25 Years of Polynomial System Solving, . . . and Now ?

Daniel Lazard

CALFOR (LIP6) and SALSA (INRIA) Team - Paris

Abstract

I am working since more than 25 years on polynomial system solving. At first glance this seems to be a rather narrow subject for such a long effort. But it appears that the subject becomes wider with the scientific progress, and there were more than 50 submitted papers to this conference.
I'll try to explain this apparent paradox, by describing what seems to me the main progresses in the field, how these progresses set new difficult questions, and to extract to these trends the main challenges for the future research in this domain.

Solving in the seventeens and in the eighteens

At that time, the polynomial systems which were considered were systems of equations which were supposed to have finitely many complex solutions (inequations and inequalities were not yet really taken into account, except in the theory of quantifier elimination, but the strong relationship between this theory and polynomial system solving were not yet really understood). In the seventeens there were already efficients numerical algorithms for finding solutions of such system, but there were no way to know if all the solutions have been found. For example, in the beginning of the seventeen, I have found a solution of a system of 81 quadratic equations in 54 unknowns, by minimizing the sum of their squares.
On the other hand, there were known theoretical algorithms for solving algebraically a polynomial system (elimination theory), but they have a complexity which were too high to be practically implemented, except in the two- or threevariate cases, were resultant and gcd computations allow to reduce rather easily to a univariate equation.
In the meeting EUROCAM'79 (an ancestor of ISSAC held in Marseilles), I presented the first solving algorithm (based on multivariate resultants) which has a complexity which is simply exponential in the number of the variables and Bruno Buchberger presented the Gröbner bases and the two criteria to eliminate unnecessary critical pairs.
During the eighteens, most of the research work was devoted to the theoretical improvement of the algorithms and to their complexity. Also, several alternative methods for solving were proposed, the main one being Wu Wentsün approach through characteristic sets. It appeared that, any solving algorithm has an exponential complexity, that the worst case complexity is doubly exponential and that a single exponential complexity may be reached in most (sufficiently regular) cases. However, the practical implementations were unable to reach this single exponential complexity, mainly because of the swell of the intermediate expression.
This had the consequence that, from a practical point of view, there were only experimental implementations, which were rarely able to solve problems not accessible by hand. When such a problem were solved, the algebraic methods provided only the number of solutions, proving that the set of solutions which were found by other methods were complete. This especially the case for the systems of equation known as cyclic(5) and cyclic(6) which have been proved to have respectively 50 and 156 complex solutions easily found by hand computation.

Solving in the nineteens

As many important papers dealing with complexity and theoretical algorithms appeared in 1991, we consider here that the nineteens start around this time.
The main research effort during the nineteens was devoted to obtain efficient implementations, especially for Gröbner bases, but also for multivariate resultants, triangular systems, numerical solving through homotopy and cylindrical algebraic decomposition.

It appeared that Gröbner bases were huge data (the Gröbner basis for cyclic(9) needs more tha one gigabyte to be stored) from which the dimension of the set of solutions and, if it is 0, their number are easy to deduce. But it general computing Gröbner bases is not solving but only a step through solving.
This set an important question: *What does mean solving?* In fact this question arises already for solving univariate equation, for which there are several different answers. A first one is *solving by radicals*, which has been shown around 1830 to be generally impossible. A second meaning is *numerical solving*, which is always possible, but some information is lost; for example it is impossible to decide, from numerical approximations if to solutions are equal or only close together. A third meaning of *solving* is simply to consider it as a synonym of *factor*: factoring simplify numerical solving by reducing the degree(s) of the polynomial(s) to be solved, the roots of these polynomials are all distinct and the multiplicities of the roots of the input polynomial are given by the multiplicity of the factor.
In the multivariate case, when the number of complex solutions is finite, it appears that similar questions arise and are well solved by expressing the solutions as rational functions of the roots of a univariate polynomial (Rational Univariate Representation or RUR, see Rouillier paper in these proceedings). From this representation, numerical approximations of the solutions may be computed, but it is not as easy as it may seem because of the numerical instability which may cause that a very high precision of the roots of the univariate polynomial may be needed in order to have an acceptable precision on the solutions.
Nevertheless, with the package Gb of Jean-Charles Faugère for computing Gröbner bases and the package RS of Fabrice Rouillier for deducing a RUR and computing the real solutions, it is now a routine task of solving systems of several hundreds of complex solutions.
During the same time, several other ways for solving were developped and implemented, especially those based on multivariate resultants, on triangular sets, and on homotopy. One may also mention the geometrical resolution which may be view as another approach for computing a RUR, but, for the moment, they are less efficient (or less robust) on practical problems than the approach through Gröbner bases and RUR.
During these ten years, some progresses were down on applications and on systems of positive dimensions, but these set many new important questions, and therefore we consider them in the next section.

And now?

As said before, we dispose now of rather efficient software for solving polynomial systems with a finite number of complex solutions, usually called *zero-dimensional systems*. We dispose also of software which allow to extract efficiently useful information on positive dimensional systems.
A first important question which remains partially open is **To what purpose these software are useful?** In fact, polynomial systems do not appear directly in Nature. They appear in models for some problems which may be modelled in various ways. The simplest example of this are the trigonometrical equations: there are not polynomial, but an equation which is polynomial in $\cos(x)$ and $\sin(x)$ becomes polynomial if sine and cosine are replaced by new variables c and s and if the equation $c^2 + s^2 - 1$ is added.
Thus, the previous question may be reformulated as **In the various scientific domain, which are the problems which may be modelled by polynomial systems and which are those which may be reduced to zero-dimensional systems?** When trying to solve this, we encounter a subsidiary important question: **For these problems, what is the best way to express them as polynomial systems and what is the most efficient solving algorithm among algebraic solving, numerical solving and a mixture of both?**
These questions are very wide, as they imply knowledge in algebraic solving as well as in numerical methods and in the various implied scientific domains. It needs also new mathematical developpements, even if this is not a priori evident.
For example, let us consider the problem of polynomial optimization which consists in minimizing a polynomial function whose variables are subject to polynomial constraints (polynomial equations and possibly polynomial inequalities). As it is stated, this problem may be easily written as a quantified formula, and solving it is equivalent to eliminate the quantifiers. Unfortunately, the general algorithms for quantifier elimination are not efficient enough for solving non trivial examples. But it is easy to remark that the minimum (and all local extrema) is obttained when the gradient of the function to minimize is orthogonal to the tangent space of the variety of the constraints. If this variety is smooth and without border, this orthogonality leads generically to a zero-dimensional system much easier to solve. If this variety is singular, one may show that one may construct a finite number of zero-dimentional systems whose solutions contain the

local extrema. The construction of these systems may be costly but the whole computation is much more efficient than a general quantifier elimination.
The problem of polynomial optimization is a general problem which arise in many scientific fields, and we already know several examples where algebraic methods give the global minimum when the numerical optimization gives only local minima in the same order of time.
A special instance of the polynomial optimization, which is important in geometric modelling is the following: *Find the distance from a point to a parameterized variet y and the corresponding values of the parameters.* The most interesting instance is when the point is the approximation of a point of the variety. This problem may arise in many areas, when $k+1$ measurable quantities are rational functions of k hidden state variables of a physical system. In this case, retrieving the hidden variables from the measures leads to an overdetermined system depending on approximate coefficients which is not solvable directly.
It is noteworthy that this special but yet quiet general instance of the polynomial optimization reduces easily (algorithmically, but a mathematical proof is needed) to a single zero-dimensional system, and this provides a robust and efficient way to solve this class of problems.
These examples shows that it is necessary to extend the notion of a polynomial system to *any quantified formula (of the first order logic) involving equalities and inequalities between polynomials.* But most of these generalized systems have infinitely many solutions and this set again a question that I think as a fundamental one since more than 10 years: **What does it mean solving?** Mathematically, the answer could be *extract as many information as possible on the topology of the set of solutions.* But practically, people which are faced to a polynomial system never need a full description of the whole set of solutions; usually they want solutions satisfying further properties as in polynomial optimization problem, or they want qualitative information such as the number of connected components of the set of the solutions or the existence (or not) of singularities.
It follows that the field of *polynomial system solving* is faced to a number of challenging problems, despite the dramatic progresses of these last years (and maybe because of these progresses). Here is a list of the problems which seems the most important to me.

- In various scientific areas, identify the problems which may be modelled by polynomial system, select the best way of modelling them as systems of polynomial equations and find a specification of the answer which is together wanted and computable. This task has to be done in collaboration with specialists of these scientific domains, but it needs efforts by the specialists of polynomial system solving to adapt the input-output specifications to the state of the art in polynomial system solving. I know work of this kind in robotics, signal processing, control theory, applied geometry, cryptography, . . ., but there are certainly many other domains where this kind of work would be useful.

- From all these applied problems, select the mathematical questions which are computable and of general interest. For these mathematical questions, find algorithms for reducing them to the basic algorithms. Here is a list of such questions which is far to be complete.

  – Polynomial optimization (see above and also M. Safey el Din in these proceedings).
  – Systems depending on parameters (see Lazard-Rouillier in these proceedings)
  – Determination of the connected components of a semi algebraic variety (see M. Safey el Din in these proceedings).
  – Computation of the topology of a semi-algebraic variety. This amounts to compute a cellular decomposition, i.e a decomposition in cells analytically isomorphic to $\mathbb{R}^k$ together with the relation of adjacency between the cells. Cylindrical algebraic decomposition allows to compute this, but it has a doubly exponential complexty, and I guess that this problem may be solved practically in single exponential complexity.
  – . . .

- Improve the basic algorithms (Gröbner bases, prime decomposition of the radical of an ideal, cylindrical decomposition, . . .) for their general specifications, as well as for subclasses which appear in above problems. For example, in most cases where a cylyndrical algebraic decomposition is useful, the full decomposotion is not needed, but only the cells of maximal dimension.

As one can seen, with the questions which have not yet be discovered, there is work for more than 25 years.

References :