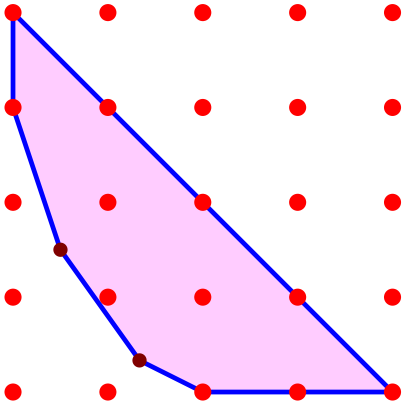
Certification for polynomial systems via square subsystems

SIAM Minisymposium on
Applications of Algebraic Geometry
SIAM TX/LA Meeting, SMU, 3 November 2019

Frank Sottile

sottile@math.tamu.edu



Work with Timothy Duff and Nickolas Hein.

Why Certify?

When we 'solve' a system $f\colon \mathbb{C}^n \to \mathbb{C}^m$ of polynomials, we compute numerical approximations to the points of $f^{-1}(0)$.

How do we know (or prove to others that)
(1) Each computed point 'is' a solution?
(2) We have all (meaningful) solutions?

—Trust/improve heuristics (typically this will satisfy you).

—Actually provide a proof, certifying output (which may satisfy others).

While this is hard, and even when possible, computationally intensive, it is sometimes necessary.

If numerical methods are to be taken seriously in mathematics, and also in some applications, we must prove that our output is what we say it is.

Smale's α-theory

When $g\colon \mathbb{C}^n \to \mathbb{C}^n$ is square (# of eqns = # of vars), there are approaches to certification using Newton's Method. One such is *Smale's α-theory*.

A *Newton step* is $\mathcal{N}_g(x) \;:=\; x \;-\; (\mathrm{D}_g(x))^{-1}g(x)$.

Suppose that $\hat{\zeta} \in \mathbb{C}^n$ a point where the *Jacobian* D_g is invertible. Set

$$\alpha(g,\hat{\zeta}) \;:=\; \beta(g,\hat{\zeta})\cdot\gamma(g,\hat{\zeta})\ , \quad \text{where}$$

$$\beta(g,\hat{\zeta}) \;:=\; \|\hat{\zeta}-\mathcal{N}_g(\hat{\zeta})\| \;=\; \|\mathrm{D}_g(\hat{\zeta})^{-1}g(\hat{\zeta})\|\ , \quad \text{and}$$

$$\gamma(g,\hat{\zeta}) \;:=\; \sup_{k\geq 2}\left\|\frac{\mathrm{D}_g(\hat{\zeta})^{-1}(\mathrm{D}^k g)_{\hat{\zeta}}}{k!}\right\|^{\frac{1}{k-1}}\ .$$

If $\alpha(g,\hat{\zeta}) < \frac{13-3\sqrt{17}}{4} \approx 0.15767$, then $\exists\zeta\in\mathbb{C}^n$ such that $\|\zeta-\mathcal{N}_g^k(\hat{\zeta})\| < 2^{1-2^k}\|\zeta-\hat{\zeta}\|$, ($\mathcal{N}_g^k(\hat{\zeta})$ *converges quadratically*).

Overdetermined systems are ubiquitous

The only problem with Smale's α-theory is that overdetermined systems are ubiquitous, and α-theory requires square systems.

Example. Which lines in $\mathbb{P}^5$ meet four general 2-planes?
Set $H := (I_2|X)^T$ with X a 2×4 matrix of indeterminates,
and $K_i \in \mathbb{C}^{6\times 3}$, for $i = 1, \dots, 4$.

rank$(H|K_i) \leq 4$ for each i gives 24 quadratic equations in 8 variables. This overdermined system has 3 solutions.

We square this up to rank$(H|K_i|L_{i,j}) \leq 5$ (a determinant),
where $L_{i,j} \in \mathbb{C}^{6\times 1}$ for $i = 1, \dots, 4$ and $j = 1, 2$.

This is a square system with 14 solutions.

Goal: Give methods to certify solutions to overdetermined systems using square subsystems.

Certifying Nonsolutions

Let g be a polynomial system and $\delta > 0$. A point $\hat{\zeta} \in \mathbb{C}^n$ is a δ-approximate solution to g if there is a map $N_g \colon \mathbb{C}^n \to \mathbb{C}^n$ s.t.

(1) there is a point $\zeta \in \mathcal{V}(g)$ with $\|\zeta - \hat{\zeta}\| < \delta$, and

(2) the sequence $N_g^k(\hat{\zeta})$ converges to ζ.

N_g may be any map, including Newton for a square subsystem.

We may certify that ζ is a nonsolution to another polynomial.

Proposition. *For any polynomial f, if*

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

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

Proof. Use the Taylor expansion of f.

Let $\delta(f, g, \hat{\zeta})$ be the *Taylor residual*, the quantity in (1). For a polynomial system $f = (f_1, \ldots, f_m)$, set $\delta(f, g, \hat{\zeta}) := \max_i \delta(f_i, g, \hat{\zeta})$.

One approach to certification

Suppose that we have a system f with a square subsystem g, and we know an integer d s.t.

$$d \;=\; \#(\mathcal{V}(g) \smallsetminus \mathcal{V}(f))\,.$$

Let $S = \{\hat{\zeta}_1, \ldots, \hat{\zeta}_e\}$ be a set of δ-approximate solutions to g with distinct associated solutions.

For each $\hat{\zeta}$ in S, if $\delta(f, g, \hat{\zeta}) > 0$, we discard $\hat{\zeta}$.

If we have discarded d solutions, the remaining are certified soutions to f.

If not, then we may use Newton steps to refine the approximate solutions to g, and repeat. The quadratic convergence of $\mathcal{N}_g$ guarantees that, after sufficient refinement, we will discard exactly the nonsolutions to f.

Newton-Okounkov bodies

A natural question is how do we determine such a number $d = \#(\mathcal{V}(g) \smallsetminus \mathcal{V}(f))$?

Kaveh and Khovanskii showed that, given $f = f_1, \ldots, f_m$, the number of solutions $\mathcal{V}(g) \smallsetminus \mathcal{V}(f)$ for general square subsystems g is the volume of a Newton-Okounkov body associated to f.

While this convex body is difficult to determine. When we can determine the NOBody, this number d is available to us.

Elise Walker's talk suggested one use of this new theory in applications, and this is another.

What is interesting from this point of view is that the soutions $\mathcal{V}(f)$ to the overdetermined system that we want are the undesirable *base points* of f.

Another approach

Suppose that we have an overdetermined system f, we know $e = \#\mathcal{V}(f)$, and that the square subsystems g of f satisfy $d = \#\mathcal{V}(g)$ with $d > e$. Intersection theory may give such information.

Computing the solutions to g and to another square subsystem g', we may

—certify both sets of d solutions.

—Refine them so that each is contained in a ball containing the associated solution and separated from the other $d-1$ solutions to the same subsystem.

Suppose that e balls of g meet a *unique* ball of g'.

Then this set e solutions/balls is a set of approximate solutions to f.

There are other approaches....

Certification is possible for overdetermined systems, but it requires extra global information.