EXACTA Task 1 Milestone Deliverables

Exact/Certified Computation with Algebraic Systems:
Design and Analysis of Algorithms

INRIA/LIP6 · KLMM · SKLOIS · LMIB
(EXACTA Project Partners)

2011
EXACTA (Exact/Certified Computation with Algebraic Systems) is a Franco-Chinese cooperation project supported by l’Agence Nationale de la Recherche (ANR grant no. ANR-09-BLAN-0371-01) and the National Natural Science Foundation of China (NSFC grant no. 60911130369).
This collection of EXACTA deliverables reproduces research papers written jointly by both French and Chinese project participants on Task 1, which have already been published or accepted for publication. In these papers, financial support of l’Agence Nationale de la Recherche (ANR grant no. ANR-09-BLAN-0371-01) and the National Natural Science Foundation of China (NSFC grant no. 60911130369) has been explicitly acknowledged. Task 1 of EXACTA focuses on the design and implementation of fundamental algorithms for exact and/or certified computation with algebraic systems. The deliverables in this collection represent the joint work and accomplishments of the project participants from France and China on Task 1 in the first 18 months, devoted mainly to the design and analysis of algorithms with applications. We give a brief review of the 9 papers and one poster in order of their appearance in the collection and on the basis of their original abstracts and introductions.

Faugère and Liang study artificial discontinuities (a kind of singularity at a parametric point in computing the Gröbner basis of a specialized parametric ideal with respect to a certain term order) in the single-parametric case by proposing a solid theoretical foundation. They provide a criterion to recognize artificial discontinuities by comparing the zero point numbers of specialized parametric ideals. Moreover, they prove that for a single-parametric polynomial ideal with some restrictions, its artificially discontinuous specializations can be locally repaired to continuous specializations by the Term Substitution with Variables (TSV) strategy.

Faugère and Liang also show when and how the phenomenon of artificial discontinuity may be detected and repaired by using the TSV strategy. For a zero-dimensional polynomial ideal, any monomial basis (containing 1) of the quotient ring can be found by using the TSV strategy. This observation allows the authors to use the TSV strategy to relax term order while keeping the framework of the Gröbner basis method so that existing efficient algorithms like F5 can be used to compute approximate Gröbner bases. The main algorithms designed by the authors can be used to repair artificial epsilon-discontinuities and their effectiveness for some non-trivial problems is demonstrated by experiments.

Faugère and Mou propose an algorithm for changing the ordering of Gröbner bases of any zero-dimensional ideal that takes advantage of the sparsity structure of appearing multiplication matrices. This sparsity structure arises even when the input polynomial system defining the ideal is dense. As a by-product, they obtain an implementation which is able to manipulate zero-dimensional ideals over a prime field of degree greater than 30000. It outperforms the Magma/Singular/FGb implementations of FGLM. The proposed algorithm is dynamic in the sense that it selects automatically which strategy to use depending on the input. Its key ingredients are the Wiedemann algorithm to handle one-dimensional linear recurrence (for the shape position case) and the Berlekamp-Massey-Sakata algorithm from Coding Theory to handle multi-dimensional linearly recurring sequences in the general case.

Guo, Safey El Din, and Zhi consider the problem of computing the global infimum of a bounded polynomial with real coefficients. They prove the equivalence between the existence of a certain Zariski-closed subset of invertible matrices with complex entries and the existence of sums of squares of some special polynomials with real coefficients; the result is used to formulate the original optimization problem as semidefinite programs, which can be solved efficiently. They also discuss how to exploit the sparsity to overcome the ill-conditionedness of semidefinite program problems when the infimum is not attained.

The paper by Li, Mou, Niu, and Wang deals with the problem of stability analysis of biological networks modeled as discrete and finite dynamical systems. The authors show how to use
algebraic methods based on quantifier elimination, real solution classification, and discriminant varieties to detect steady states and to analyze their stability and bifurcations for discrete dynamical systems. For finite dynamical systems, methods based on Gröbner bases and triangular sets are applied to detect steady states. The feasibility of their approach is demonstrated by the analysis of stability and bifurcations of several discrete biological models using implementations of algebraic methods.

The paper by Li, Mou, and Wang presents algorithms for decomposing any zero-dimensional polynomial set into simple sets over an arbitrary finite field. As a key ingredient of the algorithms, the authors generalize the squarefree decomposition approach for univariate polynomials over a finite field to that over the field product determined by a simple set. As a subprocedure of the generalized squarefree decomposition approach, a method is proposed to extract the $p$th root of any element in the field product. The authors also provide experiments to show the effectiveness of their algorithms.

Lin, Faugère, Perret, and Wang introduce a new framework to study the counting problem associated to the isomorphism of polynomials, one of the most fundamental problems in multivariate public key cryptography (MPKC). They present tools of finite geometry to investigate the counting problem and focus their study on enumerating or estimating the number of isomorphism equivalence classes of homogeneous quadratic polynomial systems. These problems are equivalent to finding the scale of the key space of a multivariate cryptosystem and the total number of different multivariate cryptographic schemes respectively, which might impact the security and the potential capability of MPKC. The authors also consider the applications of their framework in the analysis of a specific multivariate public key cryptosystem. Their results not only answer how many cryptographic schemes can be derived from monomials and how big the key space is for a fixed scheme, but also show that quite many HFE cryptosystems are equivalent to a Matsumoto-Imai scheme.

Safey El Din and Zhi propose an algorithm which decides whether a convex semi-algebraic set contains a rational point and, in the affirmative case, computes such a point. They bound the number of bit operations that the algorithm performs with respect to the number of polynomials, their degrees, and the maximum bit length of their input coefficients and give upper bounds on the bit length of the coordinates of the outputted rational point when such a point exists. They also obtain a procedure for deciding whether a polynomial with integer coefficients is a sum of squares of polynomials with rational coefficients and establish bounds on the number of bit operations for the sum-of-squares decomposition and on the bit length of the coefficients of polynomials in the decomposition.

Zhao, Wang, and Hong present a real convention (for square and cubic roots) which provides correct interpretations of the Lagrange formula for all cubic polynomial equations with real coefficients. Using this convention, they also present a real solution formula for the general cubic equation with real coefficients under equality and inequality constraints.

The poster by Albrecht, Faugère, Lin, and Perret presents results of investigation on the hardness of solving nonlinear equations modulo a prime with noise. The problem, called Polynomial With Errors (PWE), is a nonlinear and rather natural generalization of the Learning With Errors problem. The hardness of PWE is supported by the hardness of solving algebraic equations without errors. The authors prove that a PWE with a bounded number of samples (called bPWE) has a decision/search equivalence and average-case/worst-case reduction. As a by-product, they show that such results also hold for bPWE without noise.

Thanks to the support of ANR and NSFC and owing to the joint effort of the project participants, EXACTA has not only helped strengthen the cooperation between French and Chinese
partners and produced a remarkable number of research results, but also enabled the project members to initiate and participate in many scientific activities at the international level and inspired several new research directions, such as structured polynomial system solving, computation of roadmaps, and algebraic analysis of flight dynamics. Other papers than those reviewed above, published or accepted for publication, in the frame of the EXACTA project are listed below and several (joint) papers submitted for publication are not included in the lists. It is hoped that the research productivity of the EXACTA team will remain high in the next 18 months.

September 2011
Dongming Wang

Mono-partner publications (in which EXACTA is acknowledged)


Contents


