Talk Abstracts

Plenary Talks

Symbolic Computation and Complexity Theory

Erich Kaltofen
North Carolina State University, USA

The discipline of symbolic computation goes back to be beginnings of computers, as early on scientists carried out symbolic (exact) and algebraic manipulation of polynomials and quantified formulas on early computers. The theory of NP-completeness has exposed many of the investigated problems hard in the worst case. As it turned out in the 1980s, an exception is the problem of polynomial factoring, that unlike the problem of integer factoring is in random polynomial time even when representing the input polynomial by a straight-line program.

Today's highly sophisticated and finely tuned algorithms, e.g., for Groebner basis reduction and real algebraic geometry, can solve many of the mathematical problems arising in science and engineering. Symbolic and hybrid symbolic-numeric methods operate on the fine line between the doable and the hard, that also when the difference is a quadratic vs. a linear complexity but when the intermediate data is exceedingly large.

By way of examples ranging from sparse linear algebra over factorization to Reed-Solomon decoding, in my talk I will attempt to separate algorithmic problems that are doable from those that are provably hard. I will give my answer on the role of algorithms whose running time is exponential in input size.

Automatic Discovery of Transform Algorithms

Markus Püschel
ETH Zürich, Switzerland

Linear transforms that compute base changes are among the most important functions used in computational science and engineering. Examples include the discrete Fourier transform and the larger class of trigonometric transforms used in signal and image processing. Many of these transforms possess fast algorithms that allow their computation in $O(nlogn)$ instead of $O(n^2)$. These algorithms can be expressed as factorizations of the transform matrix into products of sparse matrices and are usually found by tedious manipulation of the matrix entries as done in hundreds of publications on this topic. In this talk I tell the story about our research on unraveling the reason for the existence of these algorithms. It starts with a computer program (developed jointly with Sebastian Egner) that discovers certain fast transforms algorithms. The underlying algorithm relies on a definition of symmetry as an invariance of the matrix under a group operation. Using constructive representation theory, this symmetry is then used to factorize the matrix. We applied the program successfully to many known transforms, thus revealing previously unknown algebraic properties. Based on this discovery we could then develop an algebraic theory of transform algorithms (joint work with José Moura) that derives and explains the entire space of algorithms for trigonometric transforms.

More information: SMART project

Factorization of Motions in 3D Space into Rotations/Translations

Josef Schicho
RICAM, Austrian Academy of Sciences, Austria

A motion polynomial is an element in the ring of left polynomials over the skew ring of dual quaternions subject to the condition that it is normed and its norm polynomial is real. Such polynomials define motions in 3D space. In the special case of linear motion polynomials, the motion is either a rotation around a fixed axis or a translation in a fixed direction. We introduce a method to factor a motion polynomial into linear factors; this corresponds to the realisation of the motion as the coupler curve in a linkage. In the second part of the talk, we explain some consequences for the (still open) classification problem of closed 6R linkages.

Sparse Polynomial Interpolation by Variable Shift in the Presence of Noise and Outliers in the Evaluations

Brice Boyer, Matthew Comer and Erich Kaltofen
North Carolina State University, USA

We compute approximate sparse polynomial models of the form $\tilde{f}(x) = \sum_{j=1}^{t} \tilde{c}_j (x - \tilde{s})^{e_j}$ to a function $f(x)$, of which an approximation of the evaluation $f(\zeta)$ at any complex argument value ζ can be obtained. We assume that several of the returned function evaluations $f(\zeta)$ are perturbed not just by approximation/noise errors but also by highly perturbed outliers. None of the $\tilde{c}_j$, $\tilde{s}$, e_j and the location of the outliers are known before-hand. We use a numerical version of an exact algorithm by [GKL03] together with a numerical version of the Reed-Solomon error correcting coding algorithm. We also compare with a simpler approach based on root finding of derivatives, while restricted to characteristic 0. In this preliminary report, we discuss how some of the problems of numerical instability and ill-conditioning in the arising optimization problems can be overcome. By way of experiments, we show that our techniques can recover approximate sparse shifted polynomial models, provided that there are few terms t, few outliers and that the sparse shift is relatively small.

References

[GKL03] M. Giesbrecht, E. Kaltofen, and W. Lee. Algorithms for computing sparsest shifts of polynomials in power, Chebychev, and Pochhammer bases. *J. Symbolic Comput.*, 36(3C4): 401C424, 2003. Special issue Internat. Symp. Symbolic Algebraic Comput. (ISSAC 2002). Guest editors: M. Giusti and L. M. Pardo. URL:http://www.math.ncsu.edu/~kaltofen/bibliography/03/GKL03.pdf.

Rational Elements of the Tensor Product of Solutions of Difference Operators

Yongjae Cha [1] and Mark van Hoeij [2]
[1]Risc-Linz, Johannes Kepler University, Austria
[2]Florida State University, USA

Let $D := \mathbb{C}(x)[\tau, \tau^{-1}]$ be the ring of difference operators with rational function coefficients, and let $M, N \in D$. Denote $V(M)$ and $V(N)$ as their solution spaces inside a universal extension. In this talk, we will present an algorithm that computes rational elements (invariant under the difference Galois group) of $V(M) \otimes V(N)$.

We define a space $\mathcal{M}(M, N)$ that is isomorphic to $V(M) \otimes V(N)$ and compute its rational elements. This is done by working directly with M and N, we avoid computing large operators such as the symmetric product of M and N

An Incremental Algorithm for Computing Cylindrical Algebraic Decompositions

Changbo Chen and Marc Moreno Maza
University of Western Ontario, Canada

In this paper, we propose an incremental algorithm for computing cylindrical algebraic decompositions. The algorithm consists of two parts: computing a complex cylindrical tree and refining this complex tree into a cylindrical tree in real space. The incrementality comes from the first part of the algorithm, where a complex cylindrical tree is constructed by refining a previous complex cylindrical tree with a polynomial constraint. We have implemented our algorithm in Maple. The experimentation shows that the proposed algorithm outperforms existing ones for many examples taken from the literature.

Finding the Symbolic Solution of a Geometric Optimization Problem through Numeric Computations

Liangyu Chen[1], Liyong Shen[2], Min Wu[1], Zhengfeng Yang[1] and Zhenbing Zeng[1]
[1]East China Normal University, China
[2]University of Chinese Academy of Sciences, China

In this paper we prove that if L is the maximal perimeter of triangles inscribed in an ellipse with a, b as semi-axes, then

$$(a^2-b^2)^2\cdot L^4-8(2a^2-b^2)(2b^2-a^2)(a^2+b^2)\cdot L^2-432a^4b^4=0$$

by accomplishing the following tasks through numeric computations: (1) compute the determinants of matrices of order from 25 to 34 whose entries are polynomials of degree up to 44, (2) construct a series of rectangles $R_1, R_2, \cdots, R_N$ so that if L, a, b satisfies the relation $f(L,a,b)=0$ then

$$C_1 := \{(b,L)|f(L,1,b)=0, 0\le b\le 1\}\subset R_1\cup R_2\cup\cdots\cup R_N,$$

and, (3) present a mechanical procedure to decide the validity of

$$R\cap C(F)=\emptyset,$$

where R is a closed rectangle region and $C(F)$ is an algebraic curve defined by $F(x,y)=0$.

keywords: Symbolic Solution, Optimization, Resultant, Lower and Upper Bounds, Algebraic Curves

References

[Chen2001] Dingxing Chen, Mathematical Thinking and Method (in Chinese), Press of Southeast University, Nanjing, China, 2001.
[CZ2012] Liangyu Chen, Zhenbing Zeng, Paralle computation of determinants of matrices with multivariate polynomial entries, Science in China, ser. F, (accepted), 2012.
[Xiao2008] Wenqiang Xiao, Mathematical Proofs (in Chinese), Dalian University of Technology Press, Dalian, China, 2008.
[ZZ2010] Zhenbing Zeng, Jingzhong Zhang, A mechanical proof to a geometric inequality of Zirakzadeh through rectangular partition of polyhedra, J. Sys. Sci & Math. Sci. 30(11), 1430-1458, 2010.

A New Formula for the Values of Dirichlet Beta Function at Odd Positive Integers Based on the WZ Method

Yijun Chen
South China Normal University, China

By using the related results in the WZ theory, a new (as far as I know) formula for the values of Dirichlet beta function $\beta(s)=\sum\limits_{n=1}^{+\infty}\frac{(-1)^{n-1}}{(2n-1)^s}$ (where $Re(s)>0$) at odd positive integers was given. The main result in this paper is the following theorem.

Theorem. Let $\zeta(s)=\sum\limits_{n=1}^{+\infty}\frac{1}{n^s}$ (where $Re(s)>1$), $\lambda(s)=\sum\limits_{n=1}^{+\infty}\frac{1}{(2n-1)^s}$ (where $Re(s)>1$), $\beta(s)=\sum\limits_{n=1}^{+\infty}\frac{(-1)^{n-1}}{(2n-1)^s}$ (where $Re(s)>0$), then we have $\beta(1)=\frac{\pi}{4}$, $\beta(3)=\frac{\pi^3}{32}$, $\beta(5)=\frac{5\pi^5}{1536}$, more generally, for all $l\in N$, we have

$$\begin{aligned}\beta(2l-1) &= \frac{(-1)^{l+1}\pi^{2l-1}}{2^{2l}}\left[\frac{1}{\Gamma(2l-1)}+2\sum_{j=1}^{l-1}\frac{(-1)^j2^{2j}\lambda(2j)}{\Gamma(2l-2j)\pi^{2j}}\right]\\ &= \frac{(-1)^{l+1}\pi^{2l-1}}{2^{2l}}\left[\frac{1}{\Gamma(2l-1)}+2\sum_{j=1}^{l-1}\frac{(-1)^j(2^{2j}-1)\zeta(2j)}{\Gamma(2l-2j)\pi^{2j}}\right]\\ &= \frac{(-1)^{l+1}\pi^{2l-1}}{2^{2l}}\left[\frac{1}{\Gamma(2l-1)}-\sum_{j=1}^{l-1}\frac{2^{2j}(2^{2j}-1)B_{2j}}{\Gamma(2l-2j)\Gamma(2j+1)}\right],\end{aligned}$$

and

$$E_{2l}=1-\frac{1}{2l+1}\sum_{j=1}^{l}\binom{2l+1}{2j}2^{2j}(2^{2j}-1)B_{2j},$$

where $l \in N_0$, $\sum_{k=1}^{0} a(k) = 0$ is a convention, B_n is Bernoulli number, and E_n is Euler number, which are given by the following formulas respectively

$$\frac{x}{e^x - 1} = \sum_{n=0}^{+\infty} \frac{B_n}{n!} x^n, \quad \frac{2}{e^x + e^{-x}} = \sum_{n=0}^{+\infty} \frac{E_n}{n!} x^n.$$

.

A Simple Quantifier-free Formula of Positive Semidefinite Cyclic Ternary Quartic Forms

Jingjun Han
Peking University, China

In this paper, we consider the quantifier-free formula of positive semidefinite cyclic ternary quartic forms, namely, the quantifier-free formula of

$$(\forall x, y, z \in \mathbb{R})[F(x, y, z) = \sum_{cyc} x^4 + k \sum_{cyc} x^2y^2 + l \sum_{cyc} x^2yz + m \sum_{cyc} x^3y + n \sum_{cyc} xy^3 \geq 0],$$

which is similar to, yet also more complex than the famous *quartic problem* [Co98]. We first apply the *Criterions on Equality of Symmetric Inequalities method* [Han11] to reduce the number of quantifiers of the problem to one. Thus, it suffices to obtain the quantifier-free formula of

$$(\forall t \in \mathbb{R})[g(t) := 3(2 + k - m - n)t^4 + 3(4 + m + n - l)t^2 + k + 1 + m + n + l - \sqrt{27(m - n)^2 + (4k + m + n - 8 - 2l)^2}\, t^3 \geq 0].$$

Then we apply function `RealTriangularize` in Maple15 and the theory of *complete discrimination systems* [Yang99] for solving the reduced case. The equivalent simple quantifier-free formula is difficult to obtain automatically by previous methods or quantifier elimination tools.
Keyword: Positive semidefinite, quantifier-free formula, ternary quartic.

References

[Co98] G. E. Collins: Quantifier elimination by cylindrical algebraic decomposition - 20 years of progress. In: Quantifier Elimination and Cylindrical Algebraic Decomposition (Caviness, B. and Johnson, J. eds.), 8–23. Springer-Verlag, New York (1998).

[Han11] Han J J. An Introduction to the Proving of Elementary Inequalities. Harbin: Harbin Institute of Technology Press, 234–266, 2011 (in Chinese).

[Yang99] L. Yang: Recent advances on determining the number of real roots of parametric polynomials. J. Symbolic Computation, 28: 225–242, 1999.

A Homotopy Method for Computing All Isolated Solvents of a Quadratic Matrix Equation $AX^2 + BX + C = 0$

Yongwen Hou and Bo Yu
Dalian University of Technology, China

Nonlinear matrix equations occur in a wide variety of applications, most of them arising in the control theory. Our interest is the quadratic matrix equation (QME)

$$P(X) = AX^2 + BX + C = 0, \quad A, B, C \in \mathbb{C}^{n \times n}, \tag{1}$$

one of the simplest nonlinear matrix equations, and a solution of (1) is called a *solvent* .

In this paper, we consider locating all isolated solvents and propose a homotopy method respecting to its matrix form:

$$H(X, t) = \gamma(1 - t)Q(X) + tP(X), \tag{2}$$

where $t \in [0, 1]$ and γ is a random complex number, and the start equation

$$Q(X) = MX^2 + CX + K = 0 \tag{3}$$

has exactly $\binom{2n}{n}$ known isolated solvents. We give a scheme to construct $Q(X)$ by solving a special quadratic inverse eigenvalue problem. We have proved that all isolated solvents of (1) can be found by tracing $\binom{2n}{n}$ continuous curves generated by those of (3) from the theories of homotopy method for solving polynomial systems. A path-tracking algorithm is also given, in which n-dimensional generalized sylvester equations need to be solved.

For two special classes of problems, we can obtain better results: (i) by considering the equation of the form

$$X^2 - Z = 0,$$

which has at most 2^n isolated solvents for general $n \times n$ complex matrix Z, we present a homotopy map of a easier form, to find all isolated square roots of Z if there exists. (ii) The overdamped problem of the form (1) is of great interest in applications, in which A and B are symmetric positive definite, C is symmetric positive semidefinite and $(z^TBz)^2 > 4(z^TAz)(z^TCz)$ for all $z \neq 0$, our homotopy method guarantees that a dominant solvent of an overdamped target matrix equation can be located by tracing the solution curve starting from that of an overdamped start matrix equation, and similarly for the minimal one.

The Vanishing Ideal of a Finite Set of Points with Multiplicity Structure

Na Lei, Xiaopeng Zheng and Yuxue Ren

Given a finite set of points with multiplicity structures, we present an algorithm to compute the reduced Gröbner basis of the vanishing ideal under the lexicographic ordering. Our method discloses the essential geometric connection between the relative position of the points with multiplicity structures and the quotient basis of the vanishing ideal, so we will explicitly know the set of leading terms of elements of I. We solve the problem by induction over variables and we split the problem into smaller problems and then use the Extended Euclidean Algorithm to get the answer of the original problem.

Keywords: vanishing ideal, points with multiplicity structures, reduced Gröbner basis.

Signature-based Method of Deciding Program Termination

Yaohui Li
Tianjin University of Technology and Education, China

In this paper, we decide the termination of linear program such as the following style

$$P : while(\boldsymbol{c}^T\boldsymbol{x} > 0)\{\boldsymbol{x} := A\boldsymbol{x}\} \tag{1}$$

where $\boldsymbol{x} \in R^n$ and A is a $M \times N$ matrix. This method uses the discriminant sequence and Gröbner bases to verify the termination of a class of linear program. In the method, we regard $\boldsymbol{c}^T\boldsymbol{x} > 0$ as constraint condition $G(x)$ and gets the characteristic polynomial cp of matrix $\boldsymbol{A}$ at first. Then the following is to construct a $2n \times 2n$ matrix $M =$

$$\begin{pmatrix} a_0 & a_1 & a_2 & \cdots & a_m & & \\ 0 & b_1 & b_2 & \cdots & b_m & & \\ & a_0 & a_1 & a_2 & \cdots & a_m & \\ & 0 & b_1 & b_2 & \cdots & b_m & \\ & & & \vdots & \vdots & \vdots & \\ & & a_0 & a_1 & a_2 & \cdots & a_m \\ & & 0 & b_1 & b_2 & \cdots & b_m \end{pmatrix}$$

by using the coefficients of cp and $rem(cp'h, cp)$, where cp' is the discriminant of cp. After that, list the principal minor of even order to generate discriminant sequence. On the base of this, we compute the number of real zeros by counting sign changes in the list. Thus, program termination of p is decided accurately. However, this method is inefficient because of determinants computation of the submatrix of M many times in it. Hence, we use Gröbner basis method to improve the construction of sign list of positive real eigenvalue which satisfies $\boldsymbol{c^T v} > 0$. The algorithm is implemented by using symbolic computation and the experiment results demonstrate its correctness.

Keywords: Linear loop program, termination, program verification, Gröbner basis, Sturm sequence

The Differential Invariant Algebra of an Integrable rmdKP Equations

Jianqin Mei and Haiyan Wang
Dalian University of Technology, China

Based on the theory of equivariant moving frame, the generating set of the differential invariant algebra and their syzygies for the symmetry groups of a r-th modified dispersionless Kadomtsev-Petviashvili equation have been constructed.

POLY : A New Polynomial Data Structure for Maple

Michael Monagan and Roman Pearce
Simon Fraser University, Canada

We demonstrate how a new data structure for sparse distributed polynomials in the Maple kernel significantly accelerates several key Maple library routines. The POLY data structure and its associated kernel operations (degree, coeff, subs, has, diff, eval, ...) are programmed for high scalability with very low overhead. This enables polynomial to have tens of millions of terms, increases parallel speedup in existing routines and dramatically improves the performance of high level Maple library routines.

Degree and Dimension Estimates for Invariant Ideals of P-solvable Recurrences

Marc Moreno Maza and Rong Xiao
University of Western Ontario, Canada

Motivated by the generation of polynomial loop invariants of computer programs, we study P-solvable recurrences. While these recurrences may contain non-linear terms, we show that the solutions of any such relation can be obtained by solving a system of linear recurrences.

We also study invariant ideals of P-solvable recurrences (or equivalently of while loops with no branches). We establish sharp degree and dimension estimates of those invariant ideals.

On the Complexity of Multivariate Interpolation with Multiplicities and of Simultaneous Polynomial Approximations

Vincent Neiger[1], Muhammad F. I. Chowdhury[2], Claude-Pierre Jeannerod[1],
Éric Schost[2] and Gilles Villard[1]
[1]ENS Lyon, France
[2]University of Western Ontario, Canada

The first step in Guruswami and Sudan's list-decoding algorithm amounts to bivariate interpolation with prescribed multiplicities and degree constraints. To perform this task, essentially two approaches have been proposed so far: the first one involves polynomial lattices and leads to a cost of $\mathcal{O}^{\sim}(\ell^{\omega} mn)$ field operations, with ℓ the list size, m the multiplicity, n the number of interpolation points, and ω the exponent of matrix multiplication [Cohn and Heninger (2011)]; the second approach solves a set of so-called key equations, and the best cost reported for it is in $\mathcal{O}(\ell m^4 n^2)$ [Zeh, Gentner, and Augot (2011)]. In this talk we shall focus on this second approach in the more general context of multivariate interpolation (which appears in particular when list-decoding folded Reed-Solomon codes [Guruswami and Rudra, 2006]).

Our contributions are as follows. First, we extend the key-equation approach to the multivariate case and show that it can benefit directly from existing fast structured linear solvers. Then, we show that multivariate interpolation with multiplicities can be reduced to a problem of simultaneous polynomial approximations, and that this second problem can also be solved by means of structured linear algebra; in the special bivariate case, this allows to perform Guruswami and Sudan's interpolation step in expected time $\mathcal{O}^{\sim}(\ell^{\omega-1} m^2 n)$, thus improving upon the cost of the polynomial lattice approach by a factor ℓ/m.

A Symbolic Computation Approach to the Projection Method

Nam Pham and Mark Giesbrecht
University of Waterloo, Canada

We present a hybrid symbolic-numeric approach for the projection method of [Bla92] for solving the parameterized differential-algebraic constraint equations associated with multibody mechanical systems. To apply this method in symbolic modelling and simulating multibody systems such as MapleSim, we

need an effective algorithm to compute the symbolic orthogonal complement matrix of the constraint Jacobian matrix, which contains several parameters and modelling parameters. The primary computational problem in this approach is computing a null-space basis of a matrix of multivariate rational functions, the Jacobian of the symbolic constraint matrix. A purely symbolic approach is untenable in terms of the sheer size of the output, whereas a purely numerical approach does not offer the flexibility of leaving some or all parameters unspecified. Instead we propose a hybrid approach, which does a symbolic preconditioning similar to the static pivoting approach of [LiDem98]. This allows us to generate straight-line C code for the null-space basis which is the main computation bottleneck. We do this in a numerically sensitive way by estimating pivot size through random evaluations. Our algorithm is verified by experimental results on inputs from typical multibody models.

References

[Bla92] Wojciech Blajer. A Projection Method Approach to Constrained Dynamic Analysis. *Journal of Applied Mechanics*, 59(3):643, 1992.

[LiDem98] Xiaoye S. Li and James W. Demmel. Making sparse gaussian elimination scalable by static pivoting. In *Proc. Supercomputing '98*, pages 1-17, 1998.

Real Root Isolation of Polynomial Equations Based on Hybrid Computation

Fei Shen[1], Wenyuan Wu[2] and Bican Xia[1]
[1]Peking University, China
[2]Chongqing Institute of Green and Intelligent Technology, CAS, China

A new algorithm for real root isolation of polynomial equations based on hybrid computation is presented in this paper. Firstly, the approximate (complex) zeros of the given polynomial equations are obtained via homotopy continuation method. Then, for each approximate zero, an initial box relying on the Kantorovich theorem is constructed, which contains the corresponding accurate zero. Finally, the Krawczyk interval iteration with interval arithmetic is applied to the initial boxes so as to check whether or not the corresponding approximate zeros are real and to obtain the real root isolation boxes. Meanwhile, an empirical construction of initial box is provided for higher performance. Our experiments on many benchmarks show that the new hybrid method is more efficient, compared with the traditional symbolic approaches.

keywords: Polynomial equations, real root isolation, hybrid computation.

Overview of the Mathemagix type system

Joris van der Hoeven
LIX, CNRS,École polytechnique, France

The goal of the Mathemagix project is to develop a new and free software for computer algebra and computer analysis, based on a strongly typed and compiled language. In this paper, we focus on the underlying type system of this language, which allows for heavy overloading, including parameterized overloading with parameters in so called "categories". The exposition is informal and aims at giving the reader an overview of the main concepts, ideas and differences with existing languages. In a forthcoming paper, we intend to describe the formal semantics of the type system in more details.

Keywords: Mathemagix, type system, overload, parametric polymorphism, language design, computer algebra

A Note on the Almkvist–Zeilberger Algorithm

Xiaoli Wu
Hangzhou Dianzi University, China

In this note, we describe a special structure of differential Gosper forms of rational functions, which allows us to design a new and simple algorithm for constructing differential Gosper forms without the resultant computation and integer-root finding. Moreover, we present an algorithm for computing a universal denominator of the first-order linear differential equation which the Almkvist–Zeilberger algorithm solves.

Symbolic Computation Techniques for Advanced Mathematical Modeling

Junlin Xu
Cybernet Systems China

Many scientific and engineering applications have to obey tight performance tolerances. Initial designs are often sub-optimal, and to arrive at better operating conditions, manual iterative processes using, for example, calculators or spreadsheets, are applied. This can take many hours, or even days. Often the solution obtained through such processes is still far from adequate. Over the last few decades, software tools boasting advanced nonlinear systems modeling and optimization algorithms have become significantly simpler to use, and no longer require specialized knowledge; this has accelerated the productivity of technical professionals across all domains. With Maple, the worlds most advanced symbolic computation engine, you can take the result of over twenty-five years of continual investment in research and design to better model and optimize scientific and engineering designs in less time.

This webinar will demonstrate, through several applications and numerous case studies, how Maple is helping companies worldwide, including NASA, JPL, Toyota, Argiva, and Marquardt Gmbh, save time and reduce cost by providing more efficient and smarter methods for mathematical analysis. Within Maple, you can take advantage of some of the most advanced optimization techniques in the world. In addition, Maple provides thousands of functions for integral transforms, ODE, PDE, and DAE solving, linear algebra, statistics, finance, signal processing, and much more. Find out how Maples computational engine can help you tackle even your most complex mathematical problems.

ImUp: A Maple Package for Uniformity-Improved Reparameterization of Plane Curves

[1]Jing Yang, [2]Dongming Wang and [3]Hoon Hong
[1]Beihang University, China
[2] CNRS – Universite Pierre et Marie Curie, France
[3]North Carolina State University, USA

We present a software package for computing piecewise rational reparameterizations of parametric plane curves which have improved uniformities of angular speed. The package ImUp is implemented in Maple on the basis of some recently developed algorithms of reparameterization using piecewise Möbius transformations. We discuss some implementation issues and illustrate the capability and performance of the public functions of ImUp with examples and experiments. It is shown that the quality of plots of plane curves may be effectively improved by means of reparameterization using ImUp.

Finding Conjugate Orthogonal Diagonal Latin Squares Using Finite Model Generators

[1]Hantao Zhang and [2]Jian Zhang
[1]The University of Iowa, U.S.A
[2]Institute of Software, Chinese Academy of Sciences, China

A *transversal* in a Latin square is a set of positions, one per row and one per column, among which the symbols occur precisely once each. A *diagonal Latin square* is a Latin square whose main and back diagonals are transversals. A Latin square which is orthogonal to its (i,j,k)-conjugate will be called an (i,j,k)-*conjugate orthogonal* Latin square, where $\{i,j,k\} = \{1,2,3\}$. An (i,j,k)-conjugate orthogonal diagonal Latin square, denoted by (i,j,k)-CODLS(v), is a diagonal Latin square which is orthogonal to its (i,j,k)-conjugate.

Let $H \subset Q$, $n = |H|$, $v = |Q|$, and $(Q,\otimes)$ be a Latin square with the symbols indexed by H missing from $(Q,\otimes)$ and the missing symbols consist of a missing subsquare right in the center of $(Q,\otimes)$. If we fill the missing square with an (i,j,k)-CODLS(n) over the subset H and the result is an (i,j,k)-CODLS(v) over Q, we say $(Q,\otimes)$ is an *incomplete* (i,j,k)-*conjugate orthogonal diagonal Latin square of order* v *with a missing subsquare of size* n, denoted by (i,j,k)-ICODLS(v,n). The subset H as well as the missing subsquare is called the *hole* of $(Q,\otimes)$. It is easy to see that the existence of an (i,j,k)-CODLS(v,n) requires that $v-n$ be even because the missing subsquare must be in the center. The following result is known.

Theorem 1 ([1]) *(a) A* $(3,2,1)$-*CODLS*(v) *exists for all integers* $v \geq 1$, *except* $v \in \{2,3,6\}$ *and except possibly* $v = 10$. *(b) For any integer* $1 \leq n \leq 6$, *a* $(3,2,1)$-*ICODLS*(v,n) *exists if and only if* $v \geq 3n+2$ *and* $v-n$ *is even, with the possible exception of* $(v,n) = (11,3)$. *(c) For any integer* $n \geq 1$, *a* $(3,2,1)$-*ICODLS*(v,n) *exists if* $v \geq 13n/4 + 93$ *and* $v-n$ *is even.*

Using the finite model generation tools SEM and Mace, we found a Latin square of size eleven with a missing hole of size three, which is orthogonal to its $(3,2,1)$-conjugate and both its main and back diagonals are distinct symbols. So we completely settled the existence problem for such Latin squares for all sizes. We can now state an improvement of Theorem 1(b) as follows:

Theorem 2 *For any positive integer* $1 \leq n \leq 6$, *a* $(3,2,1)$-*ICODLS*(v,n) *exists if and only if* $v \geq 3n+2$ *and* $v-n$ *is even.*

References

[1] F.E. Bennett, B. Du, and H. Zhang, *Existence of conjugate orthogonal diagonal Latin squares*, J. Combin. Designs, **5** (1997), 449-461.

On the Model AC=BD and Trigram Structures of the Soliton Theory

Hongqing Zhang and Shoufu Tian
alian University of Technology, China

By virtue of the model $AC = BD$, we systematically derive the Its-Matveev formula, super-Its-Matveev formula, and present the relationship between Trace formulas and Dubrovin-type equations, Lax equation and Sato equation, Lax equation and Zakharov-Shabat equation, Lax equation and inverse scattering (IST) scheme, Sato equation and Hirota's bilinear equation, respectively, which can be used to construct a unified model of solving soliton equation by using Tau function. In order to construct a unified and fundamental structure of soliton equations, in this paper, it is the first time to introduce our "Trigram" theory including "Trigram structures" and "Trigram identities", which is from Chinese traditional culture "Book of Changes". Employing the Trigram theory, we construct some exterior- and interior-decomposition Trigram identities, respectively, to reveal some integrable systems generated by Wronskian, Grammian, Pfaffian, discrete Wronskian, discrete Grammian, Schur functions and characteristic polynomials of Young diagram, Fock representation of Clifford algebra and Heisenberg algebra, etc, from which the Fock spaces of Clifford algebra is a Trigram space, and the one of Heisenberg algebra can be mapped into a Trigram space. Finally, we present the relationship between Tau function and Theta function, which is very meaningful to further investigate the relationship between Trigram structure and algebraic-geometry solution.

Constructing Generalized Bent Functions from Trace Forms over Galois Rings

Xiaoming Zhang, Zhuojun Liu, Baofeng Wu and Qinfang Jin
KLMM, Chinese Academy of Sciences, China

Quaternary constant-amplitude codes (codes over $\mathbb{Z}_4$) of length 2^m exist for every positive integer m, and every codeword of such a code corresponds to a function from the binary m-tuples to $\mathbb{Z}_4$ having the bent property, called a generalized bent function. In this paper, we extend previous constructions and propose a general approach which can lead to more generalized bent functions.

Keywords: generalized Boolean function, Galois ring, quadratic form, linearized polynomials.

Matrix Formula of Differential Resultant for First Order Generic Ordinary Differential Polynomials

Zhi-Yong Zhang, Chun-Ming Yuan and Xiao-Shan Gao
KLMM, Chinese Academy of Sciences, China

In this paper, a matrix representation for the differential resultant of two generic ordinary differential polynomials f_1 and f_2 in the differential indeterminate y with order one and arbitrary degree is given. That is, a non-singular matrix is constructed such that its determinant contains the differential resultant as a factor. Furthermore, the algebraic sparse resultant of $f_1, f_2, \delta f_1, \delta f_2$ treated as polynomials in y, y', y'' is shown to be a non-zero multiple of the differential resultant of f_1, f_2. Although very special, this seems to be the first matrix representation for a class of nonlinear generic differential polynomials.

Towards Guaranteed Accuracy Computations in Control

Masaaki Kanno
Niigata University, Japan

In order to achieve optimal control design, several computational steps including solution of a nonlinear problem have to be taken. While reliable numerical routines have been developed, one sometimes encounters a solution that is clearly not plausible, which is an indication of the need of verified computation. To this end, this talk considers polynomial spectral factorization, one of important parts in optimal control design, and discusses how it can be accomplished in a guaranteed accuracy manner. The problem can be reduced to a system of algebraic equations, and it is shown how one can guarantee that, among other solutions, the desired solution is obtained. Furthermore this approach is used to carry out optimal design with guarantee for a particular design problem, namely, the H2 regulation control problem.

Verified Error Bounds for Isolated Singular Solutions of Polynomial Systems

Nan Li and Lihong Zhi
Academy of Mathematics and Systems Science, China

We generalize the algorithm by Rump and Graillat [1], as well as our works [2] to compute verified error bounds such that a slightly perturbed polynomial system is guaranteed to have an isolated singular solution within the computed bounds. Our new symbolic-numeric method is based on deflation techniques using smoothing parameters and verification methods using interval arithmetic. A numerical experiment is also presented for illustration.

References

[1] S. Rump, S. Graillat. Verified error bounds for multiple roots of systems of nonlinear equations. Numerical Algorithms, 54(3): pp. 359-377, 2009.

[2] N. Li and L. Zhi. Verified error bounds for isolated singular solutions of polynomial systems: case of breadth one. 21 pages, acceped by TCS, 2012.

On High Precision Eigenvalue Estimation for Self-adjoint Elliptic Differential Operator and Its Application

Xuefeng Liu and Shin'ichi Oishi
Waseda University, Japan

Based on several fundamental preceding research results, this talk aims to propose a framework to provide high precision bounds for the leading eigenvalues of selfadjoint elliptic differential operator over polygonal domain Ω:

$$-\operatorname{div}(a\nabla u) + cu = \lambda u \text{ in } \Omega, \quad u = 0 \text{ on } \partial\Omega \tag{2}$$

where $a \in C^1(\Omega)$ and $c \in L_\infty(\Omega)$.

The proposed framework has the following features: (1) the domain of eigenvalue problem in consideration can be of free shape, which is because the finite element method with nice flexibility is successfully adopted in bounding the eigenvalues; (2) it can deal with general selfadjoint elliptic operator, where the homotopy method plays an important role; (3) the obtained eigenvalue bounds have high precision, which is due to Lehmann-Goerisch's theorem and well constructed approximating base function.

Exact Polynomial Optimization: Algorithms, Complexity and Implementation

Mohab Safey El Din and Aurélien Greuet
Universite Pierre et Marie Curie,France

Polynomial optimization (i.e. optimizing a polynomial function under polynomial constraints) appears in many areas of engineering science. Thus, it is crucial to obtain fast and reliable implementations solving this problem. Reliability is hard to obtain because of the algebraic nature of the problem. Efficiency is also hard to reach because of the worst-case exponential complexity (in the number of variables). In this talk, we will present an exact algorithm for solving polynomial optimization problems (when the polynomial constraints satisfy some genericity conditions which are natural and frequent in applications). This algorithm can be seen as a special Quantifier Elimination algorithm over the reals dedicated to the structure of polynomial optimization problems. We will show that the degree of all objects it computes is bounded by the best known singly exponential complexity bounds. We will also present our implementation which has the ability to solve polynomial optimization problems which are out of reach of any other known symbolic method (until 10 variables).

Computing the Nearest Real Univariate Polynomial with a Real Multiple Zero and Its Application

Hiroshi Sekigawa
Tokai University, Japan

Given a real univariate polynomial f and a closed real interval I, we provide a rigorous computation method for the nearest real univariate polynomial with a real multiple zero in I. The result can be applied to computing a perturbation bound for preserving the number of real zeros of f.

More precisely, let $\mathbb{P}_n$ be the real vector space of real univariate polynomials of degree not more than n and let B_n be a basis for $\mathbb{P}_n$. Let $B \subset B_n$ and let $\mathbb{P}$ be the subspace of $\mathbb{P}_n$ generated by B. Given $f \in \mathbb{P}_n$ and a closed real interval I, which might be a point, we provide a rigorous computation method for $\tilde{f} \in \mathbb{P}_n$ satisfying (i) $\tilde{f}$ has a real multiple zero in I, (ii) $\tilde{f} - f \in \mathbb{P}$, (iii) $\|\tilde{f} - f\|_\infty$, the infinity norm of the vector of coefficients of $\tilde{f} - f$, is minimal. If I is not bounded, we further assume that $\deg(g) < \deg(f)$ for any $g \in \mathbb{P}$. $\|\tilde{f} - f\|_\infty$ is a perturbation bound for preserving the number of real zeros of f.

The computation method for $\tilde{f}$ is similar to that of the nearest real univariate polynomial with a zero in a given complex domain [1], whose bit complexity is of polynomial order in the size of the input. That is, given $\alpha \in I$, let $\tilde{f}_\alpha$ be the nearest real univariate polynomial with α as a multiple zero and let $\Phi(\alpha) = \|\tilde{f}_\alpha - f\|$. Then, we can compute the minimum of $\Phi(\alpha)$ in I because there exists $m \in \mathbb{N}$ such that $I = I_1 \cup \cdots \cup I_m$(disjoint union) and $\Phi(\alpha)$ is a rational function of α in each interval I_i $(1 \leq i \leq m)$.

Reference:

[1] H. Sekigawa, Computing the nearest polynomial with a zero in a given domain by using piecewise rational functions, Journal of Symbolic Computation, 46(12), pp. 1318–1335, 2011.

Verified Computations for Elliptic Boundary Value Problems on Arbitrary Polygonal Domains

Akitoshi Takayasu, Xuefeng Liu and Shin'ichi Oishi
Waseda University, Japan

In this talk, a computer-assisted procedure is proposed with respect to the invertibility of an elliptic operator. Based on a verified eigenvalue evaluation for the Laplace operator, the inverse of an elliptic operator is proved with computer-assistance. Whether the operator has its inverse plays important role in computer-assisted proof methods for nonlinear elliptic problems. The invertibility of the operator is related to some shifted eigenvalue or weighted eigenvalue problems. A computer-assisted analysis method, which enclose these eigenvalues on arbitrary polygonal domains, is proposed in this talk. Furthermore, some applications are presented for semilinear elliptic problems on several bounded polygonal domains.

Computer-Assisted Proof of Existence of Nash Equilibrium

Zhengyu Wang
Nanjing University

Nash equilibrium problem with shared constraints (NEPSC) is a multiagent optimization problem, in which the agents interact each other both in the level of objective functions and of strategy sets. The NEPSC has many important real world applications in, like engineering, economics and computer science.

A few numerical algorithms have been developed for NEPSC. Of course in numerical setting, without any further preinformation we have to decide whether there exists a solution at all around an approximate solution, this can usually be done via computationally testing the conditions of some existence or convergence theorems. We call a positive test of the existence as a *numerical validation*. So far there is a very few validation methods that can be applied to NEPSC, which is however far from efficiently. Validation of the existence of a solution is extremely important for NEPSC, without it, the output of a numerical algorithm may be of doubtful utility.

In this present work we propose a new validation method by making use of testing the Poincaré-Miranda theorem. This method is actually a computer-assisted proof of existence of the solution of the NEPSC. On the other hand, for a given approximate solution and an error guess, this validation method can also offer an error bound. The error bound is guaranteed if the roundoff error arising in the practical computation can be well controlled, for example with the help of some software like IntLab. Note that the NEPSC often has infinite many solutions constituting a manifold, proving the existence of the solutions is normally numerically difficult because of the non-isolated nature of the solution. Our method can fix this problem to a certain extent. Numerical results are also presented to support the analytic arguments.

Exact Safety Verification of Hybrid Systems Based on Hybrid Symbolic-Numeric Computation

Zhengfeng Yang
China East Normal University , China

In this talk, I will address the problem of safety verification of nonlinear hybrid systems. A hybrid symbolic-numeric method is presented to compute exact inequality invariants of hybrid systems efficiently. Some numerical invariants of a hybrid system can be obtained by solving a bilinear SOS programming via PENBMI solver or iterative method, then the modified Newton refinement and rational vector recovery techniques are applied to obtain exact polynomial invariants with rational coefficients, which exactly satisfy the conditions of invariants. Experiments on some benchmarks are given to illustrate the efficiency of our algorithm.

The Diagonal Reduction Algorithm Using Fast Givens

[1]Wen Zhang, [2]Sanzheng Qiao and [1]Yimin Wei
[1]Fudan University, China
[2]McMaster University, Canada

Recently, a new lattice basis reduction notion, called diagonal reduction, was proposed for lattice-reduction-aided detection (LRAD) of multiinput multioutput (MIMO) systems. In this paper, we improve the efficiency of the diagonal reduction algorithm by employing the fast Givens transformations. The technique of the fast Givens is applicable to a family of LLL-type lattice reduction methods to improve efficiency. Also, in this paper, we investigate dual diagonal reduction and derive an upper bound of the proximity factors for a family of dual reduction aided successive interference cancelation (SIC) decoding. Our upper bound not only extends an existing bound for dual LLL reduction to a family of dual reduction methods, but also improves the existing bound.

Organized Session 2: Computational Geometry

Subdivision methods in Geometric modeling

Bernard Mourrain
GALAAD, INRIA Méditerranée, France

In geometric modelling, shapes are usually represented by semi-algebraic models such as parametrized curves and surfaces or by algebraic equations. The complete description of a geometric object can be composed of many such pieces, involving polynomials usually of small degree but with approximate coefficients.

Performing geometric computations on these models require to solve efficiently fundamental operations such as isolation of intersection points, topology computation of implicit curves and surfaces, to take care of numerical issues coming from the approximate representation, and to handle combinatorial problems as they appear for instance in arrangement computation.

In this talk, we will review different subdivision methods that can be very efficient for tackling this different problems, and in particular for solving univariate and multivariate polynomial equations, for computing the topology of curves and surfaces and for computing planar arrangement of curves.

We will detail some of the methods combining symbolic-numeric computation, show some applications related to Computer Aided Geometric Design, and illustrate the methods by some experiments with the geometric modelle Axel.

Numerical Reparametrization of Rational Parametric Plane Curves

Liyong Shen
University of Chinese Academy of Sciences, China

Proper reparametrization is a basic simplifying process for rational parameterized curves.There are complete results proposed for the curves with exact coefficients but few papers discuss the situations with numerical coefficients. We focus on this numerical problem. We define the approximate improper index and we provide some properties concerning the approximate improper index and the numerical reparametrization. Finally, we propose the numerical reparametrization algorithm for algebraic plane curves, and we provide the error bound or the method presented.

Using μ-bases to Implicitize Rational Surfaces with a Pair of Orthogonal Directrices

Xiaoran Shi
Beijing Computational Science Research Center, China

A rational surface $S(s,t) = (a(t)a*(s), a(t)b*(s), b(t)c*(s), c(t)c*(s))$ can be generated from two orthogonal rational planar directrices: $P(t) = (a(t), b(t), c(t))$ in the xz-plane and $P*(s) = (a*(s), b*(s), c*(s))$ in the xy-plane. Moving a scaled copy of the curve $P*(s)$ up and down along the z-axis with the size controlled by the curve $P(t)$, we get the surface $S(s,t)$. For example, when $P*(s)$ is a circle with center at the origin, the surface $S(s,t)$ is a surface of revolution. Many other useful and interesting surfaces whose cross sections are not circles can also be generated in this manner.

The μ-bases of rational curves/surfaces are newly developed tools which play an important role in connecting parametric forms and implicit forms of rational curves/surfaces. In this talk, we construct a μ-basis for surface $S(s,t)$ generated by double planar curves $P(t)$ and $P*(s)$. To implicitize the surface $S(s,t)$, we construct a $(2m-1)n \times (2m-1)n$ sparse resultant matrix RM using μ-basis. We show that $det(RM) = 0$ is the implicit equation of the surface $S(s,t)$ with a known extraneous factor of degree $(m-1)n$. To decrease the size of this matrix and to eliminate entirely the extraneous factor, we construct a new $mn \times mn$ Sylvester style sparse matrix SM. We prove that $det(SM) = 0$ is the exact implicit equation of the surface $S(s,t)$ without any extraneous factors.

Univariate Real Root Isolation in Extension Field and Applications to Topology of Curves

Elias Tsigaridas
project POLSYS, INRIA Paris-Rocquencourt, France

We present algorithmic and complexity results for the problem of isolating the real roots of a univariate polynomial, the coefficients of which belong to a simple or multiple algebraic extensions of the rational numbers. Using these results, we present improved bounds for the problems of solving bivariate polynomial systems and for computing the topology of a real plane algebraic curve.

Organized Session 3: Parametric Polynomial Computations

Parametric Approaches to Combinatorial Problems

Shutaro Inoue
Tokyo University of Science, Japan

Algebraic Local Cohomology Classes Associated with Semi-quasihomogeneous Singularities

Katsusuke Nabeshima
Tokushima University, Japan

Stability of Gröbner Bases in Terms of a Commutative von Neumann Regular Ring

Yosuke Sato
Tokyo University of Science, Japan

Let K be a field and K' be its extension field. $K[\bar{A}, \bar{X}]$ denotes a polynomial ring with variables $\bar{A} = A_1, \ldots, A_m$ and $\bar{X} = X_1, \ldots, X_n$. Let σ be a homomorphism from $K[\bar{A}]$ to K', i.e. a specialization of $\bar{A}$ with elements $a_1, \ldots, a_m$ of K', it is also naturally extended to a homomorphism from $K[\bar{A}, \bar{X}]$ to $K'[\bar{X}]$. We fix a term order $>$ of $\bar{X}$, $LM(h)$ and $LT(h)$ denotes the leading monomial and the leading term of $h \in K[\bar{A}, \bar{X}]$ w.r.t. $>$ regarding $K[\bar{A}, \bar{X}]$ as a polynomial ring $(K[\bar{A}])[\bar{X}]$ over the coefficient ring $K[\bar{A}]$. The following fact plays an important role in Suzuki-Sato's algorithm to compute comprehensive Gröbner Systems [6].

Lemma 1
Let I be an ideal of $K[\bar{A}, \bar{X}]$ and G be its Gröbner basis w.r.t. $>$ regarding $K[\bar{A}, \bar{X}]$ as a polynomial ring $(K[\bar{A}])[\bar{X}]$ over the coefficient ring $K[\bar{A}]$. Let $G = \{g_1, \ldots, g_s, \ldots, g_t\}$ such that $G \cap K[\bar{A}] = \{g_{s+1}, \ldots, g_t\}$. If $\sigma(LM(g_1)) \neq 0, \ldots, \sigma(LM(g_s)) \neq 0$ and $\sigma(g_{s+1}) = 0, \ldots, \sigma(g_t) = 0$, then $\sigma(G) = \{\sigma(g_1), \ldots, \sigma(g_s)\}$ is a Gröbner basis of $\langle \sigma(I) \rangle$ w.r.t. $>$. Where, $\langle \sigma(I) \rangle$ denotes the ideal of $K'[\bar{X}]$ generated by $\sigma(I)$.

This lemma is a special instance of the following theorem shown as Theorem 3.1 in [1].

Theorem 1
Using the same notations as in the above lemma, If $G = \{g_1, \ldots, g_s, \ldots, g_t\}$ satisfies that $\sigma(LM(g_1)) \neq 0, \ldots, \sigma(LM(g_s)) \neq 0$ and $\sigma(LM(g_{s+1})) = 0, \ldots, \sigma(LM(g_t)) = 0$. Then $G' = \{\sigma(g_1), \ldots, \sigma(g_s)\}$ is a Gröbner basis of $\langle \sigma(I) \rangle$ in $K'[X]$ if and only if $\sigma(g_i) \xrightarrow{*}_{G'} 0$ for each $i = s+1, \ldots, t$.

The above lemma is further extended in [2] and [3] independently for improving Suzuki-Sato's algorithm.

Lemma 2([2] and [3])
Using the same notations as in the above lemma, let $G = \{g_1, \ldots, g_s, \ldots, g_t\}$ such that $G \cap K[\bar{A}] = \{g_{s+1}, \ldots, g_t\}$ and $\sigma(g_{s+1}) = 0, \ldots, \sigma(g_t) = 0$. Let $\{LT(g_{n_1}), \ldots, LT(g_{n_l})\}$ be the minimal subset of $\{LT(g_1), \ldots, LT(g_s)\}$ concerning the order of divisibility, that is each term of $\{LT(g_1), \ldots, LT(g_s)\}$ is divisible by some term of $\{LT(g_{n_1}), \ldots, LT(g_{n_l})\}$ and any term of $\{LT(g_{n_1}), \ldots, LT(g_{n_l})\}$ is not divisible by others. Then $G' = \{\sigma(g_{n_1}), \ldots, \sigma(g_{n_l})\}$ is a Gröbner basis of $\langle \sigma(I) \rangle$ w.r.t. $>$ regardless whether $\sigma(LM(g_i)) = 0$ or not for each $i \in \{1, \ldots, s\} - \{n_1, \ldots, n_l\}$.

At a glance, this extension looks a new result, however, unfortunately it is a special instance of the following theorem which is an extension of Theorem 1.

Theorem 2
Using the same notations as in the above lemma, If $G = \{g_1, \ldots, g_u, \ldots, g_s, \ldots, g_t\}$ satisfies that $\sigma(LM(g_1)) \neq 0, \ldots, \sigma(LM(g_u)) \neq 0$, each term of $\{LT(g_{u+1}), \ldots, LT(g_s)\}$ is divisible by some term of $\{LT(g_1), \ldots, LT(g_u)\}$ but none of $\{LT(g_{s+1}), \ldots, LT(g_t)\}$ is divisible by any term of $\{LT(g_1), \ldots, LT(g_u)\}$ and
$\sigma(LM(g_{s+1})) = 0, \ldots, \sigma(LM(g_t)) = 0$. Then $G' = \{\sigma(g_1), \ldots, \sigma(g_u)\}$ is a Gröbner basis of $\langle \sigma(I) \rangle$ in $K'[X]$ if and only if $\sigma(g_i) \xrightarrow{*}_{G'} 0$ for each $i = s+1, \ldots, t$.

If we carefully read the proof of Theorem 1, then we should notice the above extension is actually proved. However, the proof is based on stability of initials of ideals and is neither fundamental nor essential.

We show that Theorem 2 is almost trivial if we use the the theory of Gröbner bases in a polynomial ring over a commutative von Neumann regular ring introduced in [7] and studied in [5] from a viewpoint of comprehensive Gröbner systems.

We also show that several other results obtained in [1] are also trivial if we use the theory of Gröbner bases in a polynomial ring over a commutative von Neumann regular ring.

References

[1] Kalkbrener, M. On the Stability of Gröbner Bases Under Specializations. *J. Symbolic Computation.* Vol. 24/1, pp. 51–58. 1997.

[2] Kapur, D., Sun, Y. and Wang, D. A New Algorithm for Computing Comprehensive Gröbner Systems. *Proc. International Symposium on Symbolic and Algebraic Computation (ISSAC 2010)*, ACM Press, New York, pp. 29–36. 2010.

[3] Kurata, Y. Improving Suzuki-Sato's CGS Algorithm by Using Stability of Gröbner Bases and Basic Manipulations for Efficient Implementation. *Communications of JSSAC*. Vol. 1, pp. 43–73.

[4] Nabeshima, K. Stability Conditions of Monomial Bases and Comprehensive Gröbner Systems *Lecture Notes in Computer Science*, Vo. 7442, Computer Algebra in Scientific Computing, pp. 248–259. 2012.

[5] Suzuki, A. and Sato, Y. An alternative approach to Comprehensive Gröbner Bases. *J. Symbolic Computation*. Vol. 36/3-4, pp. 649–667. 2003.

[6] Suzuki, A. and Sato, Y. A Simple Algorithm to Compute Comprehensive Gröbner Bases Using Gröbner Bases. *Proc. International Symposium on Symbolic and Algebraic Computation (ISSAC 2006)*, ACM Press, New York, pp. 326–331. 2006.

[7] Weispfenning, V. Gröbner bases in polynomial ideals over commutative regular rings. In Davenport Ed., editor, EUROCAL1987, pages 336-347 Springer LNCS 378, 1989.

Computation of Zero Divisors in Residue Class Rings of Parametric Polynomial Ideal

Dingkang Wang
KLMM, Chinese Academy of Sciences, China

A method is proposed for deciding whether a polynomial is a zero divisors in residue class rings of parametric polynomial ideal. This method is based on computing a comprehensive Gröbner system for a given parametric polynomial system. Given a polynomial f and a parametric polynomial ideal $I \subset k[U, X]$, where $U = u_1, \cdots, u_m$ are the parameters and $X = x_1, \cdots, x_n$ are the variables, if we want to decide whether f is a zero divisors in $k[U, X]/I$, it is only needed to compute a minimal comprehensive Gröbner system (CGS) for ideal $J = I + \langle fy_1 - y_2 \rangle \subset k[U, X, y_2, y_1]$ with respect to a block order $U \ll X \ll y_2 \ll y_1$. From the minimal CGS, we can get the sufficient and necessary conditions for deciding whether f is a zero divisors in $k[U, X]/I$ under the specialization of each branch. What's more, we can also decide whether a polynomial is invertible in residue class ring of parametric polynomial ideals by using this method.

Keywords: Comprehensive Gröbner system, zero divisor.

Organized Session 4: Differential and Difference Algebra

Improved Polynomial Remainder Sequences for Ore Polynomials

Maximilian Jaroschek
Risc-Linz, Johannes Kepler University, Austria

Factorization of Differential Operators with Ordinary Differential Polynomial Coefficients

Mingbo Zhang
University of Science and Technology of China, China

In this talk, we will describe an algorithm to factor a differential operator $L = \sigma^n + c_{n-1}\sigma^{n-1} + \cdots + c_1\sigma + c_0$ with coefficients c_i in $\{y\}$, where $\mathcal{C}$ is the constant field and $\mathcal{C}\{y\}$ is the ordinary differential polynomial ring over $\mathcal{C}$. Also, we will talk about some problems in the decomposition of differential polynomials relating to it.