptyset$. The subsets $\emptyset$, $[d]$, and every singleton are blocks of every permutation group. If these trivial blocks are the only blocks, then G is *primitive* and otherwise it is *imprimitive*.

When G is imprimitive, we have a factorization $d = ab$ with $1 < a, b < d$ and there is a bijection $[a] \times [b] \leftrightarrow [d]$ such that G preserves the projection $[a] \times [b] \to [b]$. That is, the fibers $\{[a] \times \{i\} \mid i \in [b]\}$ are blocks of G, its action on this set of blocks gives a homomorphism $G \to S_b$ with transitive image, and the kernel acts transitively on each fiber $[a] \times \{i\}$. In particular, G is a subgroup of the wreath product $S_a \wr S_b = (S_a)^b \rtimes S_b$, where S_b acts on $(S_a)^b$ by permuting factors.

We observe a second characterization of imprimitive permutation groups G. Since G acts transitively, if $H \subset G$ is the stabilizer of a point $c \in [d]$, then H has index d in G and we may identify $[d]$ with the cosets G/H. If B is a nontrivial block of G containing c, then its stabilizer L is a proper subgroup of G that strictly contains H. Furthermore, using the map $G/H \to G/L$, we see that G is imprimitive if and only if the stabilizer of the point $eH \in G/H$ is not a maximal subgroup.

1.2. **Decomposable branched covers.** A branched cover $\pi\colon X \to Z$ is *decomposable* if there is a nonempty Zariski open subset $V \subset Z$ over which π factors

$$\pi^{-1}(V) \xrightarrow{\ \varphi\ } Y \xrightarrow{\ \psi\ } V\,, \tag{2}$$

with φ and ψ both nontrivial branched covers. The fibers of φ over points of $\psi^{-1}(v)$ are blocks of the action of G_π on $\pi^{-1}(v)$, which implies that G_π is imprimitive. Pirola and Schlesinger [23] observed that decomposability of π is equivalent to imprimitivity of G_π. We give a proof, as we discuss the problem of computing a decomposition.

Proposition 1. *A branched cover is decomposable if and only if its Galois group is imprimitive.*

Proof. We need only to prove the reverse direction. As above, let $\mathbb{C}(Z)$, $\mathbb{C}(X)$, and K be the function fields of Z, X, and the Galois closure of $\mathbb{C}(X)/\mathbb{C}(Z)$, respectively, and let G_π be the Galois group of $K/\mathbb{C}(Z)$. Let H be the subgroup of G_π such that $\mathbb{C}(X) = K^H$, the fixed field of H. The set of Galois conjugates of $\mathbb{C}(X)$ forms the orbit G_π/H, and the number of conjugates is the degree of the branched cover $X \to Z$.

If G_π acts imprimitively, then the stabilizer L of a nontrivial block B containing $\mathbb{C}(X)$ is a proper subgroup properly containing H. Thus its fixed field $M := K^L$, which is the intersection of the conjugates of $\mathbb{C}(X)$ in the block B, is an intermediate field between $\mathbb{C}(Z)$ and $\mathbb{C}(X)$. For any variety Y' with function field M, there will be Zariski open subsets Y of Y' and V of Z such that (2) holds. Indeed, the inclusions of function fields $\mathbb{C}(Z) \subset M \subset \mathbb{C}(X)$ give dominant rational maps $X \dashrightarrow Y' \dashrightarrow Z$. Replacing the varieties X, Y', and Z by Zariski open subsets, we may assume that these are regular maps, hence branched covers. Finally, we may replace Z by a nonempty Zariski open subset V contained in the image of X under the composition and let Y be the inverse image of V in Y'. $\qquad\square$

While imprimitivity is equivalent to decomposability, the proof does not address how to compute the variety Y of (2). One way is as follows. Replace Z and X by affine open subsets, if necessary, and let $y_1, \ldots, y_m \in \mathbb{C}[X]$ be regular functions on X that generate M over $\mathbb{C}(Z)$. Let $x_1, \ldots, x_m$ be indeterminates and let $I \subset \mathbb{C}(Z)[x_1, \ldots, x_m]$ be the kernel of the map $\mathbb{C}(Z)[x_1, \ldots, x_m] \to \mathbb{C}(X)$ given by $x_i \mapsto y_i$. This is the zero-dimensional ideal of algebraic relations satisfied by $y_1, \ldots, y_m$. Replacing Z by a Zariski open subset of affine space if necessary, we may choose generators $g_1, \ldots, g_r$ of I that lie in $\mathbb{C}[Z][x_1, \ldots, x_m]$— their coefficients are regular functions on Z. There is an open subset $V \subset Z$ such that the ideal I defines an irreducible variety $Y \subset V \times \mathbb{C}^m$ whose projection to V is a branched cover and whose function field is M. Replacing X by $\pi^{-1}(V)$, we obtain the desired decomposition, with the map $\pi^{-1}(V) \to Y$ given by the functions $y_1, \ldots, y_m$.

This does not address the practicality of computing Y, but it does indicate an approach. Given the subgroup L of G_π and a set of generators of $\mathbb{C}[X]$ over $\mathbb{C}[Z]$, if we apply the Reynolds averaging operator [6] for L to monomials in the generators, we obtain the desired generators $y_1, \ldots, y_m$ of M. One problem is that elements of G_π may not act on X, so their action on elements of $\mathbb{C}[X]$ may be hard to describe.

There is an exception to this. If $L \neq H$ normalizes H in G and $\pi \colon X \to Z$ is a covering space, then $\Gamma := L/H$ acts freely on X, preserving the fibers—it is a group of deck transformations of $X \to Z$ [22, Ch 13]. When Γ acts on the original branched cover, $Y = X/\Gamma$ is the desired space, and both Y and the map $X \to Y$ may be computed by applying the Reynolds operator for Γ to generators of $\mathbb{C}[X]$. The examples given in [1, § 5] are of this form, and the authors use this approach to compute the decomposition (2).

Example 2. Not all imprimitive groups have the property that the normalizer L of a point stabilizer H properly contains H. Consider the wreath product $G := S_3 \wr S_3$, which acts imprimitively on the nine-element set $[3] \times [3]$. The stabilizer of the point $(3,3)$ is the subgroup $H = ((S_3)^2 \times S_2) \rtimes S_2$, where $S_2 \subset S_3$ is the stabilizer of $\{3\}$. Then H is its own normalizer in G, as S_2 is its own normalizer in S_3. ◇

All imprimitive Galois groups in the Schubert calculus constructed in [19, § 3] and in [26] have the stabilizer H of $\mathbb{C}(X)$ equal to its normalizer. For these, the decomposition of the branched cover follows from a deep structural understanding of the corresponding Schubert problem. There remain many Schubert problems whose Galois group is expected to be imprimitive, yet we do not know a decomposition (2) of the corresponding branched cover.

The structure of imprimitivity/decomposability found in [19, 26] was not initially apparent, and further study was needed to determine a decomposition. In contrast, a consequence of Esterov's study of Galois groups of sparse polynomial systems is that decomposability is transparent and may be deduced by inspection and computing the decomposition (2) is algorithmic. This is explained in the following section.

2. Decomposable Sparse Systems

We discuss sparse systems of (Laurent) polynomials and interpret them as branched covers. Then we state the Bernstein-Kushnirenko Theorem for their numbers of complex isolated solutions, and give the relation between integer linear algebra and maps of algebraic tori. We then present Esterov's criteria for imprimitivity, and show how these criteria lead to decompositions of the corresponding branched cover.

2.1. **Sparse Polynomial Systems.** Let $\mathbb{C}^\times := \mathbb{C} \smallsetminus \{0\}$ be the multiplicative group of nonzero complex numbers and $(\mathbb{C}^\times)^n$ be the n-dimensional complex torus. For each $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}^n$, the *(Laurent) monomial* with exponent α,

$$x^\alpha := x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n},$$

is a character (multiplicative map) $x^\alpha \colon (\mathbb{C}^\times)^n \to \mathbb{C}^\times$. A finite linear combination

$$(3) \qquad\qquad f = \sum c_\alpha x^\alpha \qquad c_\alpha \in \mathbb{C}$$

of monomials is a *(Laurent) polynomial*, which is a function $f \colon (\mathbb{C}^\times)^n \to \mathbb{C}$.

The class of sparse polynomial systems pertains to those systems whose monomial structure for each equation is pre-determined. Our polynomial systems naturally occur in a family of sparse polynomial systems determined only by the monomials appearing in each equation of the system.

For a nonempty finite set $\mathcal{A} \subset \mathbb{Z}^n$, the set of polynomials (3) satisfying $c_\alpha \neq 0 \Rightarrow \alpha \in \mathcal{A}$ is the vector space $\mathbb{C}^{\mathcal{A}}$ of polynomials of *support* $\mathcal{A}$. Given a collection $\mathcal{A}_\bullet := (\mathcal{A}_1, \dots, \mathcal{A}_n)$ of nonempty finite subsets of $\mathbb{Z}^n$, write $\mathbb{C}^{\mathcal{A}_\bullet} := \mathbb{C}^{\mathcal{A}_1} \times \cdots \times \mathbb{C}^{\mathcal{A}_n}$ for the vector space of n-tuples $F = (f_1, \dots, f_n)$ of polynomials, where f_i has support $\mathcal{A}_i$, for each i. An element $F \in \mathbb{C}^{\mathcal{A}_\bullet}$ is a list of coefficients of these polynomials, which corresponds to a system of polynomial equations

$$f_1(x_1, \dots, x_n) \;=\; f_2(x_1, \dots, x_n) \;=\; \cdots \;=\; f_n(x_1, \dots, x_n) \;=\; 0 \,,$$

written $F(x) = 0$. Such a system of polynomial equations is called a *sparse polynomial system* of *support* $\mathcal{A}_\bullet$. Its set of solutions in $(\mathbb{C}^\times)^n$ is $\mathcal{V}(F)$.

Given supports $\mathcal{A}_\bullet = (\mathcal{A}_1, \dots, \mathcal{A}_n)$, consider the incidence variety

$$X_{\mathcal{A}_\bullet} \;:=\; \left\{ (F, x) \in \mathbb{C}^{\mathcal{A}_\bullet} \times (\mathbb{C}^\times)^n \mid F(x) = 0 \right\}.$$

equipped with projections $\pi \colon X_{\mathcal{A}_\bullet} \to \mathbb{C}^{\mathcal{A}_\bullet}$ and $p \colon X_{\mathcal{A}_\bullet} \to (\mathbb{C}^\times)^n$. For any point $x \in (\mathbb{C}^\times)^n$, the fiber $p^{-1}(x)$ is a vector subspace of $\mathbb{C}^{\mathcal{A}_\bullet}$ of codimension n. Indeed, for each $i = 1, \dots, n$, the condition that $f_i(x) = 0$ is a linear equation in the coefficients $\mathbb{C}^{\mathcal{A}_i}$ of f_i, and these n linear equations are independent. Thus $X_{\mathcal{A}_\bullet}$ is irreducible of dimension

$$\dim (\mathbb{C}^\times)^n + \dim \mathbb{C}^{\mathcal{A}_\bullet} - n \;=\; \dim \mathbb{C}^{\mathcal{A}_\bullet} \,.$$

For $F \in \mathbb{C}^{\mathcal{A}_\bullet}$, the fiber $\pi^{-1}(F)$ is the set $\mathcal{V}(F)$ of solutions in $(\mathbb{C}^\times)^n$ to $F(x) = 0$. The image of $X_{\mathcal{A}_\bullet}$ under π either lies in a proper subvariety Z of $\mathbb{C}^{\mathcal{A}_\bullet}$ or it is dense in $\mathbb{C}^{\mathcal{A}_\bullet}$. In the first case, there is a Zariski open subset $U := \mathbb{C}^{\mathcal{A}_\bullet} \smallsetminus Z$ consisting of polynomial systems $F(x) = 0$ with no solution. In the second case, $\pi \colon X_{\mathcal{A}_\bullet} \to \mathbb{C}^{\mathcal{A}_\bullet}$ is a branched cover, so there is a positive integer d and a Zariski open subset $U \subset \mathbb{C}^{\mathcal{A}_\bullet}$ consisting of polynomial systems $F(x) = 0$ with d isolated solutions. Both cases are determined by the polyhedral geometry of the supports $\mathcal{A}_\bullet$ through the Bernstein-Kushnirenko Theorem.

For convex sets $K_1, \dots, K_n \subset \mathbb{R}^n$ and nonnegative real numbers, $t_1, \dots, t_n \in \mathbb{R}_{\geq 0}$, Minkowski proved that the volume of the Minkowski sum

$$t_1 K_1 + \cdots + t_n K_n \;:=\; \{ t_1 x_1 + \cdots + t_n x_x \mid x_i \in K_i \}$$

is a homogeneous polynomial of degree n in $t_1, \dots, t_n$. Its coefficient of $t_1 \cdots t_n$ is the mixed volume of $K_1, \dots, K_n$. For $\mathcal{A}_\bullet = (\mathcal{A}_1, \dots, \mathcal{A}_n)$, let $\mathrm{MV}(\mathcal{A}_\bullet)$ be the mixed volume of $\mathrm{conv}(\mathcal{A}_1), \dots, \mathrm{conv}(\mathcal{A}_n)$, where $\mathrm{conv}(\mathcal{A}_i)$ is the convex hull of $\mathcal{A}_i$. This is described in more detail in [9, Sect. IV.3]. We give the Bernstein-Kushnirenko Theorem [3, 17].

Proposition 3. *Let $F(x) = 0$ be a system of polynomials with support $\mathcal{A}_\bullet$. The number of complex isolated solutions in $(\mathbb{C}^\times)^n$ to $F(x) = 0$ is at most $\mathrm{MV}(\mathcal{A}_\bullet)$. There is a Zariski open subset $U \subset \mathbb{C}^{\mathcal{A}_\bullet}$ consisting of systems with exactly $\mathrm{MV}(\mathcal{A}_\bullet)$ solutions.*

Thus $\pi \colon X_{\mathcal{A}_\bullet} \to \mathbb{C}^{\mathcal{A}_\bullet}$ is a branched cover if and only if $\mathrm{MV}(\mathcal{A}_\bullet) \neq 0$, which was determined by Minkowski as follows. For a nonempty subset $I \subseteq [n] := \{1, \dots, n\}$, write $\mathcal{A}_I := (\mathcal{A}_i \mid i \in I)$ and $\mathbb{Z}\mathcal{A}_I$ be the affine span of the supports in $\mathcal{A}_I$. This is the free abelian group generated by differences $\alpha - \beta$ for $\alpha, \beta \in \mathcal{A}_i$ for some $i \in I$. Then $\mathrm{MV}(\mathcal{A}_\bullet) = 0$ if and only if there exists a nonempty subset $I \subseteq [n]$ such that $|I|$ exceeds $\mathrm{rank}(\mathbb{Z}\mathcal{A}_I)$. In particular, $\mathrm{MV}(\mathcal{A}_\bullet) \neq 0$ implies that $\mathbb{Z}\mathcal{A}_\bullet = \mathbb{Z}\mathcal{A}_{[n]}$ has full rank n.

The branched cover $\pi\colon X_{\mathcal{A}_\bullet} \to \mathbb{C}^{\mathcal{A}_\bullet}$ is nontrivial when $\mathrm{MV}(\mathcal{A}_\bullet) > 1$. Given supports $\mathcal{A}_\bullet$ with $\mathrm{MV}(\mathcal{A}_\bullet) \neq 0$, let $G_{\mathcal{A}_\bullet}$ be the Galois group of the branched cover $X_{\mathcal{A}_\bullet} \to \mathbb{C}^{\mathcal{A}_\bullet}$.

2.2. **Integer linear algebra and coordinate changes.** As a monomial x^β for $\beta \in \mathbb{Z}^n$ is invertible on $(\mathbb{C}^\times)^n$, polynomials f and $x^\beta f$ have the same sets of zeroes. If $\mathcal{A}$ is the support of f, then the support of $x^\beta f$ is $\beta + \mathcal{A}$, the translation of $\mathcal{A}$ by β. Thus translating the supports of sparse polynomials by integer vectors does not change any assertions about their zeroes in $(\mathbb{C}^\times)^n$. Similarly, $\mathbb{Z}\mathcal{A} = \mathbb{Z}(\beta + \mathcal{A})$. Consequently, we will henceforth assume that $\mathbf{0} \in \mathcal{A}$, for then $\mathbb{Z}\mathcal{A}$ will be the $\mathbb{Z}$-linear span of $\mathcal{A}$.

We identify the set $\mathrm{Hom}((\mathbb{C}^\times)^n, \mathbb{C}^\times)$ of characters on $(\mathbb{C}^\times)^n$ with the free abelian group $\mathbb{Z}^n$. A group homomorphism $\Phi\colon (\mathbb{C}^\times)^m \to (\mathbb{C}^\times)^k$ is determined by k characters of $(\mathbb{C}^\times)^m$, equivalently by a homomorphism (linear map) $\varphi\colon \mathbb{Z}^k \to \mathbb{Z}^m$ of free abelian groups—φ is also the map pulling a character of $(\mathbb{C}^\times)^k$ back along Φ. In particular, an invertible map $\Phi\colon (\mathbb{C}^\times)^n \to (\mathbb{C}^\times)^n$ (a monomial change of coordinates) pulls back to an invertible map $\varphi\colon \mathbb{Z}^n \to \mathbb{Z}^n$, identifying $\mathrm{GL}(n, \mathbb{Z})$ with the group of possible monomial coordinate changes. We will write $\Phi = \varphi^*$ and $\varphi = \Phi^*$ for these. If $\Phi(x) = (x^{\alpha_1}, \ldots, x^{\alpha_n})$, then the map $\varphi = \Phi^*\colon \mathbb{Z}^n \xrightarrow{\sim} \mathbb{Z}^n$ sends the i-th standard basis vector e_i to α_i and is represented by the invertible matrix A whose i-th column is α_i. When the integer span of $\alpha_1, \ldots, \alpha_n$ is $\mathbb{Z}^n$, the map $\varphi = \Phi^*$ is invertible.

Suppose that f is a polynomial on $(\mathbb{C}^\times)^n$ with support $\mathcal{A}$. Given a homomorphism $\Phi\colon (\mathbb{C}^\times)^m \to (\mathbb{C}^\times)^n$, the composition $f(\Phi(z))$ for $z \in (\mathbb{C}^\times)^m$ is a polynomial with support $\varphi(\mathcal{A})$, where the coefficient of z^β is the sum of coefficients of x^α for $\alpha \in \varphi^{-1}(\beta) \cap \mathcal{A}$.

2.3. **Decompositions of Sparse Polynomial Systems.** We describe two properties that a collection $\mathcal{A}_\bullet$ of supports may have, lacunary and (strictly) triangular, and then recall Esterov's theorem about the Galois group $G_{\mathcal{A}_\bullet}$. We then present explicit decompositions of the projection $\pi\colon X_{\mathcal{A}_\bullet} \to \mathbb{C}^{\mathcal{A}_\bullet}$ when $\mathcal{A}_\bullet$ is lacunary and when $\mathcal{A}_\bullet$ is triangular. These form the basis for our algorithms.

Let $\mathcal{A}_\bullet = (\mathcal{A}_1, \ldots, \mathcal{A}_n)$ be a collection of supports. Assume that $\mathrm{MV}(\mathcal{A}_\bullet) > 1$. We say that $\mathcal{A}_\bullet$ is *lacunary* if the affine span $\mathbb{Z}\mathcal{A}_\bullet \neq \mathbb{Z}^n$ (it has rank n as $\mathrm{MV}(\mathcal{A}_\bullet) \neq 0$). We say that $\mathcal{A}_\bullet$ is *triangular* if there is a nonempty proper subset $\emptyset \neq I \subsetneq [n]$ such that $\mathrm{rank}(\mathbb{Z}\mathcal{A}_I) = |I|$. As we explain in Section 2.4, we may change coordinates and assume that $\mathbb{Z}\mathcal{A}_I \subset \mathbb{Z}^{|I|}$ so that $\mathrm{MV}(\mathcal{A}_I)$ is defined using $\mathrm{conv}(\mathcal{A}_i) \subset \mathbb{R}^{|I|}$ for $i \in I$. A system $\mathcal{A}_\bullet$ of triangular supports is *strictly triangular* if for some $\emptyset \neq I \subsetneq [n]$ with $\mathrm{rank}(\mathbb{Z}\mathcal{A}_I) = |I|$, we have $1 < \mathrm{MV}(\mathcal{A}_I) < \mathrm{MV}(\mathcal{A}_\bullet)$. It is elementary that if $\mathcal{A}_\bullet$ is either lacunary or strictly triangular, then the branched cover $X_{\mathcal{A}_\bullet} \to \mathbb{C}^{\mathcal{A}_\bullet}$ is decomposable and therefore $G_{\mathcal{A}_\bullet}$ is an imprimitive permutation group. We show this explicitly in Sections 2.3.1 and 2.3.2.

Proposition 4 (Esterov [8])**.** *Let $\mathcal{A}_\bullet$ be a collection of supports with $\mathrm{MV}(\mathcal{A}_\bullet) \neq 0$. The Galois group $G_{\mathcal{A}_\bullet}$ is equal to the symmetric group $S_{\mathrm{MV}(\mathcal{A}_\bullet)}$ if and only if $\mathcal{A}_\bullet$ is neither lacunary nor strictly triangular.*
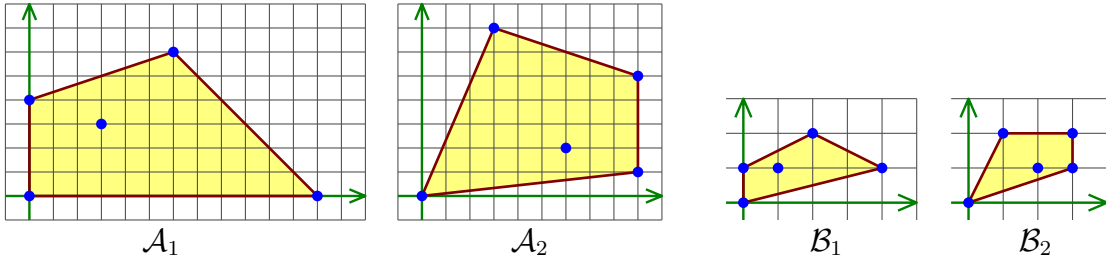
2.3.1. *Lacunary support.* Let us begin with an example when $n = 2$. We represent vectors by the columns of a matrix. Let

$$\mathcal{A}_1 := \begin{pmatrix} 0 & 0 & 3 & 6 & 12 \\ 0 & 4 & 3 & 6 & 0 \end{pmatrix} \qquad \text{and} \qquad \mathcal{A}_2 := \begin{pmatrix} 0 & 3 & 6 & 9 & 9 \\ 0 & 7 & 2 & 1 & 5 \end{pmatrix}$$

be supports in $\mathbb{Z}^2$. Then $\mathbb{Z}\mathcal{A}_\bullet$ has index 12 in $\mathbb{Z}^2$ as the map $\varphi(a,b)^T = (3a, 4b - a)^T$ is an isomorphism $\varphi \colon \mathbb{Z}^2 \xrightarrow{\sim} \mathbb{Z}\mathcal{A}_\bullet$, and $\det(\begin{smallmatrix} 3 & 0 \\ -1 & 4 \end{smallmatrix}) = 12$. If we set $\mathcal{B}_i := \varphi^{-1}(\mathcal{A}_i)$, then

$$\mathcal{B}_1 := \begin{pmatrix} 0 & 0 & 1 & 2 & 4 \\ 0 & 1 & 1 & 2 & 1 \end{pmatrix} \qquad \text{and} \qquad \mathcal{B}_2 := \begin{pmatrix} 0 & 1 & 2 & 3 & 3 \\ 0 & 2 & 1 & 1 & 2 \end{pmatrix}.$$

We display $\mathcal{A}_1$, $\mathcal{A}_2$, $\mathcal{B}_1$, and $\mathcal{B}_2$ below.

$\mathcal{A}_1$ $\qquad\qquad\qquad$ $\mathcal{A}_2$ $\qquad\qquad\qquad$ $\mathcal{B}_1$ $\qquad\qquad\qquad$ $\mathcal{B}_2$

Then the map $\Phi := \varphi^* \colon (\mathbb{C}^\times)^2 \twoheadrightarrow (\mathbb{C}^\times)^2$ is given by $\Phi(x,y) = (x^3 y^{-1}, y^4) = (z, w)$. If

$$\begin{aligned} f_1 &= 1 + 2y^4 + 4x^3 y^3 + 8x^6 y^6 + 16x^{12} \\ f_2 &= 3 + 5x^3 y^7 + 7x^6 y^2 + 11x^9 y + 13x^9 y^5 \;, \end{aligned}$$

which is a polynomial system with support $\mathcal{A}_\bullet$, then $f_i = g_i \circ \Phi$, where

$$\begin{aligned} g_1 &= 1 + 2w + 4zw + 8z^2 w^2 + 16z^4 w \\ g_2 &= 3 + 5zw^2 + 7z^2 w + 11z^3 w + 13z^3 w^2 \;, \end{aligned}$$

is a polynomial system with support $\mathcal{B}_\bullet$. Thus the branched cover $X_{\mathcal{A}_\bullet} \to \mathbb{C}^{\mathcal{A}_\bullet}$ factors $X_{\mathcal{A}_\bullet} \to X_{\mathcal{B}_\bullet} \to \mathbb{C}^{\mathcal{B}_\bullet} = \mathbb{C}^{\mathcal{A}_\bullet}$ with the map $X_{\mathcal{A}_\bullet} \to X_{\mathcal{B}_\bullet}$ induced by Φ. This implies that $G_{\mathcal{A}_\bullet} \subset (\mathbb{Z}/12\mathbb{Z})^{10} \rtimes S_{10}$, as $\mathbb{Z}^2/\mathbb{Z}\mathcal{A}_\bullet \simeq \mathbb{Z}/12\mathbb{Z}$, $\mathcal{B}_\bullet$ is neither lacunary nor triangular, and $\mathrm{MV}(\mathcal{B}_\bullet) = 10$.

We generalize this example. Suppose that $\mathcal{A}_\bullet = (\mathcal{A}_1, \ldots, \mathcal{A}_n)$ is lacunary. Then $\mathbb{Z}\mathcal{A}_\bullet$ has rank n but $\mathbb{Z}\mathcal{A}_\bullet \neq \mathbb{Z}^n$. Let $\varphi \colon \mathbb{Z}^n \xrightarrow{\sim} \mathbb{Z}\mathcal{A}_\bullet$ be an isomorphism. Then the corresponding map $\Phi = \varphi^* \colon (\mathbb{C}^\times)^n \to (\mathbb{C}^\times)^n$ is a surjection with kernel $\mathrm{Hom}(\mathbb{Z}^n/\mathbb{Z}\mathcal{A}_\bullet, \mathbb{C}^\times)$. For each $i = 1, \ldots, n$, set $\mathcal{B}_i := \varphi^{-1}(\mathcal{A}_i)$. Then $\mathcal{B}_\bullet = (\mathcal{B}_1, \ldots, \mathcal{B}_n)$ is a collection of supports with $\mathbb{Z}\mathcal{B}_\bullet = \mathbb{Z}^n$. Since φ is a bijection, we identify $\mathbb{C}^{\mathcal{B}_i}$ with $\mathbb{C}^{\mathcal{A}_i}$ and $\mathbb{C}^{\mathcal{B}_\bullet}$ with $\mathbb{C}^{\mathcal{A}_\bullet}$. Given a system $F(x) = 0$ with $F \in \mathbb{C}^{\mathcal{A}_\bullet}$, $\iota(F)(x) = 0$ with $\iota(F) \in \mathbb{C}^{\mathcal{B}_\bullet}$ is the corresponding system with support $\mathcal{B}_\bullet$.

Lemma 5. *Suppose that $\mathcal{A}_\bullet$ is lacunary, $\varphi \colon \mathbb{Z}^n \xrightarrow{\sim} \mathbb{Z}\mathcal{A}_\bullet$ is an isomorphism with corresponding surjection $\Phi \colon (\mathbb{C}^\times)^n \to (\mathbb{C}^\times)^n$. Let $\mathcal{B}_\bullet := \varphi^{-1}(\mathcal{A}_\bullet)$ and suppose that $\mathrm{MV}(\mathcal{B}_\bullet) > 1$. Then the branched cover $X_{\mathcal{A}_\bullet} \to \mathbb{C}^{\mathcal{A}_\bullet}$ is decomposable and $X_{\mathcal{A}_\bullet} \to X_{\mathcal{B}_\bullet} \to \mathbb{C}^{\mathcal{A}_\bullet} = \mathbb{C}^{\mathcal{B}_\bullet}$ is a nontrivial decomposition of branched covers induced by the map Φ.*

Proof. If g is a polynomial with support $\mathcal{B} \subset \mathbb{Z}^n$, then the composition $g \circ \Phi$ is a polynomial with support $\varphi(\mathcal{B})$, with the coefficient of x^β in g equal to the coefficient of $x^{\varphi(\beta)}$ in $g \circ \Phi$. Since $\varphi(\mathcal{B}_i) = \mathcal{A}_i$, this gives the natural identifications $\iota \colon \mathbb{C}^{\mathcal{A}_i} \xrightarrow{\sim} \mathbb{C}^{\mathcal{B}_i}$ and $\iota \colon \mathbb{C}^{\mathcal{A}_\bullet} \xrightarrow{\sim} \mathbb{C}^{\mathcal{B}_\bullet}$ mentioned before the lemma. Under this identification, we have $\iota(f)(\Phi(x)) = f(x)$.

Since $\mathrm{MV}(\mathcal{B}_\bullet) > 1$, the branched cover $X_{\mathcal{B}_\bullet} \to \mathbb{C}^{\mathcal{B}_\bullet}$ is nontrivial. The identification $\iota \colon \mathbb{C}^{\mathcal{A}_\bullet} \to \mathbb{C}^{\mathcal{B}_\bullet}$ extends to a commutative diagram

$$(4) \qquad \begin{array}{ccc} X_{\mathcal{A}_\bullet} & \xrightarrow{\;\iota \times \Phi\;} & X_{\mathcal{B}_\bullet} \\ {\scriptstyle \pi} \downarrow & & \downarrow {\scriptstyle \pi} \\ \mathbb{C}^{\mathcal{A}_\bullet} & \xrightarrow{\;\iota\;} & \mathbb{C}^{\mathcal{B}_\bullet} \end{array}$$

Here, $\iota \times \Phi$ is the restriction of the map $\iota \times \Phi \colon \mathbb{C}^{\mathcal{A}_\bullet} \times (\mathbb{C}^\times)^n \to \mathbb{C}^{\mathcal{B}_\bullet} \times (\mathbb{C}^\times)^n$ to $X_{\mathcal{A}_\bullet}$. The map $\iota \times \Phi \colon X_{\mathcal{A}_\bullet} \to X_{\mathcal{B}_\bullet}$ is a map of branched covers with $\ker \Phi$ acting freely on the fibers. If we restrict the diagram (4) to the open subset V of $\mathbb{C}^{\mathcal{B}_\bullet}$ over which $X_{\mathcal{B}_\bullet} \to \mathbb{C}^{\mathcal{B}_\bullet}$ is a covering space, we obtain a composition of covering spaces with $\ker \Phi$ acting as deck transformations on $\pi^{-1}(V) \subset X_{\mathcal{A}_\bullet}$. Thus $X_{\mathcal{A}_\bullet} \to \mathbb{C}^{\mathcal{A}_\bullet}$ is decomposable. $\qquad \square$

2.3.2. *Triangular support.* This requires more discussion before we can state the analog of Lemma 5. Let us begin with an example when $n = 3$. Suppose that

$$\mathcal{A}_1 = \mathcal{A}_2 = \mathcal{A} = \begin{pmatrix} 0 & 1 & 1 & 1 & 2 & 2 & 2 & 3 \\ 0 & 0 & 1 & 2 & 0 & 1 & 2 & 1 \\ 0 & 1 & 2 & 3 & 2 & 3 & 4 & 4 \end{pmatrix} \quad \text{and} \quad \mathcal{A}_3 = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 2 & 4 & 5 & 3 & 4 \end{pmatrix}$$

The span $\mathbb{Z}\mathcal{A}$ of the first two supports is isomorphic to $\mathbb{Z}^2$, with $\varphi(a,b)^T \mapsto (a, b, a+b)^T$ an isomorphism $\varphi \colon \mathbb{Z}^2 \xrightarrow{\sim} \mathbb{Z}\mathcal{A}_\bullet$. Set $\mathcal{B} := \varphi^{-1}(\mathcal{A})$. We display $\mathcal{A}$, $\mathcal{A}_3$, and $\mathcal{B}$ in the horizontal plane together on the left below, and $\mathcal{B}$ on the right.
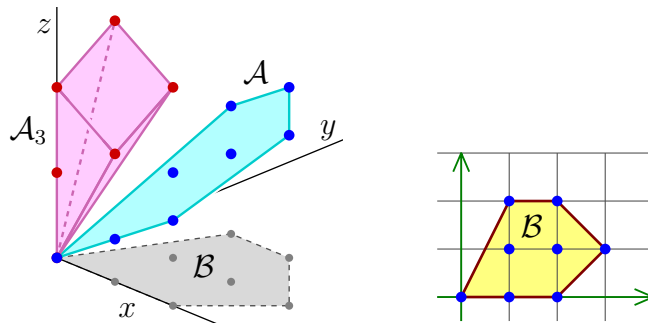
Consider the polynomial system $F = (f_1, f_2, f_3) \in \mathbb{C}[x, y, z]$ with support $\mathcal{A}_\bullet$,

$$\begin{aligned} f_1 &= 1 + 2xz + 3xyz^2 + 4xy^2z^3 + 5x^2z^2 + 6x^2yz^3 + 7x^2y^2z^4 + 8x^3yz^4 \\ f_2 &= 2 + 3xz + 5xyz^2 + 7xy^2z^3 + 11x^2z^2 + 13x^2yz^3 + 17x^2y^2z^4 + 19x^3yz^4 \\ f_3 &= 1 + 3z^2 + 9z^4 + 27yz^5 + 81xz^3 + 243xyz^4 \,. \end{aligned}$$

Let $\Phi \colon (\mathbb{C}^\times)^3 \to (\mathbb{C}^\times)^2$ be given by $\Phi(x, y, z) = (xz, yz) = (u, v)$. If

$$g_1 = 1 + 2u + 3uv + 4uv^2 + 5u^2 + 6u^2v + 7u^2v^2 + 8u^3v$$

$$g_2 = 2 + 3u + 5uv + 7uv^2 + 11u^2 + 13u^2v + 17u^2v^2 + 19u^3v,$$

then $f_i = g_i \circ \Phi$ for $i = 1, 2$. To compute $\mathcal{V}(F)$, we first may compute $\mathcal{V}(g_1, g_2)$ which consists of eight points. For each solution $(u_0, v_0) \in \mathcal{V}(g_1, g_2)$, we may identify the fiber $\Phi^{-1}(u_0, v_0)$ with $\mathbb{C}^\times$ by $z \mapsto (u_0 z^{-1}, v_0 z^{-1}, z)$. Then the restriction of f_3 to this fiber is

$$1 + (3 + 81u_0 + 243u_0v_0)z^2 + (9 + 27v_0)z^4,$$

which is a lacunary univariate polynomial with support $\{0, 2, 4\}$, and has four solutions (counted with multiplicity) when $v_0 \neq -1/3$.

This example generalizes to all triangular systems. Suppose that $\mathcal{A}_\bullet = (\mathcal{A}_1, \ldots, \mathcal{A}_n)$ is triangular. Let $\emptyset \neq I \subsetneq [n]$ be a proper subset witnessing the triangularity, so that $\mathrm{rank}(\mathbb{Z}\mathcal{A}_I) = |I|$. Set $J := [n] \smallsetminus I$. Let

$$\mathbb{Z}^I := \mathbb{Q}\mathcal{A}_I \cap \mathbb{Z}^n = \{v \in \mathbb{Z}^n \mid \exists m \in \mathbb{N} \text{ with } mv \in \mathbb{Z}\mathcal{A}_I\},$$

be the saturation of $\mathbb{Z}\mathcal{A}_I$, which is a free abelian group of rank $|I|$. As it is saturated, $\mathbb{Z}_J := \mathbb{Z}^n/\mathbb{Z}^I$ is free abelian of rank $n - |I| = |J|$.

Applying $\mathrm{Hom}(\bullet, \mathbb{C}^\times)$ to the short exact sequence $\mathbb{Z}^I \hookrightarrow \mathbb{Z}^n \twoheadrightarrow \mathbb{Z}_J$ gives the short exact sequence of tori (whose characters are $\mathbb{Z}_J$, $\mathbb{Z}^n$, and $\mathbb{Z}^I$) with indicated maps,

$$(5) \quad (\mathbb{C}^\times)^{|J|} \simeq \mathbb{T}_J := \mathrm{Hom}(\mathbb{Z}_J, \mathbb{C}^\times) \longleftrightarrow (\mathbb{C}^\times)^n \xrightarrow{\ \Phi\ } \mathbb{T}^I := \mathrm{Hom}(\mathbb{Z}^I, \mathbb{C}^\times) \simeq (\mathbb{C}^\times)^{|I|}.$$

A polynomial f with support in $\mathbb{Z}^I$ determines polynomial functions on $(\mathbb{C}^\times)^n$ and on $\mathbb{T}^I$ with the first the pullback of the second. Let f be a polynomial on $(\mathbb{C}^\times)^n$ with support $\mathcal{A} \subset \mathbb{Z}^n$. Then its restriction to a fiber $\Phi^{-1}(y_0)$ of Φ is a regular function $\overline{f}$ on the fiber, which is a coset of $\mathbb{T}_J$. Choosing an identification of $\mathbb{T}_J \simeq \Phi^{-1}(y_0)$, we obtain a polynomial $\overline{f}$ on $\mathbb{T}_J$ whose support is the image $\overline{\mathcal{A}}$ of $\mathcal{A}$ in $\mathbb{Z}_J = \mathbb{Z}^n/\mathbb{Z}^I$. This polynomial $\overline{f}$ depends upon the identification of the fiber with $\mathbb{T}_J$. Let $\overline{\mathcal{A}_J}$ be the image in $\mathbb{Z}_J$ of the collection $\mathcal{A}_J$ of supports. Then we have the product formula (see [27, Lem. 6] or [8, Thm. 1.10])

$$(6) \quad \mathrm{MV}(\mathcal{A}_\bullet) = \mathrm{MV}(\mathcal{A}_I) \cdot \mathrm{MV}(\overline{\mathcal{A}_J}).$$

Since $\mathcal{A}_\bullet = \mathcal{A}_I \sqcup \mathcal{A}_J$, we have the identification $\mathbb{C}^{\mathcal{A}_\bullet} = \mathbb{C}^{\mathcal{A}_I} \oplus \mathbb{C}^{\mathcal{A}_J}$. Suppose that $F(x) = 0$ is a polynomial system with support $\mathcal{A}_\bullet$. Write $F_I \in \mathbb{C}^{\mathcal{A}_I}$ for its restriction to the indices in I, and the same for F_J. We have the diagram

$$(7) \quad \begin{array}{ccc} X_{\mathcal{A}_\bullet} & \xrightarrow{\ p_I \times \Phi\ } & X_{\mathcal{A}_I} \\ \pi \downarrow & & \downarrow \pi \\ \mathbb{C}^{\mathcal{A}_\bullet} & \xrightarrow{\ \ p_I\ \ } & \mathbb{C}^{\mathcal{A}_I} \end{array} \ .$$

Here, $p_I \times \Phi$ is the restriction of the map $p_I \times \Phi \colon \mathbb{C}^{\mathcal{A}_\bullet} \times (\mathbb{C}^\times)^n \to \mathbb{C}^{\mathcal{A}_I} \times \mathbb{T}^I$ to $X_{\mathcal{A}_\bullet}$.

Let $V_{\mathcal{A}_\bullet} \subset \mathbb{C}^{\mathcal{A}_\bullet}$ be the maximal Zariski open subset over which $X_{\mathcal{A}_\bullet}$ is a covering space. This is the set of polynomial systems $F(x) = 0$ with support $\mathcal{A}_\bullet$ which have exactly $\mathrm{MV}(\mathcal{A}_\bullet)$ solutions in $(\mathbb{C}^\times)^n$. Similarly, let $V_{\mathcal{A}_I} \subset \mathbb{C}^{\mathcal{A}_I}$ be the maximal Zariski open subset where $X_{\mathcal{A}_I} \to \mathbb{C}^{\mathcal{A}_I}$ is a covering space. We will show that under the projection $\mathbb{C}^{\mathcal{A}_\bullet} \to \mathbb{C}^{\mathcal{A}_I}$,

the image of $V_{\mathcal{A}_\bullet}$ is a subset of $V_{\mathcal{A}_I}$. Define $Y_{\mathcal{A}_\bullet} \to V_{\mathcal{A}_\bullet}$ to be the restriction of $X_{\mathcal{A}_\bullet} \to \mathbb{C}^{\mathcal{A}_\bullet}$ to the Zariski open set $V_{\mathcal{A}_\bullet}$. Also define $Y_{\mathcal{A}_I} \to V_{\mathcal{A}_\bullet}$ to be the pullback of $X_{\mathcal{A}_I} \to \mathbb{C}^{\mathcal{A}_I}$ along the map $V_{\mathcal{A}_\bullet} \to V_{\mathcal{A}_I}$. Write $\Phi \colon Y_{\mathcal{A}_\bullet} \to Y_{\mathcal{A}_I}$ for the map induced by Φ.

Lemma 6. *Suppose that $\mathcal{A}_\bullet$ is a triangular set of supports in $\mathbb{Z}^n$ witnessed by $I \subsetneq [n]$. Then $Y_{\mathcal{A}_\bullet} \to Y_{\mathcal{A}_I} \to V_{\mathcal{A}_\bullet}$ a composition of covering spaces. If $1 < \mathrm{MV}(\mathcal{A}_I) < \mathrm{MV}(\mathcal{A}_\bullet)$, then this decomposition is nontrivial, so that $X_{\mathcal{A}_\bullet} \to \mathbb{C}^{\mathcal{A}_\bullet}$ is decomposable.*

Furthermore, each fiber of the map $Y_{\mathcal{A}_\bullet} \to Y_{\mathcal{A}_I}$ may be identified with the set of solutions to a polynomial system with support $\overline{\mathcal{A}_J}$.

Proof. Let $F \in V_{\mathcal{A}_\bullet}$. Then its number of solutions is $\#\mathcal{V}(F) = \mathrm{MV}(\mathcal{A}_\bullet)$. If $x \in \mathcal{V}(F)$, then $\Phi(x) \in \mathbb{T}^I$ is a solution to $f_i = 0$ for $i \in I$. Thus $\Phi(\mathcal{V}(F)) \subset \mathcal{V}(F_I)$, the latter being the solutions to $F_I(x) = 0$ on $\mathbb{T}^I$. For any $y \in \mathcal{V}(F_I)$, if we choose an identification $\mathbb{T}^J \simeq \Phi^{-1}(y)$ of the fiber, then the restriction of F to $\Phi^{-1}(y)$ is the system $\overline{F_J} = \{\overline{f_j} \mid j \in J\}$. By the Bernstein-Kushnirenko Theorem, this has at most $\mathrm{MV}(\overline{\mathcal{A}_J})$ solutions. By the product formula (6) and our assumption on $\#\mathcal{V}(F)$, we conclude that the system $F_I(x) = 0$ has $\mathrm{MV}(\mathcal{A}_I)$ solutions, and for each $y \in \mathcal{V}(F_I)$, the system $\overline{F_J}$ has $\mathrm{MV}(\overline{\mathcal{A}_J})$ solutions.

In particular, this implies that the image of $V_{\mathcal{A}_\bullet}$ in $\mathbb{C}^{\mathcal{A}_I}$ is a subset of $V_{\mathcal{A}_I}$. As $V_{\mathcal{A}_\bullet}$ is open and dense in $\mathbb{C}^{\mathcal{A}_\bullet}$, its image contains an open dense subset. This proves the assertion that $Y_{\mathcal{A}_\bullet} \to Y_{\mathcal{A}_I} \to V_{\mathcal{A}_\bullet}$ is a decomposition of covering spaces. We have already shown that each fiber of the map $Y_{\mathcal{A}_\bullet} \to Y_{\mathcal{A}_I}$ is a polynomial system with support $\overline{\mathcal{A}_J}$ with exactly $\mathrm{MV}(\overline{\mathcal{A}_J})$ solutions. Thus when $1 < \mathrm{MV}(\mathcal{A}_I) < \mathrm{MV}(\mathcal{A}_\bullet)$, we have $\mathrm{MV}(\overline{\mathcal{A}_J}) > 1$, which shows that this decomposition is nontrivial. $\square$

2.4. **Computing the Decompositions.** We show how to compute the decompositions of $X_{\mathcal{A}_\bullet} \to \mathbb{C}^{\mathcal{A}_\bullet}$ from Section 2.3 when $\mathcal{A}_\bullet$ is either lacunary or strictly triangular.

Let $\mathcal{A} = \{0, \alpha_1, \ldots, \alpha_m\} \subset \mathbb{Z}^n$ be a collection of integer vectors. The subgroup $\mathbb{Z}\mathcal{A} \subset \mathbb{Z}^n$ that it generates is the image of a $\mathbb{Z}$-linear map $\mathbb{Z}^m \to \mathbb{Z}^n$ and is represented by a $n \times m$ integer matrix A whose columns are the vectors a_i. Suppose that $\mathbb{Z}\mathcal{A}$ has rank k. A *Smith normal form* of A is a factorization into integer matrices

$$(8) \qquad\qquad A = PDQ,$$

where $P \in \mathrm{GL}_n(\mathbb{Z})$ and $Q \in \mathrm{GL}_m(\mathbb{Z})$ are invertible, and D is the rectangular matrix whose only nonzero entries are $d_1, \ldots, d_k$ along the diagonal of its principal $k \times k$ submatrix. These are the *invariant factors* of A and they satisfy $d_1|d_2|d_3|\cdots|d_k$.

The subgroup $\mathbb{Z}\mathcal{A} \subset \mathbb{Z}^n$ has a basis given by the columns of the matrix PD. If we apply the coordinate change P^{-1} to $\mathbb{Z}^n$, then $\mathbb{Z}\mathcal{A}$ becomes the subset of the coordinate space $\mathbb{Z}^k \oplus \mathbf{0}^{n-k}$ given by $d_1\mathbb{Z} \oplus d_2\mathbb{Z} \oplus \cdots \oplus d_k\mathbb{Z} \oplus \mathbf{0}^{n-k}$.

Let us consider a Smith normal form (8) when $\mathcal{A}$ is the collection of vectors in $\mathcal{A}_\bullet$ and $\mathrm{MV}(\mathcal{A}_\bullet) > 0$. Then $d_n > 0$ as $\mathbb{Z}\mathcal{A}_\bullet$ has rank n, and $\mathcal{A}_\bullet$ is lacunary when $d_n > 1$. In this case, an identification $\varphi \colon \mathbb{Z}^n \xrightarrow{\sim} \mathbb{Z}\mathcal{A}$ is given by PD_n, where D_n is the principal $n \times n$ submatrix of D. Recall from § 2.2 that the corresponding surjection $\varphi^* = \Phi \colon (\mathbb{C}^\times)^n \to (\mathbb{C}^\times)^n$ has kernel $\mathrm{Hom}(\mathbb{Z}^n/\mathbb{Z}\mathcal{A}_\bullet, \mathbb{C}^\times)$. Let $\psi := P^{-1}$. Then $\psi \circ \varphi = D_n$, so that if we set

$\Psi := \psi^*$, then $\Phi \circ \Psi \colon (\mathbb{C}^\times)^n \to (\mathbb{C}^\times)^n$ is diagonal,

$$(9) \qquad \Phi \circ \Psi(x_1, \ldots, x_n) \;=\; (x_1^{d_1}, \ldots, x_n^{d_n}).$$

Let $y = (y_1, \ldots, y_n) \in (\mathbb{C}^\times)^n$. If we set $\rho_i := |y_i|$ and $\zeta_i := \arg(y_i)$ so that $y_i = \rho_i e^{\sqrt{-1}\zeta_i}$, then $(\Phi \circ \Psi)^{-1}(y)$ is the set

$$(10) \qquad \left\{ \left(\rho_1^{1/d_1} e^{\sqrt{-1}\theta_1}, \; \ldots, \; \rho_n^{1/d_n} e^{\sqrt{-1}\theta_n} \right) \;\middle|\; \theta_i = \tfrac{\zeta_i + 2\pi j}{d_i} \text{ for } j = 0, \ldots, d_i{-}1 \right\}.$$

This ends the discussion of lacunary sparse polynomial systems.

Suppose that $\mathcal{A}_\bullet$ is triangular, and let us use the notation of § 2.3.2. We suppose that $I = [k] = \{1, \ldots, k\}$ and $J = \{k{+}1, \ldots, n\}$. Given a polynomial f on $(\mathbb{C}^\times)^n$, its restriction $\overline{f}$ to a fiber of $\Phi \colon (\mathbb{C}^\times)^n \to \mathbb{T}^I$ is a regular function on the fiber, which is isomorphic to $\mathbb{T}_J$. To represent $\overline{f}$ as a polynomial on $\mathbb{T}_J$ depends on the choice of a point in that fiber. Indeed, suppose that $f = \sum_{\alpha \in \mathcal{A}} c_\alpha x^\alpha$. Let $y \in \mathbb{T}^I$ and $y_0 \in \Phi^{-1}(y)$ be a point in the fiber above y, so that $\mathbb{T}_J \ni z \mapsto y_0 z \in \Phi^{-1}(y)$ parameterizes $\Phi^{-1}(y)$. If we write $\overline{\alpha}$ for the image of $\alpha \in \mathbb{Z}^n$ in $\mathbb{Z}_J = \mathbb{Z}^n / \mathbb{Z}^I$, then

$$(11) \qquad \overline{f}(z) \;=\; \sum_{\alpha \in \mathcal{A}} c_\alpha (y_0 z)^\alpha \;=\; \sum_{\beta \in \overline{\mathcal{A}}} z^\beta \left(\sum_{\alpha \in \mathcal{A} \text{ with } \overline{\alpha} = \beta} c_\alpha y_0^\alpha \right).$$

A uniform choice of a point in each fiber is given by a splitting $\mathbb{T}^I \hookrightarrow (\mathbb{C}^\times)^n$ of the map $\Phi \colon (\mathbb{C}^\times)^n \twoheadrightarrow \mathbb{T}^I$. This gives an identification $(\mathbb{C}^\times)^n = \mathbb{T}^I \times \mathbb{T}_J$. Then points $y \in \mathbb{T}^I$ are canonical representatives of cosets of $\mathbb{T}_J$. As $k = |I|$, we may further fix isomorphisms $\mathbb{T}^I \simeq (\mathbb{C}^\times)^k$ giving $\mathbb{Z}^I \simeq \mathbb{Z}^k$ and $\mathbb{T}_J \simeq (\mathbb{C}^\times)^{n-k}$ giving $\mathbb{Z}_J \simeq \mathbb{Z}^{n-k}$.

Suppose now that $\mathcal{A} = \mathcal{A}_I$, and we compute a decomposition (8). Since $\mathbb{Z}\mathcal{A}_I$ has rank k, the diagonal matrix D has k nonzero invariant factors. The saturation L of $\mathbb{Z}\mathcal{A}_I$ is the image of $P I_k$, where I_k is the $n \times n$ matrix whose only nonzero entries are in its principal $k \times k$ submatrix, which forms an identity matrix. Then $\varphi = P I_k$ and $\Phi = \varphi^*$. Applying the coordinate change $\psi := P^{-1}$ to $\mathbb{Z}^n$ identifies this saturation as the coordinate plane $\mathbb{Z}^k \oplus \mathbf{0}^{n-k}$ and the free abelian group $\mathbb{Z}\mathcal{A}_I$ as $d_1\mathbb{Z} \oplus d_2\mathbb{Z} \oplus \cdots \oplus d_k\mathbb{Z} \oplus \mathbf{0}^{n-k}$. As in Section 2.3.2, this identifies $\mathbb{Z}/L$ with the complementary coordinate plane, $\mathbf{0}^k \oplus \mathbb{Z}^{n-k}$. Setting $\Psi := \psi^*$, the composition $\Phi \circ \Psi$ is the projection to the first k coordinates,

$$(12) \qquad \Phi \circ \Psi \;:\; (\mathbb{C}^\times)^n \; \longrightarrow\!\!\!\!\!\rightarrow \; (\mathbb{C}^\times)^k$$

and we identify $\mathbb{T}_J = 1^k \times (\mathbb{C}^\times)^{n-k}$ and $\mathbb{T}^I = (\mathbb{C}^\times)^k \times 1^{n-k}$.

3. Algorithms for Solving Sparse Decomposable Systems

We describe algorithms for solving sparse decomposable systems, and suggest an application of these algorithms to computing a start system to solve general systems (not necessarily decomposable) of sparse polynomials. They are based on numerical homotopy continuation [20]. By "solve a system of polynomials", we mean compute numerical approximations to the complex isolated solutions which may then be refined using Newton iterations. The expected numbers of isolated solutions to the systems we consider are mixed volumes as explained in the Bernstein-Kushnirenko Theorem. In principle, as the

systems are square and we know the expected number of isolated solutions, Smale's α-theory [24] enables approximations to solutions to be certified as approximate solutions in that Newton iterations converge quadratically to solutions, as explained in [13].

Let $\mathcal{A}_\bullet$ be a collection of supports with $\mathrm{MV}(\mathcal{A}_\bullet) > 0$, so that $\pi \colon X_{\mathcal{A}_\bullet} \to \mathbb{C}^{\mathcal{A}_\bullet}$ is a branched cover and let $F \in \mathbb{C}^{\mathcal{A}_\bullet}$. A *start system* for $\mathcal{A}_\bullet$ is a pair $(G, \mathcal{V}(G))$ where $G \in \mathbb{C}^{\mathcal{A}_\bullet}$ and $\mathcal{V}(G)$ consists of $\mathrm{MV}(\mathcal{A}_\bullet)$ distinct points. The convex combination of systems

(13) $$H(t) \;=\; tF + (1-t)G \qquad \text{for } t \;\in\; \mathbb{C} \,,$$

is a straight-line homotopy. Then $\mathcal{V}(H(t)) \subset (\mathbb{C}^\times)^{\mathcal{A}_\bullet} \times \mathbb{C}$ defines a curve C. Forgetting the x-coordinates gives a dominant map $C \to \mathbb{C}$. Restricting to points above $t \in [0,1]$ gives a family of arcs on C. Starting with the points of $\mathcal{V}(G)$ at $t = 0$, path-tracking along these arcs using $H(t)$ will give isolated solutions to $\mathcal{V}(F)$ at $t = 1$ when F is a regular value of π. This is an instance of a *(parameter) homotopy* [18, 21]. If F is not a regular value but $\mathcal{V}(F)$ is still finite, then $\mathcal{V}(F)$ may be computed using endgames [2, 16]. Problems of numerically tracking solutions are treated in [20, 25].

3.1. **Solving decomposable sparse systems.** We describe algorithms that use Esterov's conditions to solve a decomposable sparse polynomial system. In each, we let SOLVE be an arbitrary algorithm for solving a polynomial system. We assume that it is known that the system $F(x) = 0$ to be solved is general given its support $\mathcal{A}_\bullet$ in that it has $\mathrm{MV}(\mathcal{A}_\bullet)$ solutions in $(\mathbb{C}^\times)^n$. If not, then one instead solves a polynomial system with support $A_\bullet$ whose coefficients are random complex numbers. With probability one, this system is generic and one may use a homotopy together with endgames to compute the isolated solutions to $\mathcal{V}(F)$.

Our main algorithm (Algorithm 9) takes a sparse system and checks Esterov's criteria for decomposability. If the system is decomposable, the algorithm calls Algorithm 7 (if lacunary) or Algorithm 8 (if triangular), and in each of these algorithms calls to the solver SOLVE are assumed to be recursive calls back to Algorithm 9. If the polynomial system is indecomposable, then Algorithm 9 calls a black box solver BLACKBOX.

Recall from Section 2.2 the relation between the linear map $\varphi = \Phi^*$ and the group homomorphism $\Phi = \varphi^*$. Furthermore, recall the identification ι in (4).

Algorithm 7 (SolveLacunary).
  Input: *A general polynomial system $F(x) = 0$ whose support $\mathcal{A}_\bullet$ is lacunary.*
  Output: *All isolated solutions $\mathcal{V}(F) \subset (\mathbb{C}^\times)^n$.*
  Do:
   (1) *Compute a Smith normal form (8) of $\mathcal{A}_\bullet$, giving $\varphi = PD_n$, $\Phi = \varphi^*$, $\psi = P^{-1}$, and $\Psi = \psi^*$, so that $\Phi \circ \Psi$ is diagonal (9).*
   (2) *Use SOLVE to compute isolated solutions of $\iota(F)(x) = 0$ in $(\mathbb{C}^\times)^n$.*
   (3) *Using the formula (10) to compute $(\Phi \circ \Psi)^{-1}(y)$ for $y \in \mathcal{V}(\iota(F))$, return*

$$\{\Psi(w) \mid w \in \bigcup_{y \in \mathcal{V}(\iota(F))} (\Phi \circ \Psi)^{-1}(y)\} \,.$$

Proof of Correctness. By Lemma 5, $\mathcal{V}(F) = \Phi^{-1}(\mathcal{V}(\iota(F)))$. We apply Ψ to points of $(\Phi \circ \Psi)^{-1}(y)$ for $y \in \mathcal{V}(\iota(F))$ to obtain points of $\mathcal{V}(F)$ in their original coordinates. $\qquad\square$

Recall the notation $F_I \in \mathbb{C}^{\mathcal{A}_I}$ used in (7).

Algorithm 8 (SolveTriangular)**.**
   Input: *A general polynomial system $F(x) = 0$ whose support $\mathcal{A}_\bullet$ is triangular, witnessed by $0 < k < n$ such that $\mathrm{rank}(\mathbb{Z}\mathcal{A}_{[k]}) = k$.*
   Output: *All isolated solutions to $\mathcal{V}(F) \subset (\mathbb{C}^\times)^n$.*
   Do:

   (1) *Compute a Smith normal form (8) of $\mathcal{A}_{[k]}$, giving $\varphi = PI_k$, $\Phi = \varphi^*$, $\psi = P^{-1}$, and $\Psi = \psi^*$, so that $\Phi \circ \Psi$ is the projection (12).*
   (2) *Use **SOLVE** to compute isolated solutions to $F_{[k]}(x) = 0$ in $(\mathbb{C}^\times)^k$.*
   (3) *Choose $y_0 \in \mathcal{V}(F_{[k]})$. Use **SOLVE** to compute the points of the fiber $(\Phi \circ \Psi)^{-1}(y_0)$ in $Y_{\mathcal{A}_\bullet}$, which are $\mathcal{V}(\overline{F_J}) \subset \{y_0\} \times (\mathbb{C}^\times)^{n-k}$, where $\overline{F_J}(x) = 0$ has support $\overline{\mathcal{A}_J}$ and $J := [n] \setminus [k]$.*
   (4) *For each $y \in \mathcal{V}(F_{[k]})$ use a homotopy (13) with start system $\mathcal{V}(\overline{F_J})$ to compute $(\Phi \circ \Psi)^{-1}(y)$ and return*

$$\left\{ \Psi(w) \mid w \in \bigcup_{y \in \mathcal{V}(F_{[k]})} (\Phi \circ \Psi)^{-1}(y) \right\}.$$

Proof of Correctness. By Lemma 6, every solution $x \in \mathcal{V}(F)$ lies over a solution $y = \Phi(x)$ to $F_{[k]}(x) = 0$ in $(\mathbb{C}^\times)^k$. As explained in Section 2.4, the map $\Phi \circ \Psi$ is a coordinate projection and $(\Phi \circ \Psi)^{-1}(y) = \mathcal{V}(\overline{F_J})$. Here, $\overline{F_J} = (\overline{f_{k+1}}, \dots, \overline{f_n})$ where $\overline{f_j}$ has support $\overline{\mathcal{A}_j}$ and is computed using (11). We apply Ψ to convert these points to the original coordinates. $\qquad\square$

The previous two algorithms handle decomposable systems that are lacunary or triangular. We now state our main algorithm and later illustrate it in detail for a decomposable support $\mathcal{A}_\bullet$ in Example 13. We remark that our methods can be used as a preprocessing step for a black box solver.

Algorithm 9 (SolveDecomposable)**.**
   Input: *A generic polynomial system $F(x) = 0$ with support $\mathcal{A}_\bullet$.*
   Output: *All isolated solutions to $\mathcal{V}(F) \subset (\mathbb{C}^\times)^n$.*
   **Do:**

   (1) *Compute a Smith normal form PDQ (8) of $\mathcal{A}_\bullet$.*
        if $d_n > 1$, *then* **return** *SolveLacunary(F)*.
        if $d_n = 1$, *then*
           for all $\emptyset \neq I \subsetneq [n]$ *compute a Smith normal form PD_IQ (8) of $\mathcal{A}_I$.*
   (2)   **if** $\mathrm{rank}(D_I) = |I|$ *for some I, reorder so that $I = [k]$ and*
                return *SolveTriangular(F, k)*.
   (3)   **else** *neither of Esterov's conditions hold and* **return** *BLACKBOX(F)*.

Proof of Correctness. First note that if the algorithm halts, then it returns the isolated solutions of $F(x) = 0$. Halting is clear in Case (3), but the other cases involve recursive calls back to Algorithm 9. In Case (1), SolveLacunary will call Algorithm 9 on a system $\iota(F)(x) = 0$ whose mixed volume is less than $\mathrm{MV}(\mathcal{A}_\bullet)$. In Case (2), SolveTriangular will

call Algorithm 9 on systems $F_{[k]}(x) = 0$ and $\overline{F_J}(x) = 0$, each involving fewer variables than $F(x) = 0$. Thus, in each recursive call back to Algorithm 9, either the mixed volume or the number of variables decreases, which proves that the algorithm halts. $\square$

3.2. **Start Systems.** The Bézout homotopy [10] is a well-known homotopy for solving a system $F = (f_1, \ldots, f_n) = 0$ where each f_i is a general polynomial of degree d_i. In it, the start system is $G = (x_1^{d_1} - z_1, \ldots, x_n^{d_n} - z_n)$, and $\mathcal{V}(G) = \Phi^{-1}(z)$, where Φ is the diagonal map (9) and $\Phi^{-1}(z)$ is determined by inspection from (10). This start system is a highly decomposable sparse polynomial system consisting of supports which are subsets of the original support of $F(x) = 0$, but have the same mixed volume. We propose a generalization, in which Algorithm 9 is used to compute a start system.

Example 10. Suppose that we have supports $\mathcal{A}_1 = \mathcal{A}_2 = \mathcal{A}$, which are given by the columns of the matrix $\left(\begin{smallmatrix} 0 & 0 & 1 & 1 & 2 & 3 & 3 & 3 & 4 & 5 & 5 & 6 \\ 0 & 2 & 0 & 1 & 3 & 0 & 1 & 4 & 2 & 3 & 4 & 4 \end{smallmatrix} \right)$. Then $\mathrm{MV}(\mathcal{A}_1, \mathcal{A}_2) = \mathrm{vol}(\mathrm{conv}(\mathcal{A})) = 30$. Let $\mathcal{B}_1 = \mathcal{B}_2 = \left(\begin{smallmatrix} 0 & 0 & 3 & 3 & 6 \\ 0 & 2 & 0 & 4 & 4 \end{smallmatrix} \right)$ be the set of vertices of $\mathrm{conv}(\mathcal{A})$. Given a general $F \in \mathbb{C}^{\mathcal{A}_\bullet}$, let $G \in \mathbb{C}^{\mathcal{B}_\bullet} \subset \mathbb{C}^{\mathcal{A}_\bullet}$ be obtained from F by restriction to the monomials in $\mathcal{B}$. (That is, we set coefficients of monomials x^α in F to zero if $\alpha \notin \mathcal{B}$.) Then $\mathcal{B}_\bullet$ is lacunary with the map $\Phi(x_1, x_2) = (x_1^3, x_2^2)$, and $\iota(G)$ has five solutions, say $(z_i, w_i) \in \mathbb{C}^2$ for $i = 1, 2, .., 5$. The left, center, and right figures give the support of the polynomials appearing in the systems $F = 0$, $G = 0$, and $\iota(G) = 0$ respectively. (The blue and red dots correspond to monomials with a nonzero coefficient.)
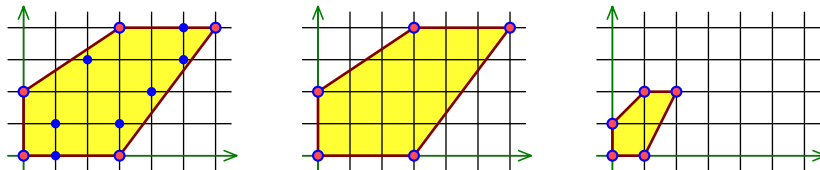
We may use Algorithm 9 (more specifically, Algorithm 7) to compute $\mathcal{V}(G)$. The thirty solutions to $G = 0$ are

$$(\sqrt[3]{z_i}, \sqrt{w_i}), \ (\eta\sqrt[3]{z_i}, \sqrt{w_i}), \ (\eta^2\sqrt[3]{z_i}, \sqrt{w_i}), \ (\sqrt[3]{z_i}, -\sqrt{w_i}), \ (\eta\sqrt[3]{z_i}, -\sqrt{w_i}), \ (\eta^2\sqrt[3]{z_i}, -\sqrt{w_i})$$

for $i = 1, 2, .., 5$ and where η is a primitive third root of unity. We compute the isolated solutions of $F(x) = 0$ using the homotopy

$$(14) \qquad\qquad H(t) = tF + (1-t)G$$

with start system $G = H(0)$ and tracking from the thirty solutions $\mathcal{V}(G)$ at $t = 0$. $\diamond$

Example 10 motivates our final algorithm. For a finite set $\mathcal{A} \subset \mathbb{Z}^n$, let $v(\mathcal{A}) \subset \mathcal{A}$ be the subset of vertices of $\mathrm{conv}(\mathcal{A})$. For a collection $\mathcal{A}_\bullet = (\mathcal{A}_1, \ldots, \mathcal{A}_n)$ of supports, let $v(\mathcal{A}_\bullet) := (v(\mathcal{A}_1), \ldots, v(\mathcal{A}_n))$. Note that if $G \in \mathbb{C}^{v(\mathcal{A}_\bullet)}$ is a regular value of the branched cover $\pi|_{X_{v(\mathcal{A}_\bullet)}} \colon X_{v(\mathcal{A}_\bullet)} \to \mathbb{C}^{v(\mathcal{A}_\bullet)}$ then G is also a regular value of $\pi \colon X_{\mathcal{A}_\bullet} \to \mathbb{C}^{\mathcal{A}_\bullet}$. As such, $G(x) = 0$ may be taken as a start system for the homotopy (14) and may be used to compute $\mathcal{V}(F)$ for any $F \in \mathbb{C}^{\mathcal{A}_\bullet}$ with $\mathcal{V}(F)$ finite. The benefit of this approach, as seen in Example 10, is that $\pi|_{X_{v(\mathcal{A}_\bullet)}}$ is more likely than π to be lacunary.

Algorithm 11 (Decomposable Start System).
   **Input:** *A set $\mathcal{A}_\bullet$ of supports.*
   Output: *A start system $(G, \mathcal{V}(G))$ for $\mathcal{A}_\bullet$.*
   Do:

   (1) *Choose a general system $G \in \mathbb{C}^{v(\mathcal{A}_\bullet)}$.*
   (2) *Compute $\mathcal{V}(G)$ using Algorithm 9.*
   (3) **return** *the pair $(G, \mathcal{V}(G))$.*

Proof of Correctness. As $G \in \mathbb{C}^{v(\mathcal{A}_\bullet)}$ is general, it has $\mathrm{MV}(v(\mathcal{A}_\bullet))$ solutions. Since for each i, $\mathrm{conv}(\mathcal{A}_i) = \mathrm{conv}(v(\mathcal{A}_i))$, we have $\mathrm{MV}(v(\mathcal{A}_\bullet)) = \mathrm{MV}(\mathcal{A}_\bullet)$. Finally, $\mathbb{C}^{v(\mathcal{A}_\bullet)}$ is the subspace of $\mathbb{C}^{\mathcal{A}_\bullet}$ where the coefficients of nonextreme monomials in each polynomial are zero. Thus $G \in \mathbb{C}^{\mathcal{A}_\bullet}$, which shows that $(G, \mathcal{V}(G))$ is a start system for $\mathcal{A}_\bullet$.   □

Remark 12. The Bézout homotopy motivated the idea behind Algorithm 11. However, if we apply Algorithm 11 to the system of supports $\mathcal{A}_\bullet$, where $\mathcal{A}_i$ is all monomials of degree at most d_i, then we will not get the start system for the Bézout homotopy. For example, when $n = 2$, $d_1 = 2$, and $d_2 = 3$, the supports are as shown.
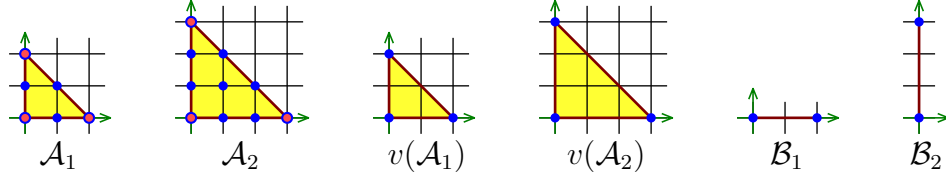

Here, $\mathcal{B}_1$ and $\mathcal{B}_2$ are the supports of the start system for the Bézout homotopy.

We leave open the challenge of finding a simple, general method to replace each set $\mathcal{A}_i$ by a subset $\mathcal{B}_i$ of $v(\mathcal{A}_i)$, so that $\mathrm{MV}(\mathcal{A}_\bullet) = \mathrm{MV}(\mathcal{B}_\bullet)$ and $\pi \colon X_{\mathcal{B}_\bullet} \to \mathbb{C}^{\mathcal{B}_\bullet}$ is decomposable. A possible first step would be to refine the methods of [5]. This may lead to a simpler start system for a homotopy to solve general systems with support $\mathcal{A}_\bullet$.   ◇

4. A COMPUTATIONAL EXPERIMENT

We explored the computational cost of using Algorithm 9 to solve sparse decomposable systems, comparing timings to PHCPack [28, 11] on a family of related systems.

Let $\mathcal{A}_1 = \left(\begin{smallmatrix} 0 & 1 & 2 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{smallmatrix} \right)$, $\mathcal{A}_2 = \left(\begin{smallmatrix} 1 & 0 & 1 & 2 & 1 \\ 0 & 1 & 1 & 1 & 2 \end{smallmatrix} \right)$, $\mathcal{B}_1 = \left(\begin{smallmatrix} 0 & 2 & 0 & 2 \\ 0 & 0 & 1 & 3 \end{smallmatrix} \right)$, and $\mathcal{B}_2 = \left(\begin{smallmatrix} 0 & 1 & 2 & 0 & 2 & 0 \\ 0 & 0 & 0 & 1 & 1 & 2 \end{smallmatrix} \right)$. We display these supports and their convex hulls below.
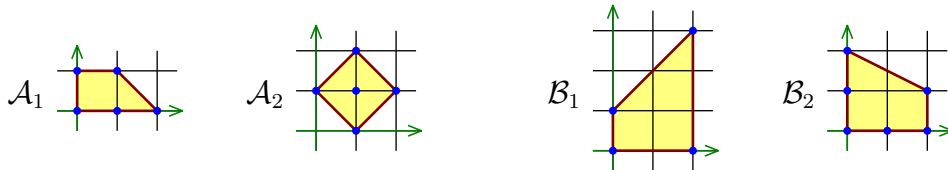
Let $\mathcal{C} := \{0, 1\}^5$ be the vertices of the five-dimensional cube. We construct sparse decomposable systems from $\mathcal{A}_\bullet := (\mathcal{A}_1, \mathcal{A}_2)$, $\mathcal{B}_\bullet := (\mathcal{B}_1, \mathcal{B}_2)$, and $\mathcal{C}$ as follows.

Choose two injections $\imath, \jmath \colon \mathbb{Z}^2 \to \mathbb{Z}^5$ such that $\imath(\mathbb{Z}^2) \cap \jmath(\mathbb{Z}^2) = \{0\}$. For example, choose four linearly independent vectors $\imath_1, \imath_2, \jmath_1, \jmath_2 \in \mathbb{Z}^5$, and define $\imath(a, b) = a\imath_1 + b\imath_2$, and the

same for $\jmath$. Let us set

$$\mathcal{A}(\imath, \jmath) := \big(\imath(\mathcal{A}_1), \imath(\mathcal{A}_2), \jmath(\mathcal{B}_1), \jmath(\mathcal{B}_2), \mathcal{C}\big).$$

Example 13. We now illustrate Algorithm 9 in detail on $\mathcal{A}(\imath, \jmath)$ by considering the case when $\imath_1, \imath_2, \jmath_1, \jmath_2$ are the first four standard unit vectors $e_1, \ldots, e_4$. Suppose $F = (f_1, f_2, g_1, g_2, h) = 0$ is a system of polynomials $\mathbb{C}[x_1, x_2, y_1, y_2, z]$ with support $\mathcal{A}(e_1, e_2, e_3, e_4)$. We use superscripts to distinguish different calls of the same algorithm. When $\texttt{SolveDecomposable}^{(1)}(F)$ is called, it first checks if F is lacunary (it is not as $\mathbb{Z}\mathcal{C} = \mathbb{Z}^5$), and then recognizes that F is triangular witnessed by (f_1, f_2). As such, it calls $\texttt{SolveTriangular}^{(1)}(F, 2)$ which computes the $\mathrm{MV}(\mathcal{A}_\bullet) = 5$ solutions $p_1, \ldots, p_5$ to $\mathcal{V}(f_1, f_2)$ with PHCPack, our choice of $\texttt{BLACKBOX}$.

As its penultimate task, $\texttt{SolveTriangular}^{(1)}$ computes a fiber of the first solution p_1 by performing the substitution $(x_1, x_2) = p_1$ in g_1, g_2 and h, and recursively calls $\texttt{SolveDecomposable}^{(2)}$ on the system $(g_1(p_1, y, z), g_2(p_1, y, z), h(p_1, y, z)) \in \mathbb{C}[y_1, y_2, z]$. This system is recognized to be triangular witnessed by (g_1, g_2) and $\texttt{SolveTriangular}^{(2)}(g_1, g_2)$ computes the $\mathrm{MV}(\mathcal{B}_\bullet) = 10$ solutions $q_1, \ldots, q_{10}$ using PHCPack. Next, $\texttt{SolveTriangular}^{(2)}$ computes a fiber above q_1 by performing the substitution $y = (y_1, y_2) = q_1$ in $h(p_1, y, z)$ producing the univariate polynomial $h(p_1, q_1, z)$ of degree 1 which has solution (p_1, q_1, z_1). Finally, $\texttt{SolveTriangular}^{(2)}$ performs a homotopy from q_1 to q_i to populate the fibers above each q_i. Thus $\texttt{SolveTriangular}^{(1)}$ populates the fiber above p_1 consisting of $10 \cdot 1 = 10$ solutions. As its final step, $\texttt{SolveTriangular}^{(1)}$ uses homotopies to take p_1 to p_i to populate all fibers producing all $5 \cdot 10 = 50$ solutions, $\mathcal{V}(F)$. $\diamond$

The overhead of this algorithm includes computing Smith normal forms and the search for subsets witnessing triangularity. Additionally, it often requires more path-tracking than a direct use of PHCPack. Nonetheless, the overhead seems to be nominal, and compared to the paths tracked in PHCPack, the paths tracked in our algorithm either involve fewer variables or polynomials of smaller degree.

For example, in Example 13, our algorithm called PHCPack to solve two sparse polynomial systems with 5 and 10 solutions respectively. A homotopy was called $10 - 1 = 9$ times on a system with 1 solution, then a different homotopy was called $5 - 1 = 4$ times on a system with 10 solutions. In total, $5 + 10 + 9 + 40 = 64$ individual paths were tracked. In contrast, a direct use of PHCPack involves tracking exactly $\mathrm{MV}(\mathcal{A}(e_1, e_2, e_3, e_4)) = 50$ paths, albeit in a higher dimensional space.

For more general $\imath$ and $\jmath$, the recursive structure of our computation is similar to Example 13. Some notable differences include

(1) $\imath(\mathcal{A}_\bullet)$ or $\jmath(\mathcal{B}_\bullet)$ may be lacunary which induces further decompositions.
(2) Monomial changes must be computed as $\imath(\mathcal{A}_\bullet)$ or $\jmath(\mathcal{B}_\bullet)$ could involve all variables.
(3) For most $\imath, \jmath$ the univariate polynomial obtained from h has degree 5 and is solved by computing eigenvalues of its companion matrix.

For example, if we choose $e_1 - e_2, e_2 - e_3, e_3 - e_4, e_4 - e_5$ for $\imath_1, \imath_2, \jmath_1, \jmath_2$, then again, no system encountered in the algorithm is lacunary, but the univariate polynomial obtained from h has support $\{0, 1, 2, 3, 4, 5\}$, so that $\mathrm{MV}(\mathcal{A}(\imath, \jmath)) = 250$.

In our computational experiment, we produced 10962 instances of $\mathcal{A}(\imath, \jmath)$ and solved each instance using our implementation of Algorithm 9 as well as with PHCPack. Due to ill-conditioning and heuristic choices of tolerances, some computations failed to produce all solutions. Such occurrences are not included in the data displayed below.

We give a scatter plot of the elapsed timings in Figure 1 with respect to the mixed volume of the system. Figure 2 displays box plots of the timings of each algorithm grouped by sizes of mixed volumes. The boxes range from the first quartile q_1 to the third quartile q_3 of the group data with whiskers extending to the smallest and largest data points which are not outliers. Outliers are the data points which are smaller than $q_1 - 1.5I$ or larger than $q_3 + 1.5I$ where I is the length of the interquartile range (q_1, q_3).
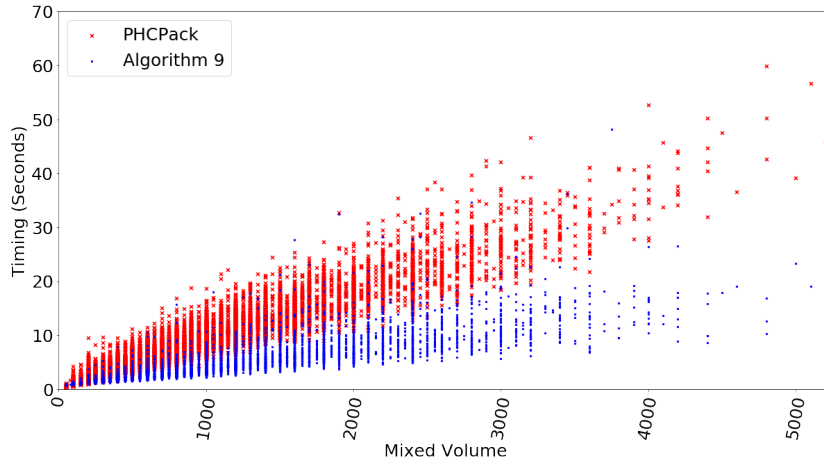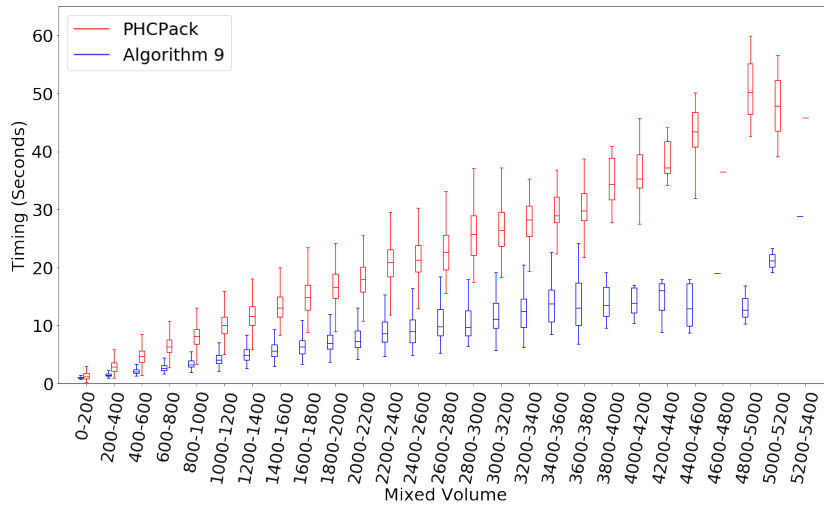

FIGURE 1. Scatter plot of timings

FIGURE 2. Box plot of timings

A more detailed account of these computations, along with our implementation in Macaulay2, may be found at the website for this paper [4].

References

1. C. Améndola and J. I. Rodriguez, *Solving parameterized polynomial systems with decomposable projections*, 2016, `arXiv:1612.08807`.
2. D. J. Bates, J. D. Hauenstein, and A. J. Sommese, *A parallel endgame*, Randomization, relaxation, and complexity in polynomial equation solving, Contemp. Math., vol. 556, Amer. Math. Soc., Providence, RI, 2011, pp. 25–35.
3. D. N. Bernstein, *The number of roots of a system of equations*, Funkcional. Anal. i Priložen. **9** (1975), no. 3, 1–4.
4. T. Brysiewicz, J.I. Rodriguez, F. Sottile, and T. Yahl, *Software for decomposable sparse polynomial systems*, 2020, `https://www.math.tamu.edu/~thomasjyahl/research/DSS/DSSsite.html`.
5. T. Chen, *Unmixing the mixed volume computation*, Discrete & Computational Geometry **62** (2019), 55–86.
6. H. Derksen and G. Kemper, *Computational invariant theory*, Invariant Theory and Algebraic Transformation Groups, I, Springer-Verlag, Berlin, 2002, Encyclopaedia of Mathematical Sciences, 130.
7. 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** (2019), no. 3, 1421–1446.
8. A. Esterov, *Galois theory for general systems of polynomial equations*, Compos. Math. **155** (2019), no. 2, 229–245.
9. G. Ewald, *Combinatorial convexity and algebraic geometry*, Graduate Texts in Mathematics, vol. 168, Springer-Verlag, New York, 1996.
10. C. B. Garcia and W. I. Zangwill, *Finding all solutions to polynomial systems and other systems of equations*, Mathematical Programming **16** (1979), no. 1, 159–176.
11. Elizabeth Gross, Sonja Petrović, and Jan Verschelde, *Interfacing with PHCpack*, J. Softw. Algebra Geom. **5** (2013), 20–25.
12. J. Harris, *Galois groups of enumerative problems*, Duke Math. Journal **46** (1979), no. 4, 685–724.
13. J. D. Hauenstein and F. Sottile, *Algorithm 921: alphacertified: certifying solutions to polynomial systems*, ACM Transactions on Mathematical Software (TOMS) **38** (2012), no. 4, 28.
14. C. Hermite, *Sur les fonctions algébriques*, CR Acad. Sci.(Paris) **32** (1851), 458–461.
15. B. Huber and B. Sturmfels, *A polyhedral method for solving sparse polynomial systems*, Math. Comp. **64** (1995), no. 212, 1541–1555.
16. B. Huber and J. Verschelde, *Polyhedral end games for polynomial continuation*, Numer. Algorithms **18** (1998), no. 1, 91–108.
17. A. G. Kušnirenko, *Newton polyhedra and Bezout's theorem*, Funkcional. Anal. i Priložen. **10** (1976), no. 3, 82–83.
18. T. Y. Li, T. Sauer, and J. A. Yorke, *The cheater's homotopy: an efficient procedure for solving systems of polynomial equations*, SIAM J. Numer. Anal. **26** (1989), no. 5, 1241–1251.
19. A. Martín del Campo-Sanchez, F. Sottile, and R. Williams, *Classification of Schubert Galois groups in $Gr(4,9)$*, `arXiv.org/1902.06809`, 2019.
20. A. P. Morgan, *Solving polynomial systems using continuation for engineering and scientific problems*, Prentice Hall, Inc., Englewood Cliffs, NJ, 1987.
21. A. P. Morgan and A. J. Sommese, *Coefficient-parameter polynomial continuation*, Appl. Math. Comput. **29** (1989), no. 2, part II, 123–160.
22. J. R. Munkres, *Topology: a first course*, Prentice-Hall, Inc., Englewood Cliffs, N.J., 1975.
23. G. P. Pirola and E. Schlesinger, *Monodromy of projective curves*, J. Algebraic Geom. **14** (2005), no. 4, 623–642.

24. S. Smale, *Newton's method estimates from data at one point*, The merging of disciplines: new directions in pure, applied, and computational mathematics, Springer, New York, 1986, pp. 185–196.
25. A. J. Sommese and C. W. Wampler, II, *The numerical solution of systems of polynomials*, World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ, 2005.
26. F. Sottile, R. Williams, and L. Ying, *Galois groups of compositions of Schubert problems*, `arXiv.org/1910.06843`, 2019.
27. R. Steffens and T. Theobald, *Mixed volume techniques for embeddings of Laman graphs*, Comput. Geom. **43** (2010), no. 2, 84–93.
28. J. Verschelde, *Algorithm 795: PHCpack: A general-purpose solver for polynomial systems by homotopy continuation*, ACM Trans. Math. Softw. **25** (1999), no. 2, 251–276, Available at http://www.math.uic.edu/~jan.
29. H. Wielandt, *Finite permutation groups*, Translated from the German by R. Bercov, Academic Press, New York-London, 1964.

T. Brysiewicz, Department of Mathematics, Texas A&M University, College Station, Texas 77843, USA
  Email address: `tbrysiewicz@math.tamu.edu`
  URL: `http://www.math.tamu.edu/~tbrysiewicz`

J. I. Rodriguez, Department of Mathematics, University of Wisconsin, Madison, WI 53706, USA
  Email address: `jRodriguez43@wisc.edu`
  URL: `http://www.math.wisc.edu/~jose/`

F. Sottile, Department of Mathematics, Texas A&M University, College Station, Texas 77843, USA
  Email address: `sottile@math.tamu.edu`
  URL: `http://www.math.tamu.edu/~sottile`

T. Yahl, Department of Mathematics, Texas A&M University, College Station, Texas 77843, USA
  Email address: `thomasjyahl@math.tamu.edu`
  URL: `http://www.math.tamu.edu/~thomasjyahl`