Mss. arXiv.org/1812.02851 7 December 2018

CERTIFICATION FOR POLYNOMIAL SYSTEMS VIA SQUARE SUBSYSTEMS

TIMOTHY DUFF AND FRANK SOTTILE

ABSTRACT. We consider numerical certification of approximate solutions to an overdetermined system of N polynomial equations in n variables where $n < N$ by passing to a square subsystem. We give two approaches which rely upon additional intersection-theoretic information. The excess solutions to a square subsystem are counted by a birationally-invariant intersection index or Newton-Okounkov body. When this number is known, we explain how to certify individual solutions to the original overdetermined system. When the number of solutions to both systems are known, we explain how to certify all solutions to the overdetermined system.

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 a computed estimate $\hat{\zeta}$ of a solution ζ to f is an approximate solution in this sense.

Many existing certification methods are for square systems, where $N = n$. These exploit that the isolated, non-singular solutions to the system are exactly the fixed points of the Newton operator $N_f \colon \mathbb{C}^n \to \mathbb{C}^n$ given 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. A notable certification procedure is Smale's α-test [16, 17].

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 an associated solution is real [6].

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 solutions to the original system. In [1] a hybrid symbolic-numeric approach is used when the polynomials in f have rational coefficients. They compute an exact rational univariate

---

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. Both authors supported by the ICERM.

representation [15] and use that to certify solutions. An alternate approach taken in [5, 7] 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 may be defined by any n polynomials $g_1, \dots, g_n$ lying 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 typically many excess solutions. While approximate solutions to g may be certified using α-theory, to certify a point as an approximate solution to f, we must distinguish it from these excess solutions.

We give two 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 numbers of solutions to f or to g (or both), and each addresses one of the problems below.

Problem 1. How may we certify that a point $z \in \mathbb{C}^n$ 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. We give an algorithm for Problem 1 in Section 3 and discuss its relation to Newton-Okounkov bodies. While that algorithm may also be applied to Problem 2, we give a different algorithm in Section 4. We give two examples illustrating our algorithms in Section 5. One involves a finite Khovanskii basis, while the other is from the Schubert calculus.

2. Certifying solutions and nonsolutions

We recall how Smale's α-theory is used to certify approximate solutions to square polynomial systems, and give a definition of an approximate solution to an overdetermined system of polynomials. We also explain how to use α-theory to certify that a solution to a square subsystem of an overdetermined system f is not a solution to f.

Let $g = (g_1, \dots, g_n)$ be a system of n polynomials in n variables $z = (z_1, \dots, z_n)$ with coefficients in $\mathbb{C}$. Write $N_g(z)$ for the Newton operator (1) and $N_g^k(z)$ for its kth iterate starting from $z \in \mathbb{C}^n$. (If the Jacobian $Dg(z)$ is not invertible, then we set $N_g(z) = z$.) Write $\|\zeta\|$ for the usual Hermitian norm on $\zeta \in \mathbb{C}^n$, $\|\zeta\| := (|\zeta_1|^2 + \cdots + |\zeta_n|^2)^{1/2}$.

A point $\hat{\zeta} \in \mathbb{C}^n$ is an *approximate solution* to g with *associated solution* $\zeta \in \mathbb{C}^n$ where $g(\zeta) = 0$ if for every $k \in \mathbb{N}$,

$$\|\zeta - N_g^k(\hat{\zeta})\| \le \left(\frac{1}{2}\right)^{2^k - 1} \|\zeta - \hat{\zeta}\|\,. \tag{3}$$

This implies that each application of $N_g(\cdot)$ doubles the number of significant digits. When (3) holds, we say that Newton iterates starting at $\hat{\zeta}$ *converge quadratically* to ζ. Smale's α-theory involves a computable constant, $\alpha(g,\hat{\zeta})$, that when sufficiently small certifies that Newton iterates starting at $\hat{\zeta}$ converge quadratically to a solution to g.

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 $\|z^k\| \leq \|z\|^k$, 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,

$$\|(D^k g)_\zeta\| \;:=\; \max_{\substack{w \in S^k\mathbb{C}^n \\ \|w\|=1}} \|(D^k g)_\zeta\,(w)\|\,. \tag{4}$$

We define the central quantities of α-theory.

Definition 1. With g as above and $\hat{\zeta} \in \mathbb{C}^n$ a point where $Dg(\hat{\zeta})$ is invertible,

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

Notice that $\beta(g,\hat{\zeta})$ is the length of a Newton step at $\hat{\zeta}$.

These provide a certificate for a point $\hat{\zeta} \in \mathbb{C}^n$ to be a approximate solution to g.

Proposition 1 ([2, 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 an approximate solution to g. Furthermore, if ζ is the associated solution to g, then $\|\zeta - \hat{\zeta}\| < 2\beta(g,\hat{\zeta})$.

Theorem 6 and Remark 9 of [2, Ch. 8] give a refined version of Proposition 1 that provides a certificate that two approximate solutions have the same associated solution.

Proposition 2. *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.

Propositions 1 and 2 enable algorithms to certify that a set of approximate solutions have pairwise disjoint associated solutions. For example, Proposition 1 implies a separation bound. If $\hat{\zeta}_1$ and $\hat{\zeta}_2$ are approximate solutions to g with

$$\|\hat{\zeta}_1 - \hat{\zeta}_2\| \;\geq\; 2(\beta(g,\hat{\zeta}_1) + \beta(g,\hat{\zeta}_2))\,, \tag{5}$$

then their associated solutions are distinct. Given an approximate solution $\hat{\zeta}$ with associated solution ζ such that $Dg(\zeta)$ is invertible, the sequence $\beta(g, N_g^k(\hat{\zeta}))$ converges to zero. As derivatives are continuous, $\gamma(g, N_g^k(\hat{\zeta}))$ is bounded, so that $\alpha(g, N_g^k(\hat{\zeta}))$ converges to zero. Thus we may refine approximate solutions $\hat{\zeta}_1$ and $\hat{\zeta}_2$ to g with Newton iterations until either (5) holds—so they represent distinct solutions to g—or Proposition 2 applies and they represent the same solution. Having obtained representatives of distinct solutions to g, we may refine them to obtain a pairwise disjoint collection of balls containing each, as well as their associated solutions to g. We summarize this discussion.

Proposition 3. *Given a square system g with approximate solutions S', we may compute a set S of refined approximate solutions and a set B of pairwise disjoint balls centered at elements of S such that each ball contains the solution to g associated to its center.*

Suppose now that f is an overdetermined polynomial system, and that $\hat{\zeta}, \zeta \in \mathbb{C}^n$ with $f(\zeta) = 0$. We say that $\hat{\zeta}$ is an *approximate solution* to f with *associated solution* ζ if there is a square subsystem g of f such that $\hat{\zeta}$ is an approximate solution to g with associated solution ζ. As we generally only know f, g, and $\hat{\zeta}$, establishing that the associated zero ζ is a solution to f seems difficult *a priori*. On the other hand, α-theory provides a simple certificate that ζ is *not* a solution to f.

Proposition 4. *Suppose that g is a square subsystem of $f = (f_1, \ldots, f_N)$ and that $\hat{\zeta}$ is an approximate solution to g with associated solution ζ. Consider*

$$\delta(f, g, \hat{\zeta}) \;:=\; \max_{1 \le j \le N} \left(|f_j(\hat{\zeta})| - \sum_{k=1}^{\deg f_j} \frac{\|(D^k f_j)_{\hat{\zeta}}\|}{k!} \cdot (2\,\beta(g, \hat{\zeta}))^k \right). \tag{6}$$

If $\delta(f, g, \hat{\zeta}) > 0$ and $\|\hat{\zeta} - z\| < 2\beta(g, \hat{\zeta})$, then $f(z) \neq 0$. In particular, $f(\zeta) \neq 0$.

Proof. This follows from Proposition 1 and Taylor expansion. □

In practice, we estimate the operator norms of the higher derivatives, as explained in [16, §I-3] and [6, §1.1].

3. Certifying individual solutions

The consequences of α-theory 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

$$\#\left(\mathcal{V}(g) \setminus \mathcal{V}(f)\right) \;=\; d\,. \tag{7}$$

If we can certify d solutions to g which are nonsolutions to f, then any other solutions to g must be solutions to f.

Algorithm 1 (Certifying individual solutions)**.**
Input: (f, g, d, S)

f — a polynomial system
g — a square subsystem of f
$d \in \mathbb{N}$ satisfying (7)
$S = \{\hat{\zeta}_1, \ldots, \hat{\zeta}_m\}$ — 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** $\delta(f, g, \hat{\zeta}) > 0$ **then** $R \leftarrow R \cup \{\zeta_j\}$
if $(\#R == d)$ **then** $T \leftarrow S \setminus R$ **, else** $T \leftarrow \emptyset$
return T

Theorem 1. *Suppose that f, g, d, S are valid input for Algorithm 1. 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 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 (7) they associate to solutions to f. □

Perhaps the main difficulty in applying Algorithm 1 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 [9, 10].

Definition 2. ([10, 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 $U_{\mathbf{L}} \setminus Z_{\mathbf{L}}$ are non-singular and their number is independent of the choice of g. The common number is the birationally invariant intersection index $[L_1, L_2, \ldots, L_n]$.

This is proven in [9, 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 (7) 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*

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

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

Proposition 5 ([10, 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 $L = \mathrm{span}_{\mathbb{C}}\{f_1, \ldots, f_N\}$, 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 5 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 [11].

Definition 3. 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 $k[z_1, \ldots, z_n]$, taking lead monomials defines a valuation $\nu\colon k[z_1, \ldots, z_n] \to (\mathbb{Z}^n, \prec)$, where $\prec$ is the reverse of $<$. A Khovanskii basis with respect this valuation is commonly known as a *SAGBI basis* [8, 14].

When the monoid $S(A_L, \nu)$ is finitely generated, there is a finite Khovanskii basis for (L, ν). (We describe such an example in Section 5.1.) When this occurs, we may compute the Khovanskii basis via a binomial-lifting/subduction algorithm such as described in [14] or [20, Ch. 11]. However, we note that the mere existence of finite Khovanskii bases is a nontrivial question in general.

Example 1 ([14, 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 5 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. 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 1 to certify approximate solutions to f, we propose an alternative method to solve this problem. Here, by square subsystem, we mean a general linear combination as in (2).

Algorithm 2 (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 3
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: $r \leftarrow \min\limits_{1 \leq i < j \leq d} \Big(|\hat{\zeta}_i - \hat{\zeta}_j| - \rho_i - \rho_i \Big)$
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

$$|\rho' - \|(\hat{\zeta}_j - \hat{\zeta}')\|| \ < \ \rho_j$$

so that this condition may be decided in rational arithmetic if a "hard" certificate is desired (see Section 5.)

Theorem 2. *Let f be a system of polynomials having e solutions whose general square subsystems have d solutions. Then Algorithm 2 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 1, 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 solutions associated to S are distinct, the quantity r is positive. Thus the refinement of each approximate zero $\hat{\zeta}'$ 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 $1 \leq i_1 < i_2 < \cdots < i_e \leq d$. Thus, if T has e elements, then the only solutions to g associated to T are also solutions to f. □

Remark 1. 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 2 returns FAIL, then $\#T > e$, and we may then further refine the solutions in S, S', and the corresponding balls until there are no extraneous pairs of balls that meet.

5. Examples

We give two examples that illustrate our certification algorithms. All computations were carried out using the computer algebra system Macaulay2 [4]. For each example, we found complex floating-point solutions to square subsystems via homotopy continuation, as implemented in the package `NumericalAlgebraicGeometry` [13]. The tests related to α-theory were performed using the package `NumericalCertification` [12]. 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 $f = (f_1, \ldots, f_{11})$, where the the f_i are given as follows:

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

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

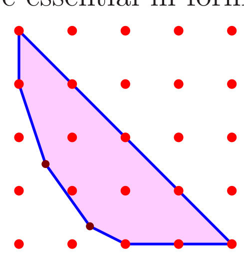
$$(4,4)\,,\ (-3,-1)\,,\ (-1,-1)\,,\ (3,3)\ \in\ \mathbb{C}^2.$$

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

Letting $L = \operatorname{span}_{\mathbb{C}}\{f_1, \ldots, f_{11}\}$, 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 $S = \{t\,f_1, t\,f_2, \ldots, t\,f_{11}, t^2\,g, t^3\,h\}$, where

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

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



The Khovanskii basis was computed using the unreleased Macaulay2 package "SubalgebraBases" [19]. 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 $f_1, \ldots, f_{11}$:

$$\begin{aligned} g = &-\frac{5452243}{3803436}f_4f_9 + \frac{1088119}{7606872}f_5f_9 - \frac{179087}{7606872}f_6f_9 - \frac{1184975}{7606872}f_8f_9 + \frac{2728589}{7606872}f_9^2 - \frac{5046}{3913}f_1f_{10} + \frac{5951}{11739}f_2f_{10} + \frac{5452243}{3803436}f_3f_{10} \\ &+ \frac{2196073}{1901718}f_4f_{10} + \frac{905753}{3803436}f_5f_{10} - \frac{129295}{1901718}f_6f_{10} + \frac{1184975}{7606872}f_7f_{10} - \frac{5983}{29484}f_8f_{10} - \frac{2728589}{7606872}f_9f_{10} - \frac{65165}{1267812}f_{10}^2 \\ &- \frac{5951}{11739}f_1f_{11} - \frac{9872411}{7606872}f_3f_{11} - \frac{1632419}{7606872}f_4f_{11} + \frac{129295}{1901718}f_5f_{11} - \frac{1184975}{7606872}f_7f_{11} + \frac{2728589}{7606872}f_8f_{11} + \frac{65165}{1267812}f_9f_{11}. \end{aligned}$$

$$\begin{aligned} h = &\frac{423458528993}{35955045627228}f_5f_9^2 - \frac{348294358499}{77902598858994}f_6f_9^2 + \frac{33023933703287}{1012733785166922}f_7f_9^2 - \frac{82250093861471}{6076402711001532}f_8f_9^2 \\ &- \frac{4432317106115}{233707796576982}f_9^3 - \frac{33023933703287}{1012733785166922}f_7f_8f_{10} + \frac{1065288183977}{37508658709886}f_3f_9f_{10} - \frac{96715490949542}{317951304645429}f_4f_9f_{10} \\ &- \frac{49052367589004489}{1695316356369427428}f_5f_9f_{10} \frac{25940308080550879}{1695316356369427428}f_6f_9f_{10} - \frac{8914885258327}{467415593153964}f_7f_9f_{10} \\ &+ \frac{848951864573779}{13671906099753447}f_8f_9f_{10} \frac{47174423433062585}{1695316356369427428}f_9^2f_{10} - \frac{13418439080090}{56262988064829}f_1f_{10}^2 + \frac{1014252370876}{12983766476499}f_2f_{10}^2 \\ &+ \frac{490676889497623}{2103370169192838}f_3f_{10}^2 + \frac{135026148156913879}{423829089092356857}f_4f_{10}^2 + \frac{1125534856927697}{27343812199506894}f_5f_{10}^2 \frac{7907079377499775}{423829089092356857}f_6f_{10}^2 \\ &+ \frac{164898009266531}{54687624399013788}f_7f_{10}^2 - \frac{5432718489778696}{141276363030785619}f_8f_{10}^2 - \frac{16931183230705166}{423829089092356857}f_9f_{10}^2 - \frac{2073065531395802}{141276363030785619}f_{10}^3 \\ &- \frac{1065288183977}{37508658709886}f_3f_8f_{11} \frac{33023933703287}{1012733785166922}f_7f_8f_{11} + \frac{13306110674011}{225051952259316}f_3f_9f_{11} + \frac{2828825493124010}{13671906099753447}f_4f_9f_{11} \\ &- \frac{4516368725120116}{423829089092356857}f_5f_9f_{11} - \frac{3780890220862891}{1695316356369427428}f_6f_9f_{11} - \frac{280393696081193}{6076402711001532}f_7f_9f_{11} \\ &- \frac{313094593927918}{13671906099753447}f_8f_9f_{11} + \frac{5042023611256019}{847658178184713714}f_9^2f_{11} + \frac{14158876247624}{168788964194487}f_1f_{10}f_{11} \\ &- \frac{8754568627342}{168788964194487}f_2f_{10}f_{11} - \frac{26911193688915259}{54687624399013788}f_3f_{10}f_{11} - \frac{4282639294736275}{18229208133004596}f_4f_{10}f_{11} \\ &- \frac{31468039434977}{4484963905739226}f_5f_{10}f_{11} + \frac{4914325106636902}{423829089092356857}f_6f_{10}f_{11} + \frac{1833610583591729}{54687624399013788}f_7f_{10}f_{11} \\ &+ \frac{16078096764903062}{423829089092356857}f_8f_{10}f_{11} + \frac{8296532868679901}{242188050909918204}f_9f_{10}f_{11} + \frac{7171418221493375}{565105452123142476}f_{10}^2f_{11} \\ &+ \frac{8754568627342}{168788964194487}f_1f_{11}^2 + \frac{5171410646788483}{27343812199506894}f_3f_{11}^2 + \frac{47304126637283297}{1695316356369427428}f_4f_{11}^2 - \frac{4914325106636902}{423829089092356857}f_5f_{11}^2 \\ &- \frac{107608086440381}{27343812199506894}f_7f_{11}^2 - \frac{33198943704009683}{1695316356369427428}f_8f_{11}^2 - \frac{7171418221493375}{565105452123142476}f_9f_{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 1, 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.** Let $Z = (z_{i,j} \mid i = 1, 2 \text{ and } j = 1, \ldots, 4)$ be a 2×4 matrix of indeterminates. The column space of the 6×2 matrix $H := (Z|I_2)^T$ is a general two-dimensional linear subspace of $\mathbb{C}^6$, one that does not meet the coordinate $\mathbb{C}^4$ spanned by the first elements in the implied ordered basis for $\mathbb{C}^6$. The matrix H consists of local Stiefel coordinates for the Grassmannian $G(2, 6)$ of 2-planes in $\mathbb{C}^6$. For more on Stiefel coordinates, the Grassmannian, and Schubert calculus, see [3].

Our overdetermined system of equations comes in $4 = \frac{1}{2} \dim G(2, 6)$ blocks, each given by rank conditions $\operatorname{rank}(H|K_k) \leq 4$ for $k = 1, \ldots, 4$, where K_k is a 6×3 matrix with independent columns. Each rank condition is given by the vanishing of six maximal

5×5 minors, and so this system is given by 24 equations, each a quadratic in the eight indeterminates $z_{i,j}$. This is known from Schubert calculus to have exactly three solutions when the column spaces of the K_k are general, which in this case means that they are pairwise in direct sum. Each rank condition $\operatorname{rank}(H|K) \leq 4$ with K a general 6×3 matrix is expressed geometrically as the column spaces of H (a 2-plane in $\mathbb{C}^6$) and K (a 3-plane) intersect in at least a one-dimensional subspace. The set of Z satisfying rank these rank conditions given by K is a Schubert subvariety of $G(2,6)$, denoted by $\Omega_{\square\square}K$.

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 1 and 2 to square subsystems—each with 14 distinct complex solutions—which can also be understood through the Schubert calculus. The subsystems are obtained block-wise from the constraints $\operatorname{rank}(H|K) \leq 4$ via linear combinations. Each such linear combination may be expressed as a determinant $\det(H|K|L)$, where L is 6×1. This defines a codimension 1 Schubert variety which we denote by $\Omega_{\square}L$—geometrically, $\Omega_{\square}L$ consists of points in $G(2,6)$ which meet the 4-plane given by $(K|L)$.

It is known that given eight general 4-planes L_k in $\mathbb{C}^6$, the corresponding Schubert varieties meet transversally in 14 points. However, if we take a second such linear combination corresponding to another column and 4-plane L', then the two linear subspaces L and L' are not general, as they intersect in K and span a 5-plane Λ. This was analyzed in [18], where it was shown that

$$\Omega_{\square}L \bigcap \Omega_{\square}L' \;=\; \Omega_{\square\square}K \cup \Omega_{\substack{\square\\\square}}\Lambda$$

is a (generically) transverse intersection, where $\Omega_{\substack{\square\\\square}}\Lambda$ is the sub Grassmannian of 2-dimensional linear subspaces of Λ. Taking similar subsystems of each of the four blocks, we get an intersection of eight Schubert varieties of the form $\Omega_{\square}L$ that meet transversally in 14 points.

Remark 2. This is the first nontrivial example of a family of examples in $G(2,n)$ for $n \geq 5$, and is representative of many others from the Schubert calculus, which will be described in the journal version of this extended abstract.

References

[1] 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.

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

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

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

[5] 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.

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

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

[8] 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.

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

[10] 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.

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

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

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

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

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

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

[17] 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.

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

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

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

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/`

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`