On the theoretical and practical complexity of the existential theory of reals.

Joos Heintz,Marie-Françoise Roy, Pablo Solernó *

1. Introduction.

In the last years significant improvments to the complexity of quantifier elimination in the real case have been achieved and while the Cylindrical Algebraic Decomposition algorithm ([Co], [C]) has a running time doubly exponential in the number of variables, new algorithms running in single exponential time in the number of variables when the number of alternation of quantifier is fixed have been described (see [Ca], [GV], [HRR], [HRS1], [HRS2], [Re1],[Re2]).

While the Cylindrical Algebraic Decomposition algorithm has been already implemented and improved in many aspects, these new algorithms have been very little experimented so far.

We shall not discuss in this paper general quantifier elimination but a restricted problem which is the existential theory of reals, that is an algorithm deciding if a semi-algebraic set has points, that we shall call "decision problem" in the sequel.

Let us fix notations. The number of variables will be n, the maximal degree of the polynomials will be d, the length of integers will be l, the number of equations will be s.

The report [Ho] concludes that for small inputs ($n = m = s = l = 2$) the running time of two single exponential algorithms ([GV]and [Re1]) would be more than one million year while the CAD runs in two seconds or less. He did not consider the algorihtm of [HRS1] or [HRS2] but it is likely that the conclusion would be similar. Making the simple remark that the running time of these algorithms is necessarily increasing with the paremeters he concludes that the values of parameters for which the single exponential methods explained in these theoretical papers would give better times than the CAD corespond to intractable problems.

We would like to propose here the following idea:

"it is possible to implement efficiently slight variants of single exponential methods well adapted to important particular cases of the decision problem"

A typical problem of this kind would be $n = 2$ (resp. $3, 4, 5$), $s = 1$, $l = 2$, $d = 20$ (resp. $6, 4, 3$) for particularly good (but generic) geometric situations, where it is expected to have a reasonnable computation time (say minutes or hour We have even the hope that better computing times than CAD, or even solution of problems intractable by CAD, could be reached by these methods.

* partially supported by POSSO BRA 6846

2. Basic ideas of single exponential method compared to CAD.

Let us go back to the basic ideas of single exponential methods and explain
the main difference with the CAD process (see also [HRR]).

As it is well known, the cylindrical algebraic decomposition method consists of two phases

a) a projection phase, where the variables are eliminated one by one,

b) a going up phase, where the sign conditions and cylinders are reconstructed progressively, going from the line to the plane, then at the end to $\mathbf{R}^n$.

In phase a) elimination theory is used: resultants, subresultants, etc.

In phase b) one starts from the univariate polynomials obtained at the end of phase a) and characterizes their roots and the intervals between their roots using, for example, a dichotomy algorithm based on Sturm's theorem [St]). Sturm's theorem is then used in the fibers to go from dimension k to dimension $k+1$.

The complexity of calculating a cylindrical algebraic decomposition is polynomial in the degree d and the number s of input equations, and doubly exponential in n, the dimension. This complexity appears to be intrinsically related to the iterative method of eliminating variables.

Indeed, if one eliminates one variable between polynomials of degree d in n variables, one gets polynomials of degree d^2 in $n-1$ variables. Eliminating a second time gives polynomials of degree d^4 in $n-2$ variables, and at the end of the process one has polynomials in one variable of degree d^{2^n}. This doubly exponential behaviour is unavoidable in the worst case, and it is possible to give doubly exponential lower bound result for quantifier elimination ([We], [DH]).

But it has been noticed that the polynomials obtained in CAD are almost always highly factorizable, and this worse case argument is not convincing for an average complexity behaviour.

The key geometric idea for new single exponential methods is the following: avoid cascading projections by working directly on the object using Morse functions with a finite number of critical points, and be reduced directly to a 0 dimensional problem whose number of solutions is single exponential in n.

Indeed if we want to decide if a given semi-algebraic set in $\mathbf{R}^n$ is

empty or not, we do not need all the information given by CAD on all its intermediate projections .

Let us take an example to illustrate this situation. If we consider a well chosen coordinate function on the torus, we shall have to deal with only four critical points (picture a)). On the other hand, if we project the same torus, we have a lot of extra points to study,that have nothing to do with the original geometric situation and are created by the chosen projection (picture b)). In general, in the first method, the

method of critical points, the number of points to consider will be single exponential, and in the second case, the CAD method, it will be doubly exponential.

The equation of the torus is

$$4X^2 + 2Y^2 + 2Z^2 - 4YZ - (X^2 + Y^2 + Z^2 + 3)$$

The Morse function we consider is the Y coordinate.

picture a)

picture b)

3. Variants of the critical points method

We shall now explain some ideas that might be useful in order to develop efficient variants of the method in [HRS1],[HRS2]. They could probably be adapted to [GV] or [Re1]

as well. The geometric tricks , like critical points infinitesimal deformations, used in our method, are closely related to ideas in [GV] that influenced us a lot, but the basic

subroutines we use are quite different. The point of view of [Re1] is quite closed but more influenced by optimization concepts.

Let us explain how would work the simplest version of the method in a particular but fundamental case. In fact the extra complications of the algorithm (that we shall explain and discuss later) are precisely designed in order to reduce the general case to this case.

3. 1. The case of a regular hypersurface

We consider an algebraic set $Z(f)$ defined as the zero set of a single equation f of degree d in n variables.

We want to decide whether $Z(f)$ is empty or not.

We make the basic geometric hypothesis

(H 1) $Z(f)$ is smooth (even in the complex field)

3.1.1. The easy smooth bounded case

Let us suppose (H 1) and moreover
(H 2) the X_n coordinate is a M-function, that is the set of critical points (real and complex) in the X_n direction is finite (even in the complex field)
(H 3) $Z(f)$ is bounded.

Then we have the following property (P 1): $Z(f)$ is non empty if an only if there are real critical points of the X_n function on $Z(f)$.

The algorithm A 1) for the decision method in this case runs as follows:

A 1 1) compute the quotient structure (a basis of the vector space and the multiplication tables) of the quotient ring A of the 0-dimensional ideal I generated by the n equations

$$f = \frac{\partial f}{\partial X_1} = \ldots = \frac{\partial f}{\partial X_{n-1}} = 0.$$

which is the set of critical points of the function X_n over $Z(f)$ (points where the tangent hyperplane is perpendicualr to the X_n axis or equivalently where the gradient is collinear to the X_n axis).

This can be done by any Groebner basis computation or, since the ideal is complete intersection (as many equations as variables) by new methods that we do not discuss here (see [Car]). In theory, the single exponential complexity is obtained by solving enormous linear systems with degree bounded by the effective version of Hilbert Nullstesllensatz (see [Bro]).

In practice a Groebner basis computation by the latest improvment of Buchberger's algorithm (see [Bu] for the basic version) is fine. The complexity and efficiency of the new methods of [Car] have not been studied yet but this method might be very useful.

A 1 2) decide if the set $Z(I)$ of critical points of the function X_n has real points. This can be done by various methods. The method we proposed in [HRS1]was based on the computation of the radical which gives an easy reduction to the univariate case (since it is possible to express, after a well chosen change of coordinates, the last coordinates of the solutions as a polynomial in the first one) and next on Sturm sequence.

One other possible method could be to compute the Groebner basis for the lexicographical ordering (directly or using for example [FGLM] to get it from another Groebner basis for another order) and to use iteratively Sturm theorem. Another method could use the algorithm of [PRS] which needs a Groebner basis, but not necessarily for the lexicographical ordering. Semi-numerical methods could be used too since the field is the field of reals.

3.1.2.The easy smooth non bounded case

Let us suppose again (H1) and (H 2) and let us replace (H 3) by

(H 4) the distance function to the origin is an M-function, that is has a finite number of critical points on $Z(f)$.

Conditions (H 1) , (H 2) and (H 4) are generically valid: equations f of

degree d in n variables verifying conditions (H 1) , (H 2) and(H 4) contain a Zariski-dense open set of all equations of degree d in n variables. It was not the case for (H 1), (H 2) and (H 3).

Now we have property (P 2): $Z(f)$ is non empty if and only if the function distance to O has real critical points on $Z(f)$.

The algorithm A 2) for the decision problem in this case runs as follows:

A 2 1) perform A 1) and decide that $Z(f)$ is non empty if there are real critical points of the X_n function on $Z(f)$ else go on with

A 2 2) compute the quotient structure (a basis of the vector space and the multiplication tables) of the quotient ring A' of the 0-dimensional ideal I' generated by the n equations

$$f = \frac{\partial f}{\partial X_1}X_n - \frac{\partial f}{\partial X_n}X_1 = \ldots = \frac{\partial f}{\partial X_{n-1}}X_n - \frac{\partial f}{\partial X_n}X_{n-1} = 0.$$

which is the set of critical points of the function distance to O over $Z(f)$ (points where the tangent hyperplane is perpendicular to the vector $(X_1, \ldots, X_n)$ or equivalently where the gradient is collinear to the the vector $(X_1, \ldots, X_n)$).

A 2 3) decide if the set $Z(I')$ of critical points of the function distance to O has real points.

The computation methods for A2 2) and A2 3) are similar to the methods for A1 1) and A1 2).

3.1.3. The general smooth case

It may happen that the X_n coordinate and the distance function to O are not M-functions. We need then to try several directions and several origins for the distance

function in order to obtain M-functions. Using the bounds on the degree given by the efficient quantifier elimination method for the algebraically closed case (see [CG], [FGM], [H]), we can find immediately a set of single exponential cardinality D (resp O) where to chose the directions (resp.

the origins), and be certain that once every element of D (resp. O) has

been tried, we have obtained an M-function, since the set of bad directions (such that the corresponding linear combinations of coordinates is not an M-function) (resp. of bad origins) is contained in a Zariski-closd set of single exponential degree.

If we are lucky, we shall end the computation after a few choices but if we are not we shall have to try all the directions in D (resp. origins in O) before finding M-functions.

So the algorithm A 3) (decision method for the general smooth case) runs as follows

A 3 1) pick a point l in D, while I_l is not 0-dimensional

(where I_l is the ideal defined by

$$f = \frac{\partial f}{\partial X'_1} = \ldots = \frac{\partial f}{\partial X'_{n-1}} = 0.$$

and $(X'_1, \ldots, X'_n)$ are coordinates of the hyperplane perpendicular to l) chose a new element of D,

A 3 2) when l with I_l 0 dimensionnal is obtained, decide whether I_l has real points. If there are , decide that $Z(f)$ is non empty else go on with

A 3 3) pick a point o in D, while I'_o is not 0-dimensional

(where I'_o is the ideal defined by

$$f = \frac{\partial f}{\partial X_1}(X_n - o_n) - \frac{\partial f}{\partial X_n}(X_1 - o_1) = \ldots = \frac{\partial f}{\partial X_{n-1}}(X_n - o_n) - \frac{\partial f}{\partial X_n}(X_{n-1} - o_{n-1}) = 0.)$$

chose a new element of O.

A 3 4) when l with I'_o 0 dimensionnal is obtained, decide whether I'_o has real points. If there are , decide that $Z(f)$ is non empty.

3. 2. The case of a general hypersurface

The idea is quite simple: in order to get $Z(f)$ smooth, we modify slightly the equation by considering a sufficiently small element ϵ and replace the original decision problem for f by the decision problem for $f^2 = \epsilon$. If ϵ is small enough, we have $Z(f^2 - \epsilon)$ smooth, and empty if and only if the set $Z(f)$ is empty.

It is necessary to make this precise to develop some rather sophisticated algorithmic and methodological equipment, in particular the study of semi-algebraic sets over a general real closed field ([B C R]).

Since we are working in a symbolic context, the small deformations cannot be performed numerically, and it is necessary to use infinitesimal deformations, that is, to work in extensions of the ground field which are fields of Puiseux series. In fact, since all the computations are based on linear algebra subroutines and are made in the ring of coefficients, no implementation of Puiseux series is needed, and all the computations take place in the polynomial ring with coeffcient in ϵ.

We have to perform the computations of A 2) but in a context where the ring of coefficient is extended and is no more archimedean. The methods needed to decide whether or not the set of "real" critical zeroes of I (now in a field of Puiseux series) is empty can no more be semi-numerical or use isolation intervals. It is then needed to use tools based on Thom's lemma ([CR], [RS]) and [BKR]methods, that are known to be much slower than isolation interval techniques.

3. 3 The general case of a semi-algebraic-set

It is based on a reduction process to case 3.2.

Let $f_1 > 0, \ldots, f_s > 0$ be for example the semi-algebraic set we consider. Following a trick of [GV] we consider the equation $g = (f_1 + \gamma) \times \ldots \times (f_s - \gamma) - \gamma^s$ and we have to decide whether or not the hypersurface $Z(g)$ has critical points of the X_n functions verifying $f_1 > 0, \ldots, f_s > 0$. This is done by applying a variant of [BKR]'s algorithm. Computations are made with coefficients polynomial in γ.

The elevation of degrees and the additionnal variable γ make this reduction quite inefficient from a practical point of view.

Remark

4. Computational strategies

We propose the following algorithm B) for the decision problem for an hypersurface

B 1) decide if $Z(f)$ is regular by deciding whether the ideal I" generated by

$$f = \frac{\partial f}{\partial X_1} = \ldots = \frac{\partial f}{\partial X_n} = 0.$$

has an empty zero set. This is done by checking if the Groebner basis of I" is equal to 1. If $Z(f)$ is singular, replace f by $f^2 - \epsilon$ (and replace the ring K of coeffcients (in practice, the integers) by the ring

$K[\epsilon]$).

B 2) perform A 3).

This strategy can be improved. A more efficient method would provably be the following: start the computations as if the geometric situation was good and go to more spophisticated variants of the algorithm only when the situation is bad, which should be detected by a computation failure. A precise and complete computational strategy based on these ideas has to be more fully developed. It willl be part of the POSSO project to progress towards this direction.

It is already clear that for an hypersurface with $d = 20$ (resp. $6, 4, 3$), $n = 2$ (resp. $3, 4, 5$), in the good cases we have considered 3.1.1. and 3.1.2., or even for the general smooth case, and in the present state of the art, the computation time needed for obtaining the Groebner basis of I and the number of real points of its zero set is perfectly reasonable. Indeed the vector space A is of dimension at most $d(d-1)^{n-1}$ that is here no more than

200, while the degrees needed in the CAD computations increase extremally rapidly. Since the algorithms for determining the number of real zeroes of a 0-dimensional ideal are known to be polynomial in the output of the quotient computation (dimension of the quotient and multiplication tables) ([PRS]), we can reasonnably hope that in every case where the structure of the quotient A will be computable (for example through a Groebner basis), the computation of the number of real points will be practically feasible.

We thank Hoon Hong and Carlo Traverso for their useful comments on the subject.

Bibliography

[BKR] Ben-Or M., Kozen D. , Reif J. : The complexity of elementary algebra and geometry. J. of Computation and Systems Sciences 32 251-264 (1986).

[BCR] Bochnak J., Coste M., Roy M.-F.: Géométrie algébrique réelle. Springer-Verlag (1987).

[Bro] Brownawell D.: Bounds for the degrees in the

Nullstellensatz. Ann. of Math. (2) 126 37 577-591 (1987).

[Bu] Buchbrger B.: Groebner basis; an algorithmic

method in polynomial ideal theory. Multidiensionnal systems theory (N. K. Bose ed, chapter 6, D. Reidel (1985) .

[Ca1] Canny J.: Some algebraic and geometric computations in PSPACE. ACM Symposium on the theory of computation 460-467 (1988).

[Car] Cardinal J.-P. Dualité et algorithmes itératifs pour la résolution des systèmes polynomiaux. Thèse, Université de Rennes (1993).
[CG] Chistov A. L., Grigor'ev D.: Complexity of quantifier elimination in the theory of algebraically closed fields. Lect. Notes in Comp. Sci. 199 63-69, Springer-Verlag, Berlin (1984).
[Co] Collins G. : Quantifier elimination for real closed fields by cylindric algebraic decomposition. Second GI Conference on Automata Theory and Formal Languages. Lect. Notes in Comp. Sci. 33 134-183, Springer-Verlag, Berlin (1975).
[C] Coste M.: Effective semi-algebraic geometry. Lect. Notes in Comp. Sci. 391 1-27, Springer-Verlag, Berlin (1989).
[CR] Coste M. , Roy M.-F. : Thom's lemma, the coding of real algebraic numbers and the topology of semi-algebraic sets. J. of Symbolic Computation 5 121-129 (1988).
[DH] Davenport J., Heintz J.: Real quantifier elimination is doubly exponential. J. of Symbolic Computation 5 29-35 (1988).
[FGLM]Faugères J.-C., Gianni P., Lazard D., Mora T.: Efficient computations of zero dimensionnal Groebner basis by change of orderings. To appear in Journal of Symbolic Computation.
[FGM] Fitchas N., Galligo A., Morgenstern J.: Precise sequential and parallel complexity bounds for quantifier elimination over algebraically closed fields. J. Pure Appl. Algebra 67 1-14 (1990).
[GV] Grigor'ev D., Vorobjov N.: Solving systems of polynomial inequalities in subexponential time. J. Symbolic Computation 5 37-64 (1988).
[G] Grigor'ev D.: Complexity of deciding Tarski algebra. J. Symbolic Computation 5 (1988) 65-108.
[H] Heintz J.: Definability and fast quantifier elimination over algebraically closed fields. Theoret. Comp. Sci. 24 239-277 (1983).
[HRR] Heintz J., Recio T., Roy M.-F. : Algorithms in real algebraic geometry and applications to computational geometry. Dimacs series in Discrete Mathematics and Theoretical Computer Science, vol 6 137-163 (1991).
[HRS1] Heintz J., Roy M.-F., Solernó P. : On the complexity of semialgebraic sets. Proc. IFIP 89 San Francisco. North-Holland 293-298 (1989).
[HRS2] Heintz J., Roy M.-F., Solernó P.: Sur la complexité du principe de Tarski-Seidenberg. Bull. Soc. Math. France 118 101-126 (1990).
[Ho] Hong H. : Comparison of several decision algorithms for the existential theory of the reals. Technical Report, RISC Linz (1991).
[PRS] Pedersen P., Roy M.-F., Szpirglas A.: Counting zeroes in the multivariate case . To appear in MEGA 92.
[Re1] Renegar J.: On the computational complexity and geometry of the first order theory of the reals. Journal of symbolic computation (1992).
[Re2]Renegar J.: Recent progress on the complexity of the decision problem for the reals. Dimacs series in Discrete Mathematics and Theoretical Computer Science, vol 6 287-308 (1991).
[RS] Roy M.-F., Szpirglas A.: Complexity of computations with real algebraic numbers. J. of Symbolic Computation 10 39-51 (1990).

[St] Sturm C.: Mémoire sur la résolution des équations numériques. Ins. France Sc. Math. Phys. 6 (1835).
[We] Weispfenning V.: The complexity of linear problems in fields. J. Symbolic Computation 5 3-27 (1988).

Authors Joos Heintz
Mathematics Departement
Universitad de Cantabria
Santander
Spain
Marie-Françoise Roy
IRMAR (URA CNRS 305), Université de Rennes,
Campus de Beaulieu 35042 Rennes cedex FRANCE
Pablo Solernò
Instituto Argentino de Matemática
CONICET
Viamonte 1636
(1055) Buenos Aires
ARGENTINA
Corresponding author
Marie-Françoise Roy
IRMAR (URA CNRS 305), Université de Rennes,
Campus de Beaulieu 35042 Rennes cedex FRANCE
Phone (33) 99 28 60 20, fax (33) 99 28 67 90
Email costeroy@univ-rennes1.fr