Manuscript, 16 February 2023

NUMERICAL NONLINEAR ALGEBRA

DANIEL J. BATES, PAUL BREIDING, TIANRAN CHEN, JONATHAN D. HAUENSTEIN, ANTON LEYKIN, AND FRANK SOTTILE

Abstract. Numerical nonlinear algebra is a computational paradigm that uses numerical analysis to study polynomial equations. Its origins were methods to solve systems of polynomial equations based on the classical theorem of Bézout. This was decisively linked to modern developments in algebraic geometry by the polyhedral homotopy algorithm of Huber and Sturmfels, which exploited the combinatorial structure of the equations and led to efficient software for solving polynomial equations.

Subsequent growth of numerical nonlinear algebra continues to be informed by algebraic geometry and its applications. These include new approaches to solving, algorithms for studying positive-dimensional varieties, certification, and a range of applications both within mathematics and from other disciplines. With new implementations, numerical nonlinear algebra is now a fundamental computational tool for algebraic geometry and its applications.

In honor of Bernd Sturmfels on his 60th birthday

1. Introduction

Bernd Sturmfels has a knack for neologisms, minting memorable mathematical terms that pithily portray their essence and pass into general use. Nonlinear algebra [65] is a Sturmfelian neologism expressing the focus on computation in applications of algebraic geometry, the objects that appear in applications, and the theoretical underpinnings this inquiry requires. Numerical nonlinear algebra is numerical computation supporting nonlinear algebra. It is complementary to symbolic computation (also a key input to nonlinear algebra), and its development has opened up new vistas to explore and challenges to overcome.

Sturmfels did not create this field, but his work with Huber introducing the polyhedral homotopy algorithm [50] catalyzed it. This algorithm exemplifies Sturmfels' mathematical contributions, exploiting links between algebra and geometric combinatorics to address problems in other areas of mathematics, in this case the ancient problem of solving equations. He was also important for its development with his encouragement of researchers, early decisive use of its methods [9, 91], and by popularizing it [12].

In Section 2 we describe polynomial homotopy continuation and its basic use to solve systems of polynomial equations. We develop the background and present some details of the polyhedral homotopy algorithm in Section 3. Numerical algebraic geometry, which uses these tools to represent algebraic varieties on a computer, is presented in Section 4, along with new methods for solving equations that this perspective affords. A welcome and perhaps surprising feature is that there are often methods to certify the approximate solutions these algorithms provide, which is sketched in Section 5. We close this survey by presenting three domains in which numerical nonlinear algebra has been applied in Section 6.

2. What is Polynomial Homotopy Continuation?

Polynomial Homotopy Continuation is a numerical method to compute complex-number solutions to systems of polynomial equations,

$$F(x_1,\ldots,x_n) \;=\; \begin{bmatrix} f_1(x_1,\ldots,x_n) \\ \vdots \\ f_m(x_1,\ldots,x_n) \end{bmatrix} \;=\; 0\,, \tag{1}$$

where $f_i(x_1,\ldots,x_n) \in \mathbb{C}[x_1,\ldots,x_n]$ for $1 \le i \le m$. A point $\mathbf{z} \in \mathbb{C}^n$ is a *regular zero* of F if $F(\mathbf{z}) = 0$ and the Jacobian matrix JF of F at $\mathbf{z}$ has rank n. Necessarily, $m \ge n$. When $m = n$, the system is *square* and the corresponding Jacobian matrix is a square $n \times n$ matrix.

The underlying idea is simple: to solve $F(\mathbf{x}) = 0$, we construct another system $G(\mathbf{x}) = 0$ of polynomial equations with known zeroes, together with a *homotopy*. This is a family of systems $H(\mathbf{x},t)$ for $t \in \mathbb{C}$ interpolating between F and G in that $H(\mathbf{x},0) = F(\mathbf{x})$ and $H(\mathbf{x},1) = G(\mathbf{x})$. Considering one zero, $\mathbf{y}$, of $G(\mathbf{x})$ and restricting to $t \in [0,1]$, $H(\mathbf{x},t) = 0$ defines a *solution path* $\mathbf{x}(t) \subset \mathbb{C}^n$ such that $H(\mathbf{x}(t),t) = 0$ for $t \in [0,1]$ and $\mathbf{x}(1) = \mathbf{y}$. The path is followed from $t = 1$ to $t = 0$ to compute the solution $\mathbf{z} = \mathbf{x}(0)$. This is equivalent to solving the initial value problem

$$\frac{\partial}{\partial \mathbf{x}} H(\mathbf{x},t)\left(\frac{\mathrm{d}}{\mathrm{d}t}\mathbf{x}(t)\right) + \frac{\partial}{\partial t} H(\mathbf{x},t) \;=\; 0\,, \qquad \mathbf{x}(1) \;=\; \mathbf{y}\,. \tag{2}$$

This *Davidenko differential equation* [23, 24] is typically solved using a standard predictor-corrector scheme (see Section 2.4). We say that $\mathbf{x}(1) = \mathbf{y}$ gets *tracked* towards $\mathbf{x}(0)$. For this to work, $\mathbf{x}(t)$ must be a regular zero of $H(\mathbf{x},t) = 0$ for every $t \in (0,1]$. Nonregular solutions at $t = 0$ are handled with specialized numerical methods called *endgames* [70].

So far, there is nothing special about polynomials—all we need is for F, G, and H to be analytic. However, when F is a system of polynomials, we can construct a *start system* G with known zeroes such that for every isolated zero $\mathbf{z}$ of F, there is at least one zero of G that gets tracked towards $\mathbf{z}$. That is, we may compute all isolated zeros of F.

García and Zangwill [38] proposed polynomial homotopy continuation and a classic reference is Morgan's book [67]. The textbook by Sommese and Wampler [84] is now a standard reference. Historically, the first implementation with wide acceptance was `PHCpack` [94], followed a decade later by `Bertini` [5], which is also widely used. Later came the `HOM4PS` family [20, 59], `NAG4M2` [60], and `HomotopyContinuation.jl` [14]. `NAG4M2` implements interfaces to many of these other packages, for example, see [39].

We will now explain polynomial homotopy continuation in more detail. We first discuss what is meant by *numerical method* and *solution* (a synonym for zero) of a system.

2.1. The solution to a system of polynomial equations.

A solution to the system (1) is a point $\mathbf{z} \in \mathbb{C}^n$ satisfying (1). The collection of all such points is an *algebraic variety*,

$$V \;=\; \{\mathbf{z} \in \mathbb{C}^n \mid f_1(\mathbf{z}) = \cdots = f_m(\mathbf{z}) = 0\}\,. \tag{3}$$

This defines solutions $\mathbf{z}$ *implicitly*, using just the definition of F. It is hard to extract any information other than "$\mathbf{z}$ is a solution to F" from this representation. A more useful representation of V is given by a *Gröbner basis* [91, 92].

Consider a simple example of two polynomial equations in two variables,

$$x^2 + y^2 - 1 \;=\; x^2 - y^3 - y - 1 \;=\; 0\,, \tag{4}$$

describing the intersection of two plane curves. A Gröbner basis is $\{y^3+y^2+y,\ x^2+y^2-1\}$. Its triangularity facilitates solving. The first equation, $y^3+y^2+y=0$, has the three solutions $0, (-1\pm\sqrt{-3})/2$. Substituting each into the second gives two solutions, for six solutions altogether. While these equations can be solved exactly, one cannot do this in general. A Gröbner basis is an equivalent implicit representation of V from which we may transparently extract numerical invariants such as the number of solutions or the dimension and degree of V. Finer questions about individual solutions may require computing them numerically.

Numerical methods only compute numerical approximations of solutions to a system (1). Thus $(1.271 + .341\sqrt{-1}\,,\ -.500 + .866\sqrt{-1})$ is an approximation of a solution to (4). A numerical approximation of a point $\mathbf{z} \in V$ is any point $\mathbf{y} \in \mathbb{C}^n$ which is in some sense close to $\mathbf{z}$. For example, we could require that $\mathbf{y}$ is within some tolerance $\epsilon > 0$ of $\mathbf{z}$, i.e., $|\mathbf{y}-\mathbf{z}| < \epsilon$. Consequently, the concept of zero of (or solution to) a polynomial system is replaced by an *approximate zero* (defined in Section 2.4). This is fundamentally different than using exact methods like Gröbner bases, where the goal is to handle the true exact zeros of polynomial systems. As an approximate zero is not a true zero, a numerical computation does not yield all the information obtained in an exact computation. On the other hand, a numerical computation is often less costly than a symbolic computation. Other advantages are that the architecture of modern computers is optimized for floating point arithmetic and that numerical continuation is readily parallelized (see Remark 4).

Despite not containing all the information of true zeroes, we discuss in Section 5 how to use approximate zeroes to obtain precise and provable results.

2.2. **The Parameter Continuation Theorem.** Our discussion of homotopy continuation assumed that solution paths exist. The *Parameter Continuation Theorem* by Morgan and Sommese [69] asserts this when the homotopy arises from a path in *parameter* space.

Suppose the system of polynomials (1) depends on k parameters $\mathbf{p} = (p_1, \ldots, p_k) \in \mathbb{C}^k$. Write $F(\mathbf{x};\mathbf{p})$ for the polynomial system corresponding to a particular choice of $\mathbf{p}$, and further suppose that the map $\mathbf{p} \mapsto F(\mathbf{x};\mathbf{p})$ is smooth. For example, the parameters may be the coefficients in F. Consider the incidence variety

$$Z \;=\; \{(\mathbf{x},\mathbf{p}) \in \mathbb{C}^n \times \mathbb{C}^k \mid F(\mathbf{x};\mathbf{p}) = 0\} \;\subseteq\; \mathbb{C}^n \times \mathbb{C}^k\,. \tag{5}$$

Let $\pi_1\colon Z \to \mathbb{C}^n$ and $\pi_2\colon Z \to \mathbb{C}^k$ be the projections onto the first and second factors. The map π_1 identifies points in the fiber $\pi_2^{-1}(\mathbf{p})$ with solutions to $F(\mathbf{x};\mathbf{p}) = 0$.

Theorem 1 (Parameter Continuation Theorem)**.** *For $\mathbf{p} \in \mathbb{C}^k$, let $N(\mathbf{p})$ be the number of regular zeroes of $F(\mathbf{x};\mathbf{p}) = 0$. There exists a proper algebraic subvariety $B \subset \mathbb{C}^k$ and a number N, such that $N(\mathbf{p}) \le N$ for $\mathbf{p} \in \mathbb{C}^k$ and $N(\mathbf{p}) = N$ when $\mathbf{p} \notin B$.*

Set $U := \mathbb{C}^k \smallsetminus B$ and suppose that $\gamma(t)\colon [0,1] \to \mathbb{C}^k$ is a continuous path. Write $\mathbf{p}_0 := \gamma(0)$.

(1) If $\gamma([0,1]) \subset U$, then the homotopy $F(\mathbf{x};\gamma(t))$ defines N continuous, isolated smooth solution paths $\mathbf{x}(t)$.

(2) If $\gamma((0,1]) \subset U$, then as $t \to 0$, the limits of the solution paths, if they exist, include all the isolated solutions to $F(\mathbf{x};\mathbf{p}_0) = 0$. This includes both regular solutions and solutions with multiplicity greater than one.

At points $t \in [0,1]$ with $\gamma(t) \in U$ where γ is differentiable, $\mathbf{x}(t)$ is differentiable.

The point of this theorem is that any path satisfying $\gamma((0,1]) \subset U$ can be used for homotopy continuation, so that $G(\mathbf{x}) = F(\mathbf{x};\gamma(1))$ is the start system. Since the *branch*

locus $B = \mathbb{C}^k \smallsetminus U$ is a subvariety, it has real codimension at least two and typical paths in the parameter space $\mathbb{C}^k$ do not meet B. Call $\pi_2 \colon Z \to \mathbb{C}^k$ a *branched cover*. Theorem 1 can be generalized, replacing the parameter space $\mathbb{C}^k$ by an irreducible variety [84, Theorem 7.1.4]. A *parameter homotopy* is one arising from a path γ such as in Theorem 1(2).

The Parameter Continuation Theorem follows from Bertini's Theorem, other standard results in algebraic geometry, and the implicit function theorem. A proof is given in [69].

Example 2. Figure 1 shows possibilities for homotopy paths $\mathbf{x}(t)$, when Theorem 1(2) holds. The start system $G(\mathbf{x})$ at $t = 1$ has $N = 5$ regular zeros, and each lies on a unique path

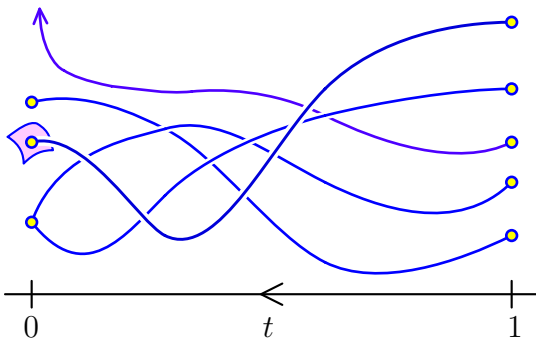


FIGURE 1. Homotopy Paths.

$\mathbf{x}(t)$ for $t \in (0, 1]$. One path has no finite limit as $t \to 0$, while the other four have limits. Two have unique limits; the endpoint of one at $t = 0$ is the regular zero of the target system $F(\mathbf{x})$, while the endpoint of the other is not an isolated zero of $F(\mathbf{x})$. Two paths have the same limit, and their common endpoint is an isolated zero of $F(\mathbf{x})$ of multiplicity two. $\diamond$

2.3. **The total degree homotopy.** To reach *all* isolated zeros of the target system, the start system must have at least as many zeros as the target system. Thus, an upper bound on the number of isolated zeros is often needed to choose a homotopy. One such upper bound is provided by Bézout's Theorem: The number of isolated zeros of the system $F = (f_1, \ldots, f_n)$ is at most $d_1 d_2 \cdots d_n$, where $d_i = \deg f_i$ for $i = 1, \ldots, n$. It inspires start systems of the form

$$\begin{bmatrix} b_0 x_1^{d_1} - b_1 \\ \vdots \\ b_0 x_n^{d_n} - b_n \end{bmatrix} . \tag{6}$$

For nonzero complex numbers $b_0, b_1, \ldots, b_n \in \mathbb{C} \smallsetminus \{0\}$, this start system is outside the branch locus B and it has $d = d_1 d_2 \cdots d_n$ solutions, which are all are easily computed. This gives the *total degree homotopy*,

$$H(x_1, \ldots, x_n, t) = t \cdot \begin{bmatrix} b_0 x_1^{d_1} - b_1 \\ \vdots \\ b_0 x_n^{d_n} - b_n \end{bmatrix} + (1-t) \cdot \begin{bmatrix} f_1(x_1, \ldots, x_n) \\ \vdots \\ f_n(x_1, \ldots, x_n) \end{bmatrix} . \tag{7}$$

Such a convex combination of two similar systems is called a *straight-line homotopy*. The straight line homotopy is a particular case of a parameter homotopy. For general choices of the parameters b_i the smoothness conditions of Theorem 1(2) hold [84, Thm. 8.4.1].

Example 3. The total degree homotopy for the system (4) has the form

$$H(x,y,t) = t \cdot \begin{bmatrix} b_0x^2 - b_1 \\ b_0y^3 - b_2 \end{bmatrix} + (1-t) \cdot \begin{bmatrix} x^2+y^2-1 \\ x^2-y^3-y-1 \end{bmatrix}. \tag{8}$$

For $b_0, b_1, b_2 \in \mathbb{C} \smallsetminus \{0\}$, the start system $H(x,y,1) = (b_0x^2 - b_1, b_0y^3 - b_2)$ has six distinct complex zeros, all of which are regular, and the zero set of $H(x,y,t)$ consists of six paths in $\mathbb{C}^2 \times [0,1]$, each smoothly parameterized by t for *almost all* choices of b_0, b_1, b_2. The parameter b_0 is used to avoid cancellation of the highest degree terms for $t \in (0,1]$. ◇

The phrase "almost all" in this example is because the set of choices of b_i for which the paths are singular (they meet the branch locus B of Theorem 1) has measure zero. Such situations occur frequently in this field, often referred to as *probability one*.

2.4. **Path-tracking.** Path-tracking is the numerical core of homotopy continuation.

Suppose that $H(\mathbf{x},t)$ for $\mathbf{x} \in \mathbb{C}^n$ and $t \in \mathbb{C}$ is a homotopy with target system $F(\mathbf{x}) = H(\mathbf{x},0)$ and start system $G(\mathbf{x}) = H(\mathbf{x},1)$. Further suppose that for $t \in (0,1]$, $H(\mathbf{x},t) = 0$ defines smooth paths $\mathbf{x}(t)\colon (0,1] \to \mathbb{C}^n$ such that each isolated solution to F is connected to at least one regular solution to G through some path, as in Theorem 1(2). By the Implicit Function Theorem, each isolated solution to G is the endpoint $\mathbf{x}(1)$ of a unique path $\mathbf{x}(t)$. Lastly, we assume that all regular solutions to G are known.

Given this, the isolated solutions to F may be computed as follows: For each regular solution $\mathbf{x}(1)$ to G, track the path $\mathbf{x}(t)$ from $t = 1$ towards $t = 0$. If it converges, then $\mathbf{x}(0) = \lim_{t\to 0} \mathbf{x}(t)$ satisfies $F(\mathbf{x}(0)) = 0$, and this will find all isolated solutions to F.

The path $\mathbf{x}(t)$ satisfies the Davidenko differential equation, and thus we may compute values $\mathbf{x}(t)$ by solving the initial value problem (2). Consequently, we may use any numerical scheme for solving initial value problems. This is not satisfactory for solving nonlinear polynomial systems due to the propagation of error.

As the solution paths $\mathbf{x}(t)$ are defined implicitly, there are standard methods to mitigate error propagation. Let E be a system of n polynomials. Given a point $\mathbf{z}_0$ where the Jacobian JE of E is invertible, we may apply the *Newton operator* N_E to $\mathbf{z}_0$, obtaining $\mathbf{z}_1$,

$$\mathbf{z}_1 \;:=\; N_E(\mathbf{z}_0) \;:=\; \mathbf{z}_0 - (JE(\mathbf{z}_0))^{-1} E(\mathbf{z}_0)\,. \tag{9}$$

We explain this: if we approximate the graph of the function E by its tangent plane at $(\mathbf{z}_0, E(\mathbf{z}_0))$, then $\mathbf{z}_1 \in \mathbb{C}^n$ is the unique zero of this linear approximation. There exists a constant $0 < c < 1$ such that when $\mathbf{z}_0$ is sufficiently close to a regular zero $\mathbf{z}$ of E, we have *quadratic convergence* in that

$$\|\mathbf{z}_1 - \mathbf{z}\| \;\leq\; c\|\mathbf{z}_0 - \mathbf{z}\|^2\,.$$

This is because $\mathbf{z}$ is a fixed point of N_E at which the derivative of N_E vanishes. The inequality follows from standard error estimates from Taylor's Theorem for N_E in a neighborhood of $\mathbf{z}$. A consequence is that when $\mathbf{z}_0$ is sufficiently close to a regular zero $\mathbf{z}$, each Newton iterate starting from $\mathbf{z}_0$ doubles the number of accurate digits. Such a point $\mathbf{z}_0$ is an *approximate zero* of F. This leads to algorithms to certify numerical output as explained in Section 5.

Predictor-corrector algorithms for solving the initial value problem for homotopy paths take a discretization $1 = t_0 > t_1 > \cdots > t_m = 0$ of the interval $[0,1]$ and iteratively compute approximations $\mathbf{x}(1) = \mathbf{x}(t_0), \mathbf{x}(t_1), \ldots, \mathbf{x}(t_m) = \mathbf{x}(0)$ to points on the solution path $\mathbf{x}(t)$. This requires an initial approximation $\mathbf{x}_0$ to $\mathbf{x}(t_0) = \mathbf{x}(1)$. Then, for $k = 0, \ldots, m-1$, given

an approximation $\mathbf{x}_k$ to $\mathbf{x}(t_k)$, a prediction $\hat{\mathbf{x}}_{k+1}$ for $\mathbf{x}(t_{k+1})$ is computed. This typically uses one step in an iterative method for solving the initial value problem (a local solver). This is the *predictor step*. Next, one or more Newton iterations N_E for $E(\mathbf{x}) = H(\mathbf{x}, t_{k+1})$ are applied to $\hat{\mathbf{x}}_{k+1}$ to obtain a new approximation $\mathbf{x}_{k+1}$ to $\mathbf{x}(t_{k+1})$. This is the *corrector step*. Predictor steps generally cause us to leave the proximity of the path being tracked; corrector steps bring us back. The process repeats until $k = m-1$.

There are a number of efficient local solvers for solving initial value problems. They typically use approximations to the Taylor series for the trajectory $\mathbf{x}(t)$ for t near t_k. For example, the Euler predictor uses the tangent line approximation,

$$\hat{\mathbf{x}}_{k+1} \;=\; \mathbf{x}_k + \Delta t_k \Delta \mathbf{x}_k \qquad \text{where} \qquad \frac{\partial H}{\partial \mathbf{x}}(\mathbf{x}_k, t_k) \cdot \Delta \mathbf{x}_k + \frac{\partial H}{\partial t}(\mathbf{x}_k, t_k) \;=\; 0\,.$$

Here, $\Delta t_k = t_{k+1} - t_k$ and $(\Delta x_k, 1)$ spans the kernel of the Jacobin $JH(\mathbf{x}_k, t_k)$.

Figure 2 illustrates an Euler prediction followed by Newton corrections. It suggests a

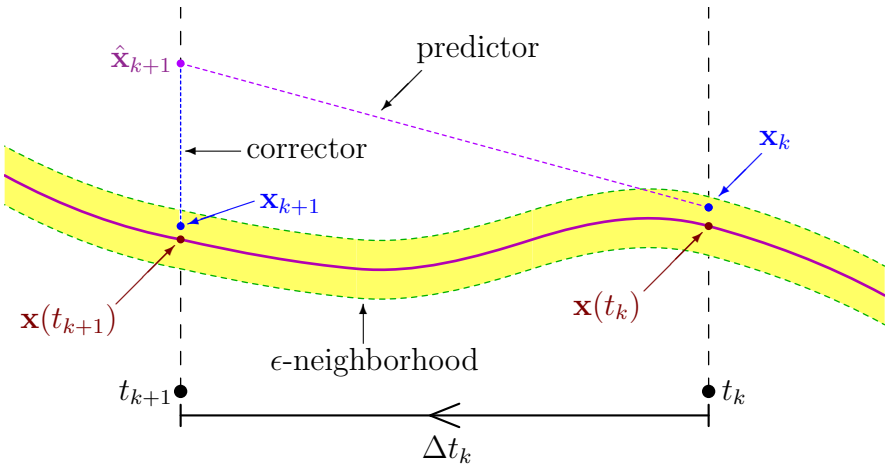


FIGURE 2. Euler prediction followed by Newton corrections. The image is adapted from [13] (we thank Sascha Timme for allowing us to use his figure).

stopping criterion for Newton iterations based on a fixed tolerance ϵ. Another is to apply Newton iterations until quadratic convergence is observed.

Remark 4. Since each solution path defined by $H(\mathbf{x}, t) = 0$ may be tracked independently, path-tracking is (in the words of Jan Verschelde) pleasingly parallelizable, which is a strength of polynomial homotopy continuation. ◇

We hardly mentioned the state of the art in path-tracking methods. There is a significant literature on other predictor-corrector schemes (see [16, Sections 15–18] for an overview), practical path-tracking heuristics [6, 93], and endgames for dealing with issues that arise near $t = 0$, such as divergent [68] or singular paths [70]. Indeed, the methods we describe suffice only for the most well-conditioned paths ending at regular solutions at $t = 0$.

2.5. **Squaring up.** It is common to need to solve *overdetermined systems*, which have more equations than variables. This presents a challenge as both the total degree homotopy of Section 2.3 and the polyhedral homotopy from the next section enable us to find all isolated solutions to a *square* system $F(\mathbf{x}) = 0$ of polynomial equations. Let us discuss an

example, and then explain the method of squaring up, which reduces the problem of solving overdetermined systems to that of solving square systems.

Example 5. Let A, B, C be the following 2×3 matrices,

$$A := \begin{pmatrix} 1 & 3 & 5 \\ 2 & 4 & 6 \end{pmatrix}, \qquad B := \begin{pmatrix} 2 & 3 & 7 \\ 2 & 5 & -11 \end{pmatrix} \quad \text{and} \quad C := \begin{pmatrix} 1 & -1 & 1 \\ -2 & 3 & -7 \end{pmatrix}.$$

We ask for the matrices of the form $D(x, y) := A + Bx + Cy$ that have rank 1. This is given by the vanishing of the three 2×2 minors of $D(x, y)$. This overdetermined system of equations in x, y has three solutions:

$$(-\tfrac{4}{5}, \tfrac{3}{5}), \ (-0.15019, 0.16729), \ (-0.95120, 2.8373). \tag{10}$$

We may find these using the total degree homotopy as follows. The determinants of the first two columns and the last two columns of $D(x, y)$ give a square subsystem of the system of three minors, and these have $4 = 2 \cdot 2$ solutions (the Bézout number). In addition to the three solutions in (10), the fourth is $(-13/14, 3/14)$. Let $f(x, y)$ be the remaining minor. Then $f(-13/14, 3/14) = -963/98$, while the three solutions in (10) evaluate (close to) zero. This is a simplification of the general scheme. ◇

Let F be an overdetermined system consisting of m polynomials in n variables, where $m > n$. *Squaring up* F replaces it by a square system $G(\mathbf{x}) := MF(\mathbf{x})$ as follows: Let M be a (randomly chosen) $n \times m$ complex matrix, so that $G(\mathbf{x})$ consists of n polynomials, each of which is a linear combination of polynomials in $F(\mathbf{x})$. Next, find all isolated solutions to $G(\mathbf{x}) = 0$. Since the solutions of $F(\mathbf{x}) = 0$ are among those of $G(\mathbf{x}) = 0$, we need only to determine the zeros of G which are not zeros of F. A simple way is to evaluate F at each of the zeros of G and discard those that do not evaluate to zero (according to some heuristic). It is numerically more stable to apply the Newton operator for the overdetermined system F [25] to the zeros of G and retain those which converge quadratically. Example 5 is a simplification, using a very specific matrix M rather than a randomly chosen matrix.

Remark 6. Suppose that the overdetermined system $F(\mathbf{x})$ depends on a parameter $\mathbf{p} \in \mathbb{C}^k$, i.e., we have $F(\mathbf{x}) = F(\mathbf{x}; \mathbf{p})$, and that for a general parameter $\mathbf{p} \in \mathbb{C}^k$ the system of equations $F(\mathbf{x}; \mathbf{p})$ has $N > 0$ isolated solutions (as in the Parameter Continuation Theorem 1). Suppose further that we have already computed all the solutions of $F(\mathbf{x}; \mathbf{p}_0) = 0$ for a fixed parameter $\mathbf{p}_0 \in \mathbb{C}^k$ (either by squaring up or by using another method). Then, we can use the Newton operator for overdetermined systems from [25] for homotopy continuation along the path $F(\mathbf{x}; t\mathbf{p}_0 + (1 - t)\mathbf{p})$ for any other parameter $\mathbf{p}$. ◇

3. Polyhedral homotopy

The total degree homotopy from Section 2.3 computes all isolated zeroes to any system of polynomial equations. Its main flaw is that it is based on the Bézout bound. Many polynomial systems arising in nature have Bézout bound dramatically larger than their number of zeroes; for these, the total degree homotopy will track many excess paths.

Example 7. Consider the following problem, posed in [26]: Find the distance from a point $\mathbf{x}^* \in \mathbb{R}^d$ to a hypersurface given by the vanishing of a single polynomial f. A first step

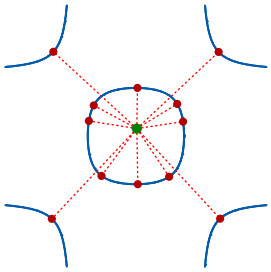
is to compute all critical points of the distance function $\|\mathbf{x}-\mathbf{x}^*\|$ for $f(\mathbf{x}) = 0$. We formulate this using a Lagrange multiplier λ,

$$f(\mathbf{x}) \;=\; 0 \qquad \text{and} \qquad \lambda(\mathbf{x}-\mathbf{x}^*) \;=\; \nabla f(\mathbf{x})\,.$$

When $d = 2$, $f = 5 - 3x_2^2 - 3x_1^2 + x_1^2x_2^2$, and $x^* = (0.025, 0.2)$, these become

$$5 - 3x_2^2 - 3x_1^2 + x_1^2x_2^2 \;=\; 0 \quad \text{and} \quad \lambda \begin{bmatrix} x_1 - 0.025 \\ x_2 - 0.2 \end{bmatrix} \;=\; \begin{bmatrix} -6x_1 + 2x_1x_2^2 \\ -6x_2 + 2x_1^2x_2 \end{bmatrix}, \tag{11}$$

which are polynomials in x_1, x_2, λ of degrees $4, 3, 3$, respectively. The system (11) has 12 solutions. We show the corresponding critical points below.



Note that a total degree homotopy for solving (11) follows $36 > 12$ homotopy paths. ◇

An alternative general-purpose homotopy is the *polyhedral homotopy* of Sturmfels and Huber. This is based on *Bernstein's bound*, which is at most the Bézout bound and at least the actual number of isolated zeros. Bernstein's bound is often significantly smaller than the Bézout bound, which makes the polyhedral homotopy an efficient tool for polynomial homotopy continuation because it produces fewer excess paths to track.

The *Polyhedral Homotopy Algorithm* is summarized in Algorithm 3.1 below. It is implemented in `PHCpack` [94], the `HOM4PS` family [20, 59], and `HomotopyContinuation.jl` [14]. To understand how it works we first develop some theory. We begin with Bernstein's bound.

3.1. **Bernstein's bound.** The polyhedral homotopy takes place on the complex torus $(\mathbb{C}^\times)^n$, where $\mathbb{C}^\times := \mathbb{C} \smallsetminus \{0\}$ is the set of invertible complex numbers. Each integer vector $\mathbf{a} \in \mathbb{Z}^n$ gives a *Laurent monomial* $\mathbf{x}^\mathbf{a} := x_1^{a_1} \cdots x_n^{a_n}$, which is a function on the torus $(\mathbb{C}^\times)^n$. A linear combination of Laurent monomials,

$$f \;:=\; \sum_{\mathbf{a}\in\mathcal{A}} c_\mathbf{a}\mathbf{x}^\mathbf{a} \qquad\qquad c_\mathbf{a} \in \mathbb{C}^\times\,,$$

is a *Laurent polynomial*. The (finite) index set $\mathcal{A} \subset \mathbb{Z}^n$ is the *support* of f. The convex hull of $\mathcal{A}$ is the *Newton polytope* of f. The polynomial f in Example 7 has support the columns of the matrix $\left(\begin{smallmatrix} 0 & 0 & 2 & 2 \\ 0 & 2 & 0 & 2 \end{smallmatrix}\right)$ and its Newton polytope is the 2×2 square, $[0, 2] \times [0, 2]$.

Bernstein's bound concerns square systems of Laurent polynomials, and it is in terms of mixed volume [31, pp. 116–118]. The *Minkowski sum* of polytopes P and Q in $\mathbb{R}^n$ is

$$P + Q \;:=\; \{\mathbf{x} + \mathbf{y} \mid \mathbf{x} \in P \text{ and } \mathbf{y} \in Q\}\,.$$

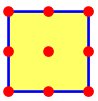
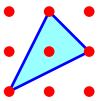
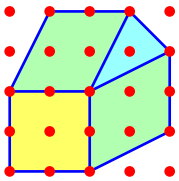
Given polytopes $P_1, \ldots, P_n$ in $\mathbb{R}^n$ and positive scalars $t_1, \ldots, t_n$, Minkowski proved that the volume $\operatorname{vol}(t_1P_1 + \cdots + t_nP_n)$ is a homogeneous polynomial in $t_1, \ldots, t_n$ of degree n. He defined

the *mixed volume* $\mathrm{MV}(P_1, \ldots, P_n)$ to be the coefficient of $t_1 \cdots t_n$ in that polynomial. While mixed volume is in general hard to compute, when $n = 2$, we have the formula

$$\mathrm{MV}(P, Q) \;=\; \mathrm{vol}(P + Q) - \mathrm{vol}(P) - \mathrm{vol}(Q)\,. \tag{12}$$

This formula and its generalizations to $n > 2$ are the *polarization identities*.

Consider (12) for the 2×2 square and triangle below.

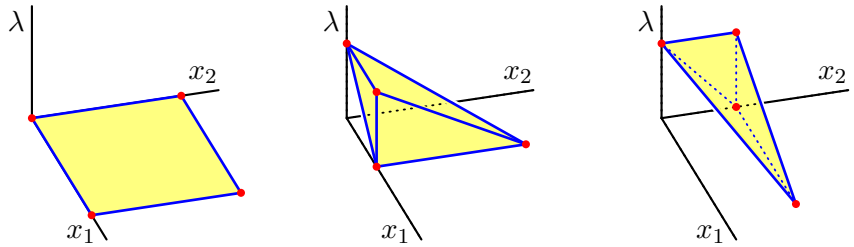
(13) $P \;=$  $Q \;=$  $P + Q \;=$ 

The final shape is the Minkowki sum $P + Q$, and the mixed volume $MV(P, Q)$ is the sum of the areas of the two (non-square) parallelograms, which is 8.

We give a version of Bernstein's Theorem [7, Thm. A].

Theorem 8 (Bernstein)**.** *Let $F = (f_1, \ldots, f_n)$ be a system of Laurent polynomials. The number of isolated solutions to F in $(\mathbb{C}^\times)^n$ is at most $\mathrm{MV}(P_1, \ldots, P_n)$, where for each $i = 1, \ldots, n$, P_i is the Newton polytope of the polynomial f_i.*

Example 9. We show the supports and Newton polytopes of the three polynomials from Example 7, f, $\lambda(x_1 - x_1^*) - \partial f/\partial x_1$, and $\lambda(x_2 - x_2^*) - \partial f/\partial x_2$ (see Equation (11)).



Their mixed volume is twelve, so the system (11) achieves the Bernstein bound. ◇

Bernstein proved that this bound is typically achieved in the following sense: For each $i = 1, \ldots, n$, let $\mathcal{A}_i$ be the support of polynomial f_i and P_i its Newton polytope. The set of polynomial systems $G = (g_1, \ldots, g_n)$ where each g_i has support a subset of $\mathcal{A}_i$ is a vector space V of dimension $|\mathcal{A}_1| + \cdots + |\mathcal{A}_n|$ whose coordinates are given by the coefficients of the polynomials g_i. Bernstein showed that there is a nonempty Zariski open subset $U \subset V$ consisting of systems G with exactly $\mathrm{MV}(P_1, \ldots, P_n)$ regular zeroes. Also, if U' is the (larger) set of systems G with exactly $\mathrm{MV}(P_1, \ldots, P_n)$ solutions, counted with multiplicity, then U' is open, and Bernstein [7, Thm. B] gave a criterion for when $G \in V \smallsetminus U'$.

We remark that Bernstein's bound and Bernstein's Theorem are often called the Bernstein-Kushnirenko-Khovanskii (BKK) bound and BKK Theorem due to their joint paper [8] and the circle of closely related work [7, 53, 55].

3.2. **Polyhedral homotopy of Huber and Sturmfels.** In their seminal work [50], Huber and Sturmfels developed a homotopy continuation method for solving systems of Laurent polynomials that takes advantage of Bernstein's bound in that it tracks only $\mathrm{MV}(P_1, \ldots, P_n)$ paths. Their work also provided a new interpretation for mixed volume in terms of mixed

cells (the parallelograms in (13)) and a new proof of Bernstein's Theorem [7, Thm. A]. We sketch its main ideas. This is also described in Sturmfels' award-winning Monthly article [90].

Suppose that $F = (f_1, \ldots, f_n)$ is a system of Laurent polynomials and that $\mathcal{A}_i$ is the support of f_i for $i = 1, \ldots, n$, so that

$$f_i \;=\; \sum_{\mathbf{a}\in\mathcal{A}_i} c_{i,\mathbf{a}}\mathbf{x}^{\mathbf{a}}\,, \quad \text{with } c_{i,\mathbf{a}} \in \mathbb{C}^\times\,. \tag{14}$$

For now, assume that F is sufficiently generic, in that F has $\mathrm{MV}(P_1, \ldots, P_n)$ regular zeroes.

In the polyhedral homotopy, the continuation parameter t appears in a very different way than in the total degree homotopy (7). First, the start system is at $t = 0$ and the target system F is at $t = 1$, but this is not the primary substantive difference. The polyhedral homotopy depends upon a choice of *lifting functions*, $\omega_i \colon \mathcal{A}_i \to \mathbb{Z}$, for $i = 1, \ldots, n$. That is, a choice of an integer $\omega_i(\mathbf{a})$ for each monomial $\mathbf{a}$ in $\mathcal{A}_i$. We address this choice later.

Given lifting functions, define the homotopy $H(\mathbf{x}, t) := (h_1, \ldots, h_n)$ by

$$h_i(\mathbf{x}, t) \;:=\; \sum_{\mathbf{a}\in\mathcal{A}_i} c_{i,\mathbf{a}}\,\mathbf{x}^{\mathbf{a}}\,t^{\omega_i(\mathbf{a})}\,.$$

By the Implicit Function Theorem and our assumption on F, over $t \in (0, 1]$ the system of equations $H(\mathbf{x}, t) = 0$ defines $\mathrm{MV}(P_1, \ldots, P_n)$ smooth paths. It is however not at all clear what happens as $t \to 0$. For example, $H(\mathbf{x}, 0)$ is undefined if some $\omega_i(\mathbf{a}) < 0$, and if $\omega_i(\mathbf{a}) > 0$ for all i and $\mathbf{a}$, then $H(\mathbf{x}, 0)$ is identically zero.

The key idea is to use an invertible linear change of coordinates to study the homotopy paths as $t \to 0$. This coordinate change depends upon a *weight* $\boldsymbol{\alpha} \in \mathbb{Z}^n$ and a positive integer r. The weight gives a *cocharacter* of the torus, for $s \in \mathbb{C}^\times$, $s^{\boldsymbol{\alpha}} := (s^{\alpha_1}, \ldots, s^{\alpha_n})$. Set

$$\mathbf{y} \;=\; \mathbf{x} \circ s^{-\boldsymbol{\alpha}} \;:=\; (x_1 s^{-\alpha_1}, \ldots, x_n s^{-\alpha_n})\,.$$

Then $\mathbf{x} = \mathbf{y} \circ s^{\boldsymbol{\alpha}}$, and we have $H^{(\boldsymbol{\alpha})}(\mathbf{y}, s) := (h_1^{(\boldsymbol{\alpha})}, \ldots, h_n^{(\boldsymbol{\alpha})})$, where for $i = 1, \ldots, n$,

$$h_i^{(\boldsymbol{\alpha})}(\mathbf{y}, s) \;:=\; s^{-\beta_i} h_i(\mathbf{y} \circ s^{\boldsymbol{\alpha}}, s^r) \;=\; \sum_{\mathbf{a}\in\mathcal{A}_i} c_{i,\mathbf{a}}\,\mathbf{y}^{\mathbf{a}}\,s^{\langle\boldsymbol{\alpha},\mathbf{a}\rangle + r\omega_i(\mathbf{a}) - \beta_i}\,, \tag{15}$$

where $\beta_i := \min\{\langle\boldsymbol{\alpha}, \mathbf{a}\rangle + r\omega_i(\mathbf{a}) \mid \mathbf{a} \in \mathcal{A}_i\}$. The purpose of β_i is to ensure that s appears in $h_i^{(\boldsymbol{\alpha})}(\mathbf{y}, s)$ with only non-negative exponents, and that $h_i^{(\boldsymbol{\alpha})}(\mathbf{y}, 0)$ is defined and not identically zero. Specifically, if $\mathcal{A}_i^{(\boldsymbol{\alpha})} := \{\mathbf{a} \in \mathcal{A}_i \mid \langle\boldsymbol{\alpha}, \mathbf{a}\rangle + r\omega_i(\mathbf{a}) = \beta_i\}$, then

$$h_i^{(\boldsymbol{\alpha})}(\mathbf{y}, 0) \;=\; \sum_{\mathbf{a}\in\mathcal{A}_i^{(\boldsymbol{\alpha})}} c_{i,\mathbf{a}}\mathbf{y}^{\mathbf{a}} \qquad \text{for } i = 1, \ldots, n\,. \tag{16}$$

The purpose of the positive integer r is to keep the exponents integral. As $r > 0$, we have that for $s \in [0, 1]$, $t = s^r \to 0$ if and only if $s \to 0$. Thus the role of r and s is to parameterize the homotopy path. We remark on this later.

We will see that for almost all $(\boldsymbol{\alpha}, r)$, $H^{(\boldsymbol{\alpha})}(\mathbf{y}, 0)$ has no zeroes, but for appropriately chosen $(\boldsymbol{\alpha}, r)$, the system $H^{(\boldsymbol{\alpha})}(\mathbf{y}, 0)$ has easily computed zeroes, each defining a homotopy path to a solution of $H^{(\boldsymbol{\alpha})}(\mathbf{y}, 1) = H(\mathbf{x}, 1)$. For such an $(\boldsymbol{\alpha}, r)$, $H^{(\boldsymbol{\alpha})}(\mathbf{y}, 0)$ is a *start subsystem*. The polyhedral homotopy algorithm consists of determining those $(\boldsymbol{\alpha}, r)$, solving the start subsystems $H^{(\boldsymbol{\alpha})}(\mathbf{y}, 0)$, and then tracking the homotopy paths from $t = 0$ to $t = 1$.

Before discussing this in more detail, including the role of the choices of lifting functions ω_i, cocharacter $\boldsymbol{\alpha}$, and positive integer r, let us consider an example.

Example 10. Let f_1 be the biquadratic from Example 7 and let $f_2 = 1 + 2x_1x_2 - 5x_1x_2^2 - 3x_1^2x_2$. Here, $\mathcal{A}_1 = \left(\begin{smallmatrix} 0 & 0 & 2 & 2 \\ 0 & 2 & 0 & 2 \end{smallmatrix}\right)$ and $\mathcal{A}_2 = \left(\begin{smallmatrix} 0 & 1 & 1 & 2 \\ 0 & 1 & 2 & 1 \end{smallmatrix}\right)$. Their Newton polygons are the square P and triangle Q in (13). Figure 3 shows their $8 = \mathrm{MV}(P, Q)$ common zeroes.

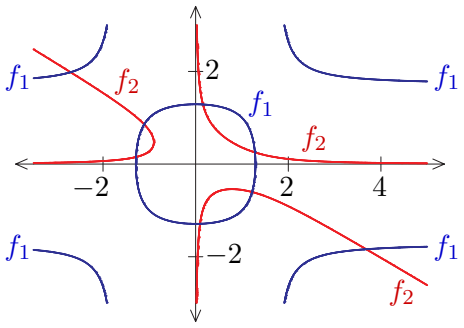


FIGURE 3. Common zeroes of f_1 and f_2.

Define ω_1 to be identically zero and set $\omega_2\left(\begin{smallmatrix} a \\ b \end{smallmatrix}\right) := a + b$. Then $h_1(\mathbf{x}, t) = f_1(\mathbf{x})$ and

$$h_2(\mathbf{x}, t) \;=\; 1 + 2x_1x_2t^2 - 5x_1x_2^2t^3 - 3x_1^2x_2t^3\,.$$

Let $\boldsymbol{\alpha} = (0, -3)$ and $r = 2$, so that $x_1 = y_1$ and $x_2 = y_2t^{-3}$. Then we may check that $\beta_1 = -6$ and $\beta_2 = \min\{0 - 0, 4 - 3, 6 - 6, 6 - 3\} = 0$, so that

$$\begin{aligned} h_1^{(\boldsymbol{\alpha})}(\mathbf{y}, s) &= \underline{-3y_2^2 + y_1^2y_2^2} \;+\; s^6(5 - 3y_1^2)\,, \\ h_2^{(\boldsymbol{\alpha})}(\mathbf{y}, s) &= \underline{1 - 5y_1y_2^2} \;+\; s(2y_1y_2 - 3y_1^2y_2s^2)\,. \end{aligned}$$

The underlined terms are the binomials $h_1^{(\boldsymbol{\alpha})}(\mathbf{y}, 0)$ and $h_2^{(\boldsymbol{\alpha})}(\mathbf{y}, 0)$. They have four solutions,

$$(\sqrt{3}, 75^{-\frac{1}{4}})\,,\;\; (\sqrt{3}, -75^{-\frac{1}{4}})\,,\;\; (-\sqrt{3}, 75^{-\frac{1}{4}})\,,\;\; (-\sqrt{3}, -75^{-\frac{1}{4}})\,.$$

These four solutions lead to four homotopy paths, which is fewer than the $8 = \mathrm{MV}(P, Q)$ paths defined by $H(\mathbf{x}, t) = 0$ over $t \in (0, 1]$.

If we let $\boldsymbol{\gamma} = (-3, 0)$ and $r = 2$, then

$$\begin{aligned} h_1^{(\boldsymbol{\gamma})}(\mathbf{y}, s) &= -3y_1^2 + y_1^2y_2^2 \;+\; s^6(5 - 3y_2^2)\,, \\ h_2^{(\boldsymbol{\gamma})}(\mathbf{y}, s) &= 1 - 3y_1^2y_2 \;+\; s(2y_1y_2 - 5y_1y_2^2s^2)\,, \end{aligned}$$

so that $h_1^{(\boldsymbol{\gamma})}(\mathbf{y}, 0)$ and $h_2^{(\boldsymbol{\gamma})}(\mathbf{y}, 0)$ are again binomials and they have four solutions

$$(27^{-\frac{1}{4}}, \sqrt{3})\,,\;\; (-27^{-\frac{1}{4}}, \sqrt{3})\,,\;\; (27^{-\frac{1}{4}}, -\sqrt{3})\,,\;\; (-27^{-\frac{1}{4}}, -\sqrt{3})\,.$$

These lead to the other four homotopy paths. The partition $4 + 4 = 8$ is seen in the decomposition of $P + Q$ in (13). The weight $\boldsymbol{\alpha}$ corresponds to the parallelogram on the upper left, which is the Minkowski sum of the supports of the components $h_1^{(\boldsymbol{\alpha})}(\mathbf{y}, 0)$ and $h_2^{(\boldsymbol{\alpha})}(\mathbf{y}, 0)$ of the start subsystem, and the weight $\boldsymbol{\gamma}$ corresponds to the parallelogram on the lower right. The only weights and positive integers for which the start subsystem has solutions are positive multiples of $(\boldsymbol{\alpha}, 2)$ and $(\boldsymbol{\gamma}, 2)$. ◇

3.3. **Computation of mixed cells.** In Example 10 only two choices of $(\boldsymbol{\alpha}, r)$ gave start subsystems $H^{(\boldsymbol{\alpha})}(\mathbf{y}, 0)$ with solutions. We now address the problem of computing the pairs $(\boldsymbol{\alpha}, r)$, such that $H^{(\boldsymbol{\alpha})}(\mathbf{y}, 0)$ has solutions. This leads to an algorithm that computes these pairs given the start system $F = (f_1, \ldots, f_n)$. We will show that the pairs $(\boldsymbol{\alpha}, r)$ which give zeros at $t = 0$ correspond to certain *mixed cells* in a decomposition of the Minkowski sum $P_1 + \cdots + P_n$, where P_i is the Newton polytope of f_i.

We examine the geometric combinatorics of the lifting functions ω_i, weights $\boldsymbol{\alpha}$, and positive integer r. Let $P \subset \mathbb{R}^{n+1}$ be a polytope. If P has the same dimension as its projection to $\mathbb{R}^n$, then it and all of its faces are *lower faces*. Otherwise, replace $\mathbb{R}^{n+1}$ by the affine span of P and assume that P has dimension $n+1$. A *lower facet* of P is a *facet* Q of P ($\dim Q = n$) whose inward-pointing normal vector has positive last coordinate. A *lower face* of P is any face lying in a lower facet. The union of lower faces forms the *lower hull* of P.

Let $\mathcal{A} \subset \mathbb{Z}^n$ be a finite set and $\omega\colon \mathcal{A} \to \mathbb{Z}$ be a lifting function. The *lift* of $\mathcal{A}$ is the set

$$\widehat{\mathcal{A}} \;:=\; \{(\mathbf{a}, \omega(\mathbf{a})) \mid \mathbf{a} \in \mathcal{A}\} \subset \mathbb{Z}^{n+1}\,.$$

Let $\widehat{P} := \operatorname{conv}(\widehat{\mathcal{A}})$ be its convex hull. Given a lower face Q of $\widehat{P}$, the projection to $\mathbb{Z}^n$ of $Q \cap \widehat{\mathcal{A}}$ is a subset $\mathcal{C}(Q)$ of $\mathcal{A}$ whose convex hull is the projection to $\mathbb{R}^n$ of Q. If $(\boldsymbol{\alpha}, r)$ is upward-pointing ($r > 0$) and $a \mapsto \langle \boldsymbol{\alpha}, \mathbf{a}\rangle + r\omega(\mathbf{a})$ achieves its minimum on Q, then $\mathcal{C}(Q) = \mathcal{A}^{(\boldsymbol{\alpha})}$.

For each $i = 1, \ldots, n$, let $\mathcal{A}_i \subset \mathbb{Z}^n$ be a finite set, $\omega_i\colon \mathcal{A}_i \to \mathbb{Z}$ be a lifting function, and set $\widehat{P}_i := \operatorname{conv}(\widehat{\mathcal{A}}_i)$. Let $\widehat{P} := \widehat{P}_1 + \cdots + \widehat{P}_n$ be their Minkowski sum. As $\widehat{P}$ is a Minkowski sum, if Q is a lower face of $\widehat{P}$, for each $i = 1, \ldots, n$ there is a lower face Q_i of $\widehat{P}_i$ with

$$Q \;=\; Q_1 + \cdots + Q_n\,. \tag{17}$$

Definition 11. Lifting functions $\omega_i\colon \mathcal{A}_i \to \mathbb{Z}$ for $i = 1, \ldots, n$ are *generic* if for each lower facet Q of P, if $Q_1, \ldots, Q_n$ are the lower faces in (17), then

$$\dim Q \;=\; n \;=\; \dim Q_1 + \cdots + \dim Q_n\,, \tag{18}$$

and when $\dim Q_i = 1$, then $\#Q_i \cap \widehat{\mathcal{A}}_i = 2$ and thus $\#\mathcal{C}(Q_i) = 2$.

A lower facet Q for which every Q_i in (18) has dimension 1 (and thus $\#Q_i \cap \widehat{\mathcal{A}}_i = 2$) is a *mixed facet* and its projection to $\mathbb{R}^n$ is a *mixed cell*. Mixed facets and mixed cells are parallelepipeds (Minkowski sums of independent line segments). ◇

Huber and Sturmfels show that almost all real lifting functions are generic and the density of rational numbers implies that there exist generic integral lifting functions. Setting $P_i := \operatorname{conv}(\mathcal{A}_i)$ for $i = 1, \ldots, n$, then the projection to $\mathbb{R}^n$ of the lower faces of $\widehat{P}$ forms a polyhedral subdivision of the Minkowski sum $P_1 + \cdots + P_n$, called a *mixed decomposition*.

This leads to a new interpretation for mixed volume.

Theorem 12 (Huber-Sturmfels)**.** *Suppose that $\omega_i\colon \mathcal{A}_i \to \mathbb{Z}$ for $i = 1, \ldots, n$ are generic lifting functions. Then the mixed volume $\operatorname{MV}(P_1, \ldots, P_n)$ is the sum of the volumes of the mixed cells in the induced polyhedral decomposition of the Minkowski sum $P_1 + \cdots + P_n$.*

Proof. These constructions—the lifts $\widehat{P}_i$, lower faces, and the mixed subdivision—scale multilinearly with positive $t_1, \ldots, t_n \in \mathbb{R}$. For example, a lower face $Q = Q_1 + \cdots + Q_n$ (17) of $\widehat{P}_1 + \cdots + \widehat{P}_n$ corresponds to a lower face $t_1Q_1 + \cdots + t_nQ_n$ of $t_1\widehat{P}_1 + \cdots + t_n\widehat{P}_n$. Let

$\pi\colon \mathbb{R}^{n+1} \to \mathbb{R}^n$ be the projection. This shows

$$\operatorname{vol}(t_1P_1 + \cdots + t_nP_n) \;=\; \sum_Q \operatorname{vol}(\pi(t_1Q_1 + \cdots + t_nQ_n))\,,$$

the sum over all lower facets Q. By Condition (18), $n = \dim(Q_1) + \cdots + \dim(Q_n)$, and thus

$$\operatorname{vol}(\pi(t_1Q_1 + \cdots + t_nQ_n)) \;=\; t_1^{\dim(Q_1)} \cdots t_n^{\dim(Q_n)} \operatorname{vol}(\pi(Q))\,.$$

Hence the coefficient of $t_1 \cdots t_n$ in $\operatorname{vol}(t_1P_1 + \cdots + t_nP_n)$ is the sum of the volumes of the mixed cells. □

Example 13. Let us consider this on our running example, using the lifts from Example 10. Figure 4 shows two views of the lower hull of the Minkowski sum $\widehat{P} + \widehat{Q}$, along with the mixed decomposition. Note that $\widehat{P} = P$ as the lifting function is 0 and $\widehat{Q}$ is

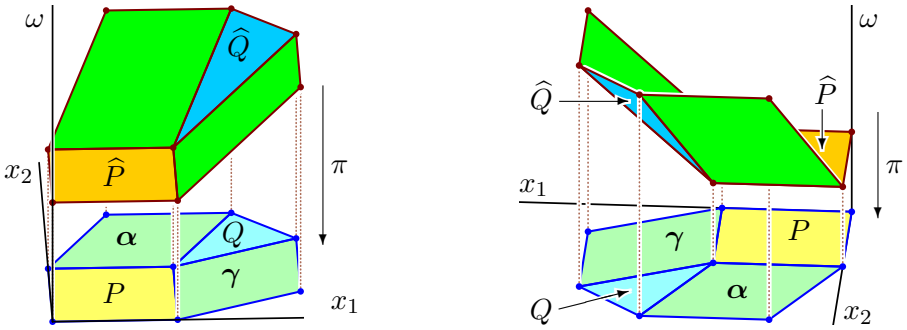


FIGURE 4. Two views of the lower hull of lift and mixed subdivision with mixed cells labeled by corresponding cocharacter.

affinely equivalent to Q. There are two mixed lower facets, whose corresponding mixed cells are the parallelograms of (13), showing them to be mixed cells of the mixed subdivision induced by these lifts. The dot product with $(\boldsymbol{\alpha}, 2) = (0, -3, 2)$ is minimized along the mixed lower facet $\operatorname{conv}\{(0,2,0),(2,2,0),(3,4,3),(1,4,3)\}$ with minimal value -6 and the dot product with $(\boldsymbol{\gamma}, 2) = (-3, 0, 2)$ is minimized along the mixed lower facet $\operatorname{conv}\{(2,0,0),(2,2,0),(4,3,3),(4,1,3)\}$ with minimal value -6. ◇

Keeping Example 13 in mind, we return to our problem of studying the homotopy given by generic lifting functions $\omega_i\colon \mathcal{A}_i \to \mathbb{Z}$ for $i = 1, \ldots, n$, for the supports of our target system (14). Let $\widehat{P} := \widehat{P}_1 + \cdots + \widehat{P}_n$ be the Minkowski sum of the convex hulls $\widehat{P}_i$ of the lifted supports $\widehat{\mathcal{A}}_i$. A vector $(\boldsymbol{\alpha}, r) \in \mathbb{Z}^{n+1}$ with $r > 0$ is *upward-pointing*, and the linear function $\langle(\boldsymbol{\alpha}, r), -\rangle$ it defines achieves its minimum on $\widehat{P}$ along a lower face Q—the lower face of $\widehat{P}$ *exposed* by $(\boldsymbol{\alpha}, r)$. When Q has the form (17), then for each $i = 1, \ldots, n$, Q_i is the lower face of $\widehat{P}_i$ exposed by $(\boldsymbol{\alpha}, r)$, and the minimum value of $\langle(\boldsymbol{\alpha}, r), -\rangle$ along Q_i is

$$\min\{\langle(\boldsymbol{\alpha}, r), (\mathbf{a}, \omega(\mathbf{a}))\rangle = \langle \boldsymbol{\alpha}, \mathbf{a}\rangle + r\omega(\mathbf{a}) \mid \mathbf{a} \in \mathcal{A}_i\} \;=\; \beta_i\,, \tag{19}$$

which explains the geometric significance of $(\boldsymbol{\alpha}, r)$ and of β_i. When Q is a facet, there is a unique primitive (components have no common factor) upward-pointing integer vector $(\boldsymbol{\alpha}, r)$ that exposes Q. In this case, $\mathcal{A}_i^{(\boldsymbol{\alpha})} = \pi(Q_i \cap \widehat{\mathcal{A}}_i) = \mathcal{C}(Q_i)$ is the support of $h^{(\boldsymbol{\alpha})}(\mathbf{y}, 0)$.

We explain the algebraic consequences. Suppose that $H^{(\boldsymbol{\alpha})}(\mathbf{y}, s)$ is the system of polynomials $h_i^{(\boldsymbol{\alpha})}(\mathbf{y}, s)$ defined by (15). Then $H^{(\boldsymbol{\alpha})}(\mathbf{y}, 0)$ is given by the polynomials $h_i^{(\boldsymbol{\alpha})}(\mathbf{y}, 0)$ of (16). If, for some i, $\#\mathcal{C}(Q_i) = 1$, so that $\dim Q_i = 0$, then $h_i^{(\boldsymbol{\alpha})}(\mathbf{y}, 0)$ is a monomial and therefore $H^{(\boldsymbol{\alpha})}(\mathbf{y}, 0)$ has no solutions in $(\mathbb{C}^\times)^n$.

Suppose that $H^{(\boldsymbol{\alpha})}(\mathbf{y}, 0)$ has solutions in $(\mathbb{C}^\times)^n$. Necessarily, $\dim Q_i \geq 1$ for all i. By (18), $\dim Q_i = 1$ and $\#\mathcal{C}(Q_i) = 2$ for all i, and thus Q is a mixed facet. Consequently, each $h_i^{(\boldsymbol{\alpha})}(\mathbf{y}, 0)$ is a binomial and $H^{(\boldsymbol{\alpha})}(\mathbf{y}, 0)$ is a system of independent binomials, which may be solved by inspection. Thus the only start subsystems $H^{(\boldsymbol{\alpha})}(\mathbf{y}, 0)$ with solutions are those for which $(\boldsymbol{\alpha}, r)$ exposes a mixed facet Q of $\widehat{P}$. The following proposition, whose proof is sketched in Section 3.5, records the number of solutions to such a mixed system.

Proposition 14. *The number of solutions to the system of binomials $H^{(\boldsymbol{\alpha})}(\mathbf{y}, 0)$ is the volume of the mixed cell $\pi(Q) = \operatorname{conv}(\mathcal{C}(Q_1) + \cdots + \mathcal{C}(Q_n))$.*

3.4. **The Polyhedral Homotopy Algorithm.** We sketch this algorithm and provide a brief argument about its correctness.

Algorithm 3.1: The Polyhedral Homotopy Algorithm

Input: A system $F = (f_1, \ldots, f_n)$ of n polynomials in n variables, where f_i has support $\mathcal{A}_i$ and Newton polytope P_i. The system F is assumed general and has $\operatorname{MV}(P_1, \ldots, P_n)$ regular solutions.

Output: All complex zeros of F.

Compute generic lifting functions $\omega_i \colon \mathcal{A}_i \to \mathbb{Z}$ (see Definition 11). They define a notion of mixed cell in the Minkowski sum $P = P_1 + \cdots + P_n$;

for *each mixed cell Q of P* **do**

  Compute the pair $(\boldsymbol{\alpha}, r)$ given as the primitive upward pointing normal of the mixed facet of $\widehat{P}$ that corresponds to Q.

  Solve the start subsystem $H^{(\boldsymbol{\alpha})}(\mathbf{y}, 0)$ and then use homotopy continuation to track those solutions along the homotopy $H^{(\boldsymbol{\alpha})}(\mathbf{y}, s)$ from $s = 0$ to $s = 1$, giving solutions to $H^{(\boldsymbol{\alpha})}(\mathbf{y}, 1)$.

end

The solutions computed in (2) to $H^{(\boldsymbol{\alpha})}(\mathbf{y}, 1) = H(\mathbf{x}, 1) = F(\mathbf{x})$ for all mixed cells are all the solutions to $F(\mathbf{x})$.

Sketch of Proof of Correctness. The system of equations $H(\mathbf{x}, t) = 0$ defines an algebraic curve C in $(\mathbb{C}^\times)^n \times \mathbb{C}_t^\times$ whose projection onto $\mathbb{C}_t^\times$ has degree equal to $\mathrm{MV} := \operatorname{MV}(P_1, \ldots, P_n)$ with the fiber over $t = 1$ having MV points. This curve has MV branches near $t = 0$, each of which is a point $\mathbf{z}(t)$ in $\mathbb{C}\{t\}^n$. Here, $\mathbb{C}\{t\}$ is the field of Puiseaux series, which contains the algebraic closure of the field $\mathbb{C}(t)$ of rational functions in t [78, Sect. 2.5.3]. Elements of $\mathbb{C}\{t\}$ may be represented by fractional power series of the form

$$\sum_{m \geq N} b_m t^{m/r},$$

where $m, N, r \in \mathbb{Z}$ with $r > 0$, and $b_m \in \mathbb{C}$. Observe that both the exponents of t and the denominators in those exponents are bounded below.

Fix a branch $\mathbf{z}(t)$ of C and let r be the least common denominator of all exponents of coordinates of $\mathbf{z}(t)$. Consider the lowest order terms of the coordinates in $\mathbf{z}(t)$,

$$(c_1 t^{\alpha_1/r}, \ldots, c_n t^{\alpha_n/r}),$$

where $\alpha_i \in \mathbb{Z}$ and $r \in \mathbb{N}$. Set $\boldsymbol{\alpha} := (\alpha_1, \ldots, \alpha_n)$. The substitution $t = s^r$ clears the denominators, converting $\mathbf{z}(t)$ to a vector $\mathbf{z}(s^r)$ of Laurent series in s. The coordinate change $\mathbf{z}(s^r) \circ s^{-\boldsymbol{\alpha}}$ converts these Laurent series to ordinary power series with constant coefficients $\mathbf{c} := (c_1, \ldots, c_n)$. Finally, $\mathbf{c}$ is a solution to the start subsystem $H^{(\boldsymbol{\alpha})}(\mathbf{y}, 0)$.

The point is that for each branch $\mathbf{z}(t)$ of C near $t = 0$, there is a weight $\boldsymbol{\alpha}$ and positive integer r such that the vector $\mathbf{c}$ of lowest order coefficients of $\mathbf{z}(t)$ is a solution to $H^{(\boldsymbol{\alpha})}(\mathbf{y}, 0)$. The discussion preceding the statement of the Polyhedral Homotopy Algorithm shows that $(\boldsymbol{\alpha}, r)$ exposes a mixed lower facet Q of $\widehat{P}$, and that $H^{(\boldsymbol{\alpha})}(\mathbf{y}, 0)$ has $\mathrm{vol}(\pi(Q))$ solutions. Furthermore, each solution $\mathbf{c}$ to $H^{(\boldsymbol{\alpha})}(\mathbf{y}, 0)$ may be developed into a power series solution $\mathbf{y}(s)$ to $H^{(\boldsymbol{\alpha})}(\mathbf{y}, s)$. Reversing the coordinate changes and reparameterization, this gives a solution $\mathbf{z}(t)$ to $H(\mathbf{x}, t) = 0$ in $(\mathbb{C}\{t\})^n$ and thus a branch of the curve C near $t = 0$.

Thus the homotopy paths for $H(\mathbf{x}, t)$ correspond to the MV distinct branches $\mathbf{z}(t)$ of C near $t = 0$ and the solutions computed in (3) give all MV solutions solutions to $F(\mathbf{x})$. □

Remark 15. The assumption that $F(\mathbf{x})$ is general in the Polyhedral Homotopy Algorithm ensures that $F(\mathbf{x})$ has MV regular solutions *and* that $H(\mathbf{x}, t)|_{t\in(0,1]}$ consists of MV smooth arcs. Thus, to solve a given system $F(\mathbf{x}) = (f_1, \ldots, f_n)$ where f_i has support $\mathcal{A}_i$, one first generates a general system $G = (g_1, \ldots, g_n)$ where g_i has support $\mathcal{A}_i$. In practice, this is done by choosing random complex numbers as coefficients, and then with probability one, $G(\mathbf{x})$ is general and satisfies the hypotheses of the Polyhedral Homotopy Algorithm. The Polyhedral Homotopy Algorithm is used to solve $G(\mathbf{x}) = 0$, and then a parameter homotopy with start system G and target system F is used to compute the solutions to $F(\mathbf{x}) = 0$. ◇

3.5. **Solving binomial systems.** To complete the discussion, we take a brief look at Step 6 in Algorithm 3.1. By construction, the subsystems $H^{(\boldsymbol{\alpha})}(\mathbf{y}, 0)$ in Step 6 are binomial systems. We explain how to solve such a system.

Suppose that $H(\mathbf{y})$ is a system of binomials

$$H(\mathbf{y}) = \begin{bmatrix} p_1 \mathbf{y}^{\mathbf{u}^{(1)}} - q_1 \mathbf{y}^{\mathbf{v}^{(1)}} & \ldots & p_n \mathbf{y}^{\mathbf{u}^{(n)}} - q_n \mathbf{y}^{\mathbf{v}^{(n)}} \end{bmatrix}$$

where each $p_i, q_i \neq 0$ and $\mathbf{u}^{(1)} - \mathbf{v}^{(1)}, \ldots, \mathbf{u}^{(n)} - \mathbf{v}^{(n)}$ are linearly independent. This is equivalent to the assertion that the Minkowski sum of the supports of the binomials is a parallelepiped $\pi(Q)$ of dimension n. Then for $\mathbf{y} \in (\mathbb{C}^\times)^n$, $H(\mathbf{y}) = 0$ becomes

$$\mathbf{y}^{\mathbf{u}^{(i)} - \mathbf{v}^{(i)}} = q_i/p_i \qquad \text{for } i = 1, \ldots, n. \tag{20}$$

Let A be the $n \times n$ matrix with rows $\mathbf{u}^{(1)} - \mathbf{v}^{(1)}, \ldots, \mathbf{u}^{(n)} - \mathbf{v}^{(n)}$. Then $\det A = \mathrm{vol}(\pi(Q))$. The *Smith normal form* of A consists of unimodular integer matrices X, Y (integer matrices with determinant 1) and a diagonal matrix $D = \mathrm{diag}(d_1, \ldots, d_n)$ such that $XAY = D$ and thus $\det A = \det D = d_1 \cdot d_2 \cdots d_n$. The unimodular matrices X and Y give coordinate changes on $(\mathbb{C}^\times)^n$ which convert the system (20) into a diagonal system of the form

$$x_i^{d_i} = b_i \qquad \text{for } i = 1, \ldots, n.$$

All $d_1 \cdots d_n$ solutions may be found by inspection, and then the coordinate changes may be reversed to obtain all solutions to the original system $H(\mathbf{y})$.

4. Numerical Algebraic Geometry

We have described methods to compute all isolated solutions to a system of polynomial equations. *Numerical algebraic geometry* uses this ability to compute zero-dimensional algebraic varieties to represent and manipulate higher-dimensional algebraic varieties on a computer. This is an essential component of numerical nonlinear algebra. Besides expanding the reach of numerical methods, the geometric ideas behind numerical algebraic geometry have led to new methods for solving systems of polynomial equations, including regeneration and monodromy. While the term was coined in [81], the fundamental ideas were developed in a series of papers including [80, 82], and a more thorough treatment is in [84, Part III].

Example 16. Consider the following square system of polynomials in the variables x, y, z:

$$F(x,y,z) \;=\; \begin{bmatrix} f(x,y,z)g(x,y,z)(x-4)(x-6) \\ f(x,y,z)g(x,y,z)(y-3)(y-5) \\ f(x,y,z)(z-2)(z-5) \end{bmatrix}, \tag{21}$$

where

$$f(x,y,z) \;=\; \tfrac{1}{40}(2xy - x^2) - z - 1 \qquad \text{and} \qquad g(x,y,z) \;=\; x^4 - 4x^2 - y - 1\,.$$

Figure 5 shows the real part of the variety V of $F(x,y,z) = 0$, consisting of a quadric (degree 2) surface, two quartic (degree 4) curves (at $z = 2$ and $z = 5$, respectively), and eight points. The surface is in blue, the two curves in red, and the eight points in green. ⋄

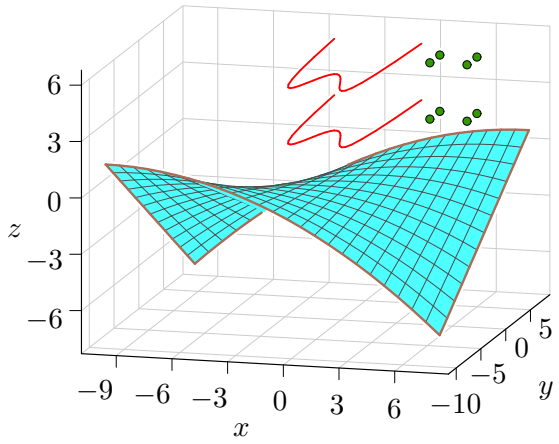


Figure 5. A reducible variety, defined implicitly by (21).

Given any system $F(\mathbf{x})$ defining a reducible variety V, implemented symbolic algorithms (primary decomposition and computing radicals) will decompose the variety V as follows. These methods will compute a list $I_1, \ldots, I_r$, where each I_i is the ideal of an irreducible component V_i of V. Each ideal I_i is represented by a Gröbner basis, which is a finite set of generators, and thus serves as a data structure encoding information about V_i. For example, the dimension and degree of a component V_i may be computed from the data I_i.

In numerical algebraic geometry, the data structure to represent a positive-dimensional component of a variety is a witness set. Suppose that $F(\mathbf{x})$ is a system of polynomials, and let V be an irreducible component of the variety defined by $F(\mathbf{x}) = 0$. A *witness*

set W for the component V is a triple $W = (F, L, L \cap V)$, where L is a general linear subspace complimentary to V in that $\operatorname{codim}(L) = \dim(V)$ and $L \cap V$ consists of numerical approximations of the points in the intersection of L and V. Generality (see Section 4.1) ensures that the *linear slice* $L \cap V$ is transverse and consists of $\deg(V)$ points. In practice, L is represented by $\dim(V)$ randomly chosen polynomials of degree one.

The simple algorithm of *membership testing* illustrates the utility of this data structure. Given a witness set $W = (F, L, L \cap V)$ for an irreducible variety $V \subset \mathbb{C}^n$ and a point $\mathbf{x}_0 \in \mathbb{C}^n$, we would like to determine if $\mathbf{x}_0 \in V$. Evaluating F at $\mathbf{x}_0$ only implies that $\mathbf{x}_0$ lies near the variety defined by F, not that it lies near the irreducible component V. We instead choose a general linear subspace L' with the same codimension as L, but for which $\mathbf{x}_0 \in L'$ (that is, L' is otherwise general, given that $\mathbf{x}_0 \in L'$). Next, form the *linear slice homotopy*,

$$H(\mathbf{x}, t) \;:=\; (F(\mathbf{x}),\, tL(\mathbf{x}) + (1-t)L'(\mathbf{x}))\,, \tag{22}$$

and use it to track the points of $L \cap V$ from $t = 1$ to $t = 0$, obtaining the points of $L' \cap V$. As the intersection of V with the other components of the variety of F has lower dimension than V, and its complement in V is path-connected, $\mathbf{x}_0$ lies in $L' \cap V$ if and only if $\mathbf{x}_0 \in V$.

The core of this membership test reveals another algorithm involving witness sets. Given a witness set $W = (F, L, L \cap V)$ and a general linear subspace L' with the same codimension as L, the step of following the points of $L \cap V$ along the homotopy (22) to obtain the points $L' \cap V$ is called *moving a witness set*. This is because $W' = (F, L', L' \cap V)$ is a new witness set for V. This may also be considered to be an algorithm for sampling points of V.

The rest of this section discusses algorithms for computing a witness set and the corresponding numerical irreducible decomposition of a variety V. It concludes with a summary of regeneration and monodromy, two new methods for solving systems of polynomials.

Remark 17. The set of points in the linear slice $L \cap V$ is considered a concrete version of André Weil's generic points of a variety [95]. We call it *witness point set*.

A witness point set is related to Chow groups from intersection theory [36]. Indeed, a witness set for an irreducible variety V may be interpreted as a specific way to represent the class of V in the Chow ring of $\mathbb{P}^n$. In [86] this point of view was used to extend witness sets to represent subvarieties of varieties other than $\mathbb{P}^n$.

4.1. **More on linear slices.** An irreducible algebraic subvariety V of affine or projective space has two fundamental invariants—its *dimension*, $\dim(V)$, and its *degree*, $\deg(V)$. The dimension of V is the dimension of its (dense subset of) smooth points, as a complex manifold. Equivalently, this is the dimension of its tangent space at any smooth point.

By Bertini's theorem [78, Thm. 2, §6.2], there is a dense Zariski-open subset of (affine) linear spaces L of codimension $\dim(V)$ such that the linear slice $L \cap V$ is transverse. Here, a codimension d linear subspace is defined by d independent degree one polynomials. The degree of V is the maximal number of points in such an intersection. By Bertini again, this maximum is achieved by linear spaces lying in Zariski open subset of linear subspaces.

In practice, L is represented by $\dim(V)$ random degree one polynomials (their coefficients are chosen randomly). By the nature of Zariski open sets, for most reasonable probability distributions on these coefficients, a suitably general L will be found with probability one.

When the variety V defined by the vanishing of $F(\mathbf{x})$ is reducible and the maximum dimension of an irreducible component is d, then a randomly-chosen linear subspace L of codimension d will meet each irreducible component V' of V of dimension d in $\deg(V')$ points

$L \cap V'$, and it will not intersect any components of V of dimension less than d. If V' is the unique component of dimension d, then $(F, L, L \cap V')$ is a witness set for V'.

Example 18. We continue Example 16. To compute the linear slice $L \cap V$ with the line L parameterized by $(t, -t-2, -3+t/4)$, we add to F two degree one polynomials $x+y+2$ and $z+3-x/4$. The augmented system defines the intersection $L \cap V$. It has two solutions $(10/3, -16/3, -13/6)$ and $(-8, 6, -5)$. The line L is sufficiently general so that it only meets the two-dimensional surface defined by $f(x, y, z)$, and neither of the curves nor any isolated points. Figure 6 shows this configuration. ◇

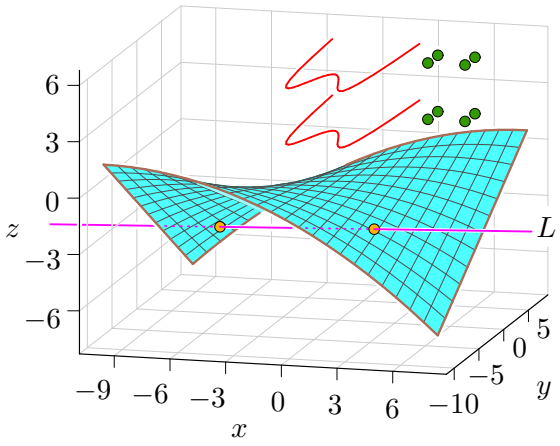


FIGURE 6. Slice of V by a line L.

While finding a witness point set for the top-dimensional component of V in Example 18 was straightforward, finding witness point sets for the other components is not as simple. To find points on curves, we intersect V with the vertical plane P defined by $x+y-2=0$, finding eight isolated solutions. These come from the two curves of degree four, each contributing four points. This number eight does not yet tell us that there are two curves, there may be a single curve of degree eight or some other configuration. Furthermore, the plane intersects the surface in a curve C, and we may have found additional non-isolated points on C. This is displayed in Figure 7. Methods to remove points on higher-dimensional components and to determine which points lie on which components of the same dimension are described in the next subsection.

4.2. **Numerical irreducible decomposition.** A system $F(\mathbf{x})$ of polynomials in n variables defines the algebraic variety $V := \{\mathbf{x} \in \mathbb{C}^n \mid F(\mathbf{x}) = 0\}$. Were V irreducible, a witness set would be an acceptable representation for V. An analog when V is reducible is a *numerical irreducible decomposition* of V. This data structure for representing V consists of a collection of witness sets $(F, L', L' \cap V')$, one for each irreducible component V' of V. We present a

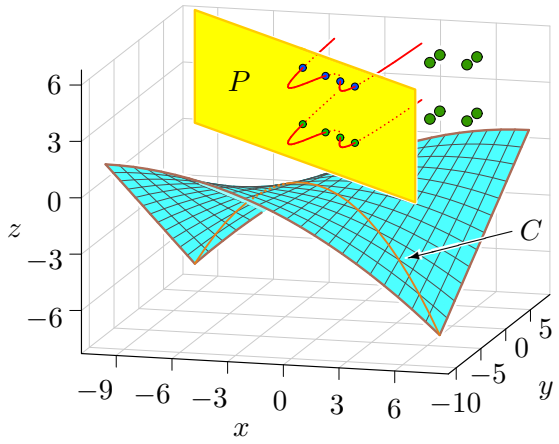


FIGURE 7. The plane P intersects V in eight isolated points and a curve C.

numerical irreducible decomposition for our running example:

$$\big(F, [x{+}y{+}2, z{+}3{-}\tfrac{x}{4}], \{(\tfrac{10}{3}, -\tfrac{16}{3}, -\tfrac{13}{6}), (-8, 6, -5)\}\big)$$
$$(F, [x{+}y{+}2], \{(-2.06, 0.06, 2), (-0.40, -1.60, 2), (0.69, -2.69, 2), (1.76, -3.76, 2)\}) \ ,$$
$$(F, [x{+}y{+}2], \{(-2.06, 0.06, 5), (-0.40, -1.60, 5), (0.69, -2.69, 5), (1.76, -3.76, 5)\}) \ ,$$
$$(F, [], \{(4, 3, 2)\}) \ , \ (F, [], \{(4, 3, 5)\}) \ , \ (F, [], \{(4, 5, 2)\}) \ , \ (F, [], \{(4, 5, 5)\}) \ ,$$
$$(F, [], \{(6, 3, 2)\}) \ , \ (F, [], \{(6, 3, 5)\}) \ , \ (F, [], \{(6, 5, 2)\}) \ , \ (F, [], \{(6, 5, 5)\}) \ .$$

We later present the *Cascade Algorithm* 4.2 to compute a numerical irreducible decomposition. We first explain its constituents.

4.2.1. *Witness point supersets.* A starting point is to compute, for each i, a set of points U_i in a linear slice $L \cap V$ of V with a codimension i linear space L, where U_i contains all witness point sets $L \cap V'$ for V' an irreducible component of dimension i. For this, let $\ell_1, \ldots, \ell_{n-1}$ be randomly chosen (and hence independent) degree one polynomials. For each i, let L^i be defined by $\ell_1, \ldots, \ell_i$, and let F_i be a subsystem of F consisting of $n - i$ randomly chosen linear combinations of elements of F. Then $(F_i, \ell_1, \ldots, \ell_i)$ is a square subsystem of (F, L^i), and we may use it to compute points U_i that lie in $L^i \cap V$, as explained in Section 2.5.

By the generality of $\ell_1, \ldots, \ell_{n-1}$, there will be no solutions to $(F_i, \ell_1, \ldots, \ell_i)$ when i exceeds the dimension d of V. (This is another application of Bertini's theorem.) By the same generality, the set U_i contains witness point sets for each irreducible component of V of dimension i, and perhaps some points on irreducible components of V of larger dimension. The next two sections describe how to remove points of U_i that lie on components of V of dimension exceeding i, and then how to decompose such an equidimensional slice into witness point sets for the irreducible components of V of dimension i.

4.2.2. *Removing points on higher-dimensional components.* Suppose that we have computed $U_0, U_1, \ldots, U_d$, where d is the dimension of V as in Section 4.2.1. By the generality of $\ell_1, \ldots, \ell_d$, U_d is equal to the linear slice $L^d \cap V$, and thus is the union of witness point sets for the irreducible components of V of dimension d. For each $i = 0, \ldots, d$, let V_i be the union of all irreducible components of V of dimension i. Then $W_i := L^i \cap V_i \subset U_i$ consists of points

in U_i lying on some component of V of dimension i. This union of the witness point sets of i-dimensional components of V is an *equidimensional slice*. Also, note that $W_d = U_d$.

Since points of $U_i \smallsetminus W_i$ lie on $V_{i+1}, \ldots, V_d$, downward induction on i and the membership test computes $U_i \smallsetminus W_i$ and thus W_i. This uses the observation that the membership test, starting with $W_j = L^j \cap V_j$, may be used to determine if a point $\mathbf{x}_0 \in U_i$ lies on V_j, for any $j > i$. This is invoked in Step 7 in Algorithm 4.1 for computing such equidimensional slices.

Algorithm 4.1: Computing equidimensional slices

1 **Input:** $F(\mathbf{x})$, $\ell_1, \ldots, \ell_d$, $U_1, \ldots, U_d$ as above.
2 **Output:** Equidimensional slices $W_0, \ldots, W_d$ of V.
3 Set $W_d := U_d$.
4 **for** *i from* $d-1$ *down to* 0 **do**
5 Set $W_i := \{\}$.
6 **for** *each point* $\mathbf{x}_0 \in U_i$ **do**
7 If $\mathbf{x}_0 \notin V_{i+1} \cup \cdots \cup V_d$, then $W_i := W_i \cup \{\mathbf{x}_0\}$.
8 **end**
9 **end**
10 Return $W_d, \ldots, W_1, W_0$.

Remark 19. An alternative to Algorithm 4.1 is a *local dimension test* [4], which can determine if a point $\mathbf{x}_0 \in U_i$ lies on a component of dimension exceeding i.

4.2.3. *Decomposing equidimensional slices.* Suppose that we have the equidimensional slices $W_0, \ldots, W_d$ of V, where $W_i = L^i \cap V_i$ for each i, as computed in Algorithm 4.1. Fix i and suppose that the irreducible decomposition of V_i is

$$V_i \;=\; X_1 \cup X_2 \cup \cdots \cup X_r\,,$$

so that $X_1, \ldots, X_r$ are all of the irreducible components of V of dimension i. Then

$$W_i \;=\; L^i \cap V_i \;=\; \big(L^i \cap X_1\big) \sqcup \big(L^i \cap X_2\big) \sqcup \cdots \sqcup \big(L^i \cap X_r\big)\;. \tag{23}$$

This union is disjoint by the generality of $\ell_1, \ldots, \ell_d$, as the intersection of $X_j \cap X_k$ with $j \neq k$ has dimension less than i. Call (23) the *witness set partition* of equidimensional slice W_i. Each part $L^i \cap X_j$ is a witness point set for X_j. Computing a witness set partition of W_i is tantamount to computing a numerical irreducible decomposition of V_i.

Suppose that $H(\mathbf{x}, t) := (F(\mathbf{x}), tL^i(\mathbf{x}) + (1-t)L'(\mathbf{x}))$ is a linear slice homotopy (22). As with moving a witness set, if we track a point $\mathbf{x} \in L^i \cap X_j$ to a point $\mathbf{x}' \in L' \cap V$, then all points of the homotopy path, including its endpoint $\mathbf{x}'$, lie on X_j.

Suppose that we combine linear slice homotopies together, moving points of $W_i = L^i \cap V_i$ to $L' \cap V_i$ on to $L'' \cap V_i$, and then back to $L^i \cap V_i$. The three convex combinations,

$$tL^i(\mathbf{x}) + (1-t)L'(\mathbf{x})\,,\quad tL'(\mathbf{x}) + (1-t)L''(\mathbf{x})\,,\quad \text{and}\quad tL''(\mathbf{x}) + (1-t)L^i(\mathbf{x})\,,$$

for $t \in [0,1]$ together form a based loop in the space of codimension i affine linear subspaces. Tracking each $\mathbf{x}_0 \in W_i$ along the three homotopies gives another point $\sigma(\mathbf{x}_0) \in W_i$. This computes a *monodromy permutation* σ of W_i. This has the property that the partition of W_i into the cycles of σ refines the witness set partition (23).

Following additional based loops may lead to other partitions of W_i into cycles of monodromy permutations. The common coarsening of these monodromy cycle partitions is an *empirical partition* of W_i. Every empirical partition is a refinement of the witness set partition. Since the smooth locus of $X_j \smallsetminus (\bigcup_{k \neq j} X_k)$ is path-connected, the common coarsening of all empirical partitions is the witness set partition. Thus computing monodromy permutations will eventually give the witness set partition.

The problem with this approach to numerical irreducible decomposition is that only when V_i is irreducible is there a stopping criterion. Namely, if we discover an empirical partition consisting of a single part, then we conclude that V_i is irreducible, and (F, L^i, W_i) is a numerical irreducible decomposition of V_i. All other cases lack a stopping criterion.

A common heuristic stopping criterion is the trace test [82]. To begin, form a linear slice homotopy (22) using a linear subspace L' such that $L^i \cap L'$ has codimension $i+1$. Then the convex combination $tL^i(\mathbf{x}) + (1-t)L'(\mathbf{x})$ forms a *pencil*. The *trace test* follows from the observation that while each homotopy path $\mathbf{x}(t)$ for $t \in [0,1]$ tracked from a point $\mathbf{x} \in W_i$ is nonlinear, if we sum over all points $\mathbf{x} \in L^i \cap X_j$ in a single part of the witness set partition, then that sum or its average is an affine-linear function of the homotopy parameter t. Given a subset $S \subset W_i$, the average of the points tracked from S is the *trace* of S. The trace is an affine-linear function if and only if S is the full witness point set [84, Theorem 15.5.1].

Example 20. Consider the folium of Descartes which is defined by $f = x^3 + y^3 - 3xy$. A general line ℓ meets the folium in three points W with the triple (f, ℓ, W) forming a witness set for the folium. Figure 8 shows these witness sets on four parallel lines, which lie in a pencil. Note that the four traces are collinear. ◇

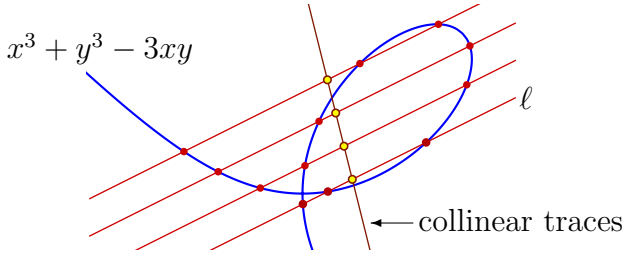


FIGURE 8. The trace test for the folium of Descartes.

The collinearity of traces may be seen as a consequence of Viète's formula that the sum of the roots of a monic polynomial of degree δ in y is the coefficient of $-y^\delta$ [61].

This gives the following stopping criterion for computing a numerical irreducible decomposition. Given a part S of an empirical partition of W_i, track all points of S along a linear slice homotopy given by a pencil containing L^i. If the traces are collinear, then S is a witness point set for some component of V_i. Otherwise, either compute more monodromy permutations to coarsen the empirical partition or check the collinearity of the trace for the union of S with other parts of the empirical partition. This is called the *trace test*.

Example 21. Suppose that V is the union of the ellipse $8(x+1)^2 + 3(2y+x+1)^2 = 8$ and the folium, as in Figure 9. A witness set for V consists of the five points $W = V \cap \ell$. Tracking points of W as ℓ varies over several loops in the space of lines gives an empirical

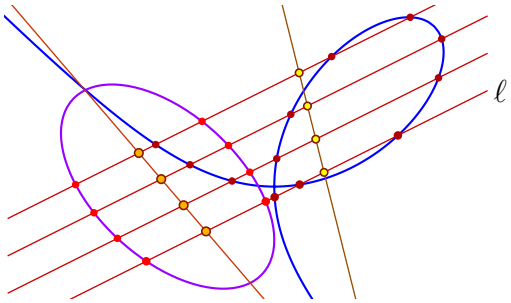


FIGURE 9. Numerical irreducible decomposition for the ellipse and folium.

partition of W into two sets, of cardinalities two and three, respectively. Applying the trace test to each subset verifies that each is a witness set of a component of V. ◇

The methods described in this and the previous subsections combine to give the *Cascade Algorithm* for computing a numerical irreducible decomposition. This was introduced in [80] and is implemented in `PHCpack` [94], `Bertini` [5] and `HomotopyContinuation.jl` [14], and in `NAG4M2` [60] through its interfaces. We present a simplified form in Algorithm 4.2.

Algorithm 4.2: The Cascade Algorithm

Input: A system $F(\mathbf{x})$ of polynomials in n variables defining a variety V of dimension d.
Output: A numerical irreducible decomposition of V.
for *each dimension i from d down to* 0 **do**
  Choose a codimension i linear space L^i and compute $L^i \cap V$, yielding points U_i.
  Remove from U_i any points lying on higher-dimensional components as in Algorithm 4.1. Call the remaining points W_i.
  Compute the witness set partition $W_i = S_1 \sqcup \cdots \sqcup S_r$ using monodromy and the trace test as explained in Section 4.2.3.
  Return (F, L^i, S_j) for $j = 1, \ldots, r$. These are witness sets for the irreducible components of V of dimension i.
end

4.3. **Advanced methods for solving.** The perspective afforded by numerical algebraic geometry and its tools—witness sets and monodromy—lead to new algorithms for solving systems of equations. We describe two such algorithms. Regeneration [45] is a bootstrap method that constructs a numerical irreducible decomposition one equation at a time. Monodromy solving [28] exploits that it is often easier to find a system of equations for which a given point is a solution than to find a solution to a given system.

4.3.1. *Regeneration.* Let $F := (f_1, \ldots, f_m)$ be a system of polynomials in n variables. Rather than solve all equations at once as in (3), we instead consider the sequence of varieties

$$\mathbb{C}^n \;=\; V_0 \supset V_1 \supset V_2 \supset \cdots \supset V_m = V\,,$$

where V_i is defined by the first i polynomials in F. The approach of *equation-by-equation solvers* [45, 46, 83] is to iteratively compute V_i given V_{i-1} for each $i = 1, \ldots, m$.

Let $X \subset V_{i-1}$ be an irreducible component of dimension d. Then

$$X \cap V_i \;=\; \{\mathbf{x} \in X \mid f_i(\mathbf{x}) = 0\}\,.$$

If f_i vanishes identically on X, then X is an irreducible component of V_i. Otherwise $X \cap V_i$, if nonempty, is a union of irreducible components of V_i of dimension $d-1$. We explain how to obtain a numerical irreducible decomposition of $X \cap V_i$ given a witness set for X.

Let $((f_1, \ldots, f_{i-1}), L^d, L^d \cap X)$ be a witness set for X. By the generality of L^d, with probability one we may conclude that a general polynomial f vanishes on X only if f vanishes at each point of $W := L^d \cap X$. *Regeneration* is a method to use W to compute a witness point superset for $X \cap V_i$. Let $\ell_1, \ldots, \ell_d$ be d linear polynomials defining L^d, and suppose that δ is the degree of f_i. Form the convex combination $\ell(t) := t\ell_d + (1-t)\ell'$ of ℓ_d with a new general degree one polynomial, ℓ'. Use the straight-line homotopy

$$(f_1, \ldots, f_{i-1}\,,\; \ell(t)\,,\; \ell_1, \ldots, \ell_{d-1})$$

to move the witness point set $W_1 = W = L^d \cap X$ at $t = 1$ to witness point sets $W_2, \ldots, W_\delta$ at distinct points $t = t_2, \ldots, t_\delta$, respectively.

Then the product $f := \ell_d \cdot \ell(t_2) \cdots \ell(t_\delta)$ has degree δ in $\mathbf{x}$ and we have

$$U' \;=\; W_1 \cup W_2 \cup \cdots \cup W_\delta \;=\; L^{d-1} \cap (X \cap \{\mathbf{x} \mid f(\mathbf{x}) = 0\})\,,$$

where L^{d-1} is defined by $\ell_1, \ldots, \ell_{d-1}$. Use the straight-line homotopy

$$(f_1, \ldots, f_{i-1}\,,\; tf + (1-t)f_i\,,\; \ell_1, \ldots, \ell_{d-1})$$

to track the points of U' at $t = 1$ to the set U at $t = 0$. Then

$$U \;=\; L^{d-1} \;\cap\; \big(X \;\cap\; V_i\big)$$

is a witness point superset for $X \cap V_i$. Finally, use monodromy and the trace test of Section 4.2.3 to decompose U into witness point sets for the irreducible components of $X \cap V_i$.

As regeneration computes a numerical irreducible decomposition of the variety V of F, it will also compute all isolated solutions to F.

4.3.2. *Solving by monodromy.* Suppose that we wish to solve a system $F = F(\mathbf{x}; \mathbf{p})$ of polynomials that lies in a parameter space of polynomial systems as in Section 2.2, and that evaluation at a general point $\mathbf{x}_0 \in \mathbb{C}^n$ gives n independent linear equations in the parameters $\mathbf{p} \in \mathbb{C}^k$. For example, $F(\mathbf{x}; \mathbf{p})$ could be the family of all polynomial systems $f_1(\mathbf{x}), \ldots, f_d(\mathbf{x})$ where the degree of f_i is d_i and $\mathbf{p} \in \mathbb{C}^k$ is the vector of coefficients. More generally, each $f_i(\mathbf{x})$ could be a sparse polynomial of support $\mathcal{A}_i$.

Consider the incidence variety (5) with projections π_1 to $\mathbb{C}^n$ and π_2 to $\mathbb{C}^k$.

$$\begin{array}{ccc} Z \;=\; \{(\mathbf{x}, \mathbf{p}) \in \mathbb{C}^n \times \mathbb{C}^k \mid F(\mathbf{x}; \mathbf{p}) = 0\} & \subseteq & \mathbb{C}^n \times \mathbb{C}^k \\ {\scriptstyle \pi_1}\swarrow \quad \searrow{\scriptstyle \pi_2} & & \\ \mathbb{C}^n \qquad \mathbb{C}^k & & \end{array} \tag{24}$$

For any parameters $\mathbf{p} \in \mathbb{C}^k$, $\pi_2^{-1}(\mathbf{p})$ is the set of solutions $\mathbf{x} \in \mathbb{C}^n$ to $F(\mathbf{x}; \mathbf{p}) = 0$. On the other hand, if we fix a general $\mathbf{x}_0 \in \mathbb{C}^n$, then $\pi_1^{-1}(\mathbf{x}_0) \subset \mathbb{C}^k$ is defined by n independent linear equations on $\mathbb{C}^k$, and is thus a linear subspace of dimension $k-n$. (This implies that Z is irreducible and has dimension k, which explains why the general fiber $\pi_2^{-1}(\mathbf{p})$ is finite and $\pi_2 \colon Z \to \mathbb{C}^k$ is a branched cover.) Imposing $k-n$ additional general degree one equations on

$\pi_1^{-1}(\mathbf{x}_0)$ gives a single parameter value $\mathbf{p}_0 \in \mathbb{C}^k$ such that $F(\mathbf{x}_0; \mathbf{p}_0) = 0$, that is, a system of polynomials $F(\mathbf{x}; \mathbf{p}_0)$ in the family Z for which $\mathbf{x}_0$ is a solution.

The underlying idea of monodromy solving [28] is to use monodromy to discover all solutions to $F(\mathbf{x}; \mathbf{p}_0) = 0$ and then use a parameter homotopy to find solutions to any desired system of polynomials in the family. Similar to the description of monodromy in Section 4.2.3, if we choose general points $\mathbf{p}_1, \mathbf{p}_2 \in \mathbb{C}^k$, we may form the trio of parameter homotopies $F(\mathbf{x}; t\mathbf{p}_0 + (1-t)\mathbf{p}_1)$, $F(\mathbf{x}; t\mathbf{p}_1 + (1-t)\mathbf{p}_2)$, and $F(\mathbf{x}; t\mathbf{p}_2 + (1-t)\mathbf{p}_0)$. For $t \in [0, 1]$, these form a loop in the parameter space based at $\mathbf{p}_0$, and we may track the point $\mathbf{x}_0$ along this loop to obtain a possibly new point $\mathbf{x}' \in \pi_2^{-1}(\mathbf{p}_0)$ so that $F(\mathbf{x}'; \mathbf{p}_0) = 0$.

More generally, given a subset $S \subset \pi_2^{-1}(\mathbf{p}_0)$ of computed points, we may track it along a possibly new loop in $\mathbb{C}^k$ based at $\mathbf{p}_0$ to obtain a subset $S' \subset \pi_2^{-1}(\mathbf{p}_0)$. Thus we may discover additional solutions to $F(\mathbf{x}; \mathbf{p}_0) = 0$.

When the number N of solutions to a general system in the family is known (e.g., via Bernstein's bound for the sparse systems of Section 3.1), this method has a stopping criterion. Otherwise, some heuristic may be used once sufficiently many solutions are known. The technique of solving using monodromy was introduced in [28], where a more complete description may be found. It is implemented in `HomotopyContinuation.jl` [14] and widely used, in particular when it is not necessary to compute all solutions to a given system.

Suppose that we have a branched cover $\pi\colon Z \to Y$ with Y rational (e.g. as in (24) where $Y = \mathbb{C}^k$), and we know all solutions $\pi^{-1}(\mathbf{y}_0)$ for a parameter value $\mathbf{y}_0$ not in the branch locus, B. As in Section 4.2.3, tracking all points in $\pi^{-1}(\mathbf{y})$ as $\mathbf{y}$ varies along a loop in $Y \setminus B$ based at $\mathbf{y}_0$ gives a monodromy permutation σ of $\pi^{-1}(\mathbf{y}_0)$, which we regard as an element of the symmetric group S_N, where $N = |\pi^{-1}(\mathbf{y}_0)|$. The set of all monodromy permutations forms the *monodromy group* of the branched cover Z.

This is in fact a Galois group [41, 52, 87]: Let $\mathbb{K} = \mathbb{C}(Y)$ be the field of rational functions on the parameter space Y and let $\mathbb{L} = \mathbb{C}(Z)$ be the function field of the incidence variety Z. As π is dominant, we may regard $\mathbb{K}$ as a subfield of $\mathbb{L}$ via π^{-1}, and $\mathbb{L}/\mathbb{K}$ is a field extension of degree N. The Galois group of the normal closure of $\mathbb{L}/\mathbb{K}$ is equal to the monodromy group of Z, and we call it the Galois group of the branched cover Z, $\mathcal{G}(Z)$.

There are several approaches to computing Galois groups using methods from numerical nonlinear algebra. In [62], monodromy permutations were computed and used to show some Galois groups were the full symmetric group (see Section 6.2). Other approaches, including methods guaranteed to compute generators of Galois groups, were developed in [43]. Yahl [97] introduced a method to certify that a Galois group contains a simple transposition, using ideas from this section and from Section 5.

A Galois group that is imprimitive (preserves a partition of the solitions) is equivalent to the branched cover decomposing as a comosition of branched covers, and this may be exploited for solving (comuting points in a fiber). This is explained in [2, 15].

5. Certification

Let F be a square system of polynomials and $\mathbf{z}_0$ be a point presumed to be an approximation of a solution to F. We discuss methods that can give a computational proof that Newton iterates starting from $\mathbf{z}_0$ converge to a nearby regular zero $\mathbf{z}$ of F. Such methods

certify the numerical solution $\mathbf{z}_0$ to F. Certification methods can also prove that two numerical solutions correspond to two distinct zeroes, and are thus a useful tool in both theoretical and applied problems in numerical nonlinear algebra.

There are two main strategies to certify solutions to square polynomial systems, *Smale's α-theory* and *Krawczyk's method*. A difference is that Smale's α-theory uses exact arithmetic, while Krawczyk's method uses floating-point arithmetic.

Remark 22. There are other approaches. In [27] the authors develop methods to certify overdetermined systems which require global information. In [44], overdetermined systems are reformulated as square systems to enable certification. ◇

5.1. **Smale's α-theory.** Smale's α-theory certifies approximate zeroes of a square system F. An approximate zero of F is a data structure representing a solution to F. Mentioned in Section 2.4, we now give a more formal definition.

Definition 23. Let $F(\mathbf{x})$ be a square system of n polynomials in n variables. Writing $JF := \frac{\partial F}{\partial \mathbf{x}}$ for its Jacobian matrix, its Newton operator N_F (9) is $N_F(\mathbf{x}) := \mathbf{x} - (JF(\mathbf{x}))^{-1} F(\mathbf{x})$. A point $\mathbf{z}_0 \in \mathbb{C}^n$ is an *approximate zero* of F if there exists a regular zero $\mathbf{z} \in \mathbb{C}^n$ of F such that the sequence $\{\mathbf{z}_k \mid k \geq 0\}$ of Newton iterates defined by $\mathbf{z}_{k+1} = N_F(\mathbf{z}_k)$ for $k \geq 0$ converges quadratically to $\mathbf{z}$ in that

$$\|\mathbf{z}_{k+1} - \mathbf{z}\| \;\leq\; \frac{1}{2}\|\mathbf{z}_k - \mathbf{z}\|^2 \qquad \forall k \;\geq\; 0\,.$$

We call $\mathbf{z}$ the *associated zero* of $\mathbf{z}_0$. ◇

Smale's α-theory certifies that a point $\mathbf{x}$ is an approximate zero using only local information encoded in two functions of F and $\mathbf{x}$,

$$\beta(F,\mathbf{x}) \;:=\; \|JF(\mathbf{x})^{-1}F(\mathbf{x})\| \quad \text{and} \quad \gamma(F,\mathbf{x}) \;:=\; \max_{k\geq 2} \Big\| \frac{1}{k!}\, JF(\mathbf{x})^{-1}\mathrm{D}^k F(\mathbf{x}) \Big\|^{\frac{1}{k-1}}\,.$$

Here, β is the size of a Newton step, $\mathrm{D}^k F(\mathbf{x})$ is the tensor of derivatives of order k at $\mathbf{x}$, and $JF(\mathbf{x})^{-1}\mathrm{D}^k F(\mathbf{x})$ is the corresponding multilinear map $(\mathbb{C}^n)^k \to \mathbb{C}^n$. The norm is the operator norm $\|A\| := \max_{\|v\|=1} \|A(v,\ldots,v)\|$.

Let $\alpha(F,\mathbf{x}) := \beta(F,\mathbf{x})\cdot\gamma(F,\mathbf{x})$ be the product of these two functions. We state two results of Smale [10, Theorem 4 and Remark 6 in Chapter 8].

Theorem 24. *Let $\mathbf{x} \in \mathbb{C}^n$ and F be a system of n polynomials in n variables.*

(1) If $\alpha(F,\mathbf{x}) < \frac{13-3\sqrt{17}}{4} \approx 0.15767$, then $\mathbf{x}$ is an approximate zero of F whose associated zero $\mathbf{z}$ satisfies $\|\mathbf{x}-\mathbf{z}\| \leq 2\beta(F,\mathbf{x})$.

(2) If $\mathbf{x}$ is an approximate zero of F and $\mathbf{y} \in \mathbb{C}^n$ satisfies $\|\mathbf{x}-\mathbf{y}\| < \frac{1}{20\,\gamma(F,\mathbf{x})}$, then $\mathbf{y}$ is also an approximate zero of F with the same associated zero as $\mathbf{x}$.

Shub and Smale [79] derived an upper bound for $\gamma(F,\mathbf{x})$ which can be computed using exact arithmetic, and thus one may decide algorithmically if $\mathbf{x}$ is an approximate zero of F, using only data of F and the point $\mathbf{x}$ itself.

The software `alphaCertified` [47] uses this theorem in an algorithm. An implementation is publicly available for download[1]. If the polynomial system F has only real coefficients, then `alphaCertified` can decide if an associated zero is real. The idea is as follows. Let

[1] https://www.math.tamu.edu/~sottile/research/stories/alphaCertified/index.html

$\mathbf{x} \in \mathbb{C}^n$ be an approximate zero of F with associated zero $\mathbf{z}$. Since the Newton operator has real coefficients, $N_F(\overline{\mathbf{x}}) = \overline{N_F(\mathbf{x})}$, we see that $\overline{\mathbf{x}}$ is an approximate zero of F with associated zero $\overline{\mathbf{z}}$. Consequently, if $\|\mathbf{x} - \overline{\mathbf{x}}\| < \frac{1}{20\gamma(F,\mathbf{x})}$, then $\mathbf{z} = \overline{\mathbf{z}}$ by Theorem 24(2).

5.2. **Krawczyk's method.** Interval arithmetic certifies computations using floating-point arithmetic. *Krawczyk's method* [56] adapts Newton's method to interval arithmetic and can certify zeros of analytic function $\mathbb{C}^n \to \mathbb{C}^n$. This is explained in [74].

Real interval arithmetic involves the set of compact real intervals,

$$\mathbb{IR} \;:=\; \{[x,y] \mid x,y \in \mathbb{R}, x \le y\}\,.$$

For $X, Y \in \mathbb{IR}$ and $\circ \in \{+,-,\cdot,\div\}$, we define $X \circ Y := \{x \circ y \,|\, x \in X, y \in Y\}$. (For $\div$ we require that $0 \notin Y$.) For intervals $I, J, K \in \mathbb{IR}$ we have $I \cdot (J+K) \subseteq I \cdot J + I \cdot K$, but the inclusion may be strict. Indeed,

$$\begin{aligned} [0,1] \cdot ([-1,0] + [1,1]) \;&=\; [0,1] \cdot [0,1] \;=\; [0,1] \quad \text{but} \\ [0,1] \cdot [-1,0] + [0,1] \cdot [1,1] \;&=\; [-1,0] + [0,1] \;=\; [-1,1]\,. \end{aligned}$$

Thus there is no distributive law in interval arithmetic.

Complex intervals are rectangles in the complex plane of the form

$$X + \sqrt{-1}Y \;=\; \{x + \sqrt{-1}y \mid x \in X, y \in Y\}\,, \quad \text{where } X, Y \in \mathbb{IR}\,.$$

Let $\mathbb{IC}$ be the set of all complex intervals. Writing $\frac{X}{Y}$ for $X \div Y$, we define arithmetic for complex intervals $I = X + \sqrt{-1}\,Y$ and $J = W + \sqrt{-1}Z$ as follows.

$$\begin{aligned} I + J &:= (X+W) + \sqrt{-1}\,(Y+Z) & I \cdot J &:= (X \cdot W - Y \cdot Z) + \sqrt{-1}\,(X \cdot Z + Y \cdot W) \\ I - J &:= (X-W) + \sqrt{-1}\,(Y-Z) & \frac{I}{J} &:= \frac{X \cdot W + Y \cdot Z}{W \cdot W + Z \cdot Z} + \sqrt{-1}\,\frac{Y \cdot W - X \cdot Z}{W \cdot W + Z \cdot Z} \end{aligned}$$

As before, for $\frac{I}{J}$ we assume that $0 \notin (W \cdot W + Z \cdot Z)$.

As with real intervals, there is no distributive law for complex intervals. Consequently, evaluating a polynomial at intervals is not well-defined. Evaluation at intervals is well-defined for expressions of a polynomial as a straight-line program, which is an evaluation of the polynomial via a sequence of arithmetic operations that does not involve distributivity.

Example 25. Consider the polynomial $f(x,y,z) = x(y+z) = xy+xz$. These two expressions of the distributive law are different straight-line programs for f, and we have shown that they have distinct evaluations on the triple $([0,1],[-1,0],[1,1])$. ◇

We sidestep this issue with the notion of an interval enclosure.

Definition 26. Let F be a system of n polynomials in n variables. We call a map

$$\Box F \colon (\mathbb{IC})^n \to (\mathbb{IC})^n$$

such that $\{F(\mathbf{x}) \mid \mathbf{x} \in \mathbf{I}\} \subseteq \Box F(\mathbf{I})$ for every $\mathbf{I} \in (\mathbb{IC})^n$ an *interval enclosure* of F. ◇

Let $\Box F$ be an interval enclosure of a square polynomial system F and $\Box JF$ be an interval enclosure of its Jacobian map $JF \colon \mathbb{C}^n \to \mathbb{C}^{n \times n}$. Furthermore, let $\mathbf{I} \in (\mathbb{IC})^n$, $\mathbf{x} \in \mathbb{C}^n$, and let $Y \in \mathbb{C}^{n \times n}$ be an invertible matrix. The *Krawczyk operator* these define is

$$K_{\mathbf{x},Y}(\mathbf{I}) := \; \mathbf{x} - Y \cdot \Box F(\mathbf{x}) + (\mathbf{1}_n - Y \cdot \Box \mathrm{J}F(I))(\mathbf{I} - \mathbf{x})\,.$$

The norm of a matrix interval $A \in (\mathbb{IC})^{n\times n}$ is $\|A\|_\infty := \max_{B\in A}\max_{\mathbf{v}\in\mathbb{C}^n} \|B\mathbf{v}\|_\infty/\|\mathbf{v}\|_\infty$, where $\|(v_1,\ldots,v_n)\|_\infty = \max_{1\le i\le n}|v_i|$ for $\mathbf{v}\in\mathbb{C}^n$.

We state the main theorem underlying Krawczyk's method, which is proven in [74].

Theorem 27. *Let $F = (f_1,\ldots,f_n)$ be a system of n polynomials in n variables, $\mathbf{I}\in(\mathbb{IC})^n$, $\mathbf{x}\in\mathbf{I}$, and let $Y\in\mathbb{C}^{n\times n}$ be invertible.*

(1) If $K_{\mathbf{x},Y}(\mathbf{I})\subset\mathbf{I}$, there is a zero of F in $\mathbf{I}$.
(2) If $\sqrt{2}\,\|\mathbf{1}_n - Y\cdot\square JF(\mathbf{I})\|_\infty < 1$, then F has a unique zero in $\mathbf{I}$.

Several choices have to be made to implement Krawczyk's method. For instance, we have to choose interval enclosures of both F and its Jacobian JF. Example 25 shows that this is nontrivial as different straight-line programs for the same polynomial system can produce different results in interval arithmetic. Furthermore, choosing $\mathbf{I}$ in Theorem 27 too small might cause the true zero not to lie in $\mathbf{I}$, while choosing $\mathbf{I}$ too large can be an obstacle for the contraction property in (1). Heuristics are usually implemented to address these issues.

Krawczyk's method is implemented in the commercial `MATLAB` package `INTLAB` [75], the `Macaulay2` package `NumericalCertification` [58], and in `HomotopyContinuation.jl` [11, 14]. Krawczyk's method can also certify the reality of a zero: Assume that F has real coefficients. Suppose that we have found an interval $\mathbf{I}\in(\mathbb{IC})^n$ and a matrix $Y\in\mathbb{C}^{n\times n}$ such that $K_{\mathbf{x},Y}(\mathbf{I})\subset\mathbf{I}$ and $\sqrt{2}\,\|\mathbf{1}_n - Y\cdot\square JF(\mathbf{I})\|_\infty < 1$. By Theorem 27, F has a unique zero $\mathbf{z}$ in $\mathbf{I}$. Since $\overline{\mathbf{z}}$ is also a zero of F, if $\{\overline{\mathbf{y}} \mid \mathbf{y}\in K_{\mathbf{x},Y}(\mathbf{I})\}\subset\mathbf{I}$, then $\mathbf{z}=\overline{\mathbf{z}}$.

6. Applications

While we have largely discussed the theory and many aspects, methods, and some implementations of numerical nonlinear algebra, these were all motivated by its applications to questions within and from outside of mathematics. Many of these are well-known and may be found in other contributions in this volume. We present three such here, involving synchronization of oscillators, enumerative geometry, and computer vision.

6.1. The Kuramoto model.

In his 1673 treatise on pendulums and horology [51], Christiaan Huygens observed an "odd kind of sympathy" between pendulum clocks, which was one of the earliest observations of synchronization among coupled oscillators. Other examples range from pacemaker cells in the heart to the formation of circadian rhythm in the brain to synchronized flashing of fireflies. The Kuramoto model emerged from this study and has many interesting applications that have fueled several decades of active research [1].

A network of oscillators can be modeled as a swarm of points circling the origin which pull on each other. For weakly coupled and nearly identical oscillators, the natural separation of timescales [57, 96] allows a simple description of the long-term behavior in terms of phases of the oscillators. Kuramoto singled out the simplest case governed by equations

$$\dot\theta_i \;=\; \omega_i - \sum_{j\sim i} k_{ij}\sin(\theta_i-\theta_j) \qquad \text{for } i=0,\ldots,n\,. \tag{25}$$

Here, $\theta_0,\ldots,\theta_n\in[0,2\pi)$ are the phases of the oscillators, ω_i are their natural frequencies, $k_{ij} = k_{ij}$ are coupling coefficients, and $j\sim i$ is adjacency in the graph G underlying the network. This is the Kuramoto model [57]. It is simple enough to be analyzed yet it exhibits interesting emergent behaviors, and has initiated an active research field [89].

One core problem that can be studied algebraically is *frequency synchronization*. This occurs when the tendency of oscillators to relax to their limit cycles and the influences of their neighbors reach equilibrium, and the oscillators are all tuned to their mean frequency. Such synchronized configurations correspond to equilibria of (25), which are solutions to a nonlinear system of equations. Even though this system is derived from a simplification of the oscillator model, its utility extends far beyond this narrow setting. For example, in electric engineering, it coincides with a special case of the power flow equations, derived from laws of alternating current circuits [30].

The equilibrium equations become algebraic after a change of variables. Numerical nonlinear algebra has been used to solve these and related families of equations finding synchronization configurations that cannot be found by simulations or symbolic computation. For example, the IEEE 14 bus system from electric engineering is a well-studied test case, yet its full set of solutions remained unknown until it was computed using total degree and polyhedral homotopy methods by Mehta, et al. [64], using `Bertini` [5] and `HOM4PS-2.0` [59].

For rank one coupling, Coss, et al. [21] showed that the equilibrium equation of (25) may be reformulated as a set of decoupled univariate radical equations, which are easy to solve.

Determining the number of complex equilibira (solutions to the equilibrium equations (25)) is another line of research that has used numerical nonlinear algebra. In the 1980s, Baillieul and Byrnes [3] showed that a complete network of three oscillators has at most six complex equilibria, and all may be real. For a complete network of four oscillators, they constructed 14 real equilibria. There are 20 complex equilibria. In the 2010s, Molzahn, et al. [66] showed there could be 16 real equilibria and in 2020, Lindberg et al. [63] improved this to 18. It remains unknown if all 20 complex equilibria can be real.

We have a more complete answer for the enumeration of complex equilibria. Using the bihomogeneous Bézout bound of an algebraic formulation of the equilibrium equations of (25), Baillieul and Byrnes showed that a network of $n{+}1$ oscillators has at most $\binom{2n}{n}$ complex equilibria. This upper bound is attained for generic parameters $\{\omega_i\}$ and $\{k_{ij}\}$ whose network is a complete graph.

For sparse networks whose underlying graph is not complete, the bihomogeneous Bézout bound is not sharp, as the equations are sparse in the sense of Section 3. Bernstein's Theorem 8 is used in [64] to give a bound that depends upon the underlying graph. This is elegantly expressed in terms of the normalized volumes of symmetric edge polytopes. To a G connected graph we associated its *symmetric edge polytope*, which is defined by

$$\Delta_G \;:=\; \operatorname{conv}\{e_i - e_j \mid i \sim j \text{ in } G\}\,. \tag{26}$$

For a network of $n{+}1$ oscillators this has dimension n. Figure 10 shows symmetric edge polytopes for connected graphs on three vertices. A result in [19] is that for a connected

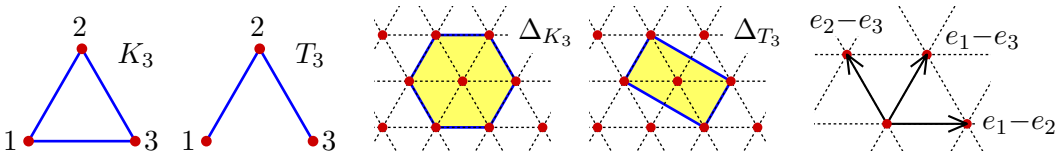


FIGURE 10. Connected graphs on three vertices, their symmetric edge polytopes, and the coordinates.

graph G and generic parameters, there are exactly $n!\mathrm{vol}(\Delta_G)$ complex equilibria. We may

see the bound of six from [3] for the network K_3 in Figure 10; the hexagon Δ_{K_3} is composed of six primitive triangles.

This symmetric edge polytope Δ_G is quite natural and has been independently studied in geometry and number theory [22]. Table 1 shows examples of the numbers of complex equilibria obtained through this connection. Finding exact formula for other families of

TABLE 1. Known results for the generic and maximum complex equilibria of (25)

A tree network with $n+1$ nodes [18]	2^n
A cycle network with $n+1$ nodes [18]	$(n+1)\binom{n}{\lfloor n/2 \rfloor}$
Cycles of lengths $2m_1, \ldots, 2m_k$ joined along an edge [22]	$\frac{1}{2^{k-1}} \prod_{i=1}^{k} m_i \binom{2m_i}{m_i}$
Cycles of lengths $2m_1{+}1$ and $2m_2{+}1$ joined along an edge [22]	$(m_1{+}m_2{+}2m_1m_2)\binom{2m_1}{m_1}\binom{2m_2}{m_2}$
A wheel graph with $n+1$ nodes for odd n [22]	$(1-\sqrt{3})^n + (1+\sqrt{3})^n$
A wheel graph with $n+1$ nodes for even n [22]	$(1-\sqrt{3})^n + (1+\sqrt{3})^n - 2$

networks remains an active topic. For trees and cycle networks, is is possible for all complex equilibria to be real. It is still unknown if the same holds for other families of networks.

6.2. **Numerical nonlinear algebra in enumerative geometry.** Paraphrasing Schubert [76], enumerative geometry is the art of counting geometric figures satisfying conditions imposed by other, fixed, geometric figures. Traditionally, these counting problems are solved by understanding the structure of the space of figures we are to count well enough to construct their cohomology or Chow rings [36], where the computations are carried out. Numerical nonlinear algebra allows us to actually compute the solutions to a given instance of an enumerative problem and then glean information about the problem that is not attainable by other means.

While the polyhedral homotopy of Section 3 based on Bernstein's Theorem may be viewed as a numerical homotopy method to solve a class of enumerative problems, perhaps the first systematic foray in this direction was in [49] by Sturmfels and coauthors, who exploited structures in the Grassmannian to give three homotopy methods for solving simple Schubert problems. These are enumerative problems that ask for the k-planes in $\mathbb{C}^n$ that meet a collection of linear subspaces non-trivially, such as finding all (462) 3-planes in $\mathbb{C}^7$ that meet twelve 4-planes [77]. Their number may be computed using Pieri's formula. The Pieri homotopy algorithm from [49] was later used [62] to study Galois groups in Schubert calculus. This included showing that a particular Schubert problem with 17589 solutions had Galois group the full symmetric group S_{17589}.

One of the most famous and historically important enumerative problems is the problem of five conics: How many plane conics are simultaneously tangent to five given plane conics? This was posed by Steiner [88] who gave the answer 7776. Briefly, a conic $ax^2 + bxy + cy^2 + dxz + eyz + fz^2 = 0$ in $\mathbb{P}^2$ is given by the point $[a, b, c, d, e, f]$ in $\mathbb{P}^5$, and the condition to be tangent to a given conic is a sextic in $a, b, \ldots, f$. By Bézout's Theorem, Steiner expected $6^5 = 7776$. The only problem with this approach is that every "doubled-line conic", one of the form $(\alpha x + \beta y + \gamma z)^2$, is tangent to every conic, and thus the Bézout count of 7776

includes a contribution from the doubled-line conics. Chasles [17] essentially introduced the Chow ring of smooth conics to give the correct answer of 3264 [54].

Fulton [37, p. 55] asked how many of the 3264 conics could be real, later determining that all can be real, but he did not publish his argument. His argument involves deforming an asymmetric pentagonal arrangement of lines and points to prove the *existence* of five real conics having all 3264 tangent conics real. Ronga, Tognoli, and Vust [73] published a different proof of existence via a delicate local computation near a symmetric arrangement that had 102 tangent conics, each of multiplicity 32. Fulton's argument is sketched in [85, Ch. 9] and Sturmfels with coauthors wrote a delightful article "3264 conics in a second" [12] in which they give an explicit five real conics with 3264 real tangent conics, together with a proof using certification as in Section 5 using numerical nonlinear algebra. Figure 11 shows a picture.

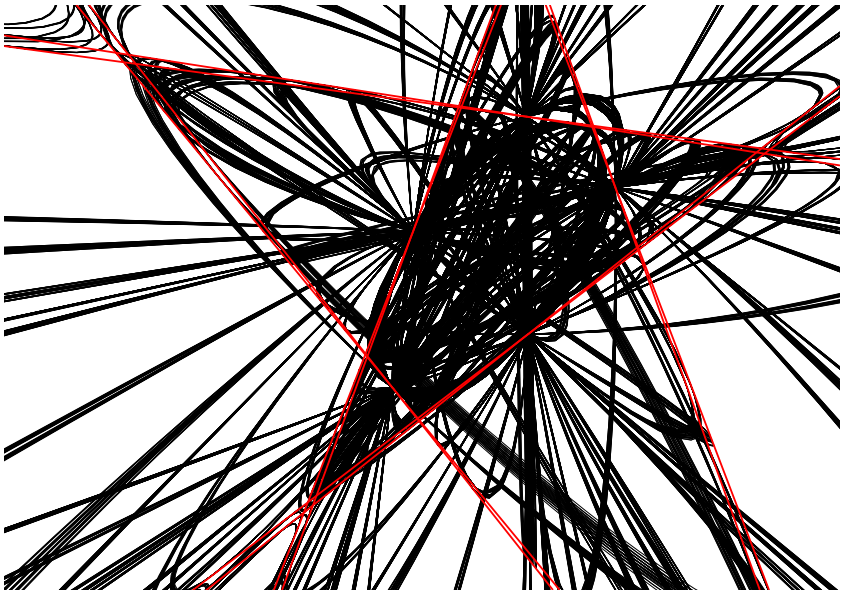


FIGURE 11. 3264 real conics tangent to five (nearly degenerate) conics.

6.3. **Computer vision.** Computer vision is a field of artificial intelligence that trains computers to interpret and understand the visual world. Several types of problems in computer vision are amenable to algebraic computational methods. We shall focus on one type—minimal problems—and one method—homotopy continuation. Minimal problems are the backbone of the *structure from motion* pipeline that is used for three-dimensional (3D) reconstruction in applications from medical imaging to autonomous vehicles.

The chapter "Snapshot of Algebraic Vision" in this volume treats other types of problems and other algebraic methods, including symbolic computation.

All problems amenable to this algebraic analysis share a purely geometric problem at their core. For computer vision, this often begins with basic projective geometry. We consider the projective space $\mathbb{P}^3$ as the 3D world, as it compactifies the Euclidean space $\mathbb{R}^3$. A mathematical model of a pin-hole camera C is a projective linear map given by a matrix

$$C \;:=\; [R \mid t]\,, \quad R \in \mathbb{R}^{3\times 3} \;\text{ and }\; t \in \mathbb{R}^{3\times 1}\,,$$

which captures the images of world points in the *image plane* $\mathbb{P}^2$. A *calibrated* camera C has $R \in \mathrm{SO}(3)$. While this is formulated in the $\mathbb{P}^3$ compactifying $\mathbb{R}^3$, for computations we extend scalars to the complex numbers.

We may also interpret a calabrated camera as an element of the special Euclidean group $\mathrm{SE}(3)$ acting on $\mathbb{R}^3$, the rotation R followed by the translation t. It is convenient to operate in a fixed affine chart on $\mathbb{P}^3$ and consider the (affine) camera plane as a plane of points with the third coordinate equal to 1 in $\mathbb{R}^3$ (the local affine coordinates of the camera). The image of a point is obtained intersecting the image plane with the line going through the point and the center of the camera. Figure 12 illustrates this as well as the definition of *depth*. The

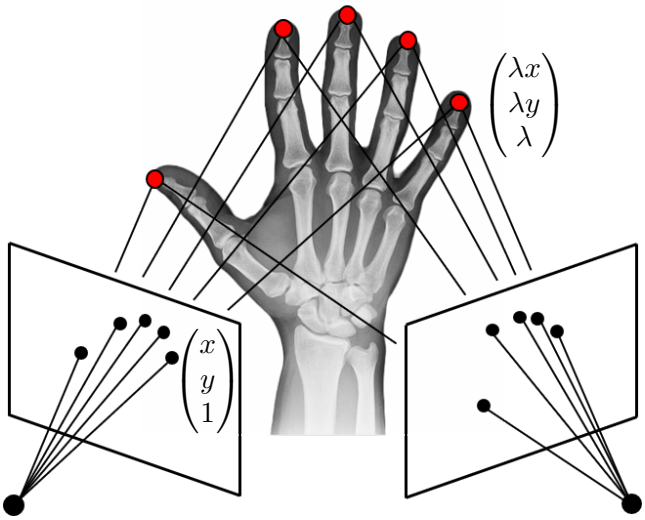


FIGURE 12. *5pt problem*: given images of five points in two views, find the relative pose $[R \mid t]$ of the two cameras with $t = (t_1, t_2, 1)^T$.

relative positions of the two cameras is encoded by an element $[R \mid t]$ of the Euclidean special group $\mathrm{SE}(3)$. The third coordinate of t is set equal to 1 to remove a scaling ambiguity. In the (3D) coordinate frame of the first camera the image of the tip of the little finger lies in the camera plane and the actual tip is the point obtained by scaling this by the *depth* λ.

6.3.1. *Minimal problems.* A reconstruction problem is *minimal* if it has a finite number of (complex) solutions for general values of the parameters. As in Sections 2.2 and 4.3.2, a minimal problem gives rise to a branched cover $\pi\colon \mathcal{M} \to \mathcal{P}$, where base space $\mathcal{P}$ the *problem space* and total space $\mathcal{M}$ (incidence variety) the *problem-solution* manifold. The number of the solutions, which is the degree of the branched cover, is the *degree* of the problem.

Example 28. A classical minimal problem is computing the calibrated camera [42] from three points in space and their image projections. A classical formulation [40] is as a system of three quadratic polynomial equations

$$\begin{aligned}\|X_1 - X_2\|^2 &= \|\lambda_1 x_1 - \lambda_2 x_2\|^2\\ \|X_2 - X_3\|^2 &= \|\lambda_2 x_2 - \lambda_3 x_3\|^2\\ \|X_3 - X_1\|^2 &= \|\lambda_3 x_3 - \lambda_1 x_1\|^2\end{aligned}$$

in three unknown *depths* $\lambda_1, \lambda_2, \lambda_3$. The parameters are the three $(i = 1, 2, 3)$ world points points $X_i \in \mathbb{R}^3$ and the points $x_i = (x_{i1}, x_{i2}, 1)^T \in \mathbb{R}^3$ representing three images in $\mathbb{P}^2$.

This formulation implicitly uses that R is orthogonal and preserves the norm. Recovery of the camera $C = [R \mid t]$ from the depths is an exercise in linear algebra.

This problem has degree eight. That is, for generic X_i and x_i, $i = 1, 2, 3$, the system has eight complex solutions[34]. In practice, there are fewer solutions with positive depths λ_i. This gives a branched cover of degree eight over the problem manifold $\mathcal{P} \cong \mathbb{C}^{15}$. ◇

We formulate perhaps the most consequential of all 3D reconstruction problems.

Example 29. The *5pt problem* of computing the relative pose of two calibrated cameras from 5 point correspondences in two images is featured in Figure 12.

Consider (paired) images $x_i = (x_{i1}, x_{i2}, 1)^T$, $y_i = (y_{i1}, y_{i2}, 1)^T$ and depths λ_i and μ_i, where $i = 1, \ldots, 5$, in the first and second cameras, respectively. Write down all or sufficiently many of $\binom{5}{2}$ same-distance equations

$$\|\lambda_i x_i - \lambda_j x_j\|^2 \;=\; \|\mu_i y_i - \mu_j y_j\|^2, \quad (1 \le i < j \le 5)\,,$$

between the image points, and one same-orientation equation

$$\begin{aligned}\det[\lambda_1 x_1 - \lambda_2 x_2 \mid \lambda_1 x_1 - \lambda_3 x_3 \mid \lambda_1 x_1 - \lambda_4 x_4] \\ = \det[\mu_1 x_1 - \mu_2 x_2 \mid \mu_1 x_1 - \mu_3 x_3 \mid \mu_1 x_1 - \mu_4 x_4]\,.\end{aligned}$$

These determinants are the signed volume of the same tetrahedron (formed by the world points $X_1, \ldots, X_4$ in different coordinate frames). The equality of the volumes is implied by the same-distance equations but not the equality of signs. Fix one depth, $\lambda_1 = 1$, to fix the ambiguity in scaling. This gives a system of equations in the remaining nine unknown depths λ and μ.

The solution space is the space of vectors of non-fixed depths $\mathcal{P} = \mathbb{R}^9$. The projection from the incidence variety problem-solution mainfold to $\mathcal{P}$ gives a covering of degree 20. ◇

As in Section 4.3.2, we may analize the Galois group of the branched cover. Decomposing a monodromy group of a minimal problem as shown in [29] may lead to an easier 3D reconstruction. The classical *epipolar geometry* approach to the 5pt problem [42, Sect. 9] is realized in this way. This gives a two-stage procedure for the relative pose recovery with the essential stage being a problem of degree 10.

6.3.2. *Engineering meets mathematics.* The 5pt problem of Example 29 plays a practical role in solvers for geometric optimization problems in vision based on RANSAC [35, 72]. This problem has many practical solutions based on or inspired by Gröbner basis techniques that also use the epipolar geometry formulation [71].

Recently, homotopy continuation has found practical use for minimal problems whose degrees are too high for efficient symbolic computation. The first step toward practical fast computation was a special solver MINUS [32] based on Macaulay2 core C++ code for homotopy continuation and optimized for performance on modern hardware. Featured in [33], it is deployed on two minimal problems of degrees 216 and 312 involving point as well as line correspondences. This computes *all* complex solutions and uses postprocessing to filter out irrelevant solutions.

Unlike [33], the work in [48] combines a neural network classifier with homotopy continuation. Rather than compute all solutions and then pick a relevant one, it follows only one continuation path (over $\mathbb{R}$). That strategy finds the relevant solution with high probability

in several practical scenarios. It is comparable to state-of-art algorithms for the 5pt problem and exceeds the performance for a 4pt problem. While matching four points in three calibrated views is not a minimal problem, there is a relaxation of degree 272 that is minimal, and the solution of the relaxation may be verified by using the original (overdetermined) formulation.

References

1. Juan A. Acebrón, L. L. Bonilla, Conrad J. Pérez Vicente, Félix Ritort, and Renato Spigler, *The Kuramoto model: A simple paradigm for synchronization phenomena*, Reviews of Modern Physics **77** (2005), no. 1, 137–185.
2. Carlos Améndola, Julia Lindberg, and Jose Israel Rodriguez, *Solving parameterized polynomial systems with decomposable projections*, 2016, `arXiv:1612.08807`.
3. J. Baillieul and C. Byrnes, *Geometric critical point analysis of lossless power system models*, IEEE Transactions on Circuits and Systems **29** (1982), no. 11, 724–737.
4. Daniel J. Bates, Jonathan D. Hauenstein, Chris Peterson, and Andrew J. Sommese, *A numerical local dimension test for points on the solution set of a system of polynomial equations*, SIAM Journal on Numerical Analysis **47** (2009), no. 5, 3608–3623.
5. Daniel J. Bates, Jonathan D. Hauenstein, Andrew J. Sommese, and Charles W. Wampler, *Bertini: Software for Numerical Algebraic Geometry*, Available at bertini.nd.edu with permanent doi: dx.doi.org/10.7274/R0H41PB5.
6. _____, *Numerically solving polynomial systems with Bertini*, SIAM, 2013.
7. D. N. Bernstein, *The number of roots of a system of equations*, Funkcional. Anal. i Priložen. **9** (1975), no. 3, 1–4.
8. D. N. Bernstein, A. G. Kušnirenko, and A. G. Hovanskiĭ, *Newton polyhedra*, Uspehi Mat. Nauk **31** (1976), no. 3(189), 201–202.
9. Grigoriy Blekherman, Jonathan Hauenstein, John Christian Ottem, Kristian Ranestad, and Bernd Sturmfels, *Algebraic boundaries of Hilbert's SOS cones*, Compos. Math. **148** (2012), no. 6, 1717–1735.
10. Lenore Blum, Felipe Cucker, Mike Shub, and Stephen Smale, *Complexity and real computation*, Springer-Verlag, New York, 1998. MR 1479636
11. Paul Breiding, Kemal Rose, and Sascha Timme, *Certifying zeros of polynomial systems using interval arithmetic*, 2020, `arXiv:2011.05000`.
12. Paul Breiding, Bernd Sturmfels, and Sascha Timme, *3264 conics in a second*, Notices Amer. Math. Soc. **67** (2020), no. 1, 30–37. MR 3970037
13. Paul Breiding and Sascha Timme, *An introduction to the numerical solution of polynomial systems*, https://www.juliahomotopycontinuation.org/guides/introduction/.
14. _____, *HomotopyContinuation.jl: A Package for Homotopy Continuation in Julia*, Mathematical Software – ICMS 2018 (Cham), Springer International Publishing, 2018, pp. 458–465.
15. Taylor Brysiewicz, Jose Israel Rodriguez, Frank Sottile, and Thomas Yahl, *Solving decomposable sparse systems*, Numerical Algorithms **88** (2021), no. 1, 453–474.
16. Peter Bürgisser and Felipe Cucker, *Condition: The Geometry of Numerical Algorithms*, Springer, Heidelberg, 2013. MR 3098452

17. M. Chasles, *Construction des coniques qui satisfont à cinque conditions*, C. R. Acad. Sci. Paris **58** (1864), 297–308.
18. Tianran Chen, Robert Davis, and Dhagash Mehta, *Counting equilibria of the Kuramoto model using birationally invariant intersection index*, SIAM J. Appl. Algebra Geom. **2** (2018), no. 4, 489–507. MR 3867607
19. Tianran Chen, Evgeniia Korchevskaia, and Julia Lindberg, *On the typical and atypical solutions to the Kuramoto equations*, arXiv (2022).
20. Tianran Chen, Tsung-Lin Lee, and Tien-Yien Li, *Hom4PS-3: A Parallel Numerical Solver for Systems of Polynomial Equations Based on Polyhedral Homotopy Continuation Methods*, Mathematical Software – ICMS 2014 (Hoon Hong and Chee Yap, eds.), Springer Berlin Heidelberg, 2014, pp. 183–190.
21. Owen Coss, Jonathan D. Hauenstein, Hoon Hong, and Daniel K. Molzahn, *Locating and Counting Equilibria of the Kuramoto Model with Rank-One Coupling*, SIAM Journal on Applied Algebra and Geometry **2** (2018), no. 1, 45–71.
22. Alessio D'Alì, Emanuele Delucchi, and Mateusz Michał ek, *Many faces of symmetric edge polytopes*, Electron. J. Combin. **29** (2022), no. 3, Paper No. 3.24, 42.
23. D.F. Davidenko, *On a new method of numerical solution of systems of nonlinear equations*, Doklady Akad. Nauk SSSR (N.S.) **88** (1953), 601–602.
24. ———, *On approximate solution of systems of nonlinear equations*, Ukrain. Mat. Žurnal **5** (1953), 196–206.
25. Jean-Pierre Dedieu and Michael Shub, *Newton's method for overdetermined systems of equations*, Math. Comp. **69** (2000), 1099–1115.
26. J. Draisma, E. Horobeţ, G. Ottaviani, B. Sturmfels, and R. R. Thomas, *The euclidean distance degree of an algebraic variety*, Foundations of Computational Mathematics **16** (2016), no. 1, 99–149.
27. Timothy Duff, Nickolas Hein, and Frank Sottile, *Certification for polynomial systems via square subsystems*, J. Symbolic Comput. **109** (2022), 367–385. MR 4316045
28. Timothy Duff, Cvetelina Hill, Anders Jensen, Kisun Lee, Anton Leykin, and Jeff Sommars, *Solving polynomial systems via homotopy continuation and monodromy*, IMA J. Numer. Anal. **39** (2019), no. 3, 1421–1446. MR 3984062
29. Timothy Duff, Viktor Korotynskiy, Tomas Pajdla, and Margaret H. Regan, *Galois/Monodromy groups for decomposing minimal problems in 3D reconstruction*, SIAM J. Appl. Algebra Geom. **6** (2022), no. 4, 740–772. MR 4522866
30. Florian Dörfler and Francesco Bullo, *Synchronization in complex networks of phase oscillators: A survey*, Automatica **50** (2014), no. 6, 1539–1564.
31. Günter Ewald, *Combinatorial convexity and algebraic geometry*, Graduate Texts in Mathematics, vol. 168, Springer-Verlag, New York, 1996.
32. Ricardo Fabbri, *MINUS: MInimial problem NUmerical continuation Solver*, https://github.com/rfabbri/minus.
33. Ricardo Fabbri, Timothy Duff, Hongyi Fan, Margaret H. Regan, David da Costa de Pinho, Elias P. Tsigaridas, Charles W. Wampler, Jonathan D. Hauenstein, Peter J. Giblin, Benjamin B. Kimia, Anton Leykin, and Tomás Pajdla, *TRPLP - Trifocal relative pose from lines at points*, 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition, CVPR 2020, Seattle, WA, USA, June 13-19, 2020, IEEE, 2020, pp. 12070–12080.

34. Jean-Charles Faugère, Guillaume Moroz, Fabrice Rouillier, and Mohab Safey El Din, *Classification of the perspective-three-point problem, discriminant variety and real solving polynomial systems of inequalities*, Symbolic and Algebraic Computation, International Symposium, ISSAC 2008, Linz/Hagenberg, Austria, July 20-23, 2008, Proceedings (J. Rafael Sendra and Laureano González-Vega, eds.), ACM, 2008, pp. 79–86.
35. M. A. Fischler and R. C. Bolles, *Random sample consensus: a paradigm for model fitting with applications to image analysis and automated cartography*, Commun. ACM **24** (1981), no. 6, 381–395.
36. William Fulton, *Intersection theory*, second ed., Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge., vol. 2, Springer-Verlag, Berlin, 1998. MR 1644323
37. Wm. Fulton, *Introduction to intersection theory in algebraic geometry*, CBMS Regional Conference Series in Mathematics, vol. 54, CBMS, Washington, DC, 1984.
38. C. B. García and W. I. Zangwill, *Finding all solutions to polynomial systems and other systems of equations*, Math. Programming **16** (1979), no. 2, 159–176.
39. Elizabeth Gross, Sonja Petrović, and Jan Verschelde, *Interfacing with PHCpack*, J. Softw. Algebra Geom. **5** (2013), 20–25.
40. J. A. Grunert, *Das pothenotische Problem in erweiterter Gestalt nebst über seine Anwendungen in Geodäsie*, In Grunerts Archiv für Mathematik und Physik (1841).
41. J. Harris, *Galois groups of enumerative problems*, Duke Math. Journal **46** (1979), no. 4, 685–724.
42. Richard Hartley and Andrew Zisserman, *Multiple view geometry in computer vision*, 2nd ed., Cambridge, 2003.
43. J. D. Hauenstein, J.I. Rodriguez, and F. Sottile, *Numerical computation of Galois groups*, Found. Comput. Math. **18** (2018), no. 4, 867–890.
44. Jonathan D. Hauenstein, Nickolas Hein, and Frank Sottile, *A primal-dual formulation for certifiable computations in Schubert calculus*, Found. Comput. Math. **16** (2016), no. 4, 941–963.
45. Jonathan D. Hauenstein, Andrew J. Sommese, and Charles W. Wampler, *Regeneration homotopies for solving systems of polynomials*, Math. Comp. **80** (2011), no. 273, 345–377.
46. _____, *Regenerative cascade homotopies for solving polynomial systems*, Appl. Math. Comput. **218** (2011), no. 4, 1240–1246.
47. Jonathan D. Hauenstein and F. Sottile, *Algorithm 921: alphaCertified: certifying solutions to polynomial systems*, ACM Trans. Math. Software **38** (2012), no. 4, Art. 28, 20. MR 2972672
48. Petr Hruby, Timothy Duff, Anton Leykin, and Tomas Pajdla, *Learning to solve hard minimal problems*, Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, 2022, pp. 5532–5542.
49. Birkett Huber, Frank Sottile, and Bernd Sturmfels, *Numerical Schubert calculus*, J. Symbolic Comput. **26** (1998), no. 6, 767–788.
50. Birkett Huber and Bernd Sturmfels, *A polyhedral method for solving sparse polynomial systems*, Math. Comp. **64** (1995), no. 212, 1541–1555.
51. Christiaan Huygens, *Horologium oscillatorium: Sive de motu pendulorum ad horologia aptato demonstrationes geometricae*, F. Muguet, Paris, 1673.
52. C. Jordan, *Traité des Substitutions et des Équations algébriques*, Gauthier-Villars, Paris, 1870.

53. A. G. Khovanskii, *Newton polyhedra and the genus of complete intersections*, Functional Analysis and Its Applications **12** (1978), 38–46.
54. S. L. Kleiman, *Chasles's enumerative theory of conics: a historical introduction*, Studies in algebraic geometry, MAA Stud. Math., vol. 20, Math. Assoc. America, Washington, D.C., 1980, pp. 117–138.
55. A. G. Kouchnirenko, *Polyèdres de Newton et nombres de Milnor*, Inventiones Mathematicae **32** (1976), 1–31.
56. Rudolf Krawczyk, *Newton-Algorithmen zur Bestimmung von Nullstellen mit Fehlerschranken*, Computing **4** (1969), no. 3, 187–201.
57. Yoshiki Kuramoto, *International Symposium on Mathematical Problems in Theoretical Physics, January 23–29, 1975, Kyoto University, Kyoto/Japan*, Lecture Notes in Physics (2005), 420–422.
58. Kisun Lee, *Certifying approximate solutions to polynomial systems on Macaulay2*, ACM Communications in Computer Algebra **53** (2019), no. 2, 45–48.
59. T. L. Lee, T. Y. Li, and C. H. Tsai, *Hom4ps-2.0: A software package for solving polynomial systems by the polyhedral homotopy continuation method*, Computing (Vienna/New York) **83** (2008), 109–133.
60. Anton Leykin, *Numerical algebraic geometry*, J. Softw. Algebra Geom. **3** (2011), 5–10. MR 2881262
61. Anton Leykin, Jose Israel Rodriguez, and Frank Sottile, *Trace test*, Arnold Math. J. **4** (2018), no. 1, 113–125.
62. Anton Leykin and Frank Sottile, *Galois groups of Schubert problems via homotopy computation*, Math. Comp. **78** (2009), no. 267, 1749–1765.
63. Julia Lindberg, Alisha Zachariah, Nigel Boston, and Bernard Lesieutre, *The distribution of the number of real solutions to the power flow equations*, IEEE Transactions on Power Systems (2022), 1–1.
64. Dhagash Mehta, Hung Dinh Nguyen, and Konstantin Turitsyn, *Numerical polynomial homotopy continuation method to locate all the power flow solutions*, IET Generation, Transmission & Distribution **10** (2016), no. 12, 2972–2980.
65. Mateusz Michałek and Bernd Sturmfels, *Invitation to nonlinear algebra*, Graduate Studies in Mathematics, vol. 211, American Mathematical Society, 2021.
66. Daniel Molzahn, Matthew Niemerg, Dhagash Mehta, and Jonathan Hauenstein, *Investigating the maximum number of real solutions to the power flow equations: Analysis of lossless four-bus systems*, 2016, `ArXiv:1603.05908`.
67. Alexander Morgan, *Solving polynomial systems using continuation for engineering and scientific problems*, Classics in Applied Mathematics, vol. 57, Society for Industrial and Applied Mathematics (SIAM), Philadelphia, PA, 2009, reprint of the 1987 edition.
68. Alexander P. Morgan, *A transformation to avoid solutions at infinity for polynomial systems*, Applied mathematics and computation **18** (1986), no. 1, 77–86.
69. Alexander P. Morgan and Andrew J. Sommese, *Coefficient-parameter polynomial continuation*, Applied Mathematics and Computation **29** (1989), no. 2, 123–160.
70. Alexander P. Morgan, Andrew J Sommese, and Charles W. Wampler, *Computing singular solutions to polynomial systems*, Advances in Applied Mathematics **13** (1992), no. 3, 305–327.

71. D. Nistér, *An efficient solution to the five-point relative pose problem*, IEEE Transactions on Pattern Analysis and Machine Intelligence **26** (2004), no. 6, 756–770.
72. R. Raguram, O. Chum, M. Pollefeys, J. Matas, and J.-M. Frahm, *USAC: A universal framework for random sample consensus*, IEEE Transactions on Pattern Analysis Machine Intelligence **35** (2013), no. 8, 2022–2038.
73. F. Ronga, A. Tognoli, and Th. Vust, *The number of conics tangent to 5 given conics: the real case*, Rev. Mat. Univ. Complut. Madrid **10** (1997), 391–421.
74. Siegfried M. Rump, *Solving algebraic problems with high accuracy*, Proc. of the Symposium on A New Approach to Scientific Computation (USA), Academic Press Professional, Inc., 1983, pp. 51–120.
75. S.M. Rump, *INTLAB - INTerval LABoratory*, Developments in Reliable Computing, Kluwer Academic Publishers, 1999, pp. 77–104.
76. H. Schubert, *Kalkul der abzählenden Geometrie*, Springer-Verlag, 1879, reprinted with an introduction by S. Kleiman, 1979.
77. _____, *Losüng des Charakteritiken-Problems für lineare Räume beliebiger Dimension*, Mittheil. Math. Ges. Hamburg (1886), 135–155, (dated 1885).
78. I. R. Shafarevich, *Basic algebraic geometry. 1*, second ed., Springer-Verlag, Berlin, 1994, Varieties in projective space.
79. Michael Shub and Steve Smale, *Complexity of Bezout's Theorem i: Geometric aspects*, Journal of the American Mathematical Society **6** (1993), no. 2, 459–501.
80. Andrew J. Sommese and Jan Verschelde, *Numerical homotopies to compute generic points on positive dimensional algebraic sets*, Journal of Complexity **16** (2000), no. 3, 572–602.
81. Andrew J. Sommese, Jan Verschelde, and Charles W. Wampler, *Numerical algebraic geometry*, The Mathematics of Numerical Analysis, volume 32 of Lectures in Applied Mathematics, AMS, 1996, pp. 749–763.
82. Andrew J. Sommese, Jan Verschelde, and Charles W. Wampler, *Symmetric functions applied to decomposing solution sets of polynomial systems*, SIAM Journal on Numerical Analysis **40** (2002), no. 6, 2026–2046.
83. _____, *Solving polynomial systems equation by equation*, Algorithms in algebraic geometry, IMA Vol. Math. Appl., vol. 146, Springer, New York, 2008, pp. 133–152.
84. Andrew J. Sommese and Charles W. Wampler, *The Numerical Solution of Systems of Polynomials Arising in Engineering and Science*, World Scientific, 2005.
85. F. Sottile, *Real solutions to equations from geometry*, University Lecture Series, vol. 57, American Mathematical Society, Providence, RI, 2011.
86. _____, *General witness sets for numerical algebraic geometry*, ISSAC'20—Proceedings of the 45th International Symposium on Symbolic and Algebraic Computation, ACM, New York, [2020] ©2020, pp. 418–425. MR 4144068
87. F. Sottile and T. Yahl, *Galois groups in enumerative geometry and applications*, 2021, `arXiv:2108.07905`.
88. J. Steiner, *Elementare Lösung einer geometrischen Aufgabe, und über einige damit in Beziehung stehende Eigenschaften der Kegelschnitte*, J. reine angew. Math. **37** (1848), 161–192.

89. Steven H. Strogatz, *From Kuramoto to Crawford: exploring the onset of synchronization in populations of coupled oscillators*, Physica D: Nonlinear Phenomena **143** (2000), no. 1-4, 1–20.
90. Bernd Sturmfels, *Polynomial equations and convex polytopes*, Amer. Math. Monthly **105** (1998), no. 10, 907–922.
91. ———, *Solving Systems of Polynomial Equations*, CBMS Regional Conferences Series, no. 97, American Mathematical Society, 2002.
92. ———, *What is . . . a Gröbner basis?*, Notices Amer. Math. Soc. **52** (2005), no. 10, 1199–1200.
93. Sascha Timme, *Mixed precision path tracking for polynomial homotopy continuation*, Advances in Computational Mathematics **47** (2021), no. 5, 75.
94. Jan Verschelde, *Algorithm 795: PHCpack: A General-Purpose Solver for Polynomial Systems by Homotopy Continuation*, ACM Trans. Math. Softw. **25** (1999), no. 2, 251–276.
95. André Weil, *Foundations of algebraic geometry*, American Mathematical Society, Providence, R.I., 1962. MR 0144898
96. A.T. Winfree, *Biological rhythms and the behavior of populations of coupled oscillators*, Journal of theoretical biology **16** (1967), no. 1, 15–42.
97. T. Yahl, *Computing Galois groups of Fano problems*, 2022, arXiv:2209.07010.

Daniel J. Bates, Department of Mathematics, U.S. Naval Academy, 572C Holloway Road, Mail Stop 9E, Annapolis, MD 21402, USA
Email address: dbates@usna.edu

Paul Breiding, Universität Osnabrück, FB Mathematik/Informatik, Albrechtstr. 28a, 49076 Osnabrück, Germany
Email address: pbreiding@uni-osnabrueck.de
URL: http://www.paulbreiding.org

Tianran Chen, Department of Mathematics, Auburn University at Montgomery, Montgomery, Alabama 36116, USA
Email address: ti@nranchen.org
URL: http://www.tianranchen.org

Jonathan D. Hauenstein, Department of Applied & Computational Mathematics & Statistics, University of Notre Dame, Notre Dame, IN 46556, USA
Email address: hauenstein@nd.edu
URL: http://www.nd.edu/~jhauenst

Anton Leykin, School of Mathematics, Georgia Institute of Technology, 686 Cherry Street, Atlanta, GA 30332-0160, USA
Email address: leykin@math.gatech.edu

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