Gröbner Bases and Structured Systems: an overview

Jean-Charles Faugère

INRIA, Équipe POLSYS, Centre Paris – Rocquencourt,
F-75005, Paris, France.
Sorbonne Universités, UPMC Univ Paris 06, Équipe POLSYS,
LIP6, F-75005, Paris, France.
CNRS, UMR 7606, LIP6, F-75005, Paris, France.

Joint work with Jules Svartz and Pierre-Jean Spaenlehauer.

June 12, 2015

Structured systems.

A major challenge in polynomial system solving is that, in most cases, the number of solutions of a polynomial system is *exponential*. Moreover, in finite fields, solving polynomial systems is a NP-hard problem. However problems coming from applications usually have additional structures. Consequently, a fundamental issue is to design a new generation of algorithms exploiting the special structures that appear ubiquitously in the applications.

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: we obtain dedicated algorithm and sharp complexity results too handle a particular structure. For instance, we handle bilinear systems by reducing the problem to determinantal ideals; we also propose ad-hoc techniques to handle symmetries. We show that Gröbner bases for weighted homogeneous systems can be computed by adapting existing algorithms.

All these results have been obtained *separately* by studying each structure one by one. Recently we found a new unified way to analyze these problems based on monomial sparsity. To this end, we introduce a new notion of sparse Gröbner bases, an analog of classical Gröbner bases for semigroup algebras. We propose sparse variants of the F_4/F_5 and FGLM algorithms to compute them and we obtain new and sharp estimates on the complexity of solving them (for zero-dimensional systems where all polynomials share the same Newton polytope). As a by product, we can generalize to the multihomogeneous case the already useful bounds obtained in the bilinear case. We can now handle in a uniform way several type of structured systems (at least when the type of structure is the same for every polynomial). From a practical point of view, all these results lead to a striking improvement in the execution time.

More recently, we investigate the non convex case when only a small subset of monomials appear in the equations: the emphfewnomial case. We can relate the complexity of solving the corresponding algebraic system with some combinatorial property of a graph associated with the support of the polynomials. We show that, in some cases, the systems can be solved in polynomial time.