INTERNATIONAL CONFERENCE ON MATHEMATICS MECHANIZATION

ICMM'09

In honor of Professor Wen-Tsun Wu's ninetieth birthday

Poster Abstracts

May 11-13, 2009

Academy of Mathematics and Systems Science

Beijing, China

Computing Cylindrical Algebraic Decomposition via Triangular Decomposition

Changbo Chen, Marc Moreno Maza, Bican Xia and Lu Yang
Email: moreno@scl.csd.uwo.ca, luyang@casit.ac.cn

Cylindrical algebraic decomposition is one of the most important tools for computing with semi-algebraic sets, while triangular decomposition is among the most important approaches for manipulating constructible sets. In this paper, for an arbitrary finite set $F \subset R[y_1, \ldots, y_n]$ we apply comprehensive triangular decomposition in order to obtain an F-invariant cylindrical decomposition of the n-dimensional complex space, from which we extract an F-invariant cylindrical algebraic decomposition of the n-dimensional real space. We report on an implementation of this new approach for constructing cylindrical algebraic decompositions.

Implicitization and Parametrization of Steiner Surfaces Using Moving Surfaces

Falai Chen and Xuhui Wang
University of Science and Technology of China, China
Email: chenfl@ustc.edu.cn,wangxh05@mail.ustc.edu.cn

A Steiner surface is a quadratically parametrizable surface without base points. To make Steiner surfaces more applicable in Computer Aided Geometric Design and Geometric Modeling, this paper discusses implicitization, parametrization and singularity computation of Steiner surfaces using the moving surface technique. For implicitization, we prove that there exist two linearly independent moving planes with total degree one in the parametric variables. Unifying with the work of Cox et al. (2000), the implicit equation can be expressed as a 3×3 determinant. Inversion formula and singularities for the Steiner surface can also be easily computed from the moving planes. For parametrization, we first compute the singularities of the Steiner surface in implicit form. Based on the singularities, we can find some special moving planes, from which a quadratic parametrization of the Steiner surface can be retrieved.

A Speed-Up of the Hermite Reduction for Rational Functions

Shaoshi Chen   Ziming Li
Key Lab of Mathematics Mechanization, AMSS,
Chinese Academy of Sciences, China
Email: schen@amss.ac.cn, zmli@mmrc.iss.ac.cn

The Hermite reduction decomposes a rational function $f(x)$ into two rational functions $g(x)$ and $h(x)$ such that

$$f = \frac{dg}{dx} + h,$$

and that h has a square-free denominator. The reduction is a basis for many algorithms in symbolic integration.

Let K be the coefficient field of rational functions. During the Hermite reduction, the following two calculations frequently occur:

- Given b, $a_1, \ldots, a_m$ in $K[x]$, compute r in $K[x]$ such that

$$\deg(r) < \deg(b) \quad \text{and} \quad a_1 \cdots a_m \equiv r \mod b.$$

- Given b, $a_1, \ldots, a_m$ in $K[x]$ with $\gcd(b, a_i) = 1$ for $i = 1, \ldots, m$, compute $s, t \in K[x]$ such that

$$\deg(s) < \deg(b) \quad \text{and} \quad s\, a_1 \cdots a_m + t\, b = 1.$$

The first calculation requires polynomial division, and the second requires the extended Euclidean algorithm (EEA). Instead of expanding $a_1 \cdots a_m$ or using division and EEA naively, we compute r, s, and t using the factors. Importing this trick into the Hermite reduction algorithm (linear version) in [1], we gain a significant speed-up when K is a field of rational functions in other variables.

The poster outlines our idea, reports experimental results, and presents an application in the construction of Zeilberger pairs for bivariate rational functions.

References

[1] M. Bronstein. *Symbolic Integration I: Transcedental Functions*, second edition, Springer-Verlag, 2005.

Ambient Isotopic Meshing of Implicit Algebraic Surface with Singularities

Jin-San Cheng[1,2], Xiao-Shan Gao[1], Jia Li[1]
[1]Key Lab of Mathematics Mechanization, AMSS, CAS, China
[2]Loria, INRIA Nancy, France
Email: jcheng@amss.ac.cn, xgao@mmrc.iss.ac.cn

A complete method is proposed to compute a certified, or ambient isotopic, meshing for an implicit algebraic surface with singularities. By certified, we mean a meshing with correct topology and any given geometric precision. We propose a symbolic-numeric method to compute a certified meshing for the surface inside a box containing singularities and use a modified Plantinga-Vegter marching cube method to compute a certified meshing for the surface inside a box without singularities. Nontrivial examples are given to show the effectiveness of the algorithm. To our knowledge, this is the first method to compute a certified meshing for surfaces with singularities.

m-Hilbert Polynomial and Arbitrariness of the General Solution of Partial Differential Equations

Qi Ding and Hongqing Zhang
Dalian University of Technology, China
Email: dingqi.dl@gmail.com,zhanghq@dlut.edu.cn

Using the framework of formal theory of partial differential equations, we consider a method of computation of the m-Hilbert polynomial (i.e. Hilbert polynomial with multivariable), which generalizes the Seiler's theorem of Hilbert polynomial with single variable. Next we present an approach to compute the number of arbitrary functions of positive differential order in the general solution. Finally, as applications the Maxwell equations and weakly overdetermined equations are considered.

Efficient Characteristic Set Algorithms for Equation Solving in Finite Fields

Xiao-Shan Gao and Zhenyu Huang
Institute of Systems Science, AMSS, CAS, China
Email: xgao@mmrc.iss.ac.cn, huangzhenyu@mmrc.iss.ac.cn

Efficient characteristic set methods for computing solutions of a polynomial equation system in a finite field are proposed.

We introduce the concept of proper triangular sets and prove that proper triangular sets are square-free in certain sense. We present an improved algorithm which can be used to reduce the zero set of an equation system in general form as the union of zero sets of proper triangular sets. As a consequence, we can give an explicit formula for the number of solutions of an equation system.

We also give a characteristic set method for equation solving in F_2 with better complexity bounds than the general characteristic set method. The methods are implemented and extensive experiments show that they are quite efficient for solving a class of equations raised in analyzing stream ciphers.

Keywords: Characteristic set, ascending chain, finite field, Boolean functions.

Multiple Small-Amplitude Limit Cycles for Polynomial Lienard Systems

Bi He[1], Suqing Lin [2] Zhengyi Lu[1,2] and Yong Luo[1]
[1]Wenzhou University, China
[2]Sichuan Normal University, China
Email: zhengyilu@hotmail.com

Consider a Liénard system

$$\ddot{x} + f(x)\dot{x} + g(x) = 0,$$

where $f(x)$ and $g(x)$ are polynomials. Let $F'(x) = f(x),\ \dot{y} = -g(x)$, we can rewrite it into a two-dimensional form

$$\dot{x} = y - F(x),\ \dot{y} = -g(x). \tag{1.1}$$

Let $\mathrm{H}(i,j)$ denote the maximumal number of limit cycles, where i is the degree of f and j the degree of g. In 1977, Lins, de Melo and Pugh considered system (1.1) and proved that H(2,1)=1. They conjectured that if $i = 2n$ or $2n+1$, there could be no more than n limit cycles for system (1.1). Coppel proved that H(1,2)=1. In 1996 and 1997, Dumortier and Li proved that H(1,3)=1 and H(2,2)=1.

The global results for the maximal number of limit cycles for system (1.1) are relatively few. In recent years many results have been obtained for small amplitude limit cycles for system (1.1). We use $\hat{\mathrm{H}}(i,j)$ to denote the maximal number of small amplitude limit cycles, which can be bifurcated within a small neighborhood of the origin for system (1.1).

As we all known, the first step for constructing small amplitude limit cycles is to compute the Liapunov quantities (or focal values) for a system and then to solve the principal unknown from the corresponding polynomial of Liapunov quantities after triangularizing all of them. In this paper, we shall deal with the triangularized polynomials of Liapunov quantities by an algorithm of real root isolation without solving the principal unknowns and then construct small amplitude limit cycles based on the independence of these Liapunov quantities.

Based on an algorithm for computing focal values given by Chicone C. and Jacobs M.[1] and an algorithm of real root isolation for multivariant polynomials by Lu Z.Y., He B. and Luo Y. [4], an algorithmic construction of small amplitude limit cycles for a class of Liénard systems is proposed. The maximal number of small amplitude limit cycles for a class of Liénard systems are obtained.

THEOREM 1. [2, 3, 4] $\hat{\mathrm{H}}(7,4) = 8$, $\hat{\mathrm{H}}(7,5) = 9$, $\hat{\mathrm{H}}(8,4) = 9$, $\hat{\mathrm{H}}(5,5) = 6$, $\hat{\mathrm{H}}(6,5) = 8$, $\hat{\mathrm{H}}(4,6) = 7$, $\hat{\mathrm{H}}(5,6) = 8$, $\hat{\mathrm{H}}(4,7) = 8$, $\hat{\mathrm{H}}(4,8) = 9$, $\hat{\mathrm{H}}(8,5) = 10$.

Furthermore, we have a result for some general value $\hat{\mathrm{H}}(n,m)$.

THEOREM 2. [4] $n+1-\left\lceil \dfrac{n+2}{m+1} \right\rceil \le \hat{\mathrm{H}}(n,m) \le n+m-1-\left\lceil \dfrac{n+2}{m+1} \right\rceil$.

References

[1] Chicone C. and Jacobs M., Bifurcation of critical periods for plane vector fields, Tran. AMS, 1989, 433-486.

[2] He B. Lin S. Lu Z., The Construction of Small-amplitude Limit Cycles for Liénard Systems Based on an Algorithm of Real Root Isolation, preprint.

[3] Lin S. Lu Z., The Number of Small Amplitude Limit cycles for a polynomial Liénard system with degrees (8,5), preprint.

[4] Lu Z.Y., He B., Luo Y. An algorithm of real root isolation for polynomial systems, Sci. Press, 2004 (in Chinese).

Quasi-Classical Semantics and Tableau Calculus of Description Logics for Paraconsistent Reasoning in the Semantic Web

Hui Hou[1] and Jinzhao Wu[1,2]
[1]Chengdu Institute of Computer Applications,CAS, China
[2]Beijing Jiaotong University, China
Email: houhui06@mails.gucas.ac.cn, himrwujz@yahoo.com.cn

The forthcoming Semantic Web evolving from the current World Wide Web is designed to define the semantics of information and services on the web, thereby endowing the web with intelligence to automatically reason about the web contents. Description Logics (DLs) play a substantial role in the Semantic Web, since they underlie the W3Crecommended Web Ontology language (OWL), which is derived from ontology research in Artificial Intelligence (AI) in order to achieve the goal of the Semantic Web. However, the knowledge and data in the Semantic Web are large-scale, dispersive, multi-authored and therefore usually inconsistent. It is reasonable and imperative to develop practical reasoning techniques for inconsistent ontologies. In this paper, we propose a new type of paraconsistent description logics based on Hunters Quasi- Classical Logic (QCL), which are termed as Quasi-Classical Description Logics (QCDLs). QCDLs avoid logical explosion. We construct a semantic tableau calculus for QCDLs. Furthermore, we define a sound, complete and decidable consequence relation based on the calculus. These enable an complete framework for paraconsistent reasoning in the Semantic Web. A comparison with other key paraconsistent description logics is also given. It is shown that QCDLs possess more expressive semantics and stronger reasoning capability, and that its connectives behave classically at the object level.

A New Advance in Dense Packing of Equal Circles in a Circle

(In honor of Prof. Wen-Tsun Wu's ninetieth birthday)

Wenqi Huang and Tao Ye
Huazhong University of Science and Technology, China
Email: wqhuang@mail.hust.edu.cn

The problem is to find a densest packing of $N (N = 1, 2, 3, ...)$ equal disks which can be put in a possibly smallest circular container.

A quasi-physical descent strategy and a quasi-physical basin-hopping strategy are proposed. By a combining of these two strategies, a global optimization algorithm is formed to solve the problem.

The best-known packings of $N (N = 1, 2, 3, ..., 150)$ equal circles in a circle were used to test this algorithm.

The algorithm achieved 33 new packings which are better than the best-known ones in literature.

Keywords: packing; equal circles; quasi-physical algorithm; combinatorial optimization.

Exact Certification in Global Polynomial Optimization via Sums-of-Squares of Rational Functions with Rational Coefficients

Erich Kaltofen[1], Bin Li[2], Zhengfeng Yang[3] and Lihong Zhi[2]
[1]North Carolina State University, USA
kaltofen@math.ncsu.edu; http://www.kaltofen.us
[2]Key Laboratory of Mathematics Mechanization, AMSS, China
{bli,lzhi}@mmrc.iss.ac.cn; http://www.mmrc.iss.ac.cn/~lzhi/
[3]East China Normal University, China
zfyang@sei.ecnu.edu.cn

We present a hybrid symbolic-numeric algorithm for certifying a polynomial or rational function with rational coefficients to be non-negative for all real values of the variables by computing a representation for it as a fraction of two polynomial sum-of-squares (SOS) with rational coefficients. Our new approach turns the earlier methods by Peyrl and Parrilo at SNC'07 and ours

at ISSAC'08 both based on polynomial SOS, which do not always exist, into a universal algorithm for all inputs via Artin's theorem.

Furthermore, we scrutinize the all-important process of converting the numerical SOS numerators and denominators produced by block semidefinite programming into an exact rational identity. We improve on our own Newton iteration-based high precision refinement algorithm by compressing the initial Gram matrices and by deploying rational vector recovery aside from orthogonal projection. We successfully demonstrate our algorithm on 1. various exceptional SOS problems with necessary polynomial denominators from the literature, on 2. very large (thousands of variables) SOS lower bound certificates for Rump's model problem (up to $n = 18$, factor degree = 17) and on 3. a proof of the monotone column permanent (MCP) conjecture for dimension 4, which is sufficient to show that 4 polynomials are nonnegative for all real values of the variables.

Analysis of Mechanized Topology

(Extended Abstract)

Hidetsune Kobayashi[1], Yoko Ono[2] and Zhengbing Zeng[3]
[1]Nihon University, Japan
[2]Niigata University of International and Information Studies, Japan
[3]East China Normal University, China
Email: hd_coba@yahoo.co.jp, zbzeng@sei.ecnu.edu.cn

Mathematics mechanization has got great success in past three decades in many areas including geometry, real algebra, and differential equations there the the- orem proving can be reduced to the symbolic manipulation for algebraic equa- tions and inequalities. But mechanization for mathematical fields like topology the first difficulty we need to overcome in the beginning is how to semantically represent the abstract concepts like neighborhood and open sets in appropri- ate forms. A feasible tool available for doing this knowledge representation job would be the formalization language. The formalization system was originally developed as proof checker and soon after a wide variety of application was found in pure mathematics, verification of industrial hardware. ProofGeneral made it possible to make interactive theorem proving. Several successful works have been done for formalization of set theory, abstract algebra, valuation the- ory and many branches of mathematics with using of Formalization system and its various dialects like Isabelle, Coq and Mizar. The formalization of machine proof to four color theorem and the Kepler's conjecture can also be considered as specic examples of this category.

In this poster we present our joint work on formalized topology in Isabelle/HOL. We see propositions and proofs to them step by step with logical calculation exe- cuted according to given proof methods and propositions. Since the proofs allow no logical gaps, most of those proofs are tedious. In addition, unless enough formalized background knowledge, the main proof stream is disturbed by that of preliminary facts, and this makes a proof complicated. Even though the proof is correct, if it is too hard to read then it is not helpful for us. Therefore we have to give concise proofs.

We analyze structure of mechanized topology, and present some points to make short mechanized proofs running with the aid of automated reasoning. In section 1 we present a part of mechanized topology to show how a lemma in topology is formalized. In section 2 we discuss maturity of formalization language. In human language we have several expressions for one object and we can use those expressions representing the same object freely. But, in formalized mathematics, it takes long steps to see one expression is the same as another one, even if we can see apparently these have the same contents. In section 3 we discuss cutting out preliminary properties. Proving such preliminary properties in advance and put them in some le, we can write clear proof. In section 4 we discuss key ideas and a total idea of a proof. Some lemmas can be proved only after giving a key idea found by a/some mathematician/s. If a proof to a lemma requires long step, it is quite hard to prove the lemma automatically, even conning to a part of the proof it is also very hard to prove it automatically. If we have a mechanism to interpret key ideas and a total idea of a proof, then it will be useful to make an automated reasoning system. In section 5 we explain the proof given in section 1 and discuss possibility of automated reasoning system.

The Selection of c in the Extension Ideal of I

Jinwang Liu and Dongmei Li
Hunan University of Science and Technology, China
Email: jwliu@hnust.edu.cn

1. Introduction

Let $k[x_1, x_2, \dots, x_n]$ be a polynomial ring in the variables $x_1, x_2, \dots, x_n$ with coefficients from an arbitrary field k. I is a zero-dimensional ideal in $k[x_1, \cdots, x_n]$. We can quickly obtain the primary decomposition of I when I is normal position with respect to a variable. Otherwise, when I is not normal with respect to every variable, a general method is that introduce a new variable z and pick $c = (c_1, \cdots, c_n) \in k^n$, then let $g = z - c_1x_1 - \cdots - c_nx_n \in k[x_1, \cdots, x_n, z]$, $J =< I, g >$,we get the extension ideal J of I. And J is normal position with respect to the variable z. But the selection of c in the extension ideal of I is an important and difficult problem in the primary decomposition of I. In this paper we discuss this problem and give an efficient method to pick c.

2. main method.

Let K is the algebraic closed field of k,$Z_1, Z_2, \cdots, Z_{r+s} \in K^n$ are the zeroes of the ideal I. Assume that

$$Z_i = (Z_{i1}, Z_{i2}, \cdots, Z_{in}), i = 1, 2, \cdots, r + s$$

The key of the method is to find a list of $c = (c_1, \cdots, c_n)$ such that

$$\sum_{i=1}^{n} c_i Z_{ji} \neq \sum_{i=1}^{n} c_i Z_{ki} \tag{1}$$

Here $Z_j \neq Z_k, j, k = 1, 2, \cdots, r + s$. Let

$$\begin{cases} Z_{11}c_1 + Z_{12}c_2 + \cdots + Z_{1n}c_n = b_1 \\ \vdots \\ Z_{r1}c_1 + Z_{r2}c_2 + \cdots + Z_{rn}c_n = b_r \\ \vdots \\ Z_{r+s,1}c_1 + Z_{r+s,2}c_2 + \cdots + Z_{r+s,n}c_n = b_{r+s} \end{cases} \tag{2}$$

We request only $b_1, b_2, \cdots, b_{r+s}$ are pairwise different.We regard $Z_1, Z_2, \cdots$, Z_{r+s} as $r+s$ vectors in K^n. Without loss of generality, we assume $Z_1, Z_2, \cdots, Z_r$ is a maximal linear independent subset of $Z_1, Z_2, \cdots, Z_{r+s}$, then we know that we only need select $b_1, \cdots, b_r$ pairwise different such that $\sum_{i=1}^{r} b_i a_{ji} \neq \sum_{i=1}^{r} b_i a_{li} \neq b_k$, then $b_1, b_2, \cdots, b_{r+s}$ are pairwise different,here $1 \leq j \neq l \leq s, 1 \leq k \leq r$. Solving equation (2), we shall obtain c.

3. main result.

We proved that we can pick the above $b_1, b_2, \cdots, b_r$. When $s = 0$, we only need pick pairwise different $b_1, b_2, \cdots, b_r$ and solve(2),then We can easily get the requisition $c_1, c_2, \cdots, c_n$. When the value of s is little,picking

$b_1, b_2, \cdots, b_r$ is also easy. Since $r \leq n$, so the number of $b_i (1 \leq i \leq r)$ is no more than $c_i (1 \leq i \leq n)$, some time is much less. So we pick b_i is much easy than select c_i directly. So our method is more easy than Beck's find out a list of $\underline{c} = (c_1, \cdots, c_n)$.

Comparison Between JPEG2000 and H.264 for Digital Cinema

Boxin Shi, Lin Liu and Chao Xu
Peking University, China
Email: xuchao@cis.pku.edu.cn

JPEG2000 and H.264 are the latest image and video coding standards respectively. Digital cinema is a new kind of application for super high definition video. The DCI (Digital Cinema Initiative) specification published in 2005 has selected JPEG2000 instead of H.264 as the video coding standard for digital cinema. In this paper, based on JPEG2000, H.264 intra and inter-frame coding, we compare the coding efficiency and subjective image quality on multiple series of test sequences from low to super high resolutions. The experiment results demonstrate some regularity for JPEG2000 and H.264 video coding, and reveal JPEG2000 is more suitable for digital cinema.

Differential Characteristic Set Algorithm for the Complete Symmetry Classification of (Partial) Differential Equations

Chaolu T
Shanghai Maritime University
Email: tmchaolu@dbc.shmtu.edu.cn

A differential polynomial characteristic set algorithm for the complete symmetry classification of (partial) differential equations with some parameters is given, which makes solution of the complete symmetry classification problem for (partial) differential equations become direct and systematic; As an illustrative example, the complete potential symmetry classifications of nonlinear and linear wave equations with an arbitrary function parameter are presented. This is a new application of differential form characteristic set algorithm (differential form Wu's method) in the field of differential equations.

The Formula for Non-uniform B-Spline Basis Function with Multiple Parameters

Guozhao Wang
Zhejiang University, China
Email: wanggz@zju.edu.cn

B-spline curve is a very important tool in computer aided design. The B-spline curves which use the B-spline basis function with parameters are called as the B-spline with parameters. Their advantage is to provide more flexibility of curve adjustment.

There is a method to construct uniform B-spline basis function with multiple parameters, and a method to construct non-uniform B-spline basis function with one parameter.

In this paper, we give a formula for non-uniform B-spline basis function with multiple parameters. The formula is a new one. The idea of the formula is based on the degree elevation of B-spline curves and corner cutting. The basis functions propose the properties of B-spline curve, such as positivity, local support, decompose of unity.

The non-uniform B-spline with multiple parameters is extension of B-spline. The curve defined by these basis functions proposes the properties of B-spline curve, such as shape preservation, V.D. They provide a way which can adjust the shape of B-spline curve greatly without changing the control polygon.

Keywords: B-spline curve with parameter; degree elevation; B-spline.

Results and Problems on Factorizations of $n-D$ Polynomial Matrices

Mingsheng Wang
Institute of Software, CAS, China
Email: mingsheng_wang@yahoo.com.cn

Multivariate (nD) polynomial matrix factorizations are basic research problems in multidimensional systems theory.

Let n be an integer with $n \geq 1$. Let k be a field, $R = k[z_1, \ldots, z_n]$ be the polynomial ring in variables $z_1, \ldots, z_n$ over k, and $Q(R)$ be its fraction field. $R^{l\times m}$ denotes the free module of $l \times m$ matrices with entries in R. We also write $R^{1\times m}$ as R^m which is a free module of rank m over R.

Let $F \in R^{l\times m}$ be of full row rank, we denote the greatest common divisor of all the $i \times i$ minors of F by $\mathrm{d}_i(F)$, $i = 1, \ldots, l$. We set $\mathrm{d}(F) = \mathrm{d}_l(F)$, and $\rho(F)$ denotes the submodule generated by rows of F.

In order to state the research problems, some basic definitions are needed:

Definition 0.1 *Let $F \in R^{l\times m}$ be of full row rank. Then F is said to be:*

(i) zero left prime (ZLP) if all the $l \times l$ minors of F generate the unit ideal R;

(ii) minor left prime (MLP) if all the $l \times l$ minors of F are relatively prime, i.e., $\mathrm{d}(F)$ is a nonzero constant;

(iii) factor left prime (FLP) if in any polynomial matrix factorization $F = F_1F_2$ in which F_1 is a square matrix, F_1 is necessarily a unimodular matrix, i.e., $\det F_1$ is a nonzero constant in k.

Zero right prime (ZRP), and minor right prime (MRP) etc. can be similarly defined for matrices $F \in R^{m\times l}$ with $m \geq l$.

Notice that ZLP $\Rightarrow$ MLP $\Rightarrow$ FLP. When $n \geq 3$, these concepts are pairwise different, when $n = 2$, ZLP is not equivalent to MLP, but MLP is the same as FLP, when $n = 1$ all three concepts coincide.

Definition 0.2 *Let $F \in R^{l\times m}$ be of full row rank, and f be a divisor (not necessarily the gcd) of $\mathrm{d}(F)$, that is, $a_i = f\, b_i$, where $a_1, \ldots, a_\beta$ are all the $l \times l$-minors, and $b_i \in R$, $i = 1, \ldots, \beta$. We say that F has a matrix factorization with respect to f if F can be factorized as*

$$F = G_1\, F_1 \tag{1}$$

such that $F_1 \in R^{l\times m}$, $G_1 \in R^{l\times l}$ with $\det G_1 = f$.

In above Definition, when $l < m$, and $f = \mathrm{d}(F)$, (1) is called an MLP factorization of F; if F_1 is ZLP, then (1) is called a ZLP factorization of F; when F_1 is FLP, we say that (1) is a FLP factorization of F with respect to f.

The aim of this poster is to survey recent research results and problems for $n - D$ polynomial matrix factorizations.

A Bivariate Preprocessing Paradigm for Buchberger-Möller Algorithm

Xiaoying Wang, Shugong Zhang and Tian Dong
Jilin University, China
Email: dongtian@jlu.edu.cn

For the last almost three decades, since the famous Buchberger-Möller (BM) algorithm emerged, there has been wide interest in vanishing ideals of affine points and associated interpolation polynomials. For the sake of reducing the complexity of BM algorithm, we propose a preprocessing paradigm for BM algorithm in bivariate cases. First, we will give an estimation of certain aspect of the geometry of the points. Next, we will introduce our main algorithm for finding a maximal lower subset of the original points and then constructing associated Newton-type polynomials that are part of the output of BM algorithm w.r.t. some rearrangement of the order of the points. These results can be used by BM procedure directly hence simplify the computation.

On Invariance of Dynamic Model Checking in Iterative Designs of Flow Control Oriented

Jinzhao Wu[1], Shihan Yang[2] and Hui Hou[2]
[1]Beijing Jiaotong University, China
[2]Chengdu Institute of Computer Applications, CAS, China
Email: dr.yangsh@gmail.com

Model checking is a promising approach to verifying digital hardware systems, in which a state-transition graph model of the sys- tem behavior is compared with a temporal logic formula. Iteration is a common strategy in digital hardware design. However, it is expensive and impractical to use model checking technologies along iterative pro-cesses because of the high cost of rechecking. One solution to this is the methodology of so-called dynamic model checking (informally, a sequence of common model checking) forthcoming in recent years, where a key is- sue is to seek the invariance of dynamic model checking. A predicate that, if true, will remain true

throughout a specific sequence of model checking, is called an invariance to the sequence. The invariance can dramatically avoid the checking repeatedly. In this paper, we first construct a formal framework of dynamic model checking, and then propose an invariance theory of dynamic model checking based on an iterative design process of flow control oriented hardware systems (FC-oriented HS for short) described by Moore machines. The FC-oriented HS is a kind of sequen- tial circuit system stressing to handle data transformation. Furthermore, we show that some non-trivial CTL properties are preserved in the it- eration. To our best knowledge, this is the first research on invariance of dynamic model checking along the iterative hardware systems design process. This theory is an extension and a supplement of the classical CTL case.

Key words:dynamic model checking, invariance, iterative design, flow control oriented hardware system.

An Algorithm for Vector Valued Osculatory Rational Interpolation Based on Groebner Bases of R-modules

Peng Xia, Na Lei and Shugong Zhang
Jilin University, China
Email: leina@jlu.edu.cn

In this paper we convert the task of seeking the weak solution $(\vec{a}(X), b(X))$ of vector valued osculatory rational interpolation into computing the Groebner bases of R-submodule M of the free module over the polynomial ring. We compute the Groebner bases recursively so that the algorithm for rational interpolation is Newton-type. Complexity is measured in terms of $\max\{\deg(\vec{a}), \deg(b)+\xi\}$, where ξ is a given integer used in defining the term order of the R-module.

Keywords: Groebner bases, modules, weak interpolations, vector valued osculatory rational interpolation.

Balanced Dense Polynomial Multiplication on Multi-cores

Yuzhen Xie and Marc Moreno Maza
Massachusetts Institute of Technology, USA
Email: moreno@csd.uwo.ca

We discuss strategies for parallel multiplication of dense polynomials over finite fields based on FFT-techniques. We show how multivariate (and univariate) multiplication can be efficiently reduced to balanced bivariate multiplication. This approach substantially improves parallel running time for irregular input data. In addition, even if the implementation relies on serial one-dimensional FFTs, we obtain satisfactory speed-up factors on multi-cores. This allows us to use efficient non-standard FFT techniques, such as Truncated Fourier Transform, which are hard to parallelize.

Infinite Series Symmetry Reduction Solutions to the Modified KdV-Burgers Equation

Ruoxia Yao[1,2], Xiaoyu Jiao[1] and Senyue Lou[1,3]
[1]Shanghai Jiao Tong University, China
[2]Shaanxi Normal University, China
[3]Ningbo University, China
Email: rxyao2@hotmail.com

From the approximate symmetry point of view, the modified KdV-Burgers (mKdV-Burgers) equation with weak dissipation is investigated. The symmetry of a system of the corresponding PDEs which approximates the perturbed mKdV-Burgers equation is constructed and the corresponding general approximate symmetry reduction is derived, which enables infinite series solutions and general formulae. Study shows that the zero order similarity solutions satisfy the Painlevè II equation. Also, at the level of travelling wave reduction, the general solution formulae are given for any travelling wave solutions of the unperturbed mKdV equation. As an illustrating example, while choosing the zero order tanh profile solution as initial approximate, the physical approximate similarity solutions are obtained recursively under appropriate choices of parameters occurred during the computations.

Keywords: mKdV-Burgers equation, approximate symmetry reduction, series reduction.

Solving Under-constrained Geometric Constraint Problem Based on Connectivity Analysis of Graph

Gui-Fang Zhang
Beijing Forestry University, China
Email: gfzhang@bjfu.edu.cn

In this paper, we present a method based on connectivity analysis of graph to solve structurally under-constrained constraint problems frequently occurred during design process in parametric CAD. With this method, a connected, bi-connected or tri-connected structurally under-constrained problem can be transformed into a structurally well-constrained one by adding additional constraints automatically during the process to decompose it into a decomposition tree.

Principle of Duality and its Applications in Solving Some Kinds of Systems of PDEs

Hongqing Zhang and Jianqin Mei
Dalian University of Technology, China
Email: zhanghq@dlut.edu.cn

In this paper, the invariance principle and principle of duality are introduced. The uniform definition of adjoint operators of general operators has been presented. As the applications, some systems of PDEs have been solved, including linear PDEs with variable coefficients and some kinds of nonlinear PDEs.

Hybrid Divide-and-Conquer Method for Solving Deficient Polynomial Systems

(In honor of Prof. Wen-Tsun Wu's ninetieth birthday)

Jintao Zhang, Bo Dong and Bo Yu
Dalian University of Technology, China
Email: yubo@dlut.edu.cn

Homotopy method is a reliable and efficient numerical algorithm for solving a polynomial system. The standard homotopy generates Bezout number of paths while typical practical polynomial systems are deficient, i.e., they have less number of solutions than their Bezout numbers. Constructing efficient homotopy methods for solving deficient polynomial systems is the main task in the study of homotopy methods. Linear product homotopy, polyhedral homotopy and coefficient parameter homotopy (cheater's homotopy) are some efficient homotopies exploiting multi-homogeneous structure, structure of solution set at infinity, Newton polytopes and parameter structure respectively.

Linear product homotopy is very easy to implement, however, sometimes it destroys the sparse structure of the system. Polyhedral homotopy is very powerful, however, for big system, computation of mixed volume and mixed subdivision of Newton polytopes is too expensive.

In this paper, for general deficient polynomial systems, a hybrid divide-and-conquer method is proposed. At first, a hybrid homotopy is constructed. Some components of the start system are linear products while the others keep almost the same as that of the the target system so that it can preserve the sparse structure. Such a start system is not trivial to solve, however, it can be decomposed and reduced into some smaller subsystems which are much more easier to be solved by a polyhedral homotopy method. The collection of all solutions of these subsystems will serve as start points of the hybrid homotopy.

Some criterions are given for determining the partial linear product structure of the hybrid homotopy so that it is more efficient.

A Human Eye Location Algorithm Based on the Quasi Binary Image

Lina Zhao and Yan Gao
Beijing University of Chemical Technology, China
Email: zhaoln@mail.buct.edu.cn

A method for eyes localization is described in this paper. Its based on twice binary images and twice vertical projection. Firstly, the original image is decomposed with 8-level of wavelet , and then by vertical and horizontal projection, the main area for eyes is gotten. Secondly, the given image is decomposed with SVD again and 35% of the max singular value is set to be a new threshold and to reconstruct the original image for obtaining the quasi binary image which embodies eyes better. At last, eyes area is intercepted from less-noise quasi binary image by already known coordinates and finally, accurate position of eyes are achieved by vertical projection once again. Experimental results indicate that the proposed method is easy, feasible, and fairly precise for eye localization.

Maximal Equation Satisfying Problem Solving in F_2 Equations System by Particle Swarm Algorithm

(In honor of Professor Wen-Tsun Wu's ninetieth birthday)

Xinchao Zhao
Beijing University of Posts and Telecommunications, China
Email: xcmmrc@gmail.com

Boolean Equation system to be solved:

$$AX = b, \text{ where } A \in F_2^{m\times n}, X \in F_2^{n\times 1}, b \in F_2^{m\times 1} \text{ and } m \gg n.$$

Goal: It's obvious that there are *NO* exact solutions satisfying all the equations. So our goal is to find a vector $X \in F_2^{n\times 1}$ which satisfies as many equations as possible.

Method: Population heuristic particle swarm algorithm(PSA) is used. As far as I know, it's the first time to adapt the PSA to solve such discrete equations in F_2.

Results: An improved random disturbed PSA is proposed for the equations solving problem. Four randomly generated equations are solved with sizes $A \in F_2^{100\times 20}$, $A \in F_2^{300\times 50}$, $A \in F_2^{500\times 100}$ and $A \in F_2^{1000\times 200}$.