Efficient algorithms for computing structured polynomial systems and applications.

November 9, 2015

- **Thème :** Calcul formel et Systèmes Polynomiaux
- **Équipe d'accueil :**
  - Équipe POLSYS (Polynomial Systems)
  - Centre de Recherche INRIA Paris
  - Laboratoire d'Informatique de Paris 6, Univ. Pierre et Marie Curie
- **Encadrants :**
  - Jean-Charles Faugère (`Jean-Charles.Faugere@inria.fr`)

Recently [1], we have proposed variants of F_5 and $FGLM$ to solve efficiently Sparse Polynomial systems whose support lie in the same support (this case is known as the unmixed case); we have also obtained sharp complexity results when the monomials in the support are integer points in a lattice polytope. We want to investigate two new research directions. A natural possible extension of this work would be the generalization to mixed systems (where the algorithms and the complexity would depend on the Newton polytope of *each* of the polynomials of the system). Some preliminary results seem to indicate that such a generalization may be possible.

Another restriction of the result, is that the current complexity analysis (that is bounding the maximal degree occurring in the Gröbner basis computation) is 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 this work from the polytopal case to the case where only a small subset of monomials appear in the equations (*fewnomial systems*). A noticeable result would be to compute a sparse Gröbner 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, implementing efficiently this new generation of algorithms in a general framework is also a new research area. For instance, several algorithms from convex geometry or the combinatorial world would be necessary components of an efficient implementation. Also, merging the existing approach relying on the sparse-Matrix F5 with a Buchberger's type approach [2] could lead to a termination criterion of the algorithm in the non-regular cases and for positive dimensional systems.

From the application point of view applications of structured systems are also numerous. For instance, in Cryptography, the algebraic systems arising in algebraic cryptanalysis are often structured. Hence efficient computation of the discrete logarithms in finite finite fields rely on solving efficiently bilinear systems. Also the security of McEliece, one of the oldest public key cryptosystem, can be reduced to the hardness of solving a set of multi-homogeneous equations of bi-degree $(1, d)$. Consequently, a possible application is to develop the fastest asymptotic key-recovery attack against code-based schemes (for some parameters). For structured systems over finite fields, investigating whether the information on the structure could be used to improve a hybrid approach is also as new research direction.

References

[1] Jean-Charles Faugère, Pierre-Jean Spaenlehauer, and Jules Svartz. Sparse Gröbner Bases: the Unmixed Case. In *ISSAC 2014*, Kobe, Japan, July 2014. 20 pages, Corollary 6.1 has been corrected.

[2] Bernd Sturmfels. *Gröbner bases and convex polytopes*. AMS, 1996.