Decision Complexity in Dynamic Geometry

Ulrich Kortenkamp
Freie Universität Berlin

ADG 2000

1. Randomized Theorem Proving in Geometry

Given a conjecture, decide with high probability (best is 1) whether it is a theorem.

- Easy for conjectures encoded by polynomial identities $p(x_1, \ldots, x_n) = 0$

These polynomial identities can be *checked* in polynomial time. Repeated tests increase the probability – finitely many can be sufficient to give probability 1!

1.1. Schwartz-Zippel Theorem

Probabilistic version of Fundamental Theorem extended to several variables

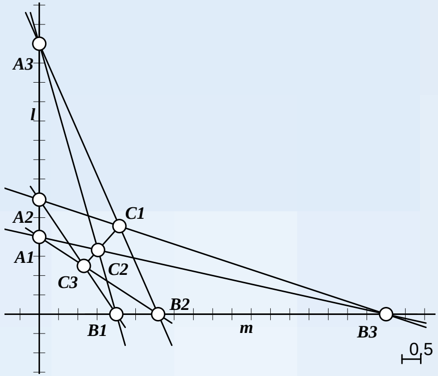
Theorem [Schwartz 79]. Let $Q(x_1,\ldots,x_n) \in \mathbb{K}[x_1,\ldots,x_n]$ be a multivariate polynomial of total degree d. Fix any finite subset $S \subset \mathbb{K}$, and let $r_1,\ldots,r_n$ be chosen independently and uniformly at random from S. Then

$$\mathbf{Pr}[Q(r_1,\ldots,r_n) = 0 \,|\, Q(x_1,\ldots,x_n) \not\equiv 0] \leq \frac{d}{|S|} \quad .$$

Can be refined to multidegree-version [Zhang 90]

1.2. Example: Pappos' Theorem

First (?) appearance: [Zhang 90] "Parallel Numerical Method"



Careful analysis of degrees in Pappos Theorem shows that we can choose $S = 0, 1, 2$ as a test set (possible values for the coordinates), and only trivial (degenerate) cases remain to check.

No computation is necessary!

1.3. How to get the polynomials

A conjecture can be encoded into a polynomial ...

- by hand
- using Gröbner bases (very much computing)
- using Wu's method (much computing)
- ...

1.4. Constructive (*sequential*) Conjectures

For *constructive* conjectures using (intersection) points and (connecting) lines only it is *very* easy to find a corresponding polynomial identity.

- Elements are given one-by-one using basic construction steps.
- Use homogeneous coordinates for points and lines
- meets and joins are done using cross products
- collinearity/concurrency tests are done using determinants.

Leads directly to a polynomial encoding the conjecture.

1.5. Encoding polynomials

The polynomials are not given symbolically, but as a *straight-line program (SLP)*.

An SLP π consists of a sequence of steps of the form

$$z_i \leftarrow x_i \circ y_i \qquad (\circ \in \{+, -, \cdot, /\})$$

where z_i is a new *programming variable* and x_i and y_i are either constants, *input variables* or old programming variables z_j, $j < i$.

These SLPs can be evaluated for given input. The last programming variable is the *value* of the polynomial.

Important: The degree of the polynomial can be exponential in the length of π.

1.6. Examples

1.6.1. Two straight-line programs for $p(x) = 3x^3 + x$:

1. $z_1 \leftarrow x \cdot x$
2. $z_2 \leftarrow z_1 \cdot x$
3. $z_3 \leftarrow 3 \cdot z_2$
4. $z_4 \leftarrow z_3 + x$

1. $z_1 \leftarrow x \cdot x$
2. $z_2 \leftarrow 1$
3. $z_3 \leftarrow 3 \cdot z_1$
4. $z_4 \leftarrow z_1 + z_2$
5. $z_5 \leftarrow z_3 \cdot x$

1.6.2. Two straight-line programs for $p(x,y) = x^2 + 2x + xy$:

1. $z_1 \leftarrow x \cdot x$
2. $z_2 \leftarrow z_1 + x$
3. $z_3 \leftarrow z_2 + x$
4. $z_4 \leftarrow x \cdot y$
5. $z_5 \leftarrow z_4 + z_3$

1. $z_1 \leftarrow x + 2$
2. $z_2 \leftarrow z_2 + y$
3. $z_3 \leftarrow z_2 \cdot x$

Remark: It is not at all trivial to check equivalence of SLPs!

2. Constructive Theorems using Circles (and Conics)

If we want to encode conjectures that use intersection points of circles (or conics), we need square (and cubic) root operations.

Can we extend SLPs to radical expressions?

Problems:

- we need complex numbers (easy)
- we must be able to calculate with radicals (ok, Core/Leda)
- we must fix our notion of conjecture/theorem (yesterday!)

2.1. Fundamental problem of Dynamic Geometry

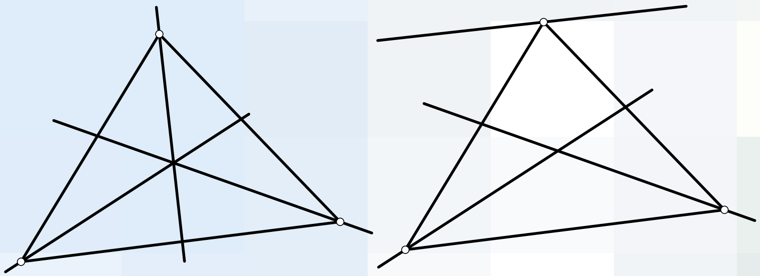
We cannot introduce a new operation $\sqrt{\cdot}$ – this is non-constructive and ambiguous.

Instead, we could introduce a new operation $\pm\sqrt{\cdot}$ and relax the notion of SLP.

A *complex GSP* (geometric SLP) is conceptually the same as an SLP, but allows ambiguous operations. An *instance* of a GSP is a “valid” assignment of values to the variables.

A constructive theorem corresponds to a complex GSP *and* an instance that identifies a set of sign decisions at the square roots, and all other instances that are connected by a continous path avoiding singularities (*analytically*) to the first instance.

2.2. Example: Bisector theorem



Are these two instances connected analytically?

(of course (?) not, but why? $\longrightarrow$ Riemann surfaces)

2.3. Ignoring Signs

[Tulone/Yap/Li 2000] give a probabilistic method for zero-testing of radical expressions based on the rewriting rule:

$$A + B\sqrt{C} \quad \mapsto \quad A^2 + B^2 C = (A + B\sqrt{C})(A - B\sqrt{C}).$$

This method ignores sign decisions.

We will know whether there is some instance with value 0 at all, but not whether we can reach this analytically.

3. Decision Complexity

[Complex Reachability Problem, CRP]
Given two instances of a complex GSP with one input variable that differ in exactly one intermediate result. Is it possible to move analytically from the first instance to the second?

is at least as hard as

[SLP zero testing, SRP0?]
Given a division-free straight-line program Γ over $\mathbb{Q}$ with one input variable. Is the polynomial p encoded by Γ the zero polynomial?

3.1. Proof (Sketch)

3.1.1. Encoding an instance

We will deal with GSP inputs that have polynomial coding length.

For each $\pm\sqrt{\cdot}$-statement we specify which solution we choose using one bit b for each decision: If $b = +$ choose the solution with the smaller or equal angle in the polar coordinate representation of the two possibilities, else the other one.

Remark: We cannot afford to evaluate a GSP!

3.1.2. Transformation of SLP0? to CRP

Assume $p_\pi(z)$ is the polynomial encoded by an SLP π. We want to check whether $p_\pi \equiv 0$. The length of π is n, so the degree of $p_\pi(z)$ is less than $2^n + 1$.

Create two GSPs that compute

$$\sqrt{zp_\pi(z) + M} \quad \text{resp.} \quad \sqrt{z^2 p_\pi(z) + M}$$

where M is a constant larger than any constant that could be evaluated by π (this is possible!) and choose the instances $(z = 0, +)$.

Let $p_1(z) := zp_\pi(z) + M$ and $p_2(z) := z^2 p_\pi(z) + M$.

(proof cont.)

Let $p_1(z) := zp_\pi(z) + M$ and $p_2(z) := z^2 p_\pi(z) + M$.

Observe: $\sqrt{p_1(z)}$ and $\sqrt{p_2(z)}$ are constant iff $p_\pi \equiv 0$

Now, if $p_\pi \equiv 0$, then $\sqrt{p_1(z)}$ and $\sqrt{p_2(z)}$ are constant as well, so their sign decision can never change, the instance $(z = 0, -)$ is not reachable.

Otherwise, if $p_\pi \not\equiv 0$, either $p_1(z)$ or $p_2(z)$ has a root α of odd multiplicity. Choosing a path that winds around that singularity α changes the sign decision from $+$ to $-$, i.e. the instance $(z = 0, -)$ is reachable for one of the two GSPs. $\square$