Proposition de recherche doctorale

Sparse Grobner Bases and Applications

Mots clés :

● Directeur de thèse : Jean-Charles Faugère
● Co-encadrant(s) :
● Unité de recherche : Laboratoire d'informatique de Paris 6
● Ecole doctorale : École Doctorale Informatique, Télécommunications, Électronique de Paris
● Domaine scientifique principal: Divers

Résumé du projet de recherche (Langue 1)
Groebner bases were introduced by Bruno Buchberger in 1965. Ten years ago, we have opened a new area for efficient Grabner basis computations by proposing algorithms F.+/Fs relying on linear algebra. Nevertheless, no general algorithm, however powerful, can take advantage of the specific nature of its input. However, problems coming from applications are not random but have an additional structure. For instance, polynomial systems can be invariant by the action of some finite groups, multi-linear (each equation is linear w.r.t. to one block of variables) or more generally multimhomogeneous. For each particular structure, we were able to identify large classes of problems whose theoretical and practical complexity could be improved and to propose in each situation dedicated algorithms. These results turned out to be a key ingredient in recent breakthroughs in cryptography (for instance the discrete logarithm problem over finite fields). At first glance, multi-homogeneity, weighted homogeneity (quasi-homogeneity), overdeterminedness, sparseness and symmetries seem to be unrelated structures. Indeed, until recently we have obtained specific results for one type of structure: hence we obtain dedicated algorithm and sharp complexity results by reducing the problem of solving bilinear systems to determinantal ideals; we also propose adhoc techniques to handle symmetries. In order to have a uniform approach of these problems, we'll introduce sparse Grabner bases, an analog of classical Grabner bases for semi group algebras, and 11-c propose sparse 1 ariants of the classical F4 / F_5 and FGLM algorithms to compute them. The PhD project will focus on the following two directions. 2 Sparse Groebner bases We have proposed variants of F_5 and FGLM to solve symbolically systems whose support lie in the same support (unmixed systems); we have also obtained sharp complexity results when the monomials in the support are integer points in a lattice polytope. We want to investigate these two new research directions. First, a possible extension of this work would be the generalization to mixed systems (where the algorithms are developed in each of the blocks of variables, and the complexity would depend on the Newton polytope of each of the monomials in each of the blocks). The current results seem to indicate that such a generalization may be possible. Another restriction of the result is that the complexity analysis (bounding the maximal degree occurring in the Gra\-ner basis computation) is for the moment restricted to the polytopal case. However, a classical question is to bound the number of solutions in the algebraic closure of a polynomial system where all polynomials have generic coefficients. When the exponent vectors of the monomials are the points with integer coordinates in a lattice polytope, Kushnirenko's theorem shows that the number of solutions is bounded by the normalized volume of the polytope. A natural question that arises is then to extend the work we have done in the polytopal case to the case where only a small subset of monomials appear in the equations (jennomial systems). A noticeable result would be to compute a sparse Grabner basis of such a system in polynomial time when the number of monomials in the support is small. From an implementation point of view, we feel that implementing efficiently this new generation of algorithms in a general framework could be a new research area. Probably algorithms from com ex geometry or the combinatorial world would be necessary components of an efficient implementation. Also, merging our existing approach (the so called sparse-Matrix F5) with a Buchberger's type approach could lead to a termination criterion of the algorithm in the non-regular cases and for positive dimensional systems. 3 Algorithms for symmetric tensor decomposition - the real case A symmetric tensor is a higher order generalization of a symmetric matrix. The decomposition of a symmetric tensor consists into writing it using a minimal number, called symmetric rank, of linear combinations of symmetric outer products of vectors. This could be seen as a generalization of cigenrnluc decomposition of symmetric matrices to higher order symmetric tensors. When the rank is small there are algorithms for computing it efficiently. However, neither their theoretical nor their practical performance is well understood. Every symmetric tensor is equivalent to a homogeneous polynomial, where the dimension of the tensor corresponds to the degree and its order corresponds to the number of variables. Therefore, the problem of symmetric tensor decomposition is equivalent to write a homogeneous polynomial as a sum of power of linear forms - A first goal is to consider algorithms with complexity $O(d^2 \log^2(d))$ where c is a constant. The aforementioned algorithms decompose the tensor over the complex numbers $\mathbb{C}$. A relevant question is to generalize the study to decompose symmetric tensors over the real numbers. We will also extend our study to decomposition algorithms over the real numbers. Such algorithms will strongly depend on real root isolation algorithms of univariate polynomial. Since real root isolation is of crucial importance for the team in many applications, if time permits, we will focus on these algorithms. We would like to mention that when the rank is big the problem of decomposition could be reduced to a highly structured polynomial system. We plan to exploit this structure and propose a new algorithm for the general problem of decomposing a symmetric tensor. This study of structured and sparse
Another restriction of the result, is that the complexity analysis (bounding the maximal degree occurring in the Grobner basis computation) is for the moment restricted to the polytopal case. However, a classical question is to bound the number of solutions in the algebraic closure of a polynomial system where all polynomials have generic coefficients. When the exponent vectors of the monomials are the points with integer coordinates in a lattice polytope, Kushnirenko’s theorem shows that the number of solutions is bounded by the normalized volume of the polytope. A natural question that arises is then to extend the work we have done in the polytopal case to the case where only a small subset of monomials appear in the equations (jewnomial systems). A noticeable result would be to compute a sparse Grobner basis of such a system in polynomial time when the number of monomials in the support is close to the number of variables. From an implementation point of view, we feel that implementing efficiently this new generation of algorithms in a general framework could be a new research area. Probably algorithms from combinatorial or complex geometry or the combinatorial world would be necessary components of an efficient implementation. Also, merging our existing approach (the so-called sparse-Matrix F5) with Buchberger’s type approach could lead to a termination criterion of the algorithm in the non-regular cases and for positive dimensional systems.