Deciding Topological Properties: Compactness of Basic Real Semialgebaic Sets (extended abstract)*

Pasqualina Conti and Carlo Traverso
Dipartimento di Matematica
Via Buonarroti 2
I-56127 PISA, ITALY
{conti,traverso}@dm.unipi.it

June 9, 2002

1 Introduction

We discuss the problem of deciding if a basic real semialgebaic set, i.e. a subset of $\mathbf{R}^n$ defined by a finite set of equations and inequalities, is compact.

Compactness is not a first-order property, hence one cannot apply quantifier elimination, but on the real field it is equivalent to closedness and boundedness, that are first orded properties, hence the problem is decidable; of course we are looking for better algorithms than elimination of quantifiers in general.

We will use a few standard notations in real algebraic geometry, for which the standard reference id [3]. The basic proof tools rely on quantifier elimination, but it is never used in algorithms, that just use standard commutative algebra tools, real root counting for zero-dimensional ideals being the only specific real algebraic geometry tool.

A preliminary version of many topics appearing here is [6].

2 Data structures: semi-ideals

A basic semialgebraic set is a subset of a real affine space $\mathbf{R}^n$ defined by a finite set of *sign conditions*, i.e. a set $\{X = (x_1, \dots, x_n) \in \mathbf{R}^n \mid f_i(X)\#_i 0,\ i = 1, \dots, m\}$ where each f_i is a real polynomial, and $\#_i$ is one of $=, \neq, >, <, \geq, \leq$. The definition can be extended to any real closed field.

*Work partly performed under Project "Tecniche per Immagini", cluster C15, progetto n. 7 "Sviluppo, Analisi ed Implementazione di Metodi Matematici Avanzati per il Trattamento di Immagini", with the contributoion of MURST

The algorithms that handle basic semialgebraic sets have to handle such sets of conditions. This in analogy to the use of ideals and sets of generators of ideals in algebraic geometry.

The algebraic structure adequate to handle these set conditions is a *semi-ideal*, i.e. a structure $\mathcal{I} = (I, f_i \#_i 0\}$ composed of an ideal I of a polynomail ring and a finite set of sign conditions not containing equalities. The coefficient field of the polynomial ring can be any ordered field.

A semi-ideal defines a basic semialgebraic set, composed by the points (on a real closed field extension of the ring of definition of the semi-ideal) for which the ideal vanishes and the sign conditions are verified, that is called the *locus* of the semi-ideal. A basic semialgebraic set does not identify a defining semi-ideal, since the set of all sign conditions verified on a basic semialgebraic set does not have a finite direct description.

Semi-ideals are necessary, since the structure corresponding to an ideal that collects all the algebraic consequences of a set of general sign conditions is not easily manegeable.

A sign condition $f\#0$ is called *closed* if $\#$ is one of $=, \leq, ge$; a semi-ideal id closed if the sign conditions are closed. The locus of a closed semi-ideal is a closed semialgebraic set, the converse is of course not true.

Everything is defined in formally real fields; indeed, the main tools in this paper require handling non-archimedean extensions of the reals. A semi-ideal requires a field of definition (the coefficient field of the polynomial ring), and the computations are all performed in purely transcendental extensions of this field of definition, that will usually be the rational field.

See [7] and [6] for further details.

3 Boundedness

To prove that a semialgebraic set A, defined by a semi-ideal $\mathcal{I}$, is bounded, it is sufficient to construct a "sufficently large box" and prove that A is inside. Let N be a "sufficiently large" number, and let $B = \{(x_1, \ldots, x_n) \mid -N < x_i < N\}$; to prove that B is completely inside B it is sufficient to prove that A does not meet any hypersurface $x_i = \pm N$, and that no connected component of A can be completely outside B. To prove this last assertion, it is sufficient to prove that N can be chosen larger than the largest coordinate of the largest local minimum and of the largest local maximum of one of the coordinates over B. It is easy to see that the set of values of such local maxima and minima is finite, and a finite set containing it can be described algebraically.

Hence boundedness is equivalent to proving the existence of an N sufficiently large. Since, given A, to prove that it is bounded, it is sufficient to prove the existence of such an N, and an explicit bound is not needed, we can prove this existence in any real closed extension. Hence, to be in the safe side, we choose an extension in which an element Ω infinitely large with respect to $\mathbf{R}$ exists, and choose $N = \Omega$. So, in this case, we have reduced a boundedness test to an emptiness test (in a suitable real closed extension).

In conclusion, we have the following theorem:

Theorem 1 *Let R be an ordered field, R' a real field containing R, and Ω in R' that is larger than any element of R. Let $R[X]$ be a polynomial ring, $X = (x_1, \ldots, x_n)$, and $\mathcal{I}$ a semi-ideal in $R[X]$. Then the locus of $\mathcal{I}$ is bounded iff the locus of every $\mathcal{I} + (x_j - \Omega) = 0$ and of every $\mathcal{I} + (x_j - \Omega = 0)$ are empty.*

How do we obtain an extension with an Ω? One has just to add an indeterminate Ω and define an ordering on $\mathbf{R}[\Omega]$ declaring that a polynomial is positive iff the leading coefficient is positive. Intersecting with $x_i = \Omega$ is just replacing an indeterminate x_i with another indeterminate Ω — the essential difference is that we have moved this indeterminate from the coordinates to the ground field — from the computational point of view this is equivalent to choose a suitable term-ordering for the computation of a Gröbner basis. Remark that the computation with $x_i = \Omega$ and $x_i = -\Omega$ is just the same, the difference being in the emptiness test, since exchanging Ω with $-\Omega$ is an automorphism, atthough not an ordeed automorphism.

A possible alternative is to consider a spheric box: instead of considering the intersections with $x_i = \Omega$, consider the unique intersection with $\sum x_i^2 = \Omega^2$; we consider this possibility an inferior one: it is true that one has to perform a single computation instead of several ones, but this computation involves one variable more and one quadratic equation more, and might be substantially harder.

Remark moreover that from a transcript of an algorithm using an extension with Ω it would be possible to recover a finite $N \in \mathbf{R}$, or even $N \in \mathbf{Z}$, such that replacing Ω with N everything works exactly in the same way. This is just following (in a special case) a proof af quantifier elimination.

4 Complexity - some unorthodox views

There are several points in which we choose an algorithm variant instead of another because of complexity consideation, although often of an highly non-standard type.

The type of problems handled by computational commutative algebra have complexity properties much different from what is standard to assume in complexity theory.

The worst-case complexity of such problems is usually double exponential. But problems with such complexity are quite unstable, and usually constructed creating inside of commutative algebra a model of a combinatorial theory.

The "generic" problems have a complexity which is smaller. But usually computational commutative algebra is used to model classes of problems, whose complexity might be even smaller than the "generic" complexity.

The algorithms in computational commutative algebra are self-adapting to the complexity of the problem, not to the worst-case complexity; hence worst-case analysis and even average complexity analysis are useless to predict running time in a special problem.

Moreover, complexity estimates are usually asymptotic estimates. The range of meaningful and interesting problems begins with very small problems, hence asymptotic analysis does not help.

Another important feature is that often the limiting feature is space, not time: large problems usually fail because of memory overflow, after a not-too-long time. Complexity theory instead often trades space for time, and this is bad in our case.

This has an important consequence; the impact of increased complexity has a threshold effect: a very moderate increase in complexity of a problem might transform an easy problem into an unfeasible problem: doubling, does not double the time needed, but produces a crash for lack of memory. If instead we can split the problem in a number of completely independent subproblems, we can solve the problem; and this even if the number of subproblems is exponential in some parameter that is not too large.

5 Closedness test for bounded basic semialgebraic sets

A simple special case is when we consider a basic semialgebraic set A defined by closed conditions (i.e. conditions of the type $f(X) = 0$ or $f(X) \geq 0$. In that case, A is automatically closed, hence one has just to decide if it is bounded.

To handle the general case, the standard trick is to replace an inequality with an equality with the addition of an indeterminate: to replace $f(x) \neq 0$ with $Sf(X) = 1$ and $f(x) > 0$ with $f(X) \neq 0$ and $f(X) = T^2$, S and T being new indeterminates.

Our point of view is that this type of transformation, although it does not change qualitatively the complexity class of the problem, has to be avoided, and we develop more direct algorithms with the introduction of towers of infinitesimal extensions.

We will rather reduce the boundedness test into a closedness test: to prove that A, closed in $\mathbf{R}^n$, is bounded, one can prove that it is closed in $\mathbf{P}_1^n$, where $\mathbf{P}_1$ is the one-dimensional real projective line.

We will hence prove that to test that A, defined by equations and $f(X) > 0$, we have just to test that A intersected with $f(X) = \epsilon$ is empty, ϵ being an infinitesimal.

Theorem 2 *Let R be an ordered field, R' a real field containing R, and ϵ in R' that is smaller than any positive element of R. Let $R[X]$ be a polynomial ring, $X = (x_1, \ldots, x_n)$, and $\mathcal{I} = (I, f_i \#_i 0)$ a semi-ideal in $R[X]$. Then the locus of $\mathcal{I}$ is closed if and only if, for every non-closed condition $f_i \#_i 0$, the locus of $\mathcal{I} + (f_i - \epsilon = 0)$ and the locus of $\mathcal{I} + (f_i + \epsilon = 0)$ are empty.*

The resulting algorithm allows, assuming the existence of an emptiness test, to decide the closedness of a bounded basic semialgebaic subset of $\mathbf{R}^n$; and this is equivalent to compactness. The algorithm is not sufficient to decide the closedness of a non-bounded basic semialgebraic set, nor to decide the compactness of a non basic semialgebraic set (a finite union of basic semialgebraic sets). In general, the problem of the relative closedness seems to be a much harder problem, and is related to the problem of getting a semi-ideal representation of the closure of a basic semialgebraic set as locus of a semiideal.

The details will appear in the full paper.

6 Testing emptiness

Emptiness tests have been more usual in computational real algebra, but usually using tools that optimize asymptotic worst case complexity at the expense of feasibility, notable exception being [13], [2] and [14].

To test if the locus of a semi-ideal $\mathcal{I} = (I, f_i \# 0)$ is empty, we proceed by induction on the dimension of I; if it is 0, one can use the method of Hermite,[11], [12] or any numerical method that can separate the roots and certify a sufficiently small neighborhood. Otherwise one proceed inductively proving that

1. The locus of $\mathcal{I}$ is compact;
2. The real subset of the set of (complex) critical points of a coordinate function is empty.

The definition of critical point, classical for smooth points, [10], can be extended in general stating that non-smooth points and boundary points are critical. Since the formula for critical points depends on the dimension of the variety, one has preliminarily to perform an equidimensional decomposition; and to allow induction, one has to ensure that the singular points are non dense, hence the equidimensional decomposition has to be a radical equidimensional decomposition. Refer to [5] for details.

There are moreover some special cases that have to be handled separately, in which all the points are critical with respect to a coordinate function, since in this case induction on dimension stops before reaching dimension zeo; for these it is sufficient to remark that if the dimension is not zero. at least one coordinate function does not fall in this case; but a cleverer handling of such a special configuration is possible.

Remark that coordinate functions have nothing special: one can take any function $f(X)$ and consider critical points of f; this is equivalent to changing the embedding adding a new coordinate T and a new equation $f(X) - T$. This might be advantageous if f can be chosen to have only isolated critical points in the non-singular part, but risks to increase the practical complexity. Functions that can be useful are linear combinations of coordinates, and distance from a point, see [2].

7 Implementation

In implementing the algorithms described, it is useful to avoid duplication of computations; hence, for example, if we prove that a set is bounded, every subset is automatically bounded.

Another point that might need considerations and experiments is the following: let A be a basic semialgebraic set, A' be the subset of A obtained adding the condition $f(X) \geq 0$ abd A'' the subset of A obtained adding the condition $f(X) > 0$. We want to test if A'' is closed in A', and we prove that A'' is closed if and only if the subset A_ϵ obtained adding the condition $f(x) = \epsilon$ is empty. If however we prove the much simpler assertion that $A' \setminus A''$ is empty, i.e. that A_0 obtained adding the condition $f(x) = 0$ is empty, the result follows. However the condition $A_0 = \emptyset$ is sufficient but not necessary. One needs experience to decide if performing the less expensive test first is good or not.

To implement the test, one needs to have, besides a basic commutative algebra package,

- a radical equidimensional decomposition algorithm
- a real root counting algorithm for ordered extensions of the real field.

The first exists in the AlPi/PoSSoLib system, [1], the second requires a small modification of the PoSSoLib, that we hope to have available soon. This will allow experimental study and algorithm optimizations.

References

[1] *AlPi: a PoSSo LISP interface*, `ftp://posso.dm.unipi.it/pub/posso/traverso/alpi.tgz` *PoSSoLib-3.0.1*, `ftp://posso.dm.unipi.it/pub/posso/traverso/PoSSoLib-3.0.1`

[2] Ph. Aubry, F. Rouillier, M. Safey El Din, *Real Solving for positive dimensional systems* `http://www.lip6.fr/reports/lip6.2000.009.html`

[3] J. Bochnak, M. Coste, M.-F. Roy, *Géométrie Algébrique Réelle*, Erg. der Mathematik, Vol. 12, Springer (1987)

[4] G. Collins, *Quantifier elimination for real closed fields by cylindrical algebraic decomposition*, Autom. Theor. form. Lang., 2nd GI Conf., Lect. Notes Comput. Sci. 33, 134-183 (1975)

[5] M. Caboara, P. Conti, C. Traverso, *Yet Another Ideal Decomposition Algorithm*, AAECC-12,LNCS 1255 (1997)

[6] P. Conti, C. Traverso, *Algorithms for the real radical*, Technical report (1998), see `http:///www.dm.unipi.it/~traverso/Papers/RealRadical.ps`.

[7] P. Conti, C. Traverso, *Algebraic and Semialgebraic Proofs: Methods and Paradoxes*, Automated Deduction in Geometry (J. Richter-Gebert and D. Wang, eds.). LNAI 2061. Springer-Verlag, Berlin Heidelberg, 2001.

[8] D. Eisenbud, *Commutative Algebra, with a view towards Algebraic Geometry*, Springer Verlag, (1994)

[9] P. Gianni, B. Trager, G. Zacharias, *Gröbner bases and primary decomposition of polynomial ideals*, J. Symb. Comp. 6, 149–167 (1988)

[10] J. Milnor, *Morse theory*, Annals of Mathematics Studies. No.51.,Princeton University Press, (1963)

[11] P. Pedersen, M.-F. Roy, A. Szpirglas: *Counting Real Zeros in the Multivariate Case*, Computational Algebraic Geometry, F. Eyssette, A. Galligo (editors), 203-223 (1993), Birkhäuser.

[12] F. Rouillier, *Algorithmes efficaces pour l' étude des zéros réels des systèmes polynomiaux*, thesis, Rennes (1996)

[13] F. Rouillier, M.-F. Roy, M. Safey, *Testing emptiness of real hypersurfaces, real algebraic sets and semi-algebraic sets*, FRISCO technical report (1998).

[14] F. Rouillier, M. Safey El Din and E. Schost, *Solving the Birkhoff Interpolation Problem via the Critical Point Method: An Experimental Study*, Automated Deduction in Geometry (J. Richter-Gebert and D. Wang, eds.). LNAI 2061. Springer-Verlag, Berlin Heidelberg, 2001.

[15] M.-F. Roy, *Basic algorithms in real algebraic geometry and their complexity: from Sturm's theorem to the existential theory of reals* Lectures on Real Geometry, in memoriam of Mario Raimondo, de Gruyter, Expositions in Mathematics (1996).