Quantifier elimination, decision algorithm, effectivenesss vs non-effectiveness in semialgebraic geometry

Michel Coste

IRMAR, Université de Rennes 1

IPAM workshop, March 2014

Outline

- Presentation of quantifier elimination and decision problem
- Quantifier elimination algorithm for real closed fields
- How to obtain effective uniform bounds for free: example of Hauptvermutung
- Semialgebraic geometry is not always effective

ref.: Acquistapace-Benedetti-Broglia 1990, C.

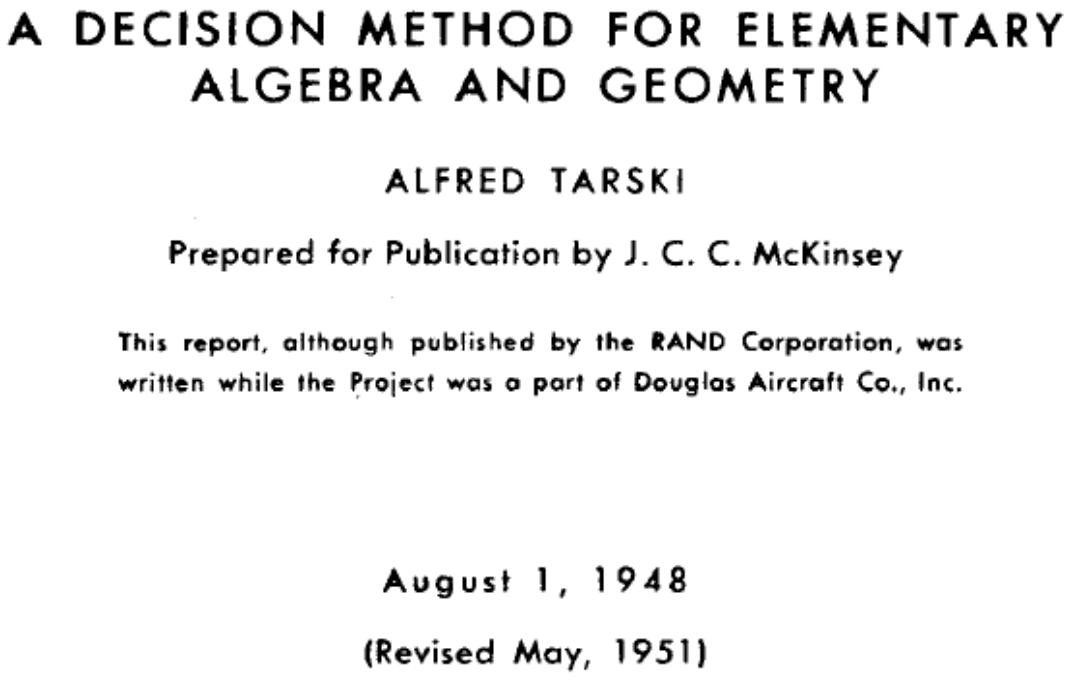
Two problems

1. Does there exist four disjoint unit spheres in $\mathbb{R}^3$ which have 12 real common tangents ?
2. Describe the set of $(A, B, C, D) \in (\mathbb{R}^3)^4$ which are the centers of distinct unit spheres in $\mathbb{R}^3$ having 12 real common tangents.

Two problems

1. Does there exist four disjoint unit spheres in $\mathbb{R}^3$ which have 12 real common tangents ?
2. Describe the set of $(A, B, C, D) \in (\mathbb{R}^3)^4$ which are the centers of distinct unit spheres in $\mathbb{R}^3$ having 12 real common tangents.

Tarski has an algorithm to solve both problems (in principle), result obtained in the 30's:



A DECISION METHOD FOR ELEMENTARY ALGEBRA AND GEOMETRY

ALFRED TARSKI

Prepared for Publication by J. C. C. McKinsey

This report, although published by the RAND Corporation, was written while the Project was a part of Douglas Aircraft Co., Inc.

August 1, 1948

(Revised May, 1951)

Elementary algebra and geometry

All that can be expressed by a formula (of the first order language of ordered fields), obtained as follows :

1. If $P \in \mathbb{Z}[X_1, \ldots, X_n]$, then $P = 0$ et $P > 0$ are formulas.
2. If Φ and Ψ are formulas, then "Φ and Ψ", "Φ or Ψ", "not Φ" are formulas.
3. If Φ is a formula and X a variable (intended to range over $\mathbb{R}$), then $\exists X\ \Phi$ and $\forall X\ \Phi$ are formulas.

Quantifier-free formula: obtained only with 1 and 2.
Closed formula: without free variable.

- Exercise: express by a formula the fact that the line through $P = (p_1, p_2, p_3)$ directed by the unit vector $U = (u_1, u_2, u_3)$ is tangent to the unit sphere with center $A = (a, b, c)$; express that the line through P directed by U is different from the line through P' directed by U'; express that the two unit spheres with center A and A' are disjoint.
- The existence of four unit spheres as in problem 1 can be expressed by a closed formula. Decision problem: decide whether it is true or not.
- The set of (A, B, C, D) as in problem 2 can be described by a formula with 12 free variables. Quantifier elimination: produce a description by a quantifier-free formula (boolean combination of polynomial equations and inequalities)

Real-closed fields

Axioms of real closed fields:

- ordered field
- intermediate value theorem for polynomials

Note: "For every polynomial ..." is not a formula. "For every polynomial of degree $\leq d$ ..." is a formula (quantification on $d+1$ coefficients). Intermediate value theorem for polynomials is expressed by infinitely many axioms.

Examples of real closed fields: $\mathbb{R}$, $\mathbb{R}_{\mathrm{alg}}$, Puiseux series $\sum_{i \geq i_0} a_i \, \epsilon^{i/q}$ with coefficients in a real-closed field...

The only archimedean real-closed fields are subfields of $\mathbb{R}$.
Archimedeanity cannot be expressed by a formula:
$\forall x \, \exists n \in \mathbb{N} \; x \leq n$ contains a quantification on a natural number, and no formula describes the set of natural numbers.

Quantifier elimination (QE)

Theorem

There is an algorithm which takes as input any formula Φ and returns a quantifier-free formula which is provably equivalent to Φ in the theory of real-closed fields.

Well known example: $\exists X\ AX^2 + BX + C = 0$ is equivalent to

$$(A \neq 0 \quad \text{and} \quad B^2 - 4AC \geq 0)$$
$$\text{or} \quad (A = 0 \quad \text{and} \quad B \neq 0) \quad \text{or} \quad (A = B = C = 0)\,.$$

Decision method

As a consequence (quantifier free closed formulas are boolean combinations of $n > 0$ or $n = 0$ where n is integer):

Theorem

There is an algorithm which takes as input any closed formula Φ (without free variable) and decides whether Φ or its negation is a theorem of the theory of real-closed fields.

In contrast, there cannot be a decision method for elementary arithmetic, i.e. the arithmetic of natural numbers with addition and multiplication (Gödel-Church-Rosser).

QE via counting roots (Tarski)

- Algorithmic reduction to an equivalent prenex form

$$Q_1 X_1 \; Q_2 X_2 \ldots Q_\ell X_\ell \; \Psi(Y_1, \ldots, Y_k, X_1, \ldots, X_\ell) \; ,$$

  where Q_i are quantifiers and Ψ is quantifier-free.
- It suffices to eliminate one quantifier at a time, and to deal with an existential quantifier.
- $\exists X \, \mathcal{S}(Y_1, \ldots, Y_k, X)$ where $\mathcal{S}$ is a system of polynomial equations and inequalities.
- Case of $P(\underline{Y}, X) = 0, Q_1(\underline{Y}, X) > 0, \ldots, Q_r(\underline{Y}, X) > 0$: variants of Sturm to produce Boolean combinations $\mathcal{T}_c$ of sign conditions on the coefficients (depending on $\underline{Y}$) satisfied iff the number of solutions in X is c.
- Primitive recursive complexity.

QE via CAD (Cylindrical Algebraic Decomposition - Collins)

- Starting with $Q_1 X_1\ Q_2 X_2 \ldots Q_\ell X_\ell\ \Psi(Y_1, \ldots, Y_k, X_1, \ldots, X_\ell)$, where Ψ is a Boolean combination of sign conditions on polynomials in a finite family $\mathcal{P}$.
- Construct a CAD of $R^{k+\ell}$ adapted to $\mathcal{P}$. The formula describes a union of cells in R^k. Already OK for decision algorithm.
- For quantifier elimination, a quantifier-free description of cells is needed. This is provided by Thom's lemma: if $\mathcal{Q} \subset R[X]$ is a finite family of polynomials closed under derivation, $\bigcap_{Q \in \mathcal{Q}} \{x \in R \mid Q(x)\ ?_Q\ 0\}$ (where $?_Q$ is either $>$, $=$, $<$) is empty, or a point or an open interval.
- Better complexity: doubly exponential in the number of variables (free and bound).

QE via critical points

- Instead of eliminating one quantifier after the other, eliminate one block of existential quantifiers at a time using a parametric version of critical point method.
- Complexity: doubly exponential in the number of alternations of quantifiers (Grigoriev-Vorobjov, Renegar, Basu-Pollack-Roy).

Semialgebraic sets

By definition, a *semialgebraic subset* in R^n (R a real closed field) is described by a quantifier-free formula with parameters in R (some free variables replaced with elements of R). Semialgebraic mapping = mapping with semialgebraic graph.

Quantifier elimination: any subset described by a formula with parameters is semialgebraic.

Coarse complexity for semialgebraic sets

A semialgebraic subset $S \subset R^n$ has *complexity* $\leq p$ if it can be described as

$$S = \bigcup_{i=1}^{q} \bigcap_{j=1}^{r_i} \{x \in R^n \mid f_{i,j}(x) \ ?_{i,j} 0\} \ ,$$

where $q \leq p$, $r_i \leq p$, $f_{i,j} \in R[X_1, \ldots, X_n]$ have degrees $\leq p$ and $?_{i,j}$ is $=$ or > 0

Quantification over semialgebraic sets or mapping is not possible within elementary algebra, but quantification on semialgebraic sets or mappings of complexity $\leq p$ is possible.

Semialgebraic triangulation

Theorem

Let S be a closed and bounded semialgebraic subset of R^n. Then there exists a finite simplicial complex K in R^n and a semialgebraic homeomorphism $\phi : |K| \to S$

Elementary proof (in the theory of real closed fields) using CAD + control on adjacency of cells.

Effective uniform bound for free

- One can algorithmically produce from (n, p, q) a formula $\Theta(n, p, q)$ which says "For every closed and bounded semialgebraic subset of R^n of complexity $\leq p$, there exists a simplical complex K in R^n with $\sharp K \leq q$ (number of simplices) and a semialgebraic homeomorphism $\phi : |K| \to S$ of complexity $\leq q$."
- Elementary proof + compactness of first-order logic $\Rightarrow$ uniform bound: for every (n, p) there is a q such that $\Theta(n, p, q)$ is a theorem.
- Decision method applied to $\Theta(n, p, 1), \Theta(n, p, 2), \Theta(n, p, 3), \ldots \Rightarrow$ this bound is effective, i.e. a recursive function of (n, p).
- Very weak result: with a little more work, doubly exponential bound .

Semialgebraic Hauptvermutung

Semialgebraic triangulations are essentially unique:

Theorem (Shiota-Yokoi 1984)

Let K, L be simplicial complexes and let $\phi : |K| \to |L|$ be a semialgebraic homeomorphism. Then there are subdivisions K' of K and L' of L such that K' is simplicially isomorphic to L'. This amounts to say that $|K|$ and $|L|$ are PL (piecewise linear)-homeomorphic.

The proof is not elementary: uses integration of vector fields, working over $\mathbb{R}$, not in the theory of real closed fields.

Note: there are homeomorphic polyhedra $|K|$ and $|L|$ which are homeomorphic but not PL-homeomorphic.

Expressing Hauptvermutung by a formula

$\Phi(n, d, p, s)$: "For every couple (K, L) of simplicial complexes in affine n-space with $\sharp K, \sharp L \leq d$ and for every semialgebraic homeomorphism $f : |K| \to |L|$ of complexity $\leq p$, there exist simplicially isomorphic subdivisions K' of K and L' of L with $\sharp K', \sharp L' \leq s$."

There is an algorithm with input (n, d, p, s) and output $\Phi(n, d, p, s)$ written as a formula (of the first order language of ordered fields).

Effective Hauptvermutung

Lemma

There exists $s(n,d)$ such that for every PL-homeomorphic polyhedra $|K|$ et $|L|$ with $\sharp K, \sharp L \leq d$, there exist simplicially isomorphic subdivisions K' of K and L' of L whith $\sharp K', \sharp L' \leq s(n,d)$.

Proof: There are finitely many such couples (K, L) up to simplicial isomorphisms.

Shiota-Yokoi + Lemma : for every n, d, p, there is s such that $\mathbb{R}$ satisfies $\Phi(n, d, p, s)$.

Effective Hauptvermutung

For such s, $\Phi(n, d, p, s)$ is a theorem of the theory of real closed fields. Applying the decision algorithm to $\Phi(n, d, p, 1), \Phi(n, d, p, 2), \Phi(n, d, p, 3), \ldots$:

Theorem

There is a recursive function $s(n, d, p)$ such that $\Phi(n, d, p, s(n, d, p))$ holds for any real closed field.

The number of vertices of the common subdivision is bounded by a recursive function of n, d, p.

- It is easy to find example of finiteness results without uniform bounds (typically, for results using archimedeanity). For instance, the fact that for every open covering $\mathcal{U}$ of $|K|$ there is a finite iterate of barycentric subdivision of K which is finer than $\mathcal{U}$. Such result does not hold over an arbitrary real closed field.
- More surprisingly, there are uniform bounds which are not effective, i.e. cannot be bounded by any recursive functions.

Semialgebraic families

- A semialgebraic family of subsets of R^n parametrized by a semialgebraic set M is a semialgebraic subset $S \subset R^n \times M$. The fiber of the family at $t \in M$ is $S_t = \{x \in R^n \mid (x, t) \in S\}$.
- If $S \subset R^n \times M$ is a semialgebraic family, there is p such that every fiber has complexity $\leq p$. The semialgebraic subsets of complexity $\leq p$ of R^n can be organized in a semialgebraic family $S(n, p) \subset R^n \times M(n, p)$.

Theorem (Hardt)

If $S \subset R^n \times M$ is a semialgebraic family, there is a finite semialgebraic partition $M = \bigcup_{i \in I} M_i$ such that there is a semialgebraic trivialization $S|_{M_i} \simeq F_i \times M_i$ over each M_i.

A non-effective uniform bound

Corollary

Given n, p, there is q such that for every couple T, U of semialgebraic subsets of R^n of complexity $\leq p$, if T and U are semialgebraically homeomorphic, then there is a semialgebraic homeomorphism $T \to U$ of complexity $\leq q$.

Proof: apply Hardt's theorem to $S(n, p) \subset R^n \times M(n, p)$.
So q is a uniform bound, but it is not effective:

Theorem

The $q(n, p)$ above cannot be bounded by any recursive function of n, p.

Proof of non-effectiveness

If $q(n,p)$ were effective, then one would have effective $s(n,d)$ such that for every simplicial complex K in $\mathbb{R}^n$ with $\sharp K \leq d$ such that $|K|$ is a PL n-ball (PL-homeomorphic to the standard simplex Δ_n), there is a semialgebraic homeomorphism $|K| \to \Delta_n$ of complexity $s(n,d)$. By the effective Hauptvermutung, there would be an effective $D(n,d)$ such that for every K as before, there would be a subdivision K' of K with $\sharp K' \leq D(n,d)$, simplicially isomorphic to a subdivision of Δ_m. This would provide an algorithm for deciding whether a polyhedron $|K|$ is a PL n-ball. By a result of Novikov, no such algorithm can exist for $n \geq 6$.