Mss., 30 September 2019 arXiv.org/1812.02851

CERTIFICATION FOR POLYNOMIAL SYSTEMS VIA SQUARE SUBSYSTEMS

TIMOTHY DUFF, NICKOLAS HEIN, AND FRANK SOTTILE

ABSTRACT. We consider numerical certification of approximate solutions to a system of polynomial equations with more equations than unknowns by first certifying solutions to a square subsystem. We give several approaches that certifiably select which are solutions to the original overdetermined system. These approaches each use different additional information for this certification, such as liaison, Newton-Okounkov bodies, or intersection theory. They may be used to certify individual solutions, reject nonsolutions, or certify that we have found all solutions.

1. INTRODUCTION

Given polynomials $f = (f_1, \ldots, f_N)$ with $f_i \in \mathbb{C}[z_1, \ldots, z_n]$, an approximate solution to the system $f_1(z) = \cdots = f_N(z) = 0$ is an estimate $\hat{\zeta}$ of some point ζ where the polynomials all vanish (ζ is a *solution* to f), such that the approximation error $\|\zeta - \hat{\zeta}\|$ can be refined efficiently as a function of the input size and desired precision. Numerical certification seeks criteria and algorithms that guarantee that a computed estimate $\hat{\zeta}$ of a solution ζ to f is an approximate solution in this sense.

Many existing certification methods [19, 30] are for square systems, where $N = n$. These exploit that the isolated, nonsingular solutions to the system are exactly the fixed points of the Newton operator $N_f\colon \mathbb{C}^n \to \mathbb{C}^n$ given (where defined) by

$$N_f(z) \ := \ z - Df(z)^{-1} f(z)\,, \tag{1}$$

where $Df(z)$ is the Jacobian matrix of the system f evaluated at z. A Newton-based certificate establishes that the sequence of Newton iterates $(N_f^k(\hat{\zeta}) \mid k \in \mathbb{N})$ converges to a solution ζ to f. Examples include both Smale's α-test [29, 30] (typically performed in rational arithmetic) and Krawczyk's method [19] (based on interval arithmetic).

Once such a certificate is in hand, we say $\hat{\zeta}$ is an approximate solution to f with associated solution ζ. Further refinements bound the distance to the associated solution $\|\zeta - \hat{\zeta}\|$, decide if two approximate solutions are associated to the same solution, and, in the case of real systems, decide if the associated solution is real [10].

In the overdetermined case, where $N > n$, an analogous Newton operator may be defined using the pseudo-inverse of the Jacobian, but its fixed points may no longer be

2010 *Mathematics Subject Classification.* 65G20, 65H05.

Key words and phrases. certified solutions, alpha theory, polynomial system, numerical algebraic geometry, Newton-Okounkov bodies, Schubert calculus.

Work of Sottile supported in part by the National Science Foundation under grant DMS-1501370.

Work of Duff supported in part by the National Science Foundation under grant DMS-1719968.

Duff and Sottile supported by the ICERM.

solutions to the original system. In [2] a hybrid symbolic-numeric approach is used when the polynomials in f have rational coefficients. This requires computing an exact rational univariate representation [28] and using that to certify solutions. An alternate approach taken in [9, 11] is to reformulate the system f, adding variables to obtain an equivalent square system, which is then used for certification.

A common approach to solve an overdetermined system is via squaring up. For instance, we may take a generic $n \times N$ matrix $A \in \mathbb{C}^{n\times N}$ and instead solve the system

$$g := \begin{pmatrix} g_1(z) \\ \vdots \\ g_n(z) \end{pmatrix} = A \begin{pmatrix} f_1(z) \\ \vdots \\ f_N(z) \end{pmatrix} = 0 . \tag{2}$$

More generally, a square subsystem of f is defined by any n polynomials $g_1, \dots, g_n$ in the ideal generated by $f_1, \dots, f_N$. The solutions to a square subsystem g include the solutions to the original overdetermined system and some excess solutions. While approximate solutions to g may be certified by previously mentioned methods, to certify a point as an approximate solution to f we must distinguish it from these excess solutions.

We give several related algorithms to certify solutions to an overdetermined system f, based on certifying approximate solutions to a square subsystem g. Each uses additional global information about the geometry of the solutions or numbers of solutions to f or to g (or both). They address the problems below.

Problem 1. How may we certify that a point $\zeta \in \mathbb{C}^n$ is an approximate solution to f?

Problem 2. Suppose it is known that f has e solutions. How may we certify that a set $Z \subset \mathbb{C}^n$ of e points consists of approximate solutions to f?

We recall the main results of Smale's α-theory in Section 2 for certifying approximate solutions to a square system and give a definition of an approximate solution to a system f that is not square. This forms the basis for our certification algorithms. Section 3 discusses a certification based on liaison theory for addressing Problem 2. We give an algorithm for Problem 1 in Section 4.1 and discuss its relation to Newton-Okounkov bodies and Khovanskii bases. This illustrates the importance of developing computational tools for Khovanskii bases. While that algorithm may also be applied to Problem 2, we give a different algorithm in Section 4.2. We give three examples illustrating our algorithms in Section 5. One involves a finite Khovanskii basis, another is from the Schubert calculus, and a third is from computer vision.

2. Approximate solutions

We discuss approximate solutions to systems of polynomial equations. Given an approximate solution to one system, we give a method to certify that a polynomial does not vanish at the associated solution. We also discuss classical methods to certify solutions to square systems. Throughout, we will fix positive integers $n \leq N$. All polynomials will lie in the ring $\mathbb{C}[x_1, \dots, x_n]$. We will write f for a system $f_1, \dots, f_N$ of N polynomials. The system f is *square* when $N = n$.

We begin with our operational definition of an approximate solution.

Definition 2.1. A *δ-approximate solution* to a polynomial system f is a triple $(\hat{\zeta}, \delta, \mathcal{N}_f)$, where $\hat{\zeta} \in \mathbb{C}^n$, $\delta \in \mathbb{R}_{>0}$, and $\mathcal{N}_f\colon U \to \mathbb{C}^n$ is a map defined on some $U \subset \mathbb{C}^n$ such that

1) There exists $\zeta \in \mathcal{V}(f)$ such that $\|\zeta - \hat{\zeta}\| < \delta$, and
2) all iterates $\mathcal{N}_f^k(\hat{\zeta})$ are defined and the sequence $\mathcal{N}_f^k(\hat{\zeta})$ converges to ζ as $k \to \infty$.

Here $\|\cdot\|$ indicates the usual Hermitian norm on $\mathbb{C}^n$. We will refer to $\hat{\zeta}$ as an approximate solution when the procedure $\mathcal{N}_f$ and constant δ are understood. We call the point $\zeta \in \mathcal{V}(f)$ in (1) the solution to f associated to $\hat{\zeta}$.

Remark 2.2. In our examples, the system f and the approximate solution $\hat{\zeta}$ are defined over the rationals $\mathbb{Q}$ or the Gaussian rationals $\mathbb{Q}[i]$. Since numerical solvers typically output floating point results, care must be taken to control rounding errors when computing certificates. One option for certification is to perform all subsequent operations in rational arithmetic. Interval and ball arithmetic give yet another approach (discussed in Subsection 2.2). A "certificate" obtained without controlling rounding errors may still be of practical value. Following [10], we call this a *soft certificate*.

Remark 2.3. In all examples considered, the map $\mathcal{N}_f$ in Definition 2.1 restricts to a computable function $\mathcal{N}_{f,\mathbb{Q}}: U \cap \mathbb{Q}[\sqrt{-1}]^n \to \mathbb{Q}[\sqrt{-1}]^n$. We take a naive approach to questions of computability and complexity, but we do not rely on special features of nonstandard models of computation such as the Blum-Shub-Smale machine [3].

Let g be a square sytem and $(\hat{\zeta}, \delta, \mathcal{N}_g)$ be an approximate solution to g with associated solution ζ. Our main concern is to certify that $\zeta \in \mathcal{V}(f)$ when g is a square subsytem of f—a seemingly difficult task *a priori.* It is however relatively simple to certify that ζ is *not* a solution to a single polynomial f, provided that δ is sufficiently small. For $k \in \mathbb{N}$, let $S^k\mathbb{C}^n$ be the kth symmetric power of $\mathbb{C}^n$. This has a norm $\|\cdot\|$ dual to the standard unitarily invariant norm on homogeneous polynomials, and which satisfies $\|z^k\| \le \|z\|^k$, for $z \in \mathbb{C}^n$. The k-th derivative of g at ζ is a linear map $(D^k g)_\zeta : S^k(\mathbb{C}^n) \to \mathbb{C}^n$ with operator norm,

$$\|(D^k g)_\zeta\| := \max_{\substack{w \in S^k\mathbb{C}^n \\ \|w\|=1}} \|(D^k g)_\zeta (w)\| . \tag{3}$$

Proposition 2.4. *Suppose that $(\hat{\zeta}, \delta, \mathcal{N}_g)$ is an approximate solution to a square polynomial system g with associated solution ζ. For any polynomial f, if*

$$\left(|f(\hat{\zeta})| - \sum_{k=1}^{\deg f_j} \frac{\|(D^k f)_{\hat{\zeta}}\|}{k!} \cdot \delta^k \right) > 0 , \tag{4}$$

then $f(\zeta) \neq 0$.

Proof. By Taylor expansion, it follows that $f(z) \neq 0$ for any $z \in B(\hat{\zeta}, \delta)$. □

Let us write $\delta(f, g, \hat{\zeta})$ for the quantity in the inequality (4), which we will call a *Taylor residual*. If $f = (f_1, \ldots, f_N)$ is a polynomial system, then we define its Taylor residual $\delta(f, g, \hat{\zeta})$ to be maximum of the Taylor residuals $\delta(f_i, g, \hat{\zeta})$, for $i = 1, \ldots, N$. For this test of nonvanishing using Taylor residuals to be practical, we need to estimate the operator norms of the higher derivatives. One possible bounding strategy, as explained in [29, §I-3] and [10, §1.1], uses the first derivative alone. Another option, less suitable for polynomials of high degree, is to bound with the entry-wise ℓ_2 or ℓ_1 norms of these tensors. Proposition 2.4 may fail to certify that ζ is not a zero of f if the number δ for the approximate solution $\hat{\zeta}$ is insufficiently small. This does not happen if we use $\mathcal{N}_g$ to refine $\hat{\zeta}$.

Corollary 2.5. *Let $f = (f_1, \ldots, f_N)$ be a system of polynomals and suppose that $\zeta \notin \mathcal{V}(f)$. There is a $k \geq 0$ such that if $i \geq k$, and we replace $\hat{\zeta}$ by $\mathcal{N}_g^i(\hat{\zeta})$, then the Taylor residual $\delta(f, g, \hat{\zeta})$ is positive and (4) holds.*

Proof. The sequence $\{\mathcal{N}_g^i(\hat{\zeta}) \mid i \in \mathbb{N}\}$ converges to ζ. Thus $\beta(g, \mathcal{N}_g^i(\hat{\zeta}))$ converges to zero and for every j, $f_j(\mathcal{N}_g^i(\hat{\zeta}))$ converges to $f_j(\zeta)$. Let j be an index such that $f_j(\zeta) \neq 0$. Then the Taylor residual $\delta(f_j, g, \mathcal{N}_g^i(\hat{\zeta}))$ converges to to $|f_j(\zeta)|$. □

A consequence of Definition 2.1 is that each iterate $\mathcal{N}_f^k(\hat{\zeta})$ is an approximate solution, as $\mathcal{N}_f^k(\hat{\zeta}) \to \zeta$. We wish to quantify this rate of convergence. The triangle inequality gives a test for when approximate solutions $(\hat{\zeta}_1, \delta_1, \mathcal{N}_f)$ and $(\hat{\zeta}_2, \delta_2, \mathcal{N}_f)$ have distinct associated solutions, namely if

$$\|\hat{\zeta}_1 - \hat{\zeta}_2\| \ > \ \delta_1 + \delta_2 \,. \tag{5}$$

It is useful to have some additional criterion when two approximate solutions have the *same* associated solutions, that is, we wish to certify *uniqueness* of the associated solution in sufficiently small region. This motivates our next definition.

Definition 2.6. An *effective approximate solution* $(\hat{\zeta}, \mathcal{N}_f, \delta, k_*)$ to a system f consists of a nonincreasing rate function $\delta\colon \mathbb{N} \to \mathbb{R}_{>0}$ with $\lim_{k\to\infty} \delta(k) = 0$, and an integer k_* such thatt

1) $\hat{\zeta}$ is a $\delta(0)$-approximate solution to f with associated solution ζ,
2) $\|\mathcal{N}_f^j(\hat{\zeta}) - \zeta\| < \delta(k)$ for all $j \geq k$, and
3) For some iterate k_*, ζ is the unique solution in the ball $B(\mathcal{N}_f^{(k_*)}(\hat{\zeta}), \delta(k_*))$.

We say the rate of convergence for the effective approximate solution has order $\delta(k)$.

The rate of convergence is *quadratic* when $\delta(k) = 2^{-2^{O(k)}}\, \|\zeta - \hat{\zeta}\|$. This implies that each application of $\mathcal{N}_f(\cdot)$ roughly doubles the number of significant digits in $\hat{\zeta}$. We generalize the method for certifying distinct solutions in [10, §I-2].

Proposition 2.7. *Given a set of effective approximate solutions $S' = \{(\hat{\zeta}_i, \mathcal{N}_f, \delta_i, k_*^i)\}$ to a system f, we may compute a set S of refined approximate solutions with distinct associated solutions comprising all solutions associated to the set S'.*

Proof. We need only replace each $\hat{\zeta}_i$ with its refinement $\mathcal{N}_f^{k_*^i}(\hat{\zeta}_i)$. After refinement, the solutions associated to $\hat{\zeta}_i$ and $\hat{\zeta}_j$ are distinct if and only if inequality (5) holds. □

Certificates for square systems are generally based on Newton's method. We observe that Definitions 2.1 and 2.6 encapsulate several existing certification paradigms for square systems.

2.1. **Smale's α-theory.** The central quantities of Smale's α-theory are defined as follows. With g as above and $\hat{\zeta} \in \mathbb{C}^n$ a point where $Dg(\hat{\zeta})$ is invertible,

$$
\begin{aligned}
\alpha(g,\hat{\zeta}) &:= \beta(g,\hat{\zeta}) \cdot \gamma(g,\hat{\zeta}) \ , \ \text{where} \\
\beta(g,\hat{\zeta}) &:= \|\hat{\zeta} - N_g(\hat{\zeta})\| \ = \ \|Dg(\hat{\zeta})^{-1} g(\hat{\zeta})\| \ , \ \text{and} \\
\gamma(g,\hat{\zeta}) &:= \sup_{k \geq 2} \left\| \frac{Dg(\hat{\zeta})^{-1}(D^k g)_{\hat{\zeta}}}{k!} \right\|^{\frac{1}{k-1}} .
\end{aligned} \tag{6}
$$

Note that $\beta(g,\hat{\zeta})$ is the length of a Newton step at $\hat{\zeta}$. The following proposition gives a criterion for approximate solutions in the sense of Definition 2.1.

Proposition 2.8 ([3, p. 160])**.** *Let g be a square polynomial system and $\hat{\zeta} \in \mathbb{C}^n$. If*

$$\alpha(g,\hat{\zeta}) \ < \ \frac{13 - 3\sqrt{17}}{4} \ \approx \ 0.15767078\,,$$

then $\hat{\zeta}$ is $2\beta(g,\hat{\zeta})$-approximate solution to g and the Newton iterates $N_g^k(\hat{\zeta})$ converge quadratically.

Criteria for quadratically convergent effective approximate solutions in the sense of Definition 2.6 can also be given in terms of $\alpha(g,\hat{\zeta})$. The analysis amounts to showing that N_g is a contraction mapping in a suitable neighborhood of ζ. This is given by the "robust" α-theorem (Theorem 6 and Remark 9 of [3, Ch. 8]).

Proposition 2.9. *Let g be a square polynomial system and $\hat{\zeta} \in \mathbb{C}^n$ an approximate solution to g with associated solution ζ and suppose that $\alpha(g,\hat{\zeta}) < 0.03$. If $\hat{\zeta}' \in \mathbb{C}^n$ satisfies*

$$\|\hat{\zeta} - \hat{\zeta}'\| < \ \frac{1}{20\gamma(g,\hat{\zeta})}\,,$$

then $\hat{\zeta}'$ is an approximate solution to g with associated solution ζ.

It follows that, for $\delta(k) = 2^{-2^{k-1}}\beta(\hat{\zeta})$, we have $(\hat{\zeta}, N_g, \delta, 0)$ is an effective approximate solution in the sense of Definition 2.6.

2.2. **Other approaches.** The classical analysis of Newton's method is due to Kantorovich. Several variations exist, all assuming some local Lipchitz condition on the Jacobian D_g and boundedness conditions on $D_g(\hat{\zeta})^{-1}$. For instance, in [34] the following conditions imply that that $\hat{\zeta}$ is an approximate solution for Newton's method.

There exist positive real numbers B, K, and η, such that

1) g is differentiable in a convex, open set $D_0 \ni \hat{\zeta}$,
2) $\|D_g(\hat{\zeta})^{-1}\| \leq B$,
3) $\|D_g(\hat{\zeta})^{-1} g(\hat{\zeta})\| \leq \eta$,
4) $\|D_g(x) - D_g(y)\| \leq K\|x - y\|$ for all $x, y \in D_0$, and
5) $BK\eta \leq 1/2$.

Explicit bounds on the rate of convergence in terms of these constants are also given. For a survey of variants and the relationship of Kantorovich's theorem to α-theory, see [21].

Approximate solutions may also be understood within the general program of interval and ball arithmetics. Both paradigms rely on defining arithmetic operations on intervals or balls and are definable in either exact or floating point arithmetic. In general, operations on intervals represent *enclosures*. In exact interval arithmetic, we define the sum by $[a, b] + [c, d] = [a + c, b + d]$. For floating point arithmetic, we may either accept a soft certificate or control rounding errors when defining arithmetic operations so as to obtain a rigorous certificate. We refer to [20, 25, 35] for a more comprehensive treatment of these notions. A variety of interval/ball-valued Newton iterations have been studied. A popular variant is the Krawcyzk Method—see [25, Chapter 6] for an introduction, [24] for quadratic convergence, and [5] for extensions to complex analytic functions. Once a Newton-like iteration is in place, we get criteria for approximate solutions in the sense of definitions 2.1 and 2.6 simply by taking midpoints/centers.

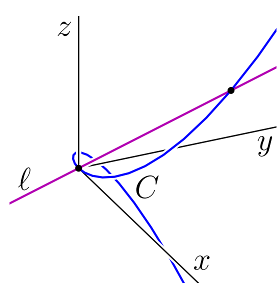
3. Certification via liaison pruning

Suppose that we have an overdetermined system f with a square subsystem g, so that $\mathcal{V}(f) \subset \mathcal{V}(g)$. Suppose further that we have a square system h with $\mathcal{V}(h) = \mathcal{V}(g) \smallsetminus \mathcal{V}(f)$. Given this, we may certify all approximate solutions to g and then certify the subset of those that are approximate solutions to h, so that the solutions in $\mathcal{V}(g) \smallsetminus \mathcal{V}(h)$ which remain are certifiably approximate solutions to f. When this occurs, we say that $\mathcal{V}(f)$ is in liaison with the complete intersection $\mathcal{V}(h)$.

Let us begin with some definitions. A system $g_1, \ldots, g_r$ of r polynomials is a *complete intersection* if the variety $\mathcal{V}(g_1, \ldots, g_r) \subset \mathbb{C}^n$ they define has dimension $n-r$, equivalently if it has *codimension* r. A square system is a zero-dimensional complete intersection.

More generally, varieties $X, Y \subset \mathbb{C}^n$ of codimension r are in *liaison* if there are polynomials $g_1, \ldots, g_r \in \mathbb{C}[x_1, \ldots, x_n]$ such that $\mathcal{V}(g_1, \ldots, g_r) = X \cup Y$. This relation has been deeply studied (see [18] and the references therein). Of particular interest is when one of the varieties, say Y, is itself a (different) complete intersection, so that X is in liaison with a complete intersection. (This is a special case of the *licci* equivalence relation.)

Example 3.1. The closure of the set $\{[1, t, t^2, t^3] \mid t \in \mathbb{C}\}$ is the rational normal curve $C \subset \mathbb{P}^3$. It is defined by three quadrics, $wy - x^2, wz - xy, xz - y^2$, and is thus not a complete intersection. In the affine patch $\mathbb{C}^3$ defined by $w = 1$, if we use the difference of the first two generators and the last generator, then $\mathcal{V}(z - y + x^2 - xy, xz - y^2) = C \cup \ell$, where $\ell = \mathcal{V}(x - y, x - z)$ is the line $\{(t, t, t) \mid t \in \mathbb{C}\}$.



◇

Let $X \subset \mathbb{C}^n$ be a variety of codimension r that is in liaison with a complete intersection Y. There are polynomials $f = (f_1, \ldots, f_s)$, $g = (g_1, \ldots, g_r)$, and $h = (h_1, \ldots, h_r)$ such that

$$X = \mathcal{V}(f), \qquad X \cup Y = \mathcal{V}(g), \qquad \text{and} \qquad Y = \mathcal{V}(h).$$

A *square system* on X consists of polynomials $g_{r+1}, \ldots, g_n$ that are sufficiently general in that $X \cap \mathcal{V}(g_{r+1}, \ldots, g_n)$ is a finite set and the intersection is transverse. Then

$$\mathcal{V}(g_1, \ldots, g_n) \;=\; (X \cap \mathcal{V}(g_{r+1}, \ldots, g_n)) \,\cup\, (Y \cap \mathcal{V}(g_{r+1}, \ldots, g_n))\,. \tag{7}$$

Thus the square system $X \cap \mathcal{V}(g_{r+1}, \ldots, g_n)$ on X is the set-theoretic difference of two square systems of polynomials, $\mathcal{V}(g_1, \ldots, g_n)$ (7) and

$$\mathcal{V}(h_1, \ldots, h_r\,,\, g_{r+1}, \ldots, g_n) \;=\; Y \cap \mathcal{V}(g_{r+1}, \ldots, g_n)\,. \tag{8}$$

For example, let C be the rational normal curve of Example 3.1 in $\mathbb{C}^3$, which has codimension 2, so that $C \cap \mathcal{V}(x+y+z+1)$ is a square system on C. Manipulating the polynomials in $\mathcal{V}(z-y+x^2-xy, xz-y^2, x+y+z+1)$ leads to the solutions

$$(-\tfrac{1}{3}, -\tfrac{1}{3}, -\tfrac{1}{3}) \;\text{ on } \ell \;\text{ and }\; (-1,1,-1) \text{ and } (\pm\sqrt{-1}, -1, \mp\sqrt{-1}) \;\text{ on } C\,.$$

As we may certifty solutions and nonsolutions to systems (7) and (8), this discussion leads to the following certification algorithm, when a variety X is in liaison with a complete intersection Y. This uses the test of Proposition 2.4, the Taylor residual (4), and Smale's α-theory for the system (8).

Algorithm 1 (Certifying solutions to a square system on a variety X)**.**
Input: (r, g, h, S)

- $r \in \mathbb{N}$
- $g = (g_1, \ldots, g_n)$ — a square polynomial system such that $\mathcal{V}(g_1, \ldots, g_r) = X \cup Y$, with both X and Y of codimension r
- $h = (h_1, \ldots, h_r)$ — polynomials such that $\mathcal{V}(h) = Y$
- $S = \{\hat{\zeta_1}, \ldots, \hat{\zeta_m}\}$ — pairwise distinct approximate solutions to g with refinement operator $\mathcal{N}_g$

Output: $T, U \subset S$ with $S = T \sqcup U$, where T consists of approximate solutions to $X \cap \mathcal{V}(g_{r+1}, \ldots, g_n)$ and U consists of approximate solutions to $Y \cap \mathcal{V}(g_{r+1}, \ldots, g_n)$.

```
1: Set f := (h_1, ..., h_r , g_{r+1}, ..., g_n), a square system on Y.
2: Initialize T ← ∅, U ← ∅
3: for ζ̂ ∈ S do
4:    ζ' ← ζ̂
5:    if α(f, ζ') < (13−3√17)/4 then U ← U ∪ {ζ̂}
6:     else if δ(f, g, ζ') > 0 then T ← T ∪ {ζ̂}
7:     else ζ' ← N_g(ζ') and return to 5.
8:    end if
9: end for
```

Remark 3.2. As in all subsequent algorithms, we assume distinct approximate solutions for $\mathcal{N}_g$ as part of the input. We could have just as easily assumed effective approximate solutions. The test in line 6 could be replaced by testing that ζ' is an approximate solution to the square system f by some criterion other than α-theory—for simplicity, we do not assume this criterion is part of the input.

Proof of correctness. As $\hat{\zeta} \in S$, it is an approximate solution to the square system g with an associated nonsingular solution $\zeta \in \mathcal{V}(g) \subset X \cup Y$. Since ζ is nonsingular, $\zeta \notin X \cap Y$, as $X \cup Y$ is singular along $X \cap Y$. Thus $\zeta \in X$ if and only if $\zeta \notin Y$. Let $\{\hat{\zeta}_i \mid i \in \mathbb{N}\}$ be the sequence of iterates using $\mathcal{N}_g$ starting at $\hat{\zeta}$. This converges to ζ.

If $\zeta \in Y$, then $\zeta \in \mathcal{V}(f)$, and the sequence $\{\hat{\zeta}_i\}$ will eventually lie in the basin of quadratic convergence for Newton iterations N_f and $\beta(f, \hat{\zeta}_i)$ converges to 0. As $\gamma(f, \hat{\zeta}_i)$ is bounded, $\alpha(f, \hat{\zeta}_i) = \gamma(f, \hat{\zeta}_i) \cdot \beta(f, \hat{\zeta}_i)$ converges to 0. Thus the condition in Step 5 will eventually hold and $\hat{\zeta}$ will be placed in U.

If $\zeta \notin Y$, then $\zeta \notin \mathcal{V}(f)$. By Corollary 2.5 the sequence $\delta(f, g, \zeta_j)$ of Taylor residuals (4) is eventually positive. Thus the condition in Step 6 will eventually hold and $\hat{\zeta}$ will be placed in T. □

We describe a more involved application of this idea. Write codim X for the codimension, $n - \dim X$, of a variety $X \subset \mathbb{C}^n$. Suppose that $X_1, \dots, X_m \subset \mathbb{C}^n$ are in general position and $\sum \operatorname{codim} X_i = n$, then Bertini's Theorem [17] implies that

$$X_1 \bigcap X_2 \bigcap \cdots \bigcap X_m \tag{9}$$

is a transverse intersection consisting of finitely many points. When $n = m$, so that each $X_i = \mathcal{V}(f_i)$ is a hypersurface, then (9) is equivalent to the square polynomial system

$$f_1 \;=\; f_2 \;=\; \cdots \;=\; f_n \;=\; 0\,.$$

As a variety need not be a complete intersection, a *square system of varieties* (9) with $m < n$ does not necessarily have a formulation as a square system of polynomials.

Suppose now that $X_1, \dots, X_m \subset \mathbb{C}^n$ form a square system of varieties (9), each X_i is in liaison with a complete intersection Y_i, and these are all in sufficiently general position. Then there are square systems $g_1, \dots, g_n$ and $h_1, \dots, h_n$ of polynomials such that if $a_\bullet\colon 0 = a_0 < a_1 < \cdots < a_m = n$ is defined by $a_i - a_{i-1} = \operatorname{codim} X_i (= \operatorname{codim} Y_i)$ for each i, then

$$\mathcal{V}(g_{1+a_{i-1}}, \dots, g_{a_i}) \;=\; X_i \cup Y_i \qquad \text{and} \qquad \mathcal{V}(h_{1+a_{i-1}}, \dots, h_{a_i}) \;=\; Y_i\,, \tag{10}$$

are complete intersections for each $i = 1, \dots, m$. Thus

$$\mathcal{V}(g) \;=\; \bigcap_{i=1}^{m} (X_i \cup Y_i)\ . \tag{11}$$

We give a more general version of Algorithm 1 that will certify solutions to the square system (9) of varieties, given solutions (11) to the square system g.

Algorithm 2 (Certifying solutions to a square system of varieties)**.**
Input: $(a_\bullet, g, h, S)$

$a_\bullet\colon 0 = a_0 < a_1 < \cdots < a_m = n$
$g = (g_1, \dots, g_n)$ and $h = (h_1, \dots, h_n)$ — square polynomial systems such that for each $i = 1, \dots, m$, (10) are complete intersections.
$S = \{\hat{\zeta}_1, \dots, \hat{\zeta}_s\}$ — pairwise distinct approximate solutions to g

Output: $T \subset S$ consisting of approximate solutions to $X_1 \cap X_2 \cap \cdots \cap X_m$.

1: **for** $i = 1, \dots, m$ **do**
2: Set $f := (g_1, \dots, g_{a_{i-1}}\,,\ h_{1+a_{i-1}}, \dots, h_{a_i}\,,\ g_{1+a_i}, \dots, g_n)$.
3: Initialize $T \leftarrow \emptyset$

4: **for** $\hat{\zeta} \in S$ **do**
5: $\zeta' \leftarrow \hat{\zeta}$
6: **if** $\alpha(f, \zeta') < \frac{13-3\sqrt{17}}{4}$ **then** discard $\hat{\zeta}$
7: **else if** $\delta(f, g, \zeta') > 0$ **then** $T \leftarrow T \cup \{\hat{\zeta}\}$
8: **else** $\zeta' \leftarrow \mathcal{N}_g(\zeta')$ and return to 6.
9: **end if**
10: **end for**
11: $S \leftarrow T$
12: **end for**

Proof of correctness. By algorithm 1, in each iteration $i = 1, \ldots, m$ of the outer loop, the algorithm constructs the set T of elements of the input S that do not lie in $Y_1 \cup \cdots \cup Y_i$. As $S \cap X_1 \cap \cdots \cap X_m = S \smallsetminus (Y_1 \cup \cdots \cup Y_m)$, we see that the algorithm performs as claimed. □

4. Certification via squaring-up

In Section 3, we used liaison theory to certify the nonsolutions $\mathcal{V}(g) \smallsetminus \mathcal{V}(f)$ to a system f among the certified solutions to a square subsystem g of f. We now present two further approaches. In Subsection 4.1, if we know the number $d = \#(\mathcal{V}(g) \smallsetminus \mathcal{V}(f))$ of nonsolutions, then we have a stopping criterion when using Proposition 2.4 to certify nonsolutions. One method to determine d is via Newton-Okounkov bodies and Khovanskii bases. In Subsection 4.2, we suppose that we have the additional information that $\#\mathcal{V}(f) = e$ and $\#\mathcal{V}(g) = d$, and use it to certify that we have found all solutions to f. One source of such detailed information is intersection theory.

4.1. Certifying individual solutions.

The consequences of α-theory and Proposition 2.4 furnish a certification procedure for overdetermined systems in the following setting— Suppose we are given a system f, a square subsystem g where we know, by some means, an integer d such that

$$d \;=\; \#\left(\mathcal{V}(g) \setminus \mathcal{V}(f)\right) . \tag{12}$$

If we can certify d solutions to g which are not solutions to f, then any other solutions to g must be solutions to f.

Algorithm 3 (Certifying individual solutions)**.**
Input: (f, g, d, S)
f — a polynomial system
g — a square subsystem of f
$d \in \mathbb{N}$ satisfying (12)
$S = \{\hat{\zeta_1}, \ldots, \hat{\zeta_m}\}$ — pairwise distinct approximate solutions to g
Output: $T \subset S$, a set of approximate solutions to f
Initialize $R \leftarrow \emptyset$
for $j = 1, \ldots, m$ **if** $\delta(f, g, \hat{\zeta}_j) > 0$ **then** $R \leftarrow R \cup \{\zeta_j\}$
if $(\#R == d)$ **then** $T \leftarrow S \smallsetminus R$ **, else** $T \leftarrow \emptyset$
return T

Remark 4.1. *A priori,* we only need to know that $d \geq \#\left(\mathcal{V}(g) \setminus \mathcal{V}(f)\right)$—if the inequality is strict, we necessarily return an empty set.

Theorem 4.2. *Suppose that f, g, d, S are valid input for Algorithm 3. Then its output consists of approximate solutions to f.*

Proof. If T is empty there is nothing to prove. Otherwise, there are d distinct solutions to g associated to points of R—by Proposition 2.4, these are not solutions to f. Since the solutions associated to points of T are disjoint from those associated to points of R, by assumption and (12) they associate to solutions to f. □

Perhaps the main difficulty in applying Algorithm 3 is obtaining the correct number d. When we square up by random matrix as in (2), this number is given by a birationally-invariant intersection index over $\mathbb{C}^n$. We summarize the basic tenets of this theory as developed in [13, 14].

Definition 4.3. ([14, Def. 4.5]) Let X be an n-dimensional irreducible variety over $\mathbb{C}$ with singular locus X_{sing}. For an n-tuple $(L_1, L_2, \ldots, L_n)$ of finite-dimensional complex subspaces of the function field $\mathbb{C}(X)$, let $\boldsymbol{L} = L_1 \times L_2 \times \cdots \times L_n$, and define

$$U_{\mathbf{L}} \ := \ \{z \in X \setminus X_{sing} \mid L_i \subset \mathcal{O}_{X,z} \text{ for } i = 1, \ldots, n\},$$

the set of smooth points where every function in each subspace L_i is regular, and

$$Z_{\mathbf{L}} \ := \ \bigcup_{i=1}^{n} \{z \in U_{\boldsymbol{L}} \mid f(z) = 0 \ \ \forall f \in L_i\},$$

the set of basepoints of $\boldsymbol{L}$. For generic $g = (g_1, \ldots, g_n) \in \boldsymbol{L}$, all solutions to the system $g_1(z) = \cdots = g_n(z) = 0$ on $U_{\mathbf{L}} \smallsetminus Z_{\mathbf{L}}$ are nonsingular and their number is independent of the choice of g. The common number is the birationally invariant intersection index $[L_1, L_2, \ldots, L_n]$.

These claims are proven in [13, Sections 4 & 5]. For our purposes, $X = \mathbb{C}^n$ and $\boldsymbol{L} = L \times \cdots \times L$ where $L \subset \mathbb{C}[z_1, \ldots, z_n]$ is the linear space spanned by the polynomials in our system f. Write d_L for this self-intersection index, note that $U_{\boldsymbol{L}} = \mathbb{C}^n$, while $Z_{\boldsymbol{L}} = \mathcal{V}(f)$. Thus (12) holds for general square subsystems of f, taking $d = d_L$.

Let $\nu\colon \mathbb{C}(X)^\times \to (\mathbb{Z}^n, \prec)$ be a surjective valuation where $\prec$ is some fixed total order on $\mathbb{Z}^n$. For example, ν could restrict to the exponent of the leading monomial in a term order $\prec$ on $\mathbb{C}[x_1, \ldots, x_n]$. We attach to (L, ν) the following data:

- $A_L = \bigoplus_{k=0}^{\infty} t^k L^k$—a graded subalgebra of $\mathbb{C}(X)[t]$.
- $S(A_L, \nu) = \{(\nu(f), k) \mid f \in L^k \text{ for some } k \in \mathbb{N}\}$, a sub-monoid of $\mathbb{Z}^n \oplus \mathbb{N}$ associated to the pair (L, ν), where L^k is the $\mathbb{C}$-span of k-fold products from L. This is the *initial algebra* of A_L with respect to the extended valuation $\nu_t\colon \mathbb{C}(X)(t)^\times \to (\mathbb{Z}^n \oplus \mathbb{Z}, \prec_t)$ defined by $\nu_t(f_k\, t^k + \cdots + f_0) \mapsto (\nu(f_k), k)$, where $\prec_t$ is the levelwise order defined by

$$(\alpha_1, k_1) \ \prec_t \ (\alpha_2, k_2) \quad \text{if} \quad k_1 \ > \ k_2 \quad \text{or} \quad k_2 \ = \ k_1 \text{ and } \quad \alpha_1 \ \prec \ \alpha_2\,.$$

- $\mathrm{ind}(A_L, \nu)$—the index of $\mathbb{Z}\, S(A_L, \nu) \cap (\mathbb{Z}^n \times \{0\})$ as a subgroup of $\mathbb{Z}^n \times \{0\}$.
- $\overline{\mathrm{Cone}(A_L, \nu)}$—the Euclidean closure of all $\mathbb{R}_{\geq 0}$-linear combinations from $S(A_L, \nu)$.

- $\Delta(A_L,\nu) = \overline{\mathrm{Cone}(A_L,\nu)} \cap (\mathbb{R}^n \times \{1\})$—the *Newton-Okounkov body.*

The linear space L induces a rational *Kodaira map*

$$\Psi_L : X \dashrightarrow \mathbb{P}(L^*) \qquad z \mapsto [f \mapsto f(z)],$$

with the section ring A_L the projective coordinate ring of the image.

Proposition 4.4 ([14, Thm. 4.9])**.** *Let L be a finite-dimensional subspace of $\mathbb{C}(X)$. Then*

$$d_L = \frac{n!\,\deg \Psi_L}{\mathrm{ind}(A_L,\nu)} \cdot \mathrm{Vol}\ \Delta(A_L,\nu).$$

Here, Vol *denotes the n-dimensional Euclidean volume in the slice $\mathbb{R}^n \times \{1\}$.*

In our setting, where $X = \mathbb{C}^n$ and $L = \mathrm{span}_{\mathbb{C}}\{f_1,\dots,f_N\}$, the Kodaira map Ψ_L is $z \mapsto [f_1(z) : f_2(z) : \cdots : f_N(z)]$. Thus, if need be, $\deg \Psi_L$ may be computed symbolically. The main difficulty in applying Proposition 4.4 is that it may be hard to determine the Newton-Okounkov body, as the monoid $S(A_L,\nu)$ need not be finitely generated. This leads us to the notion of a finite Khovanskii basis [15].

Definition 4.5. A *Khovanskii basis* for (L,ν) is a set $\{a_i \mid i \in I\}$ of generators for the algebra A_L whose values $\{\nu_t(a_i) \mid i \in I\}$ generate the monoid $S(A_L,\nu)$. If $<$ is a global monomial order on $k[z_1,\dots,z_n]$, taking lead monomials defines a valuation $\nu\colon k[z_1,\dots,z_n] \to (\mathbb{Z}^n,\prec)$, where $\prec$ is the reverse of $<$. A Khovanskii basis with respect this valuation is commonly known as a *SAGBI basis* [12, 27].

When the monoid $S(A_L,\nu)$ is finitely generated, there is a finite Khovanskii basis for (L,ν). When this occurs, we may compute the Khovanskii basis via a binomial-lifting/subduction algorithm such as described in [27] or [33, Ch. 11].

Example 4.6. We consider an "illustrative example" of an overdetermined system from [2]:

$$\begin{pmatrix} f_1(z_1,z_2,z_3) \\ f_2(z_1,z_2,z_3) \\ f_3(z_1,z_2,z_3) \\ f_4(z_1,z_2,z_3) \end{pmatrix} = \begin{pmatrix} z_1^2 + z_2^2 - 1, \\ -16\,z_2^2 + 8\,z_1 + 17, \\ -z_2^2 + z_1 - z_3 - 1, \\ 64\,z_1 z_2 + 16\,z_2 \end{pmatrix}$$

The square subsystem defiened by $f_1 = f_2 = f_3 = 0$ has two singular solutions, and f_4 is the Jacobian determinant of this subsystem. Letting $<$ be the graded reverse lexicographic ordering with $z_1 > z_2 > z_3$ and $L = \mathrm{span}_{\mathbb{C}}\{f_1,f_2,f_3,f_4\}$. We observe that the initial terms of $tf_1,\dots,tf_4 \in A_L$ under the induced order $<_t$ are given by $t\,z_1^2$, $-16\,t\,z_2^2$, $-t\,z_2^2$, 64 and $t\,z_1z_2$. The lattice points corresponding to these monomials lie in the linear subspace of $\mathbb{R}^3 \times \{1\}$ defined by $x_3 = 0$. However, we have that

$$\begin{aligned} 512\,t^2 z_1^2 z_3 + 6656\,t^2 z_1 z_3 - 6400\,t^2 z_3^2 + 14000\,t^2 z_1 - 26368\,t^2 z_3 - 27125\,t^2 \\ = t^2\left(64\,f_1 f_2 - 21\,f_2^2 - 512\,f_1 f_3 + 768\,f_2 f_3 - 6400\,f_3^2 + \tfrac{1}{8}\,f_4^2\right) \in A_L, \end{aligned}$$

giving that

$$\begin{pmatrix} 2 \\ 0 \\ 1 \\ 2 \end{pmatrix} \in S(A_L).$$

This element of A_L was obtained by the binomial-lifting/subduction algorithm—carrying this out further, we can verify that this new element together with the original generators give a finite Khovanskii basis for A_L. Thus we have

$$\Delta_L = \mathrm{conv}\left(\begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 2 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 2 \\ 0 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 1/2 \\ 1 \end{pmatrix} \right).$$

We also have that $\deg \Psi_L = 2$ and $\mathrm{ind}(A_L) = 1$. Thus, we have $[L, L, L] = 2$, giving a total root count of 4 after squaring up f.

We describe such another example of finite Khovanskii basis Section 5.1. We note that a finite Khovanskii basis may also be determined theoretically [1, 4, 16]. However, the mere existence of finite Khovanskii bases is a nontrivial matter.

Example 4.7 ([27, Ex. 1.20])**.** Let $L = \mathrm{span}_{\mathbb{C}}\{z_1 + z_2,\ z_1 z_2,\ z_1 z_2^2, 1\} \subset \mathbb{C}(z_1, z_2)$. Endow $\mathbb{Z}^2$ with the lexicographic order where $\alpha_1 < \alpha_2$ for $(\alpha_1, \alpha_2) \in \mathbb{Z}^2$, and let $\nu\colon \mathbb{C}(z_1, z_2)^\times \to \mathbb{Z}^2$ be the valuation whose restriction to polynomials takes a polynomial to its lex-minimal monomial. Noting that

$$z_1 z_2^n t^n \ = \ (z_1 + z_2)t \cdot z_1 z_2^{n-1} t^{n-1} - z_1 z_2 t \cdot z_1 z_2^{n-2} t^{n-2} \cdot t \quad \in \ t^n L^n$$

for all $n \geq 1$, we have $(1, n, n) \in S(A_L, \nu)$ for all n, which implies that $(0, 1, 1) \in \Delta(A_L, \nu)$. On the other hand, $A_L \cap k(z_2)[t] = 0$. Thus $S(A_L, \nu)$ is not finitely generated.

Despite the apparent difficulty of computing Khovanskii bases, we see from Proposition 4.4 that they enable an algorithmic study of polynomial systems based on L. Numerical certification is one application which illustrates the importance of developing more efficient and robust computational tools for Khovanskii bases.

4.2. **Certifying a set of solutions.** We give a second algorithm using α-theory to certify solutions to an overdetermined system f to solve Problem 2. Suppose that we have an overdetermined system f that is known to have e solutions whose square subsystems are known to have d solutions. While we could apply Algorithm 3 to certify approximate solutions to f, we propose an alternative method to solve this problem.

Algorithm 4 (Certifying a set of solutions)**.**
Input: (d, e, f, g, S, B)

$e \leq d$ — integers
f — a polynomial system with e solutions
g, g' — two square subsystems of f
$S = \{\hat{\zeta}_1, \ldots, \hat{\zeta}_d\}$ — a set of d distinct approximate solutions to g

$B = \{B(\hat{\zeta}_1, \rho_1), \ldots, B(\hat{\zeta}_d, \rho_d)\}$ — a set of separating balls as in Proposition 2.7
S' — a set of d distinct approximate solutions to g'

Output: $T \subset S$, a set of approximate solutions to f

1: Initialize $T \leftarrow \emptyset$
2: $r \leftarrow \min\limits_{1\le i<j\le d} \Big(\|\hat{\zeta}_i - \hat{\zeta}_j\| - (\rho_i + \rho_i) \Big)$
3: **for** $\hat{\zeta}' \in S'$ **do**
4: **repeat** $\hat{\zeta}' \leftarrow N_{g'}(\hat{\zeta}')$ **until** $2\,\beta(g', \hat{\zeta}') < r/3$
5: $\rho' \leftarrow 2\,\beta(g', \hat{\zeta}')$
6: **for** $j = 1, \ldots, d$ **if** $B(\hat{\zeta}_j, \rho_j) \cap B'(\hat{\zeta}', \rho') \neq \emptyset$ **then** $T \leftarrow T \cup \{\hat{\zeta}_j\}$
7: **end for**
8: **if** $(\#T == e)$, then **return** T **, else return** FAIL

Note that the intersection of balls in line 6 is non-empty if and only if

$$\rho' + \rho_j \;>\; \|\hat{\zeta}_j - \hat{\zeta}'\| \;,$$

so that this condition may be decided in rational arithmetic if a “hard” certificate is desired. See Remark 2.2 and Section 5.

Theorem 4.8. *Let f be a system of polynomials having e solutions whose general square subsystems have d solutions. Then Algorithm 4 either returns FAIL or it returns a set T of approximate solutions to f whose associated solutions are all the solutions to f.*

As with Algorithm 3, while the hypotheses appear restrictive, they are natural from an intersection-theoretic perspective, and are satisfied by a large class of systems of equations. We explain one such family coming from Schubert calculus in Section 5.2.

Proof. Since the balls $B(\hat{\zeta}_i, \rho_i)$ are pairwise disjoint, the quantity r is positive. Thus the refinement of each approximate solution $\hat{\zeta}'$ on line 4 terminates. Having refined each $\hat{\zeta}' \in S'$, note that $B(\hat{\zeta}', \rho')$ can intersect at most one ball from B. Now, if $\zeta_1, \ldots, \zeta_e$ are the solutions to f, then we must have that some $\hat{\zeta}_{i_j}$ is associated to each ζ_j for some indices $1 \le i_1 < i_2 < \cdots < i_e \le d$. Thus, if T has e elements, then the only solutions to g associated to T are also solutions to f. ☐

Remark 4.9. If g' is a general square subsystem of f, then it will have d solutions and the only common solutions to g and to g' are solutions to f. In this case, if Algorithm 4 returns FAIL, then $\#T > e$, so that some pair of balls in Step 6 meet, but their intersection does not contain a common solution to g and to g'. In this case, we may then further refine the solutions in S, S', and the corresponding balls until no such extraneous pair of balls meet.

Remark 4.10. An alternate approach to this algorithm is to set up a linear parameter homotopy between g and g', which is natural if both are linear combinations of elements of f. Then the solutions which are in $\mathcal{V}(f)$ are among those of $\mathcal{V}(g)$ which do not move or leave the separating balls. If exactly e solutions in $\mathcal{V}(g)$ do not leave their separating nballs, then these are the solutions in $\mathcal{V}(f)$.

A proxy for this continuation is applying the Newton operator $N_{g'}$ to each point in $\mathcal{V}(g)$.

5. Examples

We give three examples that illustrate our certification algorithms. All computations were carried out using the computer algebra system Macaulay2 [7]. For each example, we found complex floating-point solutions to square subsystems via homotopy continuation, as implemented in the package `NumericalAlgebraicGeometry` [23]. The tests related to α-theory were performed using the package `NumericalCertification` [22]. Our current certificates are "soft" in the sense that estimates are checked in floating point rather than rational arithmetic, which would give a "hard" certificate.

5.1. **Plane quartics through four points.** Consider the overdetermined system $f = (f_1, \dots, f_{11})$, where the the f_i are given as follows:

$$z_1z_2 - z_2^2 + z_1 - z_2\,,\ z_1^2 - z_2^2 + 4z_1 - 4z_2\,,\ z_2^3 - 6z_2^2 + 5z_2 + 12\,,$$
$$z_1z_2^2 - 6z_2^2 - z_1 + 6z_2 + 12\,,\ z_1^2z_2 - 6z_2^2 - 4z_1 + 9z_2 + 12\,,\ z_1^3 - 6z_2^2 - 13z_1 + 18z_2 + 12\,,$$
$$z_2^4 - 31z_2^2 + 42z_2 + 72\,,\ z_1z_2^3 - 31z_2^2 + z_1 + 41z_2 + 72\,,\ z_1^2z_2^2 - 31z_2^2 + 4z_1 + 38z_2 + 72\,,$$
$$z_1^3z_2 - 31z_2^2 + 13z_1 + 29z_2 + 72\,,\ z_1^4 - 31z_2^2 + 40z_1 + 2z_2 + 72\,.$$

These give a basis for the space of quartics passing through four points:

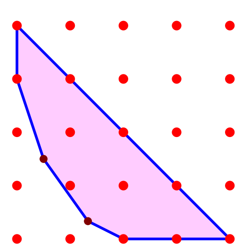
$$(4,4)\,,\ (-3,-1)\,,\ (-1,-1)\,,\ (3,3)\ \in\ \mathbb{C}^2.$$

As an illustration of our approach, we show how to certify that numerical approximations of these points represent true solutions to f.

Letting $L = \mathrm{span}_{\mathbb{C}}\{f_1, \dots, f_{11}\}$, we consider the algebra A_L. Letting $<$ be the graded-reverse lex order with $z_1 > z_2$, the algebra A_L has a finite Khovanskii-basis with respect to the $\mathbb{Z}^2$-valuation associated to $<$. It is given by $S = \{t\,f_1, t\,f_2, \dots, t\,f_{11}, t^2\,g, t^3\,h\}$, where

$$g = z_1\,z_2^3 - z_2^4 + 10\,z_1^2\,z_2 - 26\,z_1\,z_2^2 + 16\,z_2^3 + 10\,z_1^2 - 15\,z_1\,z_2 + 5\,z_2^2 + 12\,z_1 - 12\,z_2$$
$$h = 10\,z_1^4\,z_2 - 49\,z_1^3\,z_2^2 + 89\,z_1^2\,z_2^3 - 71\,z_1\,z_2^4 + 21\,z_2^5 + 10\,z_1^4 - 18\,z_1^3\,z_2 - 18\,z_1^2\,z_2^2$$
$$+ 50\,z_1\,z_2^3 - 24\,z_2^4 + 31\,z_1^3 - 83\,z_1^2\,z_2 + 73\,z_1\,z_2^2 - 21\,z_2^3 + 24\,z_1^2 - 48\,z_1\,z_2 + 24\,z_2^2.$$

The Newton-Okounkov body, depicted below, has normalized volume 12. The integer points correspond to $f_1, \dots, f_{11}$. The fractional vertices corresponding to t^2g and t^3h demonstrate that these elements are essential in forming the Khovanskii basis.



The Khovanskii basis was computed using the unreleased Macaulay2 package "SubalgebraBases" [32]. We checked this computation against our own top-level implementation of the binomial-lifting / subduction algorithm. As an additional check, we may express g

and h as homogeneous polynomials in the algebra generators $f_1, \ldots, f_{11}$:

$$\begin{aligned} g = &-\frac{5452243}{3803436} f_4 f_9 + \frac{1088119}{7606872} f_5 f_9 - \frac{179087}{7606872} f_6 f_9 - \frac{1184975}{7606872} f_8 f_9 + \frac{2728589}{7606872} f_9^2 - \frac{5046}{3913} f_1 f_{10} + \frac{5951}{11739} f_2 f_{10} + \frac{5452243}{3803436} f_3 f_{10} \\ &+ \frac{2196073}{1901718} f_4 f_{10} + \frac{905753}{3803436} f_5 f_{10} - \frac{129295}{1901718} f_6 f_{10} + \frac{1184975}{7606872} f_7 f_{10} - \frac{5983}{29484} f_8 f_{10} - \frac{2728589}{7606872} f_9 f_{10} - \frac{65165}{1267812} f_{10}^2 \\ &- \frac{5951}{11739} f_1 f_{11} - \frac{9872411}{7606872} f_3 f_{11} - \frac{1632419}{7606872} f_4 f_{11} + \frac{129295}{1901718} f_5 f_{11} - \frac{1184975}{7606872} f_7 f_{11} + \frac{2728589}{7606872} f_8 f_{11} + \frac{65165}{1267812} f_9 f_{11}. \end{aligned}$$

$$\begin{aligned} h = &\frac{423458528993}{35955045627228} f_5 f_9^2 - \frac{348294358499}{77902598858994} f_6 f_9^2 + \frac{33023933703287}{1012733785166922} f_7 f_9^2 - \frac{82250093861471}{6076402711001532} f_8 f_9^2 \\ &- \frac{4432317106115}{233707796576982} f_9^3 - \frac{33023933703287}{1012733785166922} f_7 f_8 f_{10} + \frac{1065288183977}{37508658709886} f_3 f_9 f_{10} - \frac{96715490949542}{317951304645429} f_4 f_9 f_{10} \\ &- \frac{49052367589004489}{1695316356369427428} f_5 f_9 f_{10} \frac{25940308080550879}{1695316356369427428} f_6 f_9 f_{10} - \frac{8914885258327}{467415593153964} f_7 f_9 f_{10} \\ &+ \frac{848951864573779}{13671906099753447} f_8 f_9 f_{10} \frac{47174423433062585}{1695316356369427428} f_9^2 f_{10} - \frac{13418439080090}{56262988064829} f_1 f_{10}^2 + \frac{1014252370876}{12983766476499} f_2 f_{10}^2 \\ &+ \frac{490676889497623}{2103370169192838} f_3 f_{10}^2 + \frac{135026148156913879}{423829089092356857} f_4 f_{10}^2 + \frac{1125534856927697}{27343812199506894} f_5 f_{10}^2 \frac{7907079377499775}{423829089092356857} f_6 f_{10}^2 \\ &+ \frac{164898009266531}{54687624399013788} f_7 f_{10}^2 - \frac{5432718489778696}{141276363030785619} f_8 f_{10}^2 - \frac{16931183230705166}{423829089092356857} f_9 f_{10}^2 - \frac{2073065531395802}{141276363030785619} f_{10}^3 \\ &- \frac{1065288183977}{37508658709886} f_3 f_8 f_{11} \frac{33023933703287}{1012733785166922} f_7 f_8 f_{11} + \frac{13306110674011}{225051952259316} f_3 f_9 f_{11} + \frac{2828825493124010}{13671906099753447} f_4 f_9 f_{11} \\ &- \frac{4516368725120116}{423829089092356857} f_5 f_9 f_{11} - \frac{3780890220862891}{1695316356369427428} f_6 f_9 f_{11} - \frac{280393696081193}{6076402711001532} f_7 f_9 f_{11} \\ &- \frac{313094593927918}{13671906099753447} f_8 f_9 f_{11} + \frac{5042023611256019}{847658178184713714} f_9^2 f_{11} + \frac{14158876247624}{168788964194487} f_1 f_{10} f_{11} \\ &- \frac{8754568627342}{168788964194487} f_2 f_{10} f_{11} - \frac{26911193688915259}{54687624399013788} f_3 f_{10} f_{11} - \frac{4282639294736275}{18229208133004596} f_4 f_{10} f_{11} \\ &- \frac{31468039434977}{4484963905739226} f_5 f_{10} f_{11} + \frac{4914325106636902}{423829089092356857} f_6 f_{10} f_{11} + \frac{1833610583591729}{54687624399013788} f_7 f_{10} f_{11} \\ &+ \frac{16078096764903062}{423829089092356857} f_8 f_{10} f_{11} + \frac{8296532868679901}{242188050909918204} f_9 f_{10} f_{11} + \frac{7171418221493375}{565105452123142476} f_{10}^2 f_{11} \\ &+ \frac{8754568627342}{168788964194487} f_1 f_{11}^2 + \frac{5171410646788483}{27343812199506894} f_3 f_{11}^2 + \frac{47304126637283297}{1695316356369427428} f_4 f_{11}^2 - \frac{4914325106636902}{423829089092356857} f_5 f_{11}^2 \\ &- \frac{107608086440381}{27343812199506894} f_7 f_{11}^2 - \frac{33198943704009683}{1695316356369427428} f_8 f_{11}^2 - \frac{7171418221493375}{565105452123142476} f_9 f_{11}^2. \end{aligned}$$

Now, $d_L = 12 \deg \Psi_L$, but also $d_L \leq 16$ by Bézout's theorem. This implies that $\deg \Psi_L = 1$ and hence $d_L = 12$.

We squared up f with a random matrix, $g = Af$, and found 16 complex approximate solutions to g using homotopy continuation. Each solution was softly certified distinct via α-theory. Computing values $\delta(f, g, \cdot)$ as in Algorithm 3, we softly certified 12 of these as nonsolutions to f, hence associating the four remaining to solutions to f.

5.2. **Example from Schubert calculus.** We describe a family of examples from Schubert calculus to which Algorithms 2, 3, and 4 all apply. For more on the Grassmannian and Schubert calculus, see [6]. Let $m \geq 2$ be an integer and set $n := m+2$. Consider the geometric problem of the 2-planes H in $\mathbb{C}^n$ that meet m general codimension 3 planes nontrivially. The number of such 2-planes is the Kostka number $K_{m^2,2^m}$, the first few values of which are shown below.

m	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$K_{m^2,2^m}$	0	1	1	3	6	15	36	91	232	603	1585	4213	11298	30537

This may be computed recursively. Let $\kappa_{m,i}$ be the coefficient of the Schur function $S_{(m+i,m-i)}$ in the product $(S_{(2,0)})^m$. Then $K_{m^2,2^m} = \kappa_{m,0}$. For the recursion, set $\kappa_{1,1} := 1$

and $\kappa_{1,0} = \kappa_{m,j} := 0$, when $j > m$. Then, for $m > 1$, we set $\kappa_{m,0} := \kappa_{m-1,1}$ and for $j > 0$, $\kappa_{m,j} := \kappa_{m-1,j-1} + \kappa_{m-1,j} + \kappa_{m-1,j+1}$.

We express this geometric probem in local coordinates. Write I_2 for the 2×2 identity matrix and let Z be a $2 \times m$ matrix of indeterminates, and set $H := (Z|I_2)^\top$, which has n rows and 2 columns. For any choice of $Z \in \mathrm{Mat}_{2\times m}(\mathbb{C})$, the column span of H, also written H, is a 2-plane in $\mathbb{C}^n = \mathbb{C}^m \oplus \mathbb{C}^2$ that does not meet the coordinate plane $\mathbb{C}^m \oplus \{0\}$, and $\mathrm{Mat}_{2\times m}(\mathbb{C})$ parametrizes the set of such 2-planes. For $k = 1, \dots, m$, let K_k be a general $n \times (m-1)$-matrix whose column span (also written K_k) is a general $(m-1)$-plane. Then $\dim H \cap K_k \geq 1$ if and only if the matrix $(H|K_k)$ has rank at most m. This condition is given by the n maximal minors $f_{k,1}, \dots, f_{k,n}$ of $(H|K_k)$, each of which is the determinant of the square $(n-1) \times (n-1)$-matrix obtained by deleting a row from $(H|K_k)$. This gives a system $f = (f_{k,j} \mid k = 1, \dots, m \text{ and } j = 1, \dots, n)$ of mn quadratic equations in $2m$ variables which define the solutions to our geometric problem.

Any polynomial g that is a linear combination of the $f_{k,j}$ has the form $g = \det(H|K_k|\ell)$, where the entries of ℓ are the coefficients of $(-1)^j f_{k,j}$ in that linear combination. This justifies the following scheme to obtain a square subsystem of f. For each $k = 1, \dots, m$ and $i = 1, 2$, let $L_{k,i} \supset K_k$ be an m-plane that is general given that it contains K_k. We obtain the matrix of $L_{k,i}$ by appending a general column vector to the matrix of K_k. Let $g_{k,i}$ be the determinant of the matrix $(H|L_{k,i})$—this vanishes when $\dim H \cap L_{k,i} \geq 1$. We claim that the susbsystem $g = (g_{1,1}, g_{1,2}, \dots, g_{m,1}, g_{m,2})$ of f is square.

For this, let us investigate the corresponding geometric loci in the Grassmannian $G(2, n)$. Write $\Omega_{\square\square} K_k$ for the set of all 2-planes which meet K_k nontrivially, and $\Omega_{\square} L_{k,i}$ for those that meet $L_{k,i}$ nontrivially. Let Λ_k be the hyperplane containing both $L_{k,1}$ and $L_{k,2}$, and let $\Omega_{\boxminus} \Lambda_k$ be the set of all 2-planes that are contained in Λ_k. Since $L_{k,1} \cap L_{k,2} = K_k$ and $L_{k,1} + L_{k,2} = \Lambda_k$ it was shown in [31] that

$$\Omega_{\square} L_{k,1} \bigcap \Omega_{\square} L_{k,2} \ = \ \Omega_{\square\square} K_k \cup \Omega_{\boxminus} \Lambda_k \tag{13}$$

is a (generically) transverse intersection. We explain how each algorithm applies to this geometric problem, and then discuss its certification in the case of $m = 4$.

Algorithm 2. In the local coordinates $H = (Z|I_2)^\top$, we have that $\Omega_{\square} L_{k,i} = \mathcal{V}(g_{k,i})$, so that (13) is a complete intersection and $\Omega_{\square\square} K_k = \mathcal{V}(f_{k,1}, \dots, f_{k,n})$ is in liaison with $\Omega_{\boxminus} \Lambda_k$, which we show is a complete intersection. Let λ_k be the linear form (a row vector) whose kernel is Λ_k. Then $H \in \Omega_{\boxminus} \Lambda_k$ if and only if $H \subset \Lambda_k$, so that $\lambda_k H = \binom{0}{0}$. If $h_{k,1}$ and $h_{k,2}$ are the two rows of $\lambda_k H$, then $\Omega_{\boxminus} \Lambda_k = \mathcal{V}(h_{k,1}, h_{k,2})$, showing that it is a complete intersection.

Our geometric problem of the 2-planes H that meet each of $K_1, \dots, K_m$ is equivalent to the intersection

$$\Omega_{\square\square} K_1 \bigcap \Omega_{\square\square} K_2 \bigcap \cdots \bigcap \Omega_{\square\square} K_m \,,$$

which is a square system of varieties (9). As each is in liaison with a complete intersection, Algorithm 2 applies and may be used to certify the solutions to our geometric problem. Its input is the set $\mathcal{V}(g)$, which consists of the points in the intersection

$$\Omega_{\square} L_{1,1} \bigcap \Omega_{\square} L_{1,2} \bigcap \cdots \bigcap \Omega_{\square} L_{k,i} \bigcap \cdots \bigcap \Omega_{\square} L_{m,1} \bigcap \Omega_{\square} L_{m,2} \,. \tag{14}$$

While each pair $\Omega_{\square}L_{k,1} \bigcap \Omega_{\square}L_{k,2}$ is not in general position, this intersection is generically transverse, and the different pairs are in general position, so the intersection (14) is transverse. Consequently, the number of points in the intersection (14) is the expected number, which is the Catalan number $C_m := \frac{1}{m+1}\binom{2m}{m}$.

Algorithm 3. For this algorithm, the number d of excess solutions is $\frac{1}{m+1}\binom{2m}{m} - K_{m^2,2^m}$. It starts with the set $S = \mathcal{V}(g)$ of $\frac{1}{m+1}\binom{2m}{m}$ points in the intersection (14). We run Algorithm 3, and if it finds that $\#R = d$, so that we have rejected all nonsolutions, then those that remain are certified solutions to our geometric problem $\mathcal{V}(f)$. Otherwise, we may refine the approximate solutions $\hat{\zeta}$ in S so that the Newton steps $\beta(g, \hat{\zeta})$ become small enough to reject d nonsolutions.

This algorithm is particularly easy in this case as the Taylor residual (4) of a linear function ϕ is $|\phi(\hat{\zeta})| - \|\phi'\|\delta$, where the derivative ϕ' of ϕ is a vector.

Algorithm 4. Here, $d = \frac{1}{m+1}\binom{2m}{m}$, the number of solutions to the square system g and $e = K_{m^2,2^m}$, the number of solutions to f. Suppose that we have computed d solutions $\mathcal{V}(g)$ and separating balls as in Proposition 2.7. Choose a different square subsystem g' by choosing different column vectors to append to the matrices K_k. Then a linear parameter homotopy between those two choices of vectors may be used to compute the solutions $\mathcal{V}(g')$. The solutions which remain in their separating balls include the solutions to f, as described in Remark 4.10.

Case $m = 4$**.** For randomly generated data K_1, K_2, K_3, K_4, we were able to softly certify 3 solutions to the Schubert problem $\Omega_{\square\square}K_1 \cap \Omega_{\square\square}K_2 \cap \Omega_{\square\square}K_3 \cap \Omega_{\square\square}K_4$ by applying both Algorithms 3 and 4 to square subsystems—each with 14 distinct complex solutions.

5.3. **Essential matrix estimation.** A fundamental object of study in geometric computer vision is the essential variety

$$V_{ess} := \{E \in \mathbb{P}(\mathbb{C}^{3\times 3}) \mid EE^\top E - \tfrac{1}{2}\operatorname{tr}(EE^\top)E = 0, \det E = 0\}. \tag{15}$$

This is an irreducible variety of dimension 5 and degree 10. Elements of V_{ess} are called *essential matrices*. The ten polynomials defining V_{ess} are known as the *Demazure cubics*. They minimally generate the homogeneous ideal of V_{ess}, which is not a complete intersection.

The essential variety is central to the problem of five point relative pose reconstruction. In this problem, we are given points $x_1, \ldots, x_5, y_1, \ldots, y_5 \in \mathbb{P}^2$ and wish to find $R \in \mathrm{SO}(3, \mathbb{C})$, $t \in \mathbb{P}^2$ such that

$$Rx_i + t = y_i \text{ for } i = 1, \ldots, 5. \tag{16}$$

The pair of points (x_i, y_i) are understood to be in correspondence as images of a common world point in $\mathbb{P}^3$ under two different cameras. To be more precise, these are *normalized image coordinates* relative to a pair of *calibrated projective cameras*; we refer to [8] for the relevant definitions and further background on geometric computer vision.

We associate an essential matrix to the pair (R, t) by defining

$$E = [t]_\times R, \tag{17}$$

where

$$[t]_\times = \begin{pmatrix} 0 & -t_1 & t_2 \\ t_1 & 0 & -t_3 \\ t_3 & -t_2 & 0 \end{pmatrix}$$

is the skew-symmetric matrix representing the cross product by t. We note that t is in the kernel of $E^\top$; from this and the relation $RR^\top = I$ it may be observed that any matrix of the form (17) satisfies the Demazure cubics (15) defining V_{ess}. Constraints given by point-point correspondences in (16) take the form

$$y_i^\top E x_i \text{ for } i = 1, \ldots, 5. \tag{18}$$

Equations (15) and (18) for the essential matrix recovery problem give an overdetermined system of equations with 10 solutions for *generic* data x_i, y_i. State of the art algorithms for the 5 point relative pose problem make use of the essential matrix formulation [26].

To certify essential matrices consistent with 5 point-point correspondences, we consider the square system given by equations (18) and the first three Demazure cubics: namely

$$\begin{aligned}(e_{2,1}^2 + e_{2,2}^2 + e_{2,3}^2 + e_{3,1}^2 + e_{3,2}^2 + e_{3,3}^2)e_{1,i} + (e_{1,1}e_{2,1} + e_{1,2}e_{2,2} + e_{1,3}e_{2,3})e_{2,i} \\ + (e_{1,1}e_{3,1} + e_{1,2}e_{3,2} + e_{1,3}e_{3,3})e_{3,i}\end{aligned} \tag{19}$$

The number of solutions to this square system is bounded *a priori* by 27, and it we can easily certify that this bound is attained for generic data x_i, y_i. Thus the methods described in Section 5 give us methods of certification for this problem. We consider an alternative procedure based on the exclusion criteria of Proposition 2.4 and 2.5 and the following result obtained by symbolic computation.

Proposition 5.1. *Let V_{sq} be the subvariety of $\mathbb{P}(\mathbb{C}^{3\times 3})$ defined by equations* (18) *and* (19)*. Consider the polynomials*

$$\begin{aligned} f_1 &:= e_{1,1} \\ f_2 &:= e_{1,1}e_{3,1} + e_{1,2}e_{3,2} + e_{1,3}e_{3,3} \\ f_3 &:= e_{1,1}^2 + e_{1,2}^2 + e_{1,3}^2 \end{aligned}$$

and define projective varieties as the Zariski closures of the indicated quasiprojective varieties,

$$\begin{aligned} V_1 &:= \overline{V_{sq} \setminus \mathcal{V}(f_1)} \\ V_2 &:= \overline{V_1 \setminus \mathcal{V}(f_2)} \\ V_3 &:= \overline{V_2 \setminus \mathcal{V}(f_3)} \end{aligned}$$

We have that $V_3 = V_{ess}$.

Proof. This follows by symbolically computing ideal quotients: letting I_0 by the ideal generated by (18) and (19) and $I_k = I_{k-1} : f_k$ for $k = 1, 2, 3$, we may establish that I_3 equals the ideal defining V_{ess}; for instance, by showing they have the same reduced Gröbner basis for a given term order (as is easily accomplished by Macaulay2.) □

Thus, given approximate solutions to the square system on V_{ess} which are good candidates for points on V_{ess}, we may refine them until the exclusion criteria of Proposition 2.4 and 2.5 are satisfied for f_1, f_2 and f_3.

References

[1] Dave Anderson. Okounkov bodies and toric degenerations. *Math. Ann.*, 356(3):1183–1202, 2013.

[2] Tulay Ayyildiz Akoglu, Jonathan D. Hauenstein, and Agnes Szanto. Certifying solutions to overdetermined and singular polynomial systems over $\mathbb{Q}$. *J. Symbolic Comput.*, 84:147–171, 2018.

[3] Lenore Blum, Felipe Cucker, Michael Shub, and Stephen Smale. *Complexity and real computation*. Springer-Verlag, New York, 1998.

[4] L. Bossinger, X. Fang, G. Fourier, M. Hering, and M. Lanini. Toric degenerations of $\mathrm{Gr}(2, n)$ and $\mathrm{Gr}(3, 6)$ via plabic graphs. *Ann. Comb.*, 22(3):491–512, 2018.

[5] Michael Burr, Kisun Lee, and Anton Leykin. Effective certification of approximate solutions to systems of equations involving analytic functions. In *Proceedings of the 2019 ACM on International Symposium on Symbolic and Algebraic Computation*, pages 267–274. ACM, 2019.

[6] William Fulton. *Young tableaux*. London Mathematical Society Students Texts, 35. Cambridge University Press, Cambridge, 1997.

[7] Daniel R Grayson and Michael E Stillman. Macaulay 2, a software system for research in algebraic geometry, 2002.

[8] Richard Hartley and Andrew Zisserman. *Multiple view geometry in computer vision*. Cambridge university press, 2003.

[9] Jonathan D. Hauenstein, Nickolas Hein, and Frank Sottile. A primal-dual formulation for certifiable computations in Schubert calculus. *Found. Comput. Math.*, 16(4):941–963, 2016.

[10] Jonathan D Hauenstein and Frank Sottile. Algorithm 921: alphacertified: certifying solutions to polynomial systems. *ACM Transactions on Mathematical Software (TOMS)*, 38(4):28, 2012.

[11] Nickolas Hein and Frank Sottile. A lifted square formulation for certifiable Schubert calculus. *J. Symbolic Comput.*, 79(part 3):594–608, 2017.

[12] Deepak Kapur and Klaus Madlener. A completion procedure for computing a canonical basis for a k-subalgebra. In *Computers and mathematics*, pages 1–11. Springer, 1989.

[13] Kiumars Kaveh and Askold Georgievich Khovanskii. Mixed volume and an extension of intersection theory of divisors. *Moscow Mathematical Journal*, 10(2):343–375, 2010.

[14] Kiumars Kaveh and Askold Georgievich Khovanskii. Newton-Okounkov bodies, semigroups of integral points, graded algebras and intersection theory. *Annals of Mathematics*, pages 925–978, 2012.

[15] Kiumars Kaveh and Christopher Manon. Khovanskii bases, higher rank valuations and tropical geometry. `arXiv:1610.00298`, 2016.

[16] Valentina Kiritchenko. Newton-Okounkov polytopes of flag varieties. *Transform. Groups*, 22(2):387–402, 2017.

[17] S. L. Kleiman. The transversality of a general translate. *Compositio Math.*, 28:287–297, 1974.

[18] Jan O. Kleppe, Juan C. Migliore, Rosa Miró-Roig, Uwe Nagel, and Chris Peterson. Gorenstein liaison, complete intersection liaison invariants and unobstructedness. *Mem. Amer. Math. Soc.*, 154(732):viii+116, 2001.

[19] R. Krawczyk. Newton-algorithmen zur bestimmung von nullstellen mit fehler-schranken. *Computing*, 4(3):187–201, 1969.

[20] Ulrich W Kulisch and Willard L Miranker. *Computer arithmetic in theory and practice*. Academic press, 2014.

[21] Grégoire Lecerf and Joelle Saadé. A short survey on kantorovich: like theorems for newton's method. *ACM Communications in Computer Algebra*, 50(1):1–11, 2016.

[22] Kisun Lee. `NumericalCertification`. a Macaulay 2 Package.

[23] Anton Leykin. NAG4M2: Numerical algebraic geometry for Macaulay 2. available at `people.math.gatech.edu/~aleykin3/NAG4M2`.

[24] Ramon E Moore and Sandie T Jones. Safe starting regions for iterative methods. *SIAM Journal on Numerical Analysis*, 14(6):1051–1065, 1977.

[25] Ramon E Moore, R Baker Kearfott, and Michael J Cloud. *Introduction to interval analysis*, volume 110. Siam, 2009.

[26] David Nistér. An efficient solution to the five-point relative pose problem. *IEEE transactions on pattern analysis and machine intelligence*, 26(6):0756–777, 2004.

[27] Lorenzo Robbiano and Moss Sweedler. Subalgebra bases. In *Commutative algebra*, pages 61–87. Springer, 1990.

[28] Fabrice Rouillier. Solving zero-dimensional systems through the rational univariate representation. *Appl. Algebra Engrg. Comm. Comput.*, 9(5):433–461, 1999.

[29] Michael Shub and Steve Smale. Complexity of Bezout's theorem I: Geometric aspects. *Journal of the American Mathematical Society*, 6(2):459–501, 1993.

[30] Steve Smale. Newton's method estimates from data at one point. In *The merging of disciplines: new directions in pure, applied, and computational mathematics*, pages 185–196. Springer, New York, 1986.

[31] Frank Sottile. Enumerative geometry for the real Grassmannian of lines in projective space. *Duke Math. J.*, 87(1):59–85, 1997.

[32] Michael Stillman and Harrison Tsai. Using SAGBI bases to compute invariants. *Journal of Pure and Applied Algebra*, 139(1-3):285–302, 1999.

[33] Bernd Sturmfels. *Gröbner bases and convex polytopes*, volume 8 of *University Lecture Series*. American Mathematical Society, Providence, RI, 1996.

[34] RA Tapia. The kantorovich theorem for newton's method. *The American Mathematical Monthly*, 78(4):389–392, 1971.

[35] Warwick Tucker. *Validated numerics: a short introduction to rigorous computations*. Princeton University Press, 2011.

School of Mathematics, Georgia Institute of Technology, 686 Cherry Street, Atlanta, GA 30332-0160, USA

E-mail address: tduff3@gatech.edu

URL: http://people.math.gatech.edu/~tduff3/

Department of Mathematics and Computer Science, Benedictine College, 1020 N. 2nd St, Atchison, KS 66002, USA

E-mail address: nhein@benedictine.edu

URL: https://www.benedictine.edu/faculty-staff/hein-nickolas

Frank Sottile, Department of Mathematics, Texas A&M University, College Station, Texas 77843, USA

E-mail address: sottile@math.tamu.edu

URL: www.math.tamu.edu/~sottile