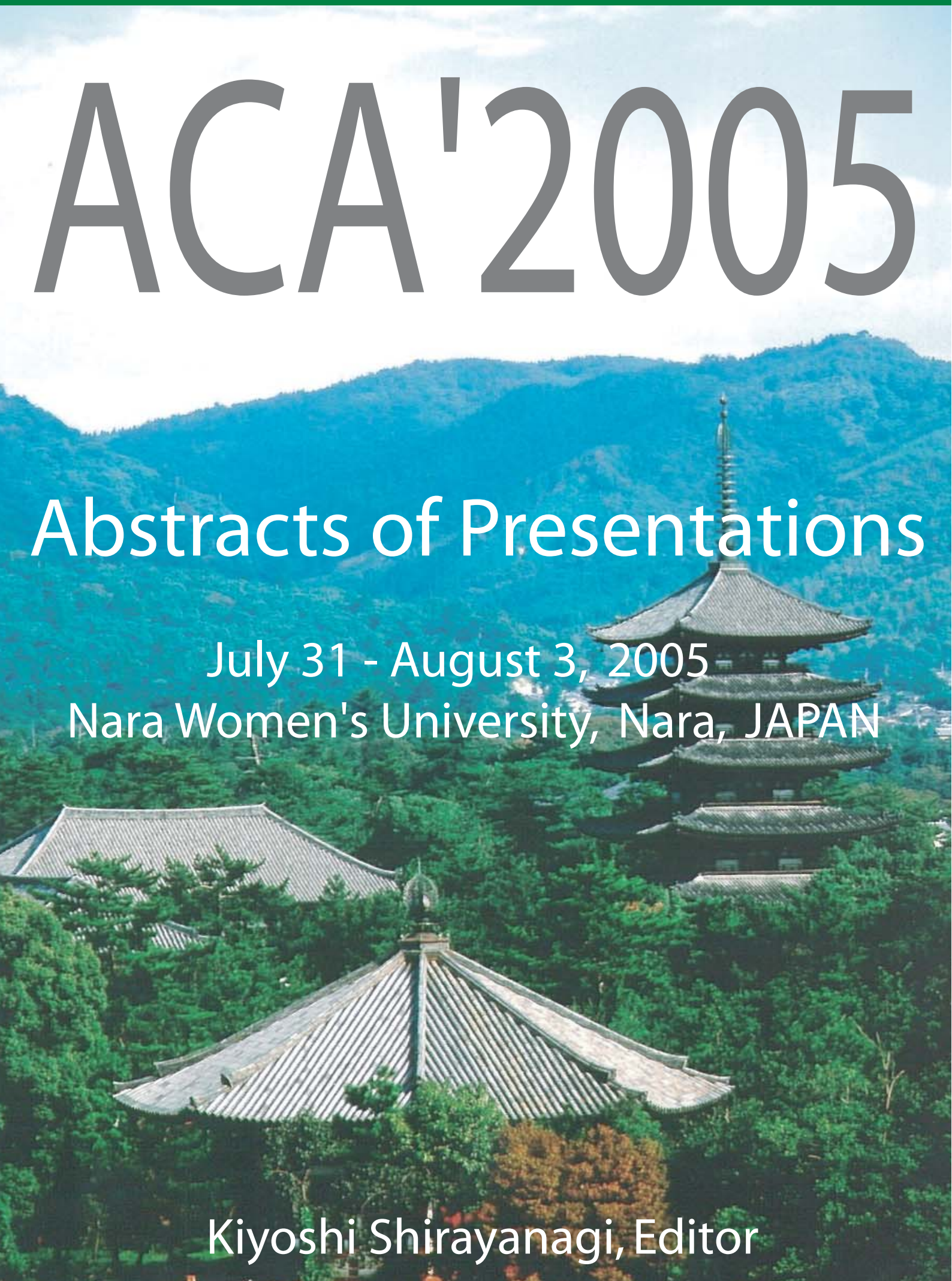
11th International Conference on Applications of Computer Algebra

ACA'2005

Abstracts of Presentations

July 31 - August 3, 2005

Nara Women's University, Nara, JAPAN



Kiyoshi Shirayanagi, Editor

PREFACE

This volume contains abstracts of the talks presented at the eleventh conference on Applications of Computer Algebra, held at Nara Women's University, Nara, Japan. ACA meetings are organized into special sessions. This meeting had 14 special sessions and 100 talks. Accordingly, the abstracts are organized by special session.

Previous ACA meetings were held at: Texas, USA, 2004, North Carolina, USA, 2003, Greece, 2002, New Mexico, USA, 2001, Russia, 2000, Spain, 1999, Czech Republic, 1998, Hawaii, USA, 1997, Austria, 1996, New Mexico, USA, 1995. ACA'2005 in Japan is the first conference of the ACA series held in Asia. Additional information about these meetings, including electronic proceedings, can be found at `http://math.unm.edu/aca`. ACA'2006 will be held in Bulgaria.

Nara, an ancient capital of Japan (710 – 794 AD), is located at the eastern end of the Silk Road. There are eight World Heritage sites designated by UNESCO in Nara. The city's richness in cultural and historical assets and natural surroundings is augmented by its steady development as an international cosmopolitan city.

Nara Women's University was first established in 1908 as Nara Women's Higher Normal School, which was a school for training women instructors and teachers for other women's normal schools. In 1949, the school was renamed Nara Women's University. Kiyoshi Oka, one of my favorite mathematicians, was professor at the university from 1949 to 1964. At present, the university has three faculties (Faculty of Letters, Faculty of Science, and Faculty of Human Life and Environment) and one graduate school (Graduate School of Humanities and Sciences). It is located in the center of Nara City and is surrounded by many cultural sites.

We graciously acknowledge Nara Women's University and the Department of Information and Computer Sciences of the Faculty of Science for their support. Moreover, we express gratitude to the Nara Convention Bureau not only for their financial support but also for various kinds of services to the local organizers.

Many people contributed to the organization of ACA'2005 and the preparation of this volume. The dedicated work of the General Chairs, Fujio Kako, Matu-Tarow Noda, Tateaki Sasaki, and Yosuke Sato, and the other Committee Members, Tetsuo Fukui, Hiroshi Kai, Tadashi Takahashi, and Akira Terui, made the conference a great success. The International Advisory Committee members and Session Organizers, through their expertise and elaborate efforts, ensured the quality of the contents of the conference. In creating this volume, Ilias Kostsireas provided assistance based on his experience at ACA'2002. My colleague, Hirokazu Noda, helped us in processing the abstract tex files efficiently. Akio Matsunaga of Japan Society for Symbolic and Algebraic Computation made arrangements with the printer. We thank all of you for your generous contributions, help, and cooperation.

We hope that the ACA series will continue to contribute to the worldwide development of computer algebra.

Dear ACA'2005 participants, we hope your stay in Japan was memorable and we thank you for making the conference a great success.

THANK YOU, ARIGATO

ACA'2005 Editor of Abstracts
Kiyoshi Shirayanagi, NTT Communication Science Laboratories, Japan

International Advisory Committee:

Alkis Akritas(Greece), Jacques Calmet(Germany), Victor Edneral(Russia), Victor Ganzha(Russia), Vladimir Gerdt(Russia), Hoon Hong(USA), Erich Kaltofen(USA), Ilias Kotsireas(Canada), Bernhard Kutzler(Austria), Richard Liska(Czech Republic), Bill Pletsch(USA), Eugenio Roanes-Lozano (Spain), Tanush Shaska(USA), Margarita Spiridonova(Bulgaria), Stanly Steinberg(USA), Agnes Szanto(USA), Quoc-Nam Tran(USA), Nikolay Vassiliev(Russia), Michael Wester(USA)

Sponsor:

Japan Society for Symbolic and Algebraic Computation

Table of Contents

Session 1	General Session	4
Session 2	Young Researchers Session	10
Session 3	Approximate Algebraic Computation	14
Session 4	Computational Algebraic Structures and Engineering Applications	18
Session 5	Computer Algebra and Coding Theory	21
Session 6	Computer Algebra in Quantum Information and Computation	24
Session 7	Computer Algebra in the Biological Sciences	27
Session 8	Computational Topology and Geometry	29
Session 9	Computer Algebra in Education	33
Session 10	Handling Large Expressions in Symbolic Computation	40
Session 11	High-Performance Computer Algebra	46
Session 12	Newton and Hensel Techniques in Scientific Computing	49
Session 13	Parametric and Nonconvex Constraint Solving	53
Session 14	Pen-Based Mathematical Computing	60
ACA '2005 List of Authors		64

Session 1:

General Session

Organizers:

Alkis Akritas
Bill Pletsch
Tateaki Sasaki and Matu-Tarow Noda

The Art of Symbolic Computation

Erich Kaltofen
North Carolina State University, USA

Abstract

Symbolic Computation in the past 40 years has brought us remarkable theory: Berlekamp-Zassenhaus; Groebner; Risch; Gosper, Karr and WZ; cylindrical algebraic decomposition; sparse polynomial interpolation; LLL; Wiedemann and block Lanczos; matrix Pade; straight-line and black box polynomial calculus; baby-steps/giant-steps and black-box linear algebra and polynomial factorization; symbolic/numeric GCD, factorization and sparse interpolation; Tellegen's principle; sparse resultants; Giesbrecht/Mulders-Storjohann diophantine linear solvers; Sasaki/van Hoeij power sums and Bostan et al. logarithmic derivatives; fast bit complexity for linear algebra over the integers; over the integers; essentially optimal polynomial matrix inversion; Skew, Ore and differential polynomial factorization; Barvinok short rational functions and supersparse polynomial factorization; and many more.

The discipline has lead to remarkable software like Mathematica and Maple, which supply implementations of these algorithms to the masses. As it turned out, a killer application of computer algebra is high energy physics, where a special purpose computer algebra system, SCHOONSHIP, helped in work worthy of a Nobel Prize in physics in 1999.

In my talk I will attempt to describe what the discipline of Symbolic Computation is and what problems it tackles. In particular, I will discuss the use of heuristics (numerical, randomized, and algorithmic) that seem necessary to solve some of today's problems in geometric modeling and equation solving. Thus, we seem to have come full cycle (the discipline may have started in the 1960s at the MIT AI Lab), but with a twist that I shall explain.

Counting Young Group Double Cosets with Computer Algebra

Bill Pletsch
Albuquerque Technical Vocational Institute Alburquerque, New Mexico, USA

Abstract

Until the advent of computer algebra, the theory of double cosets has been restricted to a few elegant but computationally impossible theorems. Impossible in the sense that in principle the calculation can be done but it will take ten thousand years. Today, using Computer Algebra

much can be calculated quickly. Using Macsyma and Maple in the special case of Young Group double cosets, we will see just how valuable Computer Algebra can be.

We will focus on the use of CA in three areas of interest: the initial calculations, the generation of novel double coset symbols, and the generalization the method of successive subtractions.

Without CA the new insights into the theory of double cosets would never have been discovered. There was no particular reason to believe that the long arduous calculations required to compute a each double coset number would yield any fruit. Thanks to the power of MACSYMA these calculations were simple to conduct. The result was a breakthrough that immediately revealed a multitude of patterns.

In follow-up research a novel system of double coset symbols was developed. The novel system uses a special canonical form that can be expressed in Maple as a subroutine. Using this subroutine and other Maple subroutines, lists of these symbols can be quickly generated.

In the initial calculations, successive subtractions of the data eventually yielded a constant: thus uncovering a data fitting polynomial (in this case a quartic). The initial calculations used successive subtractions to point at the pattern, but the pattern itself is not a proof. However, the method of successive subtractions also points to the next step. Using the lists of DC-symbols and Maple once again the method of successive subtractions is generalized by successive subtractions of sets. The patterns revealed resulted in a series of proofs.

Time permitting; sketches of the proofs will be given with special emphasis on the roles of Macsyma and Maple. It is easy to see that in all these cases, CA was a critical aid in speeding the requisite insight for the next leap in theory.

Rational Approximants of Formal Power Multivariate Series

Christiane Hespel, Cyrille Martig
IRISA-INSA
20 avenue des Buttes de Coesmes
35043 Rennes cedex, France
hespel@irisa.fr, cmartig@insa-rennes.fr

Abstract

1 Introduction

For any formal power multivariate series $s \in K[[X_i]]_{1\leq i\leq n}$ on a field K, we propose an algorithm for computing a family of rational series $(s_k)_{k\in N}$ such that the difference $s - s_k$ is at least of order k.
The method consists in using the computation in noncommutative variables: for any order k, we construct a rational (recognizable) series $s_{nc_k} \in K\langle\langle X_i\rangle\rangle_{1\leq i\leq n}$ in noncommutative variables, of minimal rank r_k, such that s_k is its commutative image. This construction uses the Hankel matrix $H(s_{nc_k})$ of the series s_{nc_k}. The rational series s_k is provided as a quotient of 2 polynomials, the denominator being at most of total degree r_k.
If s is rational, there is an order k_0 such that $\forall k \geq k_0$, the rank of s_{nc_k} is r_{k_0}. And then for $k \geq k_0$, the commutative image of s_{nc_k} is $s = P/Q, Q$ being at most of total degree r_{k_0}.

2 Algorithm

We know that a rational series in noncommutative variables

$$s_{nc} = \sum_{w \in X_1, \cdots, X_n *} \langle s_{nc} | w \rangle w$$

is such that its Hankel matrix $H(s_{nc} = (\langle s_{nc} | w_1 \cdot w_2 \rangle)_{w_1, w_2 \in \{X_1, \cdots, X_n\}^* \times \{X_1, \cdots, X_n\}^*}$ has a finite rank([1, 2]). Two presentations of s_{nc} are then availables ([3]): by a finite weighted automaton A or by a regular expression E.
The algorithm is the following: For any order k, we construct the Hankel matrix of s_{nc_k} by assigning to $\langle s_{nc_k} | X_i^p \rangle$ the value of $\langle s | X_i^p \rangle$ and by maintaining the linear dependence relations existing in the already built part of the matrix while taking into account the relation

$$\sum_{|w|_{X_1} = p_1, \cdots |w|_{X_n} = p_n} \langle s_{nc_k} | w \rangle = \langle s | X_1^{p_1} \cdots X_n^{p_n} \rangle$$

We obtain a noncommutative series s_{nc_k} of minimal rank r_k and then the corresponding regular expression E_k. Its commutative image is $s_k = P_k / Q_k$, the total degree of $Q_k \leq r_k$ and $ord(s - P_k/Q_k) \geq k$.

Example: $s = \sum_{i,j \in N} X_1^i X_2^j (\sum_{k=0}^{inf(i,j)} \begin{pmatrix} |i-j| + 2k \\ k \end{pmatrix})$
For $k = 2$, the Hankel matrix $H(s_{nc_2})$ is

	ϵ	X_1	X_2	X_1^2	X_1X_2	X_2X_1	X_2^2	$\cdots$
ϵ	1	1	1	1	2*	1*	1	$\cdots$
X_1	1	1	2*					$\cdots$
X_2	1	1*						$\cdots$
X_1^2	1							$\cdots$
X_1X_2	2*							$\cdots$
X_2X_1	1*							$\cdots$
X_2^2	1							$\cdots$
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$

where the values marked by a star are computed according to the algorithm.
Then for instance, $s_{nc_2} = (X_1 + 2X_2X_2^*X_1)(1 + X_2X_2^*)$ and $s_2 = \frac{1}{1-(X_1+X_2+X_1X_2)}$. For $k \geq 4$, $s_{nc_k} = s_{nc} = [X_1 + X_2(X_2 + 2X_1X_2)^*X_1(X_1 - X_2)]^*[1 + X_2(X_2 + 2X_1X_2)^*(1 + 2X_1)]$ and

$$s_k = s = \frac{1}{(1 - X_1X_2)(1 - (X_1 + X_2))}$$

3 Conclusion

If s is rational, then there is an order k_0 such that $\forall k \geq k_0, s_k = P/Q = s$. Otherwise, this method provides a family of rational approximants (P_k/Q_k) such that the total degree of Q_k is $\leq r_k$, r_k being the minimal rank of the noncommutative intermediary series s_{nc_k}.

References

[1] Berstel J., Reutenauer C., *Rational series and their languages*, Springer-Verlag, 1988.

[2] Fliess M., *Un outil algebrique : les séries formelles non commutatives*, in "Mathematical System Theory" (G.Marchesini and S.K.Mitter Eds.), Lecture Notes Econom. Math. Syst., Springer Verlag, vol.131, pp.122-148, 1976.

[3] Hespel C., *Une étude des séries formelles non commutatives pour l'Approximation et l'Identification des systèmes dynamiques*, Thèse d'état, Université de Lille 1, 1998.

A Unified Formula for Arbitrary Order Symbolic Derivatives and Integrals of The Power-Exponential Class

Mhenni M. Benghorbal
Center for Experimental and Constructive Mathematics
Department of Mathematics
Simon Fraser University
***Burnaby,* Canada**
mhennib@cecm.sfu.ca

Abstract

We give a complete solution to the problem of symbolic differentiation and integration of arbitrary (integer, fractional, or real) order of the *power-exponential class*

$$\left\{ f(x) : f(x) = \sum_{j=1}^{\ell} p_j(x^{\alpha_j}) e^{\beta_j x^{\gamma_j}} \, , \alpha_j \in \mathbb{C}, \beta_j \in \mathbb{C}\backslash\{0\}, \gamma_j \in \mathbb{R}\backslash\{0\} \right\} ,$$

through a unified formula in terms of the H-function which can, in many cases, be simplified to less general functions. We begin our talk by discussing a less general class of functions given by

$$\left\{ f(x) : f(x) = \sum_{j=1}^{\ell} p_j(x) e^{\beta_j x} \, , \beta_j \in \mathbb{C} \right\} ,$$

which is a subclass of the *power-exponential class*. It has the property that its nth derivative and integral formulas of integer order belongs to the same class.
In Maple, the formulas correspond to invoking the commands diff$(f(x), x\$q)$ for differentiation and int$(f(x), x\$q)$ for integration, where q is an integer, a fraction, a real, or a symbol. They enhance the ability of computer algebra systems for computing derivatives and integrals of very large arbitrary orders at a point x.
The arbitrary order of differentiation is found according to the Riemann-Liouville definition, whereas the generalized Cauchy n-fold integral is adopted for arbitrary order of integration.
One of the key points in this work is that the approach does not depend on integration techniques.

First Order Algebraic Differential Equations – A Computer Algebraic Approach

Yujie Ma
Key Laboratory of Mathematics Mechanization
Chinese Academy of Sciences
Beijing 100080, P. R. China

Abstract

In this talk, we present our computer algebraic approach to first order algebraic differential equations. We apply the algebro geometric approach to the study of first order algebraic differential equations and computer algebraic approach is given. The algebro geometric approach is used to obtain bound of the degree of rational solutions of a first order algebraic differential equation with algebraic genus greater than one and the number of rational solutions of a first order algebraic differential equation. Matsuda's and Eremenko's algorithms are explicitly given by computer algebra. The algebraic general solutions of first order algebraic differential equations were studied by using of the birational transformations of algebraic curves, and an algorithm was presented to get an algebraic general solution of first order algebraic differential equations without movable critical point if the algebraic general solution exists. We also present a polynomial algorithm for the uniform solutions of first order algebraic differential equations with constant coefficients. All of the algorithms are implemented by Maple.

References

[1] G. Chen and Y. Ma, *A computer algebra approach to first order algebraic differential equations*. Constructive and Invariant Methods In Algebraic and Differential Equations — The Sixth International Workshop on Mathematics Mechanization, Shanghai, China, May 19–21, 2004.

[2] G. Chen and Y. Ma, *Rational solutions of algebraic differential equations*. The Third International Congress of Chinese Mathematicians, Hong Kong, December 17–22, 2004.

[3] G. Chen and Y. Ma, *Algebraic solutions of a first order algebraic differential equation*, Preprint, Laboratory of P. Painlevé, 2004.

[4] G. Chen and Y. Ma, *Algorithmic reduction and rational general solutions of first order algebraic differential equations*, DESC 2004, D., Wang eds, 2005.

[5] A. Eh. Eremenko, Rational solutions of first-order differential equaitons. *Ann. Acad. Sci. Fenn.*, **23** (1998), 181–190.

[6] V. V. Golubev, Lectures on the analytic theory of diffeential equations. 2nd ed. Moscow–Leningrad: gos. Izd. Tekh. Teor. Lit. **436** p. (1950). (Russian, Chinese translation and German translation are available).

[7] M. Matsuda, *First Order Alebraic Differential Equations — A Differential Algebraic Approach*, Lecture Notes in Math. **804**, Springer-Verlag, Berlin, 1980.

[8] P. Painlevé, Leçons sur la théorie analytique des équations différentielles, 1896.

[9] H. Poincaré, Sur un théorème de M. Fuchs, *Acta Math.*, **7** (1885), 1-32. Also in *Oeuvres de Henri Poincaré*, Vol. **1**, Gauthiers-Villars et Cie, Paris, 1928.

Acknowledgment

The author is partially supported by the NKBRSF of China (No. 2004CB318000), the NNSF (No. 10301032) and by a CNRS—K. C. WONG fellowship during his visit to the Laboratoire P. Painlevé, Université de Lille 1, France.

On Computing Network Prestige

Wai-Ki Ching
Department of Mathematics
The University of Hong Kong,
Pokfulam Road, Hong Kong.

Abstract

The computation of network prestige is an important issue in studying networks such as the WWW, social networks and epidemic networks. A number of iterative methods based on solving the dominant eigenvector have been proposed for computing the prestige of symmetric or asymmetric network whose problem size is huge. The PageRank algorithm has been successfully applied in the computation of ranking of webpages. In this talk, we propose a revised PageRank algorithm for the computation of prestige of a general network and extend it to handle the case when there are negative relations among the members in the network.

Math Authoring on Xfy

Masaki Kume, Atsushi Miyamoto, Hiroshi Kai and Matu-Tarow Noda
Ehime University
Matsuyama, Japan

Abstract

Xfy is a framework provided by JUSTSYSTEM for authoring and editing compound XML documents. It enables us to handle multiple XML vocabularies, such as MathML, SVG, and so on, in a workspace. Furthermore it has extensible architecture (plugin and VCD) to manage foreign XML vocabularies. In this talk, we provide two types of plugins for authoring MathML presentation markup. One is MathML editor and another is 2D/3D plot to view algebraic functions. Editing MathML documents by the editor, the plots are updated in real time. We can apply these plugins and xfy for interactive educational contents.

Session 2:

Young Researchers Session

Organizers:

Stanly Steinberg and Tateaki Sasaki

An Interactive Algorithm Animation System for the Buchberger Algorithm

Hiromasa Nakayama, Kosuke Kuwahara
Kobe University
Kobe, Japan

Abstract

Computer algebra systems give an answer for a given problem after a heavy computation. However, it is not easy to modify the procedure of the computation interactively. Since the performance of the Buchberger algorithm changes depending on what strategy we chose, it will be worth doing to build a system to perform the Buchberger algorithm interactively. We will suppose a new interactive and animated interface for the Buchberger algorithm. In addition to this, our system aims at a system which is fun to use.

Combinatorial Criteria for Gröbner Bases

John Perry
Department of Mathematics
North Carolina State University
Raleigh, NC, United States

Abstract

Gröbner bases are an important tool of computer algebra, with applications to many fields. Their computation usually requires many reductions of S-polynomials. These reductions are computationally expensive. Bruno Buchberger discovered that sometimes we can skip the reduction of some S-polynomials. Since his two criteria consider only the leading terms of the polynomials, we call them combinatorial.

A question arises: are there other combinatorial criteria that allow us to skip S-polynomial reduction? We provide the necessary and sufficient conditions on three leading terms (the usual number used in implementation), revealing that additional combinatorial criteria exist. We also investigate how often these criteria allow us to skip an S-polynomial reduction.

Factorization of Multivariate Polynomials by Extended Hensel Construction

Daiju Inaba
Venture Business Laboratory
University of Tsukuba
Tsukuba-shi, Ibaraki 305-8571, Japan

Abstract

The extended Hensel construction is a Hensel construction at an unlucky evaluation point for the generalized Hensel construction, and it allows as to avoid shifting the origin in multivariate polynomial factorization. We have implemented a multivariate factorization algorithm which is based on the extended Hensel construction, by solving a leading coefficient problem which is peculiar to our method. We describe the algorithm and present some experimental results. Experiments show that the extended Hensel construction is quite useful for factoring multivariate polynomials which cause large expression swell by shifting the origin. We compare our algorithm with a conventional orthodox algorithm and an enhanced version by Wang's technique. We found that, for typical polynomials which cause large expression swells by the origin shifting, our algorithm is about 50 - 1000 times faster than the orthodox algorithm and about 20 - 200 times faster than the enhanced version.

Algorithm for Local Cohomology Classes Attached to an Isolated Hypersurface Singularity - Toward Computing Standard Bases -

Takayuki Abe and Shinichi Tajima
Graduate School of Science and Technology, Faculty of Engineering
Niigata University
Niigata, Japan

Abstract

In treating a hypersurface having singular points, we often perform a concrete analysis by computing the standard base of Jacobi ideal to solve a membership problem. When the defining polynomial has no parameter, we can perform various calculations with the standard base algorithm by Mora and by Lazard. On the other hand, when the defining polynomial has parameters, we face various difficulties in actual computing. In this talk, using Grothendieck duality, we develop a new method for computing standard bases. The key idea is to use an algorithm for local cohomology. The method developed is quite effective for polynomials containing parameters.

Algorithms for Partial Fraction Decomposition via Differential Equations

Takumu Shoji and Shinichi Tajima
Graduate School of Science and Technology, Faculty of Engineering
Niigata University
Niigata, Japan

Abstract

By using differential operators, we obtain new algorithms for partial fraction decomposition of rational functions. The new algorithms have the following advantages. It is fast by working in some quotient fields. It is particularly efficient and display its power, when the factors of denominator of rational functions have high multiplicity. It is suitable for "complete" partial fraction decomposition of rational functions. We also estimate efficiency of the new algorithms on computer experiments.

Hamiltonian Normal Form Computations Through Invariant Theory

Guillem Huguet and Jesús F. Palacián
Departamento de Matemática e Informática
Universidad Pública de Navarra
Pamplona, Spain

Abstract

We classify all possible Williamson normal forms related to a quadratic polynomial Hamiltonian of n degrees of freedom, with n arbitrary. Then, given a semisimple part of the quadratic Hamiltonian, we compute a fundamental set of invariants as well as a basis of its linearly independent invariants for a given degree. We consider Hamiltonian functions of the form:

$$\mathcal{H}(\mathbf{x}) = \mathcal{H}_0(\mathbf{x}) + \mathcal{H}_1(\mathbf{x}) + \ldots,$$

where $\mathbf{x}$ is a $2n$-dimensional vector in the coordinates $x_1, \ldots, x_n$ and respective momenta $X_1, \ldots, X_n$. Each $\mathcal{H}_i$ is a homogeneous polynomial in $\mathbf{x}$ of degree $i+2$. We present a combinatorial method to generate all possible normal forms corresponding to any $\mathcal{H}_0$ with n arbitrary. This classification is based on the type and number of indecomposable eigenspaces of the matrix A associated with the linear differential system derived from $\mathcal{H}_0$, and the number of normal forms is closely related to the number of partitions of the dimension of the system. Once we have determined all possible normal forms of the Hamiltonian, we compute all polynomials invariant under the action of the uniparametric group associated with $\mathcal{H}_0$. The number of linearly independent polynomial invariants of a certain degree is given by the coefficients of the Hilbert-Poincaré series associated with the action of the group aforementioned. Then, these invariants are found after solving a system of Diophantine equations. In this case we have restricted ourselves to semisimple normal forms. We have built a collection of routines and packages with MATHEMATICA to deal with the computation of the invariants and the corresponding normal forms. This contribution is part of the PhD Thesis of G. H.

Families of Factorizations of Linear Partial Differential Operators

Shemyakova Ekaterina
kath@risc.uni-linz.ac.at
Research Institute for Symbolic Computations (RISC)
J. Kepler University
Linz, Austria

Abstract

It is stated that whenever there is a factorization of given linear partial differential operator (into arbitrary number of factors of an arbitrary order), there is a family of factorizations of the same operator (an explicit formulas for the coefficients are found).

Hence, looking for factorization one may assume some of coefficients are one without loss of generality and, therefore, simplify the problem.

Session 3:

Approximate Algebraic Computation

Organizers:

Robert M. Corless

Tateaki Sasaki

Matu-Tarow Noda and Kiyoshi Shirayanagi

The Nearest Multivariate System with Given Root Structure

Scott Pope, Agnes Szanto
North Carolina State University
Raleigh, NC, USA
srpope@ncsu.edu, aszanto@ncsu.edu

Abstract

Let $f_1, \ldots, f_s$ be polynomials in $x_1, \ldots, x_n$ with finitely many common roots. Assume that $f_1, \ldots, f_s$ has roots with multiplicities, which can be described by the vanishing of certain derivatives of $f_1, \ldots, f_s$ at the roots. Given the root multiplicities, we would like to recover the roots of the system. However, even small perturbations of the coefficients can completely destroy the above root structures. This is the reason that in numerical computations handling the above systems is a major challenge: convergence to the solution is slow and the output is unreliable, or no output is returned. We propose an iterative method, which for a given (perturbed) system $F_1, \ldots, F_s$ and given root structure, computes the nearest system $f_1, \ldots, f_s$ which has roots with the given structure. The method also computes the common roots of $f_1, \ldots, f_s$ simultaneously. Similar results were only known previously in the univariate case [1, 2, 3], and our result is a generalization of them to the multivariate case.

References

[1] Zhi Lihong and Wu Wenda. Nearest Singular Polynomials. *Journal of Symbolic Computation,* 26(6):667-675, 1998.

[2] Zhonggang Zeng. Computing multiple roots of inexact polynomials. *Mathematics of Computation,* July 14, 2003.

[3] M.A. Hitz and E. Kaltofen. Efficient algorithms for computing the nearest polynomial with constrained roots. *Proc. 1998 Internat. Symp. Symbolic Algebraic Comput. (ISSAC'98),* 236-243, 1998.

On the Location of Zeros of a Complex Interval Polynomial

Hiroshi Sekigawa and Kiyoshi Shirayanagi
NTT Communication Science Laboratories
Nippon Telegraph and Telephone Corporation
3-1 Morinosato Wakamiya, Atsugi-shi, Kanagawa, 243-0198 Japan

Abstract

Given a univariate complex interval polynomial F, we provide a rigorous method for deciding whether or not there exists a polynomial in F that has a zero in a prescribed closed complex domain D. We use circular intervals and assume that the boundary C of D is a simple curve and that C is a union of a finite number of arcs, each of which is represented by a rational function. When D is not bounded, we assume further that all of the polynomials in F have the same degree. Examples of such domains are the outside of an open circle and a half-plane with boundary. The decision method uses the representation of C and the property that a polynomial in F is of degree one with respect to each coefficient regarded as a variable.

Polynomial Root-Finding with Matrix Eigen-Solving

Victor Pan
City University of New York
USA

Abstract

Numerical matrix methods are increasingly popular for polynomial root-finding. This approach usually amounts to the application of the QR algorithm to the highly structured Frobenius companion matrix of the input polynomial. The structure, however, is routinely destroyed already in the first iteration steps. To accelerate this approach, we exploit the matrix structure of the Frobenius and generalized companion matrices, employ various known and novel techniques for eigen-solving and polynomial root-finding, and in addition to the Frobenius input allow other highly structured generalized companion matrices. Employing polynomial root-finders for eigen-solving is a harder task because of the potential numerical stability problems, but we found some new promising directions, particularly for sparse and/or structured input matrices.

An Algebraic Method for Separating Close-root Clusters and the Minimum Root Separation

Tateaki Sasaki and Fujio Kako
Institute of Mathematics, Department of Information Science
University of Tsukuba, Nara Women's University
Japan

Abstract

Given a univariate polynomial over **C**, we discuss two topics, an algebraic method for separating a factor of mutually close roots from the polynomial, and a reasonable formula for the minimum root separation, by assuming that the close roots form well-separated clusters. The technique we use is very original and effective; we move the origin near to the center of a close-root cluster, then we are able to treat the other roots collectively, reducing the problem to a very simple one. Following this idea, we present a very simple and stable algebraic method for separating the close-root cluster, derive two lower-bound formulas for the distance between two close roots, and obtain a fairly simple lower bound of the minimum root separation of polynomials over **C**.

A Fast Rank-Revealing Method for Sylvester Matrix

Bingyu Li, Zhuojun Liu, Lihong Zhi
Key Laboratory of Mathematics Mechanization
AMSS, Beijing China 100080

Abstract

We propose a fast algorithm for computing Sylvester matrix's numeric rank and apply it to compute approximate GCD of univariate polynomials with floating-point coefficients. This fast rank-revealing method is based on a stabilized version of the generalized Schur algorithm in [1]. All computations can be done in $O(n^2)$ operations, compared with $O(n^3)$ operations needed in [2], where n is the sum of the degrees of polynomials.

References

[1] S.Chandrasekaran and A.H.Sayed, A fast stable solver for nonsymmetric Toeplitz and quasi-Toeplitz systems of linear equations, *SIMAX, vol.19, no.1, pp. 107-139, 1998.*

[2] Li,T.Y. and Zeng, Z. A rank-revealing method and its application, to appear: SIAM J. Matrix Anal. Appl.

On the Approximate GCD in Initial Value Problems

Stephen M. Watt

Abstract

The computation of approximate greatest common divisors of polynomials has been considered by a number of authors under various different assumptions. Approximate GCDs have a number of applications, and have been used as an approach to ill-conditioned algebraic equations [Noda and Sasaki, J Comp and App Math 1991].

This paper examines the application of the approximate GCD to initial value problems. We consider initial value problems of the form $\left[\sum_{i=0}^{n} a_i D^i\right] y(t) = f(t)$ where a_i and $y^{(i)}(0)$ are given constants. Under appropriate conditions, equations such as this may be solved by integral transform methods.

From the Laplace transform of the initial value problem, we see that $\mathcal{L}[y(t)](s)$ is a rational function whenever $\mathcal{L}[f(t)](s)$ is a rational function. Depending on a_i and $y^{(i)}(0)$, there may be a non-trivial approximate GCD between the numerator and denominator of $\mathcal{L}[y(t)](s)$. This paper examines the consequences of this fact and shows how the approximate GCD may be used to remove spurious singularities.

An Implementation Issue on SNAP and Significant Digits

Kosaku Nagasaka
Faculty of Human Development,
Kobe University,
3-11 Tsurukabuto, Nada-ku, Kobe 657-8501, Japan

Abstract

In the approximate factorization and the approximate GCD of numerical or empirical polynomials, we handle inexact coefficients. The algorithms constructed so far work well on several CASs. From the practical point of view, bounding errors by norms is not so effective as using floating-point numbers, since we have a few kind of significance arithmetics for floating-point numbers, *Mathematica*'s or Kako and Sasaki's for example. In this talk, for numerical or empirical polynomials with coefficients with significant digits, absolute irreducibility testing for bivariate polynomials and relative primality testing for univariate polynomials are formulated without using norms. Basically, our formulation is not so different from original formulation, but it will be more natural for those who use significance arithmetics. We demonstrate the difference between our formulation and conventional one based on the norm.

Session 4:

Computational Algebraic Structures and Engineering Applications

Organizers:

Alain Bretto

Bernard Laget and Luc Gillibert

Computational Approach to Nonlocal BVP by Multivariate Operational Calculus

Ivan Dimovski, Margarita Spiridonova
Institute of Mathematics and Informatics,
Bulgarian Academy of Sciences
Sofia, Bulgaria

Abstract

A large class of linear nonlocal Boundary Value Problems (BVP) for the classical equations of mathematical physics in finite domains is considered. It is assumed that a part of the boundary-value conditions are local and the others are nonlocal. Using a multivariate operational calculi, algebraization of each problem is made. Thus explicit Duhamel-type representation of the solution is obtained, using one special solution satisfying simple boundary-value conditions. The general solution is obtained as a multivariate convolution, which could be used successfully for numerical computation of the solution.

The algorithms are implemented using the computer algebra system *Mathematica*.

Hardware Implementation of a Geometric Algebra Processor Core

Biswajit Mishra and Peter Wilson
Electronics Systems Design, School of Electronics and Computer Science
University of Southampton
Southampton, United Kingdom

Abstract

The widespread use of Computer Graphics and Computer Vision applications has led to a plethoraof hardware implementations that are usually expressed using linear algebraic methods. There are two drawbacks with this approach that are posing fundamental challenges to engineers developing hardware and software applications in this area. The first is the complexity and size of the hardware blocks required to practically realise such applications particularly multiplication, addition and accumulation operations. Whether the platform is Field Programmable Gate Arrays (FPGA) or Application Specific Integrated Circuits (ASICs), in both cases there are significant issues in efficiently implementing complex geometric functions using standard mathematical techniques, particularly in floating point arithmetic. The second major issue is the complexity required for the effective solution of complex multi-dimensional

problems either for scientific computation or for advanced graphical applications. Conventional algebraic techniques do not scale well in hardware terms to more than 3 dimensional problems, so a new approach is desirable to handle these situations.

In this paper we describe a scalable n-dimensional geometric algebra processor core architecture realisable using an FPGA or ASIC platform. The designer can easily specify the floating point resolution, the order of the computation and also configure the trade-offs between IC area and speed. The VHDL has been synthesised and optimised for an FPGA platform and is re-targeted to an ASIC platform. A sub-pipelined approach has been used to reduce the area requirements and keep the throughput at a rate useful for practical real time applications.

Generalized Stewart Platforms and their Direct Kinematics

Xiao-Shan Gao
Institute of Systems Science, AMSS,
Academia Sinica,
Beijing 100080, China.

Abstract

In this talk, we introduce the generalized Stewart platform (GSP) consisting of two rigid bodies connected with six distance and/or angular constraints between six pairs of points, lines and/or planes in the base and the moving platform respectively. GSP could be considered as the most general form of parallel manipulators in certain sense. We show that there exist 16 forms of 2D GSPs and 3850 possible forms of 3D GSPs. With help of computer algebra techniques, we give the upper bounds for the number of solutions of the direct kinematics for all the 3D GSPs. We also obtain closed-form solutions and the best upper bounds of real solutions of the direct kinematics for a class of 1120 GSPs and all 2D GSPs.

On Symbolic Geometric Computation with Conformal Geometric Algebra

Hongbo Li
Key Laboratory of Mathematics Mechanization
Chinese Academy of Sciences
Beijing 100080, China

Abstract

Coordinate approach to symbolic geometric computation is limited by tremendous difficulties coming from middle expression swell. Invariant-theoretical method is applicable to projective geometry and affine geometry, but is far from being well-established in that basic computing problems like representation, expansion, contraction and factorization are either open or overlooked. Reducing the middle expression swell is not taken care of. Symbolic computation in Euclidean geometry with Geometric Algebra gives rise to more problems which are much more difficult to solve.

In this talk, we show that contrary to the common observation that invariant algebra introduces succinct algebraic description of geometric problems with the cost of significant complication in algebraic manipulation, by means of new invariant frameworks, new guidelines and new techniques for invariant computing, we can achieve amazing simplification in algebraic manipulation.

Our work in this direction includes a new invariant framework called Conformal Geometric Algebra, which is a hierarchy of geometric covariants and invariants induced by the Grassmann product and Clifford product. It is currently being used in computer vision, graphics and engineering in many research institutions around the world, and plays the central role in our Euclidean geometric computing. We further propose a new guideline for invariant computing to control the size of the middle expression at every minimum step, called BREEFS – Bracket-oriented Representation, Elimination, Expansion for Factored and Shortest result. We establish a series of new powerful techniques for invariant computing: expansion, contraction, factorization and geometric transformation.

The new framework, guideline and techniques being applied to symbolic geometric computation, can lead to significant improvement in computational efficiency, and thus lead to the solving of some hard geometric computing problems which defy any efforts of using either coordinates or classical invariant methods.

Construction and Recognition of G-graphs

***Alain Bretto*[1], *Luc Gillibert*[1], *Bernard Laget*[2], *Maria C. Marino*[3]**
(1) ***Université de Caen, GREYC CNRS UMR 6072.***
Campus II Bd Marchal Juin, BP 5186, 14032 Caen cedex, France.
(2) ***École Nationale d'Ingnieurs de Saint-Etienne.***
58 rue Jean Parot, 42023 Saint-Etienne cedex 02, France.
(3) ***University of Messina, Department of Mathematics.***
Contrada Papardo, Salita Sperone 31, 98166, Sant'Agata, Messina, Italy.

Abstract

An important part of the computer science is focused on the links that can be established between group theory and graph theory. Cayley graphs can establish such a link but meet some limitations. This paper introduces a new type of graph associated to a group: the G-graphs. We present an algorithm constructing efficiently these new graphs. Then we present the G-graph recognition problem and we exhibit a new algorithm based on the exploration of the `SmallGroups` library from GAP [3] for solving this problem. With this algorithm we establish a library of the most common G-graphs and we show that many graphs, as the generalized Petersen graphs $P_{8,3}$, $P_{4,1}$ and $P_{12,5}$, are G-graphs. More details and properties about the G-graphs are given in [1, 2].

References

[1] A. Bretto and L. Gillibert. *Graphical and computational representation of groups*, LNCS 3039, Springer-Verlag pp 343-350. Proceedings of ICCS'2004.

[2] A. Bretto and L. Gillibert. *Symmetric and Semisymmetric Graphs Construction Using G-graphs*. Accepted for the International Symposium on Symbolic and Algebraic Computation (ISSAC 2005).

[3] The GAP Team, (06 May 2002), *GAP - Reference Manual*, Release 4.3. http://www.gap-system.org

---

Session 5:

Computer Algebra and Coding Theory

Organizers:

Edgar Martinez-Moro

Ilias Kotsireas

M. Angel Borges-Trenard and Mijail Borges-Quintana

Littlewood Polynomials with High-Order Zeros

Daniel Berend and Shahar Golan
Department of Computer Science
Ben-Gurion University of the Negev
Beer-Sheva, Israel

Abstract

Let $S(N) = \{-1, 1\}^N$. A word $(a_0, a_1, ..., a_{N-1})$ in $S(N)$ is an *m-th order spectral-null word* if the polynomial $a_0 + a_1x + a_2x^2 + ... + a_{N-1}x^{N-1}$ is divisible by $(x-1)^m$. Denote by $S(N, m)$ the set of all m-th order spectral-null words of length N. Any subset of $S(N, m)$ is an *m-th order spectral-null code (SNC)* of length N. High-order SNC's can be used for error correcting and detecting purposes. In particular, the minimum Hamming distance of an m-th order SNC is at least $2m$. These codes improve the reliability of digital communication over noisy partial response channels. Let $N^*(m)$ be the minimal length of a polynomial with ± 1 coefficients divisible by $(x-1)^m$. In previous works, the value of $N^*(m)$ was found for every $m < 8$. Here we prove that $N^*(8) = 144$. Similarly, let $m^*(N)$ be the maximal power of $(x-1)$ dividing some polynomial of degree $N-1$ with ± 1 coefficients. We extend the range of N's with known $m^*(N)$ from $N < 88$ to $N < 168$.

Gröbner Bases Combinatorics for Binary Codes

M. Borges-Quintana, M.A. Borges-Trenard
Departamento de Matemáticas,
Universidad de Oriente, Cuba.
mijail@csd.uo.edu.cu, mborges@mabt.uo.edu.cu
E. Martínez-Moro
Departamento de Matemática Aplicada,
Universidad de Valladolid. edgar@maf.uva.es

Abstract

We show how many combinatorial properties of binary codes such as finding the codewords of minimal weight and decomposition of all the codewords can be studied with the help of a Gröbner basis associated to the monomial ideal associated to the code. Moreover, taking into account the connection between cycles in graph and binary codes, the set of cycles in a graph is a binary linear code of a certain vector space associated with the structure of the graph, with the help of the Gröbner basis we will obtain all the minimal cycles of a graph according to their lengths (the length of a cyclic is the number of edges).

Hadamard Matrices and Self-Dual Codes

I. S. Kotsireas and C. Koukouvinos

Abstract

1 Introduction

We propose an algebraic approach to the construction of Hadamard matrices and self-dual codes. Hadamard matrices with specific structure (one circulant core, two circulant cores [2], Williamson array with four and eight matrices, orthogonal designs, Goethals-Seidel array) have been constructed with computational algebra methods. The resulting sets of Hadamard matrices have been used to establish new lower bounds for the numbers of inequivalent Hadamard matrices in many orders. The doubling construction in conjunction with the usage of the symmetric group, yields astronomical new lower bounds for Hadamard matrices of order $8t$. The Magma Databases for Hadamard and skew-Hadamard matrices, contain matrices that were constructed in this manner. The purpose of this paper is to present an application in Coding Theory, based on a theorem of Tonchev.

2 Basic Coding Theory definitions and notations

Let $F = GF(2)$. A linear $[n, k]$ code C over F is a k-dimensional vector subspace of F^n. The elements of C are called codewords and the weight $wt(x)$ of a codeword x is the number of non-zero coordinates in x. The minimum weight of C is defined as $\min\{wt(x) \mid 0 \neq x \in C\}$. An $[n, k, d]$ code is an $[n, k]$ code with minimum weight d. A matrix whose rows generate the code C is called a generator matrix of C. The dual code $C^{\perp}$ of C is defined as $C^{\perp} = \{x \in F^n | x \cdot y = 0 \quad for\ all \quad y \in C\}$. If $C \subset C^{\perp}$, C is called a self-orthogonal code. C is called self-dual if $C = C^{\perp}$. Furthermore C is called doubly-even if the weights of all codewords of C are a multiple of four. A self-dual code is called singly-even if there exists at least one codeword whose weight is $\equiv 2 (mod 4)$.

A self-dual code is extremal if it has the largest possible minimum weight for the given length. For every doubly-even $[n, n/2, d]$ self-dual code, n is a multiple of 8 with $d \leq 4[n/24]+4$.

Conway and Sloane [1] give a list of the possible weight enumerators of binary extremal self-dual codes and details on the largest possible minimum weight for each length. The existence of some extremal self-dual codes is an open question in [1].

See [3] for more on self-dual codes.

3 A theorem of Tonchev

By J_n we denote the $n \times n$ matrix with all its entries equal to 1 while I_n denotes the identity matrix of order n.

Theorem 1 *Let H be a Hadamard matrix of order $n = 8t + 4$ such that the number of $+1's$ in each row and column is congruent to $3 (mod 4)$. Then the following matrix*

$$(I_n,\ (H + J_n)/2),$$

generates a binary self-dual doubly-even code C of length $2n$. The minimum distance of C is at least 8 if and only if each row and column of H contain at least seven $+1's$.

The above theorem of Tonchev [4], gives a simple criterion for extremality of codes arising from Hadamard matrices of order 4, 12 and 20. Starting from a particular Hadamard matrix, one can transform it into many different (but equivalent) matrices by multiplying rows and columns by -1 so that all rows and columns contain a number of +1's congruent to $3(mod 4)$. A computer search showed that at least 79 inequivalent extremal doubly-even $[40, 20, 8]$ codes arise from the three Hadamard matrices of order 20 [4].

References

[1] J.H. Conway and N.J.A. Sloane, A new upper bound on the minimal distance of self-dual codes, *IEEE Trans. Inform. Theory*, 36 (1990), pp. 1319-1333.

[2] I. S. Kotsireas, C. Koukouvinos and J. Seberry Hadamard ideals and Hadamard matrices with two circulant cores, *Europ. J. of Combin.*, (to appear)

[3] E.M. Rains and N.J.A.Sloane, Self-dual codes, in Handbook of Coding Theory, V.Pless and W.C. Huffman, (Eds.), Amsterdam, Elsevier, 1998, pp. 177-294.

[4] V.D. Tonchev, Self-orthogonal designs and extremal doubly-even codes, *J. Combin. Theory Ser. A*, 52 (1989), pp. 197-205.

Frobenius Numbers and the Postage Stamp Problem

Daniel Lichtblau
Wolfram Research

Abstract

Given a set $A = \{a_1, \ldots, a_n\}$ of positive integers with gcd 1, it is not hard to show that all "sufficiently large" integers can be represented as a nonnegative integer combination of elements of A. The Frobenius number of the set is defined as the largest integer not so representable. The Frobenius instance problem (also called the money changing or postage stamp problem) is to determine, given a positive integer M, a set of nonnegative integers $X = \{x_1, \ldots, x_n\}$ such that $X \cdot A = n$, or else show no such set exists. We will briefly recall how this can be addressed via toric Gröbner bases.

It is known that the Frobenius number problem is NP-hard in general. For dimension 2 it is trivial (Sylvester solved in two decades before Frobenius publicized the problem). In dimension 3 a very efficient method was found independently by Greenberg and Davison. For higher dimensions some quite effective methods are known for the case where one element of A is not too large (say, less than 10^7).

Recent work has given rise to methods that are effective when the above restrictions do not hold, although the dimension must be bounded by 10 or so. It turns out that there is a way to recast this work using toric Gröbner bases, wherein the "fundamental domain" for the set A is given by the staircase of the basis with respect to a particular ordering. It is reasonably efficient in dimension 4 or 5,

when the elements in the set are as large as 10^{11} or so. We will illustrate this.

Session 6:

Computer Algebra in Quantum Information and Computation

Organizers:

Yasuhito Kawano and Kiyoshi Shirayanagi

An Algorithm for Decomposing Unitary Matrices Using Cartan Decomposition

Yumi Nakajima, Yasuhito Kawano, and Hiroshi Sekigawa
NTT Communication Science Laboratories, NTT Corporation
3-1 Morinosato-Wakamiya, Atsugi, 243-0198, JAPAN

Abstract

We provide an algorithm for decomposing an arbitrary unitary matrix into a sequence of elementary operations, such as single-qubit rotations and CNOT gates. The algorithm is based on Cartan decomposition in Lie algebra theory. We also present a canonical decomposition of the quantum Fourier transform (QFT) by our algorithm and show that our algorithm decomposes the QFT into $O(n^2)$ elementary gates, which is similar to the well-known QFT circuit.

Computer Algebra-Aided Tool for Simulation of Quantum Circuits

Vladimir P.Gerdt and Vasily Severyanov
Laboratory of Information Technologies
Joint Institute for Nuclear Research
141980 Dubna, Russia
gerdt@jinr.ru severyan@jinr.ru

Abstract

In [1] it was shown that elements of the unitary matrix determined by a quantum circuit can be computed by counting the number of common roots in Z_2 for a certain set of multivariate polynomials over Z_2. Given a quantum circuit, the polynomial set is uniquely constructed. In this talk we present a C# package called QP (Quantum Polynomials) that allows a user to assemble a quantum circuit and to generate the multivariate polynomial set associated with the circuit.

The generated polynomial system can further be converted into the canonical Gröbner basis form for the lexicographical monomial order. Gröbner bases form the most universal algorithmic tool of modern computer algebra to investigate and solve systems of polynomial equations [2]. Construction of the lexicographical Gröbner basis substantially alleviates the problem of the root finding for polynomial systems. To construct such a Gröbner basis one can use efficient involutive algorithms developed in [3]. Our QP package together with a Gröbner basis software provides a tool for simulation of quantum circuits. We illustrate this tool by example from [1].

References

[1] Christopher M. Dawson et al. Quantum computing and polynomial equations over the finite field Z_2. *arXiv:quant-ph/0408129*, 2004.

[2] B.Buchberger and F.Winkler (eds.) *Gröbner Bases and Applications*. Cambridge University Press, 1998.

[3] Gerdt V.P. Involutive Algorithms for Computing Gröbner Bases. *Proceedings of the NATO Advanced Research Workshop "Computational commutative and non-commutative algebraic geometry"* (Chishinau, June 6-11, 2004), IOS Press, 2005.

On Generalized Quantum Turing Machine and its Application

Satoshi Iriyama and Masanori Ohya
Tokyo University of Science, Department of Information Sciences
Noda City, Chiba, Japan

Abstract

Ohya and Volovich have proposed a new quantum computation model with chaotic amplification to solve the SAT problem, which went beyond usual quantum algorithm. In this talk, we generalize quantum Turing machine by rewriting usual quantum Turing machine in terms of channel transformation. Moreover, we define some computational classes of generalized quantum Turing machine and show that we can treat the Ohya-Volovich (OV) SAT algorithm.

Semidefinite Programming for the Equivalence of Finite Automata and Quantum Circuits

***David Avis*[1]*, Takeshi Koshiba*[2]*, Kazuo Iwama*[3] *and Rudy Raymond*[3]**
[1] ***School of Computer Science, McGill University***
Montreal, Canada
[2] ***Department of Information and Computer Sciences, Saitama University***
Saitama, Japan
[3] ***Graduate School of Informatics, Kyoto University***
ERATO, JST Imai Quantum Computation and Information
Kyoto, Japan

Abstract

Two deterministic finite automata (DFA) are equivalent if they accept exactly the same language. It is well known that there exists an efficient algorithm to check the equivalence of DFA which furthermore enables the minimization of DFA's states. With respect to probabilistic finite automata (PFA), two probabilistic (quantum) automata are exactly (approximately) equivalent if the two automata accept every string with exactly (approximately) the same probability. Tzeng showed a polynomial-time algorithm for checking their equivalence. His results have been extended by Koshiba for checking the exact equivalence of two quantum finite automata (QFA). In this draft, we show the Semidefinite Programming (SDP) formulation for computing the difference in accepting probability between two finite automata on input of

length at most n. As consequences, we can check the equivalence of two FAs in polynomial time, thus unifying and simplifying Tzeng and Koshiba's results. Next, we show how to extend our techniques for checking the existence of quantum circuits whose output is a given quantum state and to reduce their computational complexity by considering its Second-Order Conic Programming (SOCP) formulation.

Comparison Between Quantum Turing Machines with Advice and Circuits

Harumichi Nishimura
ERATO Quantum Computation and Information Project
Japan Science and Technology Agency
Kyoto, JAPAN

Abstract

The notion of advice, a piece of additional information to help a computation, is often used in complexity theory to discuss the power of polynomial-size circuits in terms of Turing machines. In this talk, we discuss the relationships between quantum Turing machines with advice and circuits. In classical case, it is well-known that Turing machines with polynomial-size advice and polynomial-size circuits simulate each other exactly. We show that quantum Turing machines with polynomial-size advice cannot simulate polynomial-size quantum circuits with zero-error by reducing this simulation problem to a relation between an infinite set of complex numbers and an extended field of the rational numbers. On the contrary, we show that, if quantum Turing machines are allowed to have "quantum" advice, then that simulation is possible. To present this, we discuss a decomposion of unitary matrices using algebraic properties of polynomial-time computable numbers, and Nielsen's arguments on measurement-based quantum computation. Also, extending Simon's result we present a black-box problem such that it can be solved with probability 1 by polynomial-time quantum Turing machines while it cannot be solved even by classical Turing machines with polynomial advice, i.e., classical polynomial-size circuits.

Session 7:

Computer Algebra in the Biological Sciences

Organizers:

Stanly Steinberg and Michael Wester

Symbolic-Numeric Optimization for Biochemical Models by Quantifier Elimination

***Shigeo Orii*[1,2], *Katsuhisa Horimoto*[2] *and Hirokazu Anai*[3]**

[1]***Science Solutions Group***

FUJITSU LTD.

Chiba, Japan

[2]***Laboratory of Biostatistics***

Institute of Medical Science, University of Tokyo

Tokyo, Japan

[3]***IT Core Laboratories***

FUJITSU LABORATOLIES LTD./JST, CREST.

Kawasaki, Japan

Abstract

The sequencing of complete genomes allows analyses of interactions between various biological molecules on a genomic scale, which prompted us to simulate the global behaviors of biological phenomena on the molecular level. One of the basic mathematical problems in the simulation is the parameter optimization in the biochemical model for complex dynamics, and many optimization methods have been designed. Here, we introduce a new approach to optimize the parameters in biochemical models by quantifier elimination (QE), in combination with numerical simulation methods. The optimization method was applied to a model for the inhibition kinetics of HIV proteinase with ten parameters and nine variables, and attained the goodness of fit to 300 points of observed data with the same magnitude as that obtained by the previous optimization methods, remarkably by using only one or two points of data. Furthermore, the utilization of QE demonstrated the feasibility of the present method for elucidating the behavior of the parameters and the variables in the analyzed model. The present symbolic-numeric method is therefore a powerful approach to reveal the fundamental mechanisms of biochemical models, in addition to being a computational engine.

Molecular Loop Closure

Evangelos A. Coutsias and Michael J. Wester
Department of Mathematics and Statistics /
Division of Biocomputing, Biochemistry and Molecular Biology
University of New Mexico
Albuquerque, New Mexico, USA

Abstract

Determining the three-dimensional structure of a molecule from its chemical composition is the central problem of stereochemistry. Especially for large macromolecules with complex topologies and unique compositions, such as proteins and nucleic acids, the extreme complexity of the configuration space makes this problem one of the grand challenges of our time. The recent advances in the field of genomics have resulted in ever increasing numbers of proteins whose sequence can be deduced from the genome, but whose structure and function are not understood. Computer prediction has thus become an increasingly alluring alternative to costly and time consuming experimental structure determination, such as by crystallographic or NMR techniques.

In this talk, we will discuss the molecular loop closure algorithm for finding the ensemble of possible backbone conformations of a chain segment of a protein geometrically consistent with the preceding, intermediate and following portions of the chain whose structures are given. This problem can be reduced to finding the real roots of a 16th degree univariate polynomial, whose solutions will yield sets of six dihedral angles. These sets of dihedral angles can be substituted for those found in the original structure to produce alternative conformations of the backbone segment. This methodology is based on ideas from the robotics literature involving kinematics of the equivalent rotor linkage for the most general case of oblique rotors. We have implemented a version of this algorithm in Maple.

Session 8:

Computational Topology and Geometry

Organizers:

Dmytro Chibisov

Victor Ganzha and Ernst W. Mayr

Computing the Stratification of Actions of Compact Lie Groups

Thomas Bayer
Institut für Informatik
Technische Universität München
Boltzmannstr. 3, 85748 Garching, Germany
bayert@in.tum.de

Abstract

We provide a constructive approach to the stratification of the representation- and the orbit space of linear actions of compact Lie groups contained in $GL_n(\mathcal{R})$ on $\mathbf{R}^n$ and we show that any d-dimensional stratum, respectively, its closure can be described by d sharp, respectively, relaxed polynomial inequalities and that d is also a lower bound for both cases. Strata of the representation space are described as differences of closed sets given by polynomial equations while d-dimensional strata of the orbit space are represented by means of polynomial equations and inequalities. All algorithms have been implemented in SINGULAR V2.0.

Determine the Topology of Real Algebraic Surfaces

Jin-San Cheng, Xiao-Shan Gao and Ming Li
Institute of Systems Science, AMSS
Academia Sinica
Beijing 100080, China
Email: xgao@mmrc.iss.ac.cn

Abstract

In this talk, an algorithm is proposed to determine the topology of an implicit real algebraic surface in R^3. The algorithm consists of four steps: surface projection, projection curve topology determination, surface patch composition, and combination of surface patches. The algorithm gives an intrinsic representation for the topology of the surface. Some examples are used to show that the algorithm is effective.

On the Construction of Robot Navigation Function on Semi-Algebraic Sets

Dmytro Chibisov
Institut für Informatik
Technische Universität München
Email: chibisov@in.tum.de

Abstract

The construction a scalar valued "navigation" function for the specification of robot tasks is a well-known problem. Given the initial and final position of a robot as well as a set of semi-algebraic obstacles, the navigation function is required to rise in the vicinity of obstacles in the direction towards them and to decrease monotonously along some path from the initial to the final position, if and only if the path does not intersect any obstacle. In this way the problem of calculation of the collision-free path can be solved in a computationally efficient manner by reduction to the task of following the gradient of the navigation function. In the present paper, we present a new family of analytic navigation functions and investigate their properties for a large class of geometric optimization problems.

Understanding Volumes from an Algebraic Topological Perspective

R. González-Díaz, B. Medrano, P. Real, J. Sánchez Peláez
Dpto de Matemática Aplicada I
E.T.S. Ingeniería Informática
Universidad de Sevilla

Abstract

Roughly speaking, in this talk we show how to use an algebraic-topological technique developed by the authors, called AT-model, in problems of topological analysis, control, simplification and representation of 3D and 4D digital images.

Origami Construction of a Morley's Triangle with Automated Proof

Tetsuo Ida, Hidekazu Takahashi, Mircea Marin
Department of Computer Science,
University of Tsukuba

Abstract

We show origami construction of a Morley's triangle together with the automated proof of Morley's theorem and its generalization. Morley's theorem states that the three points of intersection of the adjacent interior trisectors of the angles of any triangle form an equilateral triangle. The whole process of origami construction and subsequent automated proof of the correctness of the intended construction is performed in a streamlined fashion by our Computational Origami System. We show that the computational origami system not only simulates origami construction to a precision of numeric and symbolic computation, but has the power of symbolic constraint solving and proving. The automated proof uses Groebner bases computation, and took over 16 hours to prove the generalized Morley's theorem.

Solving Cubic Equations by ORIGAMI

Shuichi Moritsugu
Graduate School of Library, Information and Media Studies
University of Tsukuba
Tsukuba, Japan

Abstract

We show an algebraic proof of the method for solving cubic equations by ORIGAMI (paper folding). Using ORIGAMI, we can solve the construction problems that are unsolvable in Euclidean geometry[2], such as angle trisection and doubling cubes.

In our formulation, first, we translate the geometrical conditions into polynomial relations among the coordinates of points[1]. Second, we compute a Gröbner basis of the ideal and solve the ideal membership problem. Consequently, cubic equations are solved as construction problems, and drawing a trisector of a given angle and the cubic root of 2 is clearly realized by ORIGAMI.

References

[1] S.-C. Chou. *Mechanical Geometry Theorem Proving*. D.Reidel, Dordrecht, 1988.

[2] T. Hull. A Note on "Impossible" Paper Folding. *American Mathematical Monthly, 103(3):240–241, 1996.*

Detecting Degeneracies in Robust Geometric Modeling

John Keyser, Koji Ouchi
Department of Computer Science
Texas A&M University

Abstract

Detecting degenerate configurations is an important part of a robust geometric modeling system. We focus specifically on the exact boundary evaluation problem. Most efficient methods currently available for exact boundary evaluation rely on a general position assumption, and fail in the presence of degeneracies. We describe a method for detecting degeneracies based on the Rational Univariate Reduction.

A dominating computation within boundary evaluation is finding common roots of systems of polynomials that describe the boundary of solids. Most degeneracies can be found as degenerate configurations of this system of polynomials. We propose the use of the *Rational Univariate Reduction* (RUR), also referred to as the Rational Univariate Representation, as an exact method for finding the zero sets of polynomial systems without multiplicities.

In the RUR, every coordinate of every point in the zero set of a system of polynomials is represented as some univariate polynomial evaluated at some root of the other univariate polynomial. Together with the classical root-bound approach to sign determination of algebraic numbers, we can perform exact computation over the points and curves, enabling us to detect and handle degenerate situations smoothly.

In this talk, we will present our algorithm, along with implementation issues, examples, and performance characteristics.

Automatic Discovering of Geometric Theorem by Computing Gröbner Bases with Parameters

Dingkang Wang, Long Lin
Key Lab of Mathematics Mechanization
Academy of Mathematics and Systems Sciences
Beijing, P.R. China

Abstract

A geometric statement of equality-type consists of two parts: hypothesis and conclusion. Both hypothesis and conclusion can be expressed in terms of polynomial equations in a number of free parameters $u_1, \cdots, u_m$ and a number of dependent variables $x_1, \cdots, x_n$. Typically, the hypothesis is composed of

$$\begin{cases} h_1(u_1, \cdots, u_m, x_1, \cdots, x_n) = 0, \\ \\ h_r(u_1, \cdots, u_m, x_1, \cdots, x_n) = 0, \end{cases} \tag{1}$$

where the h's are polynomials over a ground field K. The conclusion is

$$g(u_1, \cdots, u_m, x_1, \cdots, x_n) = 0 \tag{2}$$

where g is a polynomial over K.

If the geometric statement is not generically true, by computing Gröbner bases with parameters, we can find the conditions, which the parameters should satisfy, such that the conclusion (2) can be deduced from the hypothesis (1).

Session 9:

Computer Algebra in Education

Organizers:

Alkis Akritas
Michel Beaudin
Panos Vigklas and Michael Wester

This is Much More than just a New Way of Teaching Mathematics

Michel Beaudin
Service des enseignements généraux
École de technologie supérieure (ETS)
1100, Notre-Dame street west
Montréal, Québec, Canada, H3C 1K3
Email: michel.beaudin@etsmtl.ca

Abstract

Colleagues who are using technology in their mathematics teaching say they found "a new way of teaching mathematics"; others prefer to say that they are "making new from old". Well, first, don't expect your students to be as enthusiastic as can be if they stay inactive. This is where an affordable, powerful and easy to use graphing calculator with a built-in computer algebra system suitable for college mathematics and engineering coursework plays an important role. Each of our engineering students at ETS has a Voyage 200 graphing calculator in the classroom. Second, because technology, in mathematics education, is here to stay, teachers should use it to give live presentations of some mathematical concepts, exactly in the same way they use the blackboard. This is where Derive 6 plays it's important role of a mathematical assistant: we must not forget, as far as education is concerned, that both teachers and students still need time to concentrate on mathematical concepts, avoiding as much as possible typing long commands. In this talk, we will present examples of a classical way of teaching mathematics, showing that some of our "old" problems can have unexpected potential. By the way, this is another benefit of technology: different levels of mathematics are well served by it.

General Theory of Russian Roulette

Daisuke Minematsu, Satoshi Hashiba and Ryohei Miyadera
Kwansei Gakuin
Miyadera127@aol.com

Abstract

We denote by $F[p, n, m, v]$ the probability of death of the v-th player in a Russian roulette game with p players,n cylinders and m bullets, then the following pyramid-like figure has a

very interesting structure. See the second pyramid-like figure with fractions. The structure (1) was found by high school students and a freshman in a university.

$$\begin{array}{c} F[2,1,1,1] \\ F[2,2,1,1], F[2,2,2,1] \\ F[2,3,1,1], F[2,3,2,1], F[2,3,3,1] \\ F[2,4,1,1], F[2,4,2,1], F[2,4,3,1], F[2,4,4,1] \end{array} \tag{3}$$

$$\begin{array}{c} \frac{1}{1} \\ \frac{1}{2}, \frac{1}{1} \\ \frac{2}{3}, \frac{2}{3}, \frac{1}{1} \\ \frac{2}{4}, \frac{4}{6}, \frac{3}{4}, \frac{1}{1} \end{array}$$

The Practice of Practise: Persuading a Computer Algebra System to Help Mark Your Students' Work

Christopher J. Sangwin
Maths, Stats & OR Network, part of the Higher Education Academy
School of Mathematics
University of Birmingham, Birmingham, B15 2TT

Abstract

In learning and teaching Computer Algebra Systems (CAS) usually take the role of a *sophisticated calculator* which the student is expected to use. The well-documented purposes of using such a tool include, for example, reducing the computational load, so that attention may be focused on other aspects of a problem or to facilitate explorations by allowing rapid re-calculation.

This paper considers quite a different use for CAS: to support assessment by evaluating students' answers automatically as part of an online computer aided assessment or computer based learning system. In such a system the *student-provided answers* are evaluated using the CAS, resulting in an objective test. Note that a student does *not* select one (or more) teacher-provided answers as would be the case in a multiple response, or multiple choice question. Pedagogically this is an important distinction.

This paper compares systems which have taken this approach, including AiM, Wallis, CABLE and Stack. The comparison draws on the experiences of the author over the last five years with university mathematics students. It will include mathematical topics where such systems were used effectively, students' experiences and differences between implementations. In particular the differences between existing CAS systems used for this application will be considered.

The Development of a Multimedia Symbolic Vector Analysis Package

Yuzita Yaacob, Stanly Steinberg and Michael J. Wester
Kulliyyah of Engineering, International Islamic University Malaysia
Kuala Lumpur, Malaysia
Department of Mathematics and Statistics, University of New Mexico
Albuquerque, New Mexico, USA
Office of Biocomputing, University of New Mexico Health Sciences Center
Albuquerque, New Mexico, USA

Abstract

This talk discusses the process of developing a multimedia symbolic package in the area of vector analysis that will specifically aid in enhancing the existing packages and thus, make Computer Algebra Systems (CASs) more useful in the advanced undergraduate calculus courses and for solving a wider range of analysis problems. By using this package, it is hoped that the user will be able to enhance and develop his understanding in the area of vector analysis. The active learning environment provided by this package will encourage exploration, self-expression and a feeling of ownership by allowing the user to manipulate its components and thus, make learning stimulating, engaging and fun. Moreover, the multimedia elements incorporated in the solution process will help to reinforce a sensory rich environment and increase the user's curiosity and interest in approaching problem solving. The method used for developing this package consists of three phases: preliminary research phase, specification phase and implementation phase. In the preliminary research phase, we created a review table that consists of six well known CASs (i.e., Derive 6, Maple 9, Mathcad 11, Mathematica 5, MuPAD Pro 3.0 and REDUCE 3.8). The goal of this table is to provide a benchmark for comparing the above mentioned CASs in the area of vector analysis and multimedia capabilities. The outcome of this phase is a project plan which contains information about the development of the package. The next phase is the specification phase which is based on the notion of Package Requirement Specifications (PRS) that has been proposed by the National Bureau of Standards, IEEE (standard no: 830-1984) & US Dept. of Defense. PRS is produced at the culmination of the preliminary research phase. The outcome of this phase is a detailed description of the design of the package. Finally, in the implementation phase, the package will be implemented and the outcome is the first version of the package.

Introducing Maple V to Elementary Teachers of Mathematics

Yiu-Kwong Man
Department of Mathematics, The Hong Kong Institute of Education
New Territories, HONG KONG

Abstract

Almost all major education reforms in mathematics education have requested the pre-service or in-service mathematics teachers to be able to apply information technology for deepening the students' understanding of the subject contents, as well as developing the generic skills in learning, such as inquiry, problem solving and communication skills, etc. Accordingly, there are increasingly more elementary teachers using calculators, dynamic geometry software or spreadsheet in the classrooms. However, the use of computer algebra systems at elementary

teaching level is still very limited. Among some possible reasons behind, the lack of exposure of this kind of software to the elementary teachers should be taken into account. In this paper, we describe how to introduce the basics of Maple V in a local teacher training programme and demonstrate how to use it in mathematics lessons for inquiry, visualization or problem-solving. Sharing of teaching experience and views from the student teachers are also included.

Assessing the Use of CAS Technology in Secondary Schools

Karsten Schmidt
Faculty of Management Science & Economics
University of Applied Sciences (FH)
98574 Schmalkalden, Germany
Wolfgang Moldenhauer
Thuringian Institute for In-service Teacher Training,
Curriculum Development and Media (ThILLM)
99438 Bad Berka, Germany

Abstract

In 2003 a project on the effects of using the TI-89 in math education in 8 upper secondary schools in the German state of Thuringia was completed. Since assessment results showed that its effect on the students' math knowledge was slightly positive for most cohorts, and never negative, the authorities decided to move forward and allow all schools to decide if they should make the use of pocket calculators with a built-in Computer Algebra System (such as the TI-89) in math education compulsory.

Meanwhile, more than 25 (of about 100) upper secondary schools opted for the use of such calculators, as from grade 10 in most cases. Starting in 2000, a test was carried out every year in November with all grade 11 students from schools using the TI-89, and all grade 11 students from selected control schools. Naturally, the use of any electronic calculator was not permitted in these tests. This presentation investigates the effects of the use of CAS technology on the students' performance. Overall assessment results from the project as well as from recent years are investigated. It will also be analyzed if there are certain mathematical topics where students who had been using pocket calculators with built-in CAS tend to be particularly successful compared with students from control schools.

A Summary of the Role of Computer Algebra in an NSF Funded Project

Bill Pletsch
Albuquerque Technical Vocational Institute
Albuquerque, New Mexico, USA

Abstract

A summary of the NSF funded New Mexico Math Reform Project will be presented with a special emphasis on the role of computer algebra (CA). In the course of Project's existence, January 2001-March 2004, thanks to CA, some surprising mathematics was unearthed. This was especially true regarding exponential functions of the form Exp(P(x)), P(x) a polynomial.

The use of computer algebra in the instruction of this class of exponential functions will be discussed. Underlying all exponential functions is the concept of ratio. Using CA, it will be shown how virtually everything that is taught on exponential functions can be seen as a variation on this theme. Among the subjects to be covered are: successive quotients, instantaneous ratio, product integrals, and data sets.

Several examples of this new mathematical approach of ratio will be demonstrated using a specific computer classroom lecture. Simultaneously, the presentation will demonstrate by example, the modern method of presenting a mathematical concept from the numerical, graphical, and symbolic points of view.

A graphing calculator is not enough, since, among other things, symbol manipulation is required to do the necessary limits or to obtain the full-blown generalizations. A salient feature of the presentation will be to show the necessity of CA in order to drive home to the students the full instructional message.

Overall, it will be shown how computer algebra is in a unique position to aid in student learning. As prices continue to drop, it will come into its own. The eventual goal is, of course, to have the computer capabilities to deliver lessons in their full power.

Computer Mediated Thinking: Experience at UWO

David Jeffrey and Rob Corless
University of Western Ontario
London, Ontario, Canada

Abstract

At the University of Western Ontario, we have used calculators in classrooms for 15 years. We review our progress and the difficulties we face at present.

Dynamic Geometry Meets Computer Algebra: A Close Future

Francisco Botana
Department of Applied Mathematics I
University of Vigo at Pontevedra
Spain

Abstract

The last two decades have seen an impressive spread of dynamic geometry software in the teaching and learning of elementary geometry. Two well- known programs, Cabri Geometry and The Geometer's Sketchpad, mostly filled the practice of this paradigm. However, new academic developments have lately arisen. Cinderella, designed by German investigators at ETZH and Berlin, and Geometry Expert, developed at the MMRC of the Chinese Academy of Sciences, are being used more and more. Their main characteristic, shared with other proposals such as Dongming Wang's Geother or our own system, GDI, consists of paying a special attention to the use of mathematical techniques for obtaining sound results. Old approaches (such as "visual proving") have been efficiently replaced by symbolic methods (Groebner bases, Wu's method, ...) allowing further steps in dynamic geometry uses.

This talk gives a short review of the state of the art in the integration of dynamic geometry and symbolic methods for automated geometric proof and discovery. Pros and cons about

using computer algebra systems for symbolic methods are discussed, and the new approach is compared with the standard systems in some common teaching tasks. Some flaws of these new systems (concerning availability, cost, ease of use, ...) are also considered. Furthermore, the need for a common language in the field is highlighted, as it has been simultaneously perceived by different developers. Some proposals from other authors and groups, and the goals and preliminary results of an ongoing project on this point are presented.

(1) Partially supported by grant MTM2004-03175 from the Spanish MEC

On Some Applications of the *Fast* Discrete Fourier Transform

Alkiviadis G. Akritas
Department of Computer and Communication Engineering
University of Thessaly
Volos, Greece
and
Jerry Uhl
Department of Mathematics
University of Illinois at Urbana-Champaign
Urbana IL, USA
and
Panagiotis S. Vigklas
Department of Computer and Communication Engineering
University of Thessaly
Volos, Greece

Abstract

Motivated by the excellent work of Bill Davis and Jerry Uhl "Differential Equations & Mathematica", we present in detail several little known applications of the fast Discrete Fourier Transform (DFT), also known as FFT. Namely, we first examine the use of FFT in: (a) multiplying univariate polynomials and integers, and (b) approximating polynomials with sines and cosines (also known as fast Fourier fit or FFF). We then examine the use of the fast Fourier fit in: (c) solving differential equations with Laplace transforms, (d) "discovering" trigonometric identities, and (e) deriving the heat and wave equations.

Simulation Software Integrated with Java and Computer Algebra System

Yasuyuki Nakamura
Graduate School of Information Science
Nagoya University
Nagoya, Japan

Abstract

In a physics class, a demonstration of a motion of physical system is helpful for students to understand how the system behaves. In order to develop simulation software, Java is often used because of its flexibility of programming and graphical presentation. In many cases, only parameters or initial conditions can be set by users and an equation of motion itself can not be set because the equation have to be solved symbolically. In this talk, we would like to propose developing simulation software integrated with Java and computer algebra system. Specifically, by the use of Maple, MapleNet and its API OpenMaple, mathematical engine can be called from Java program. Advantages and disadvantages of the software are discussed.

Round Table Discussion

moderated by Michael Wester
Cotopaxi / University of New Mexico
Albuquerque, New Mexico, USA

Abstract

During the previous talks, we will collect WRITTEN questions, which can be specific or general, directed to any of the speakers or to the audience at large, and discuss as many of them as possible in the time allowed. Questions can be signed or anonymous. We want to encourage people to ask questions that they might not ordinarily because of time, language or other considerations.

Session 10:

Handling Large Expressions in Symbolic Computation

Organizers:

David Jeffrey and Wenqin Zhou

Symbolic Representation of Polynomial Systems for Efficient Manipulation and Evaluation

Daniel Bates
Department of Mathematics
University of Notre Dame
Notre Dame, IN USA

Abstract

I, with Andrew Sommese (University of Notre Dame) and Charles Wampler (GM Research & Development), with some early work of Chris Monico (Texas Tech University), have been developing a new software package, Bertini, to numerically compute the zero- and positive-dimensional solutions of polynomial systems using a number of recent techniques as well as adaptive precision.

A fundamental design issue when planning Bertini was the internal representation of polynomial systems. We chose to use straight-line programs since they allow for very efficient evaluation, simple automatic differentiation, and polynomials in nonstandard forms. In this talk, I will discuss how Bertini parses polynomials systems into straight-line programs as well as how multi-homogenization and differentiation may be carried out automatically.

Space-Efficient Evaluation of Hypergeometric Series

Howard Cheng
Dept of Mathematics and Computer Science
University of Lethbridge
Alberta, Canada

Abstract

Hypergeometric series are used to approximate many important constants, such as e and Apéry's constant $\zeta(3)$. The evaluation of such series to high precision has traditionally been done by binary splitting followed by integer division. For evaluating such a series to N digits of accuracy, the numerator and the denominator computed by binary splitting have size $O(N \log N)$ even though the reduced fraction may only have size $O(N)$.

In this talk, we show how standard computer algebra techniques including modular computation and rational reconstruction can be applied. The space complexity of our algorithm is the same as a bound on the size of the reduced fraction of the series approximation. We also show that the series approximation for $\zeta(3)$ is indeed a reduced fraction of size $O(N)$. The analysis can be related to our previous algorithm using partially factored integers (ISSAC 2000), which in turn allows our previous algorithm to be improved as well (Hanrot, Thomé, Zimmermann). This technique is also applicable to a large class of hypergeometric series.

This work was done jointly with Barry Gergel, Ethan Kim (University of Lethbridge) and Eugene Zima (Wilfrid Laurier University).

Perturbation Expansion Techniques to Solution of Fluid Flow Problem Using Symbolic Computation

I. Hashim and M. N. Mohamad-Fadzil
School of Mathematical Sciences
Universiti Kebangsaan Malaysia
43600 UKM Bangi Selangor, Malaysia

Abstract

The linearised equations and boundary conditions governing the onset of Bénard-Marangoni convection in a fluid layer subject to uniform internal heat generation are given by the boundary value problem,

$$(D^2-a^2)\left(D^2-a^2-\frac{s}{\mathrm{Pr}}\right)W(z)-a^2R\Theta = 0, \quad (4)$$

$$(D^2-a^2-s)\Theta+[1-Q(1-2z)]W(z) = 0, \quad (5)$$

subject to

$$sf-W(1) = 0, \quad (6)$$

$$\left(D^2-3a^2-\frac{s}{\mathrm{Pr}}\right)DW(1)-a^2(a^2+)f = 0, \quad (7)$$

$$(D^2+a^2)W(1)+a^2\Gamma R[\Theta-(1+Q)f] = 0, \quad (8)$$

$$D\Theta(1)+[\Theta(1)-(1+Q)f] = 0, \quad (9)$$

and

$$W(0)=0, \quad DW(0)=0, \quad \Theta(0)=0, \quad (10)$$

where $D=\mathrm{d}/\mathrm{d}z$. Since exact analytical solutions to the full problem (4)–(10) are difficult to obtain, we seek solutions for W, R, $\omega=\Im(s)$, Θ and f by perturbation expansions via a computer algebra system. In this work, we present an example of an application in which large expressions in the symbolic computations can arise.

Frontier Computations in the Dynamics of one Dimensional Maps

Ilias Kotsireas
Wilfrid Laurier University
Waterloo, ON. Canada

Abstract

The dynamics of one dimensional maps presents significant challenges for Symbolic Computation. The archetype of one dimensional maps is the logistic map. The study of the dynamics of the logistic map involves the analysis of the bifurcation points and the superstable orbits, both of whom are algebraic numbers of high degrees. The intricate interconnections between bifurcation points and superstable orbits are revealed by means of Symbolic Computation techniques such as Groebner bases and powerful factorization algorithms, in conjunction with Symbolic Dynamics techniques such as the MSS (Metropolis-Stein-Stein) algorithm. The efficient management of large expressions, resulted in the proof of the Bailey-Broadhurst conjectures on the bifurcation point B4 and some conjectural results, towards the elaboration of the degree of the bifurcation point B5.

Joint work with K. Karamanos.

Output-Sensitive Modular Algorithms for Row Reduction of Matrices of Ore Polynomials

***Howard Cheng*[1] *and George Labahn*[2]**
1: Department of Mathematics and Computer Science
University of Lethbridge
Lethbridge, Canada
2: Symbolic Computation Group
School of Computer Science
University of Waterloo
Waterloo, Canada

Abstract

We consider the problem of row reduction of a matrix of Ore polynomials with coefficients in $Z[t]$, computing both the transformation matrix and the transformed matrix. Such computations are useful for finding the rank and left nullspace of such matrices, computing GCRD and LCLM of Ore polynomials to name just a few applications.

As in any process that involves elimination operations there is a significant problem with intermediate expression swell with such computations. In our case we propose a new modular algorithm which is output sensitive, that is, the number of homomorphic images required depends on the size of the output. Furthermore, this output sensitivity does not come at the expense of any costly verification step using trial division or multiplication.

Some Recipes for Handling Large Expressions in Polynomial System Solving

Marc Moreno Maza
Ontario Research Center for Computer Algebra
University of Western Ontario
London, Canada

Abstract

Modular methods are well known techniques for controlling the swell of intermediate expressions in symbolic computations. Sometimes, the output of a computation is so large that additional techniques are needed. This is often the case with the solution set of polynomial systems, for space complexity reasons.

In this talk, we discuss various representations for such solution set that tend to be more compact than others. For instance, triangular decompositions into non-normalized regular chains. Then, we discuss various strategies for solving large systems. In particular, for computing "all of the zeros" of systems with infinitely many solutions.

Handling Large Expressions Symbolically in Transition State Theory

Jesús F. Palacián and Patricia Yanguas
Departamento de Matemática e Informática
Universidad Pública de Navarra
31006 Pamplona (Navarra) Spain

Abstract

In this talk we show the normal form approach as a way of getting an analytical handle on geometric objects, such as normally hyperbolic invariant manifolds (NHIM), and the breakthrough this is in chemistry, as well as in celestial mechanics problems. Computer visualization is used in order to "see" these objects. We illustrate the technique through several examples borrowed from chemistry and astrodynamics. Concretely, we show how to determine analytically the transition state (TS) in chemical reactions. For that we calculate the normal form and transform the original three-degree-of-freedom (3DOF) Hamiltonian to a 0DOF one. These expressions need to be known very accurately, so one carries out the computations to a high degree, therefore using very large formulae. In fact, we are able to construct three asymptotic integrals of the original Hamiltonian by inverting the normal form transformation. Moreover, we calculate in the original system the three-dimensional NHIM, its stable and unstable manifolds, as well as the transition state. We compute trajectories that start on the NHIM in the five-dimensional energy surface. Besides, we determine trajectories in either the forward or backward stable and unstable manifolds associated to the NHIM. These trajectories are simply chosen and computed from the normal form vector field. The normal form transformation then allows us to visualize them in the original coordinates. Thus, we have complete control and knowledge of the exact dynamical trajectories near the TS in a 3DOF system. For the calculations we make use of the commercial software MATHEMATICA.

Large Simplicial Expressions in Algebraic Topology

Rocío González-Díaz and Pedro Real
Dpto. Matemática Aplicada I
E.T.S. Ingeniería Informática
Universidad de Sevilla
Avda Reina Mercedes, s/n
41012 Sevilla
Spain

Abstract

Working in the context of Simplicial Topology, cohomology operations can be expressed in terms of compositions of component morphisms of an Eilenberg-Zilber chain homotopy equivalence and tensor product permutations. Taking into account that a simplicial operator can be putted into a canonical form (this process can be called normalization of the simplicial operator), such combinatorial formulation for cohomology operations admits a natural simplification in terms of simplicial expressions consisting uniquely in face operators. In order to give an efficient answer to this simplification question, we deal with here some techniques for efficiently normalizing particular large simplicial expressions.

Evaluation Techniques and Symmetric Polynomials

Éric Schost
LIX
École polytechnique
91128 Palaiseau, France

Abstract

Standard algorithms for dealing with symmetric polynomials are presented using rewriting techniques. This is for instance the case of the "fundamental theorem of symmetric polynomials", which states that any symmetric polynomial is a polynomial in the elementary symmetric ones, and whose proof involves rewriting using a suitable elimination order.

This kind approach usually spoils useful features such as sparseness, so its complexity is hard to control. By contrast, I will show how the straight-line program representation of polynomials yields improved results. My first focus is on polynomial invariants under the symmetric group, but other actions will be discussed as well.

Growth of Formulas During Quantifier Elimination by Virtual Substitution

Hitoshi Yanami
FUJITSU LABORATORIES LTD./CREST, JST
4-1-1, Kamikodanaka, Nakahara-ku
Kawasaki, Japan

Abstract

Recently symbolic computation methods have been gradually applied to solving engineering problems. We have been turning our attention to quantifier elimination (QE), which is a symbolic procedure of removing the quantified variables from a given formula. Using QE as a basic tool we have been developing Maple toolbox SyNRAC for solving real algebraic constraints. During a procedure based on QE by virtual substitution, formulas grow larger, which could sometimes halt the procedure. We discuss how we can circumvent this problem.

Hierarchical Representations in Large Expression Generations

Wenqin Zhou and David Jeffrey
Department of Applied Mathematics
University of Western Ontario
London, ON. Canda

Abstract

In this talk we propose hierarchical representations to alleviate the large expression swell problem that occurs during symbolic expression generation. The problems that we are trying to address are the kind of problems which have intermediate large expression swell problems and also have the large outputs. We use hierarchical representations to make the sizes of expressions more manageable during the symbolic expression generations. It turns out that the run time and memory used during the computation are much less than those done without hierarchical representations and the outputs are much more concise. We use a low-level package

called `LargeExpressions` in MAPLE to automatically generate the hierarchical representations for us. The advantage for this package is that we can define the size of the expression that we want to hide and the exact moment when we want to hide the complex expressions.

In order to demonstrate our idea, we use the classical symbolic LU decomposition problem as an application and build a high-level tool for doing symbolic LU decomposition with hierarchical representations. We introduce several strategies for pivoting, veiling an expression and zero-recognition in our algorithm which can be chosen based on different applications. We also can include other strategies according to different users' desires. It is very flexible and it is much faster than the existing LU decomposition in Maple. We analyze LU decomposition complexity with and without the hierarchical representation. Some benchmarks are given in the end of the talk.

Similar results can be obtained if we apply our method to compute determinants, or symbolically solve linear systems, or generate large symbolic models for multibody dynamic systems, etc.

Session 11:

High-Performance Computer Algebra

Organizers:

Jeremy Johnson and Werner Krandick

Overview of High-Performance Computer Algebra

Jeremy Johnson
Department of Computer Science
Drexel University
Philadelphia, PA, U.S.A.

Abstract

This talk surveys the features of modern processors, pipelining and hazards, superscalar execution, instruction level parallelism, vector instructions, and the memory hierarchy, that affect performance. Effective utilization of these features can be more important than reducing the number of arithmetic operations in obtaining high-performance code; however, code optimized for one architecture may be inefficient on another architecture, leading to portability issues.

We survey techniques for self-adapting code to produce optimized portable numeric libraries — ATLAS (http://math-atlas.sourceforge.net) and OSKI (http://bebop.cs.berkeley.edu), previously Sparsity, for linear algebra and FFTW (www.fftw.org) and SPIRAL (www.spiral.net) for the FFT and other signal processing algorithms — and discuss how these techniques may be used to obtain high-performance computer algebra libraries.

Efficient Polynomial Computations from a Programmer's Perspective

Xin Li
Ontario Research Centre for Computer Algebra
University of Western Ontario
London, Canada

Abstract

Our research purpose is to reduce the practical complexity and improve the performance of exact symbolic computations with polynomials

We are interested in studying known techniques such as:

1. using modular methods and asymptotically fast polynomial arithmetic
2. choosing adapted underlying data representation and appropriate algorithms
3. mixing high-level generic code and low-level machine dependent code in a transparent way for the high-level end-user

We also aim at measuring precisely the impact of these various techniques and their interactions.

We choose Axiom as the implementation language. Our Lisp, C and assembly code can be ported to other computer algebra systems.

Efficient Implementation of Multivariate Polynomial Arithmetic Based on Fast Fourier Transform

Xin Li, Marc Moreno Maza, Éric Schost
Ontario Research Centre for Computer Algebra
University of Western Ontario
London, Canada

Abstract

The goal of this work is to provide fast algorithms with efficient implementation for multivariate polynomials in a high-level language, namely AXIOM. The main application that we have in mind is supporting Hensel lifting techniques modulo big primes in order to solve systems of non-linear systems symbolically.

We focus on :

1. FFT-based univariate polynomial multiplication over finite field
2. FFT-based multivariate polynomial arithmetic
3. "Big prime" arithmetic

Our code is cross over Axiom, Lisp, C and Assembly. High performance is achieved by selecting suitable data structure, using fast integer and floating point arithmetic, understand restrictions of compiler, understand memory performance and processor's architecture.
Our implementation is based on Intel-compatible processor, running on Linux.

Using High-Performance Taylor Shift by 1 in Real Root Isolation

Anatole Ruslanov, Jeremy Johnson and Werner Krandick
Department of Computer Science
Drexel University
Philadelphia, PA, U.S.A.

Abstract

A common approach to high-performance computer algebra software consists in using high-performance low-level routines as building blocks. However, in a recent paper [2] we show that using a high-performance integer addition routine as a building block does not yield a high-performance implementation of Taylor shift by 1.

We first review the techniques from [2] and show why it is not sufficient in general to expect high-performance by plugging-in calls to efficient kernel routines (e.g., incompatible data structures, inability to apply high-level optimization across calls to the kernel routines, and need for special instances of kernel routines). Then we investigate using high-performance Taylor shift by 1 to obtaining a high-performance implementation of the Descartes method for polynomial real root isolation.

References

[1] J. R. Johnson, W. Krandick, and A. D. Ruslanov. Architecture-aware classical Taylor shift by 1. In *International Symposium on Symbolic and Algebraic Computation*. ACM Press, to appear.

Towards High-Performance High-Level Arithmetic Code

Werner Krandick
Department of Computer Science
Drexel University
Philadelphia, PA, U.S.A.

Abstract

The GNU-MP library [1] for multiprecision integer arithmetic achieves high performance by providing hand-crafted assembly language routines for a large number of architectures. By building on top of GNU-MP, computer algebra systems such as Maple [3, 5, 4] try to obtain high performance in high-level algorithms.

However, a recent paper [2] shows that this approach does not work for Taylor shift by 1, a relatively low-level operation. Moreover, relying on hand-crafted assembly code

- hides important algorithmic ideas,
- limits the portability to new processor architectures, and
- precludes benefits from optimizing compilers.

We review some of the GNU-MP routines for multiprecision integer addition and report on ongoing efforts at Drexel University to replace the GNU-MP routines with high-level programs.

References

[1] Torbjörn Granlund. *GNU MP: The GNU Multiple Precision Arithmetic Library*. Swox AB, September 2004. Edition 4.1.4.

[2] J. R. Johnson, W. Krandick, and A. D. Ruslanov. Architecture-aware classical Taylor shift by 1. In *International Symposium on Symbolic and Algebraic Computation*. ACM Press, to appear.

[3] Maplesoft. *Maple 9: Learning Guide*, 2003.

[4] M. B. Monagan, K. O. Geddes, K. M. Heal, G. Labahn, S. M. Vorkoetter, J. McCarron, and P. DeMarco. *Maple 9: Advanced Programming Guide*. Maplesoft, 2003.

[5] M. B. Monagan, K. O. Geddes, K. M. Heal, G. Labahn, S. M. Vorkoetter, J. McCarron, and P. DeMarco. *Maple 9: Introductory Programming Guide*. Maplesoft, 2003.

Session 12:

Newton and Hensel Techniques in Scientific Computing

Organizers:

Marc Moreno Maza and Eric Schost

Height Estimates for the Equiprojectable Decomposition

Xavier Dahan
LIX
École Polytechnique
Palaiseau, France
Joint work with
Marc Moreno Maza, Éric Schost, Wenyuan Wu and Yuzhen Xie

Abstract

Assume k is a perfect field and let $V \subset \overline{k}^n$ be a 0-dimensional variety. Given an ordering of the coordinates $x_1 < \cdots < x_n$, we introduced, in a previous work, the equiprojectable decomposition of V. We showed that it could be encoded by a triangular decomposition of V and that this decomposition could be computed easily from any triangular decomposition of V.

In this talk, we establish specialization properties for the equiprojectable decomposition of V. We provide also height estimates for the coefficients of the triangular decomposition encoding the equiprojectable decomposition of V. Then, we deduce Hensel lifting techniques for computing the equiprojectable decomposition of V. Finally, we report on a preliminary implementation that shows the capacity of this approach to improve the practical efficiency of triangular decomposition.

Technical Issues on Lifting and a Unified Algorithm for Factorization of Multivariate Polynomials

Maki Iwami
Graduate School of Systems and Information Engineering
University of Tsukuba
Tsukuba, Japan

Abstract

Let K be a number field of characteristic 0. Let $K[\boldsymbol{u}], K\{\boldsymbol{u}\}$ be the ring of polynomials and the ring of formal power series over K, respectively, where $(\boldsymbol{u})$ is an abbreviation of variables, $(u_1, \cdots, u_\ell)$.

It makes sense to perform analytic factorization which is a factorization over the ring of formal power series by fixing the expansion point, because $K[x, \boldsymbol{u}] \subset K\{\boldsymbol{u}\}[x]$. Therefore, the author presents two algorithms for multivariate analytic factorization. One is utilizing the extended Hensel construction [1] and the other is multivariate expansion base algorithm [2]. Therefore, the author suggests an algorithm from a unified viewpoint, which comes from the identification of "weight of expansion base" and "slope of Newton's polynomial" [3]. We can say this unified method is a blend of techniques of "multivariate expansion-base" and "the extended Hensel construction".

References

[1] M. Iwami: Analytic Factorization of the Multivariate Polynomial. Proc. of the Sixth International Workshop on Computer Algebra in Scientific Computing (CASC2003), pp.213–225 (2003).

[2] M. Iwami: Extension of Expansion Base Algorithm to Multivariate Analytic Factorization. Proc. of the Seventh International Workshop on Computer Algebra in Scientific Computing (CASC2004), pp.269–281 (2004).

[3] M. Iwami: Extension of Expansion Base Algorithm to Multivariate Analytic Factorization including the Case of Singular Leading Coefficient. accepted for CASC2005,

to appear in Lecture Notes in Computer Science, Springer-Verlag (2005).

Evaluation Techniques for Polynomial System Solving

Grégoire Lecerf
Laboratoire de Mathématiques
Université de Versailles
Versailles, France

Abstract

In this talk we will present a recent probabilistic algorithm for solving systems of polynomial equations and inequations. Our algorithm computes the equidimensional decomposition of the Zariski closure of the solution set of such systems. Each equidimensional component is encoded by a generic fiber, that is a finite set of points obtained from the intersection of the component with a generic transverse affine subspace. Our algorithm is incremental in the number of equations to be solved. Its cost is mainly cubic in the maximum of the degrees of the solution sets of the intermediate systems counting multiplicities. This behavior is reached thanks to certain lifting methods that generalize the classical Newton operator. We will make a short demonstration of our implementation called Kronecker, which is written in the Magma computer algebra system.

Improved Dense Multivariate Polynomial Factorization Algorithms

Grégoire Lecerf
Laboratoire de Mathématiques
Université de Versailles
Versailles, France

Abstract

Popularized by Zassenhaus in the seventies, several algorithms for factoring multivariate polynomials use a so called lifting and recombination scheme. In this talk, we will present a new recombination method that requires a lifting up to precision twice the total degree of the polynomial to be factored. This method leads to nearly optimal algorithms for multivariate polynomial factorization and absolute factorization.

Hensel Lifting via Groebner Bases

Daniel Lichtblau
Wolfram Research
Champaign, Illinois, USA

Abstract

In this talk I will show how one may use Groebner bases over Euclidean domains to perform Hensel lifting in some polynomial rings. The algorithm is quite simple. Moreover, for the ring of univariate polynomials over the integers, dedicated polynomial arithmetic code of around two dozen lines can implement this method quite efficiently (it compares well to the tree lifting method, which appears to be the most effective approach known). We will also see how the Groebner basis approach to lifting may be applied to bivariate polynomials over finite fields.

Toeplitz and Hankel Meet Hensel and Newton Modulo a Power of Two.

Victor Pan
The Department of Mathematics and Computer Science
The City University of New York
NY, USA

Abstract

We extend Hensel lifting for solving general and structured linear systems of equations to the rings of integers modulo nonprimes, e.g. modulo a power of two. This enables significant saving of word operations. We elaborate upon this approach in the case of Toeplitz linear systems. In this case, we initialize lifting with the MBA superfast algorithm, estimate that the overall bit operation (Boolean) cost of the solution is optimal up to roughly a logarithmic factor, and prove that the degeneration is unlikely even where the basic prime is fixed but the input matrix is random. We also comment on the extension of our algorithm to some other fundamental computations with possibly singular general and structured matrices and univariate polynomials as well as to the computation of the sign and the value of the determinant of an integer matrix.

An Approach to Singularity from Extended Hensel Construction

Tateaki Sasaki & Daiju Inaba,
Inst. Math. & Venture Business Lab.,
University of Tsukuba,
Tsukuba-shi, Ibaraki, Japan,

Kentaro Katamachi
Dept. Computer Science
Iwate Prefectural University
Morioka-shi, Iwate, Japan

Abstract

Let $F(x, u_1, \ldots, u_\ell)$, or $F(x, u)$ in short, with $\ell \geq 2$, be a multivariate polynomial over $\mathbf{C}$. The generalized Hensel construction breaks down at a point $(s_1, \ldots, s_\ell) \in \mathbf{C}$, or (s) in short, if $F(x, s) = \text{const} \times (x-\alpha)^n$. Such a point (s) is called a *singular point for the Hensel construction*, or *singular point* in short. The extended Hensel construction, or EHC in short, is the Hensel construction at the singular point. It was invented by Kuo in 1989 for monic bivariate polynomials and by Sasaki-Kako in 1993 for monic multivariate polynomials. The EHC gives the Puiseux-series roots for bivariate polynomial $F(x, u_1)$ and, for multivariate polynomial $F(x, u_1, \ldots, u_\ell)$, the roots which are fractional-power series in the total-degree variable t. In this talk, we clarify a relationship between the extended Hensel factors and the singularity of the multivariate roots.

In order to obtain Hensel factors which are linear w.r.t. the main variable x, we are necessary to perform two different kinds of EHC's; the initial factors in the first kind of EHC are chosen to be in $\mathbf{C}[x, u]$, and in the second kind of EHC, we introduce algebraic functions $\theta_1(u), \ldots, \theta_s(u)$. In both cases, rational functions appear usually in the coefficient of Hensel factors. The Hensel factors become singular at a point (s) where the leading coefficient disappears or denominators become zero. If the leading coefficient disappears, then "scaled root" $\bar{\chi}(u-s, t)$, with t the total-degree variable, becomes infinity as $(u) \to (s)$. Let $\mathcal{S}$ be a surface (a line in trivariate case) on which some denominators become zero. The singularity structure of $x = \chi(u)$ changes on $\mathcal{S}$; for example, the cube-root type singularity changes to the square-root type one.

Fast Algorithms for Newton Sums in Small Characteristic

Eric Schost
LIX
École Polytechnique
Palaiseau, France

Abstract

I consider the following problem: computing the coefficients of a polynomial from the data of its first Newton sums, over a small finite field. In large characteristic, the main tool for this task is Brent's idea of using Newton's iteration for exponentiating a power series. This algorithm fails in small characteristic because of divisions; I will show how adding only a few bits of precision makes it well-defined again. As applications, I will describe algorithms "a la Leverrier" for parallel linear algebra over finite fields, and compare these results to those of notably Schonhage, Kaltofen and Pan, Giesbrecht, and Pan. This is a joint work with Alin Bostan, Laureano Gonzalez-Vega and Hervé Perdry.

Session 13:

Parametric and Nonconvex Constraint Solving

Organizers:

Thomas Sturm and Hirokazu Anai

A Hybrid Method for Solving Quantified Constraints

Hoon Hong
North Carolina State University

Abstract

Quantified constraints are universally / existentially quantified Boolean expressions of polynomial equation / inequalities. By solving, we mean to obtain a useful description of the solution set (the set of the values of the free variables that satisfy the constraint).

Quantified constraints arise in numerous problems in mathematics, science and engineering. Due to its importance, extensive research has been done and are still being actively carried out.

This talk describe a hybrid method which is much more efficient than the previous exact methods for some important sub-class (2 free variables for now). The exact methods usually proceed by eliminating variables using (sub)resultants and variants. This process can be very time-consuming and also often yields huge extraneous factors, which are irrelevant to the solution. The hybrid method does not compute (sub)resultants. Instead, it directly estimates the boundaries of the solution set, using numerical methods and then, if necessary, carry out curve fitting to obtain an approximate symbolic expression for the solution set.

We illustrate its efficiency on several challenging problems arising from the stability analysis of a certain numerical PDE scheme and also from control system design. Many of those problems could not be solved, by using the previous methods, even after several hours of computing time. But now they can be solved approximately, using the hybrid method, within a few seconds/minutes.

Solving and Visualizing in Control

***Noriko Hyodo*[1], *Myunghoon Hong*[2] *Hirokazu Anai*[3], *and Shinji Hara*[4]**

[1] ***AlphaOmega Inc. Japan***
[2] ***Fujitsu Hyper Software Technologies LTD. Japan***
[3] ***FUJITSU LABORATOLIES LTD. / JST, CREST. Japan***
[4] ***University of Tokyo Japan***

Abstract

Recently there has been an increasing interest in the application of computer algebra to control system analysis and design. Control system design are to find out feasible design parameters for which a target system satisfies given control design specifications. Many important control system design problems are regarded as parametric and nonconvex optimization problems.

First We explain how we can practically solve such control system design problems by using algebraic methods based on quantifier elimination.

Then we show an effective visualization of the results *i.e.* the feasible regions of design parameters given as semi-algebraic sets described by disjunction/conjunction of polynomial inequalities and equations.

All these results are implemented as a MATLAB toolbox for parametric robust control. We also demonstrate our MATLAB toolbox by using actual control design problems.

Quantifier Elimination Supported Proofs in Numerical Treatment of Fluid Flows

Richard Liska
Faculty of Nuclear Sciences and Physical Engineering
Czech Technical University in Prague
Prague, Czech Republic

Abstract

The fluid flows are typically modeled by finite difference, finite volume or finite element numerical methods. Properties of these numerical methods which are essential for their correct performance include stability, order of approximation, conservation and monotonicity. Analysis of these properties is a crucial part of their design. During the analysis many subproblems can be stated as theorems/propositions which can be formulated as quantifier elimination problems and proved by quantifier elimination methods. Few case studies demonstrate the usefulness of this approach. QEPCAD, REDLOG, SLFQ and AQCS packages are employed for quantifier elimination tasks.

A Direct Products of Fields Approach to Comprehensive Gröbner Bases over Finite Fields

Katsusuke Nabeshima
Research Institute for Symbolic Computations (RISC-Linz),
Johannes Kepler University Linz,
Linz, Austria.

Abstract

We describe comprehensive Gröbner bases over finite fields by direct product of fields. In general, representatioins of comprehensive Gröbner bases have some conditions on parameters. However, in finite fields we can construct comprehensive Gröbner bases without conditions by the theory of von Neumann regular rings [2].
Alternative comprehensive Gröbner bases [1] (ACGB) are also bases on the theory of von Neumann regular rings. However, ACGB are defined for infinite fields, we can not use the method given by ACGB for finite fields. The comprehensive Gröbner bases we are to describe are defined as Gröbner bases in polynomial rings over commutative von Neumann regular rings, hence the comprehensive Gröbner bases have some nice properties which we also describe.

References

[1] Suzuki, A. and Sato, Y. (2003). *An alternative approach to Comprehensive Gröbner bases.* Journal of Symbolic Computation, Vol 36/3-4, pp.649-667.

[2] Weispfenning,V. (1989). *Gröbner bases for polynomial ideals over commutative regular rings.* EUROCAL '87. In J. H. Davenport Ed., LNCS 378, pp.336-347, Springer.

Optimization Issues in the Construction of Multidimensional Wavelets

Hyungju Park
Korea Institute for Advanced Study
Seoul, Korea

Abstract

The wavelet construction from a multiresolution generated by a finite number of compactly supported scaling functions in any dimension can be reduced to the problem of extending a matrix with Laurent polynomial entries. As the extended matrix is not unique, one can consider the set of all possible extensions which produces a design space or parametrization for wavelet construction. This presentation aims to clarify the process of obtaining such a design space and subsequently optimizing the wavelet construction with respect to certain design goals (e.g. frequency response, regularity or linear phase etc). The method relies on Gröbner basis computation to solve the algebraic relations produced during the process. We propose a conjecture regarding the feasibility of paraunitary matrix completion, which guarantees that our method always produces a solution.

Simplification of Elementary Functions

James H. Davenport, Russell Bradford, Nalina Phisanbut & James Beaumont
Department of Computer Science
University of Bath
Bath, England

Abstract

Simplification of elementary function expressions is a fundamental problem in computer algebra. This has many facets, but we are focusing on the following. Single-valued identities, such as $\log(z^2-1)-\log(z-1)-\log(z+1)=0$ for example, are not always true in the complex plane; generally they only hold on specific regions of the complex plane defined by the branch cuts of the function. Current CAS are only aware of special cases, such as the classic, $\sqrt{z^2}$ simplifies to z if $\Re(z)>0$ or $\Re(z)=0$ and $\Im(z)\geq 0$. Given $\sqrt{p^2}$ for arbitrary $p\in\mathbf{C}[z]$ say, the system will simply substitute p for z above. This is correct, but unhelpful. We need to know when they hold so that we can correctly use the identity as a valid step in a sequence of transformations. This forces one to consider the geometry of the plane induced by the branch cuts.

This talk will describe our ongoing work in this area to build a CAD-based verification system for a large class of formulae that one is likely to meet in practice. We provide an overview of the various problems one encounters, and the techniques we have used to overcome them.

Construction of Parametrized Wavelets Using Gröbner Bases

Georg Regensburger
Johann Radon Institute for Computational and Applied Mathematics (RICAM),
Austrian Academy of Sciences
A-4040 Linz, Austria

Abstract

Wavelets have become a fundamental tool in many areas of applied mathematics and engineering over the last two decades. In this talk, we first outline the construction of orthonormal wavelets based on scaling functions and the related multiresolution analysis. A scaling function satisfies a functional equation (dilation equation) given by a linear combination of filter coefficients and dilated and translated versions of the scaling function.

Conditions on the scaling functions imply, using the dilation equation, constraints on the filter coefficients. For example, orthonormality gives quadratic equations for the filter coefficients and vanishing moments of the associated wavelet linear constraints. Daubechies wavelet [1] have the maximal number of vanishing moments for a fixed number of filter coefficients. We omit some vanishing moment conditions for the associated wavelet and introduce the first discrete moments of the filter coefficients as parameters. The discrete moments can be expressed in terms of the (continuous) moments of the scaling function and thus have a natural interpretation. Moreover, we can use the fact that even moments are determined by odd up to the number of vanishing moments, see [2].

We discuss how Gröbner bases [3] can be used to solve the resulting (parametrized) polynomial equations for the filter coefficients and to construct parametrized families of wavelets. After computing and illustrating several examples we outline some applications. Finally, we demonstrate a software package to compute with parametrized wavelets and discuss possible extensions of our approach.

References

[1] I. Daubechies. *Ten lectures on wavelets*. SIAM, Philadelphia, PA, 1992.

[2] G. Regensburger and O. Scherzer. Symbolic computation for moments and filter coefficients of scaling functions. To appear in *Annals of Combinatorics*, 2005.

[3] B. Buchberger. Introduction to Gröbner bases. In B. Buchberger and F. Winkler, editors, *Gröbner bases and applications*, pages 3–31. Cambridge Univ. Press, 1998.

On Parametric Boolean Constraint Solving

Yosuke Sato
ysato@rs.kagu.tus.ac.jp
Department of Mathematical Information Science,
Tokyo University of Science,Japan

Abstract

A commutative ring with identity is called a *boolean ring* if each element is idempotent. For a boolean ring $\mathbf{B}$, a quatient ring
$\mathbf{B}[X_1,\ldots,X_n]/\langle X_1^2-X_1,\ldots,X_n^2-X_n\rangle$ is called a *boolean polynomial ring*. A Gröbner basis in a boolean polynomial ring is called a *boolean Gröbner basis*. We show that any boolean Gröbner basis w.r.t. a certain term order is always strongly stable. This result enables us to compute comprehensive Gröbner bases in boolean polynomial rings with minimum computation costs. Moreover, we can construct reduced comprehensive Gröbner bases from them, which is not possible in a polynomial ring over a field in general. Out result also gives alternative ideal theoretic proofs for several classical theorems of boolean algebra such as an extention theorem or a Nullstellensatz.

Cylindrical Subdecompositions for Local Elimination

Andreas Seidl
Fakultät für Mathematik und Informatik
Universität Passau
Passau, Germany

Abstract

A key strategy for improving the practical complexity of the cylindrical algebraic decomposition method (CAD) for real quantifier elimination is to avoid the construction of a full decomposition. Instead, one concentrates on a sufficient subdecomposition. Improvements like partial CAD, the use of equational constraints, or the utilization of a generic projection operator are examples for this.

Local elimination caters for situations, where example values of interest for some or all parameters are known. Such values can be values for which empirically a good behavior of an underlying system is verified. It is, however, desired to find an environment of one point (or of some points) such that all values from these region have the same good behavior as the given point. Such problems often occur in engineering.

We show how applying the paradigm of local elimination to the CAD method allows to restrict attention to a suitable subdecomposition. This application-oriented modification of the CAD method subsumes the general method as a special case and is compatible with other important improvements.

Exact Global Constrained Optimization with Mathematica

Adam Strzeboński
Wolfram Research Inc.
Champaign, IL, U.S.A.

Abstract

In my talk I will present Mathematica functionality for computing exact global extrema of functions on sets constrained by systems of equations and inequalities and discuss the algorithms used. The most general method is based on the cylindrical algebraic decomposition (CAD) algorithm. It applies when the objective function and the constraints are real algebraic functions. The method allows to always compute global extrema (or extremal values, if the extrema are not attained). If parameters are present, the extrema can be computed as piecewise-algebraic functions of the parameters. A downside of the method is its high, doubly exponential in the number of variables, complexity. In certain special cases not involving parameters faster methods can be used.

When the objective function and all constraints are linear, global extrema can be computed exactly using the simplex algorithm. Another approach to finding global extrema is to find all the local extrema, using the Lagrange multipliers or the KKT conditions, and pick the smallest (or the greatest). However, for a fully automatic method, there are additional complications. In addition to solving the necessary conditions for local extrema, it needs to check smoothness of the objective function and smoothness and nondegeneracy of the constraints. It also needs to check for extrema at the boundary of the set defined by the constraints and at infinity, if the set is unbounded. This in general requires exact solving of systems of equations and inequalities over the reals, which may lead to CAD computations that are harder than in the optimization-by-CAD algorithm. Currently Mathematica uses Lagrange multipliers only for equational constraints within a bounded box. The method also requires that the number of stationary points and the number of singular points of the constraints be finite. An advantage of this method over the CAD-based algorithm is that it can solve some transcendental problems, as long as they lead to systems of equations that Mathematica can solve.

Mathematica can also solve some global optimization problems over the integers. Arbitrary bounded linear problems can be solved by integer linear programming methods. Several other integer optimization problems can be solved by a combination of real optimization methods and integer solution finding. In my talk I will discuss the algorithms used and show examples.

Computation of Comprehensive Gröbner System using Gröbner Basis

Akira Suzuki
Kobe University
Kobe, Japan

Abstract

Let K be an infinite field, $\bar{X} = X_1, \ldots, X_n$ be variables, and $\bar{A} = A_1, \ldots, A_m$ be parameters such that $\{X_1, \ldots, X_n\} \cap \{A_1, \ldots, A_m\} = \emptyset$. For a given finite subset F of the polynomial ring $K[\bar{X}, \bar{A}]$, we can calculate a comprehensive Gröbner system (CGS) for F which is introduced by Weispfenning. By the way of its construction, we often consider a CGS as a finite tree whose node consists of an algebraic condition on $K[\bar{A}]$ and a basis for the ideal generated by

F, and each basis on the leaf forms a Gröbner basis. Several algorithms to calculate CGS's have been proposed, and they essentially build nodes of such trees from their roots calculating conditions and basis simultaneously.

In this talk, we give a new algorithm to compute CGS's which find each branches of the tree using usual Gröbner bases in a polynomial ring over a field. In this algorithm, we first find "main branch" and then find each branching nodes in the branch. To implement it, we assume that the compute-algebra system has algorithms to compute

1. Gröbner bases in the polynomial ring $K[\bar{X}, \bar{A}]$, and
2. primary ideal decomposition.

If the assumption is satisfied, the length of the code for the implementation will be shorter than other existing algorithms to compute CGS's.

On Systems of Algebraic Equations with Parametric Exponents

Kazuhiro Yokoyama
Department of Mathematics
Rikkyo University
3-34-1 Nishi Ikebukuro, Toshima-ku, Tokyo, 171-8501, Japan

Abstract

Systems of algebraic equations with parametric exponents are dealt. Following the author's first study presented in ISSAC 2004, where most simple cases, univariate case and 0-dimensional case, are dealt and certain "stability" and "computability" are defined successfully, Here, some extensions are added to formulation on stability and computability in ideal theory in order to widen applicable cases. Additional concrete methods are discussed for widened applicable cases.

Session 14:

Pen-Based Mathematical Computing

Organizers:

Stephen Watt and Clare So

An Authoring Tool for Math Web with Pen-Based Formula Input Interface

Masakazu Suzuki
Kyushu University
Japan

Abstract

Math Webs – from large Web-cource systems to personal Web sites of teachers – are giving an important new prospect in education for both students and teachers. However, the exisiting math web sites are, in most cases, copies of printed math texts or some extracts of them. At current stage, the development of easy methods to author more "dynamic" and "interactive" math web is desired for the success of web-based or web-assited education of mathematics. In the talk, as a first step toward this direction in our research project Infty (http://www.inftyproject.org/), I will present an authoring tool for math web having blank boxes (answer boxes) in which students can input math expressions using pen-interface. The blank boxes return some actions depending on the answers input by students.

Pen-Based Proofs

K. Sutner and V. Adamchik
Computer Science Department
Carnegie Mellon University
Pittsburgh, USA

Abstract

We present a preliminary evaluation of an outgoing project for developing a learning system for pen-based proofs in computer science. The cornerstone of the system is the concept of geometrical sketching dynamically combined with an underlying mathematical model. The system is based on several sophisticated software libraries and packages, such as a gesture-understanding MagicPaper (MIT), the computer algebra system Mathematica, and the theorem-prover Analytica (CMU).

The primary goal of the project is to develop a library of domain-based gesture recognition tools, that eventually will serve as a foundation for future pen-based interfaces to computer algebra systems. The challenge for us is getting the computer to recognize different types of geometrical drawings - to determine which parts of the sketch are intended to represent a circle, a straight line, or a polygon. On a more detailed level, the computer must distinguish a circle from an ellipse, a rectangle from a trapezoid, and so on. Another core technique with smart digital ink is to have the ability to make a distinction between handwritten words and drawings-it is human nature to annotate drawings with names of points and lines. This is an active area of research and a perfect tool for solving the above problems has not yet been developed. Even the direction of research is under question; should handwriting be only an interface or accommodated by voice and/or video recognition?

AsirPad – A Computer Algebra System with Handwriting Interface on PDA

Mitsushi Fujimoto
Department of Information Education
Fukuoka University of Education
Munakata, Japan
and
Masakazu Suzuki
Faculty of Mathematics
Kyushu University
Fukuoka, Japan

Abstract

Infty Editor [1, 2] is a editor with on-line recognition of handwritten mathematical expressions, which was developed by our research group. We ported the handwriting interface of InftyEditor to Linux PDA Zaurus. OpenXM(Open message eXchange for Mathematics) is an infrastructure for mathematical communication. We added OpenXM translator and communication controller to this interface, so that one can carry out calculations for mathematical expressions inputted by handwriting. As a result, we developed a computer algebra system *AsirPad* with handwriting interface on PDA(See demo movie [3]). Furthermore, we gave a lecture about RSA cryptography at a junior high school using AsirPad. In our talk, we will explain the details of AsirPad, and report the results of the lecture.

References

[1] M. Fujimoto, T. Kanahori and M. Suzuki: Infty Editor – A Mathematics Typesetting Tool with a Handwriting Interface and a Graphical Front-End to OpenXM Servers, RIMS Kokyuroku vol.1335, Computer Algebra – Algorithms, Implementations and Applications, (2003) 217–226.

[2] T. Kanahori, M. Fujimoto and M. Suzuki: Authoring Tool for Mathematical Documents – Infty –, Proceedings of the Workshop on Mathematical User Interfaces, online, (2004) 9 pages, `http://www.activemath.org/%7Epaul/MathUI/proceedings/`

[3] Infty Project Web Site: `http://www.inftyproject.org/`

Structural Analysis for Pen-Based Math Input Systems

Ian Rutherford and George Labahn
School of Computer Science
University of Waterloo
Waterloo, Ontario, Canada

Abstract

In this talk we will describe a real-time method for interpreting handwritten mathematics on a pen-input device. The general problem is to convert two-dimensional handwritten math into a mathematically correct expression. In our case, the conversion of our handwritten expression is stored as an annotated MathML tree, allowing us to interact with existing computer algebra systems such as Maple and Mathematica.

A Pen-based Handwriting Interface for Algebraic Expressions Input/Edit

Xiang-Yang Feng
Venture Business Laboratory
Saga University
1, Honjo-machi, Saga, 840-8502, Japan
Yasuhisa Okazaki and Hiroki Kondo
Department of Information Science

Abstract

We had developed a prototype of pen-based handwriting interface for mathematical expressions input/edit, which is applied as a user interface to an ITS (Intelligent Tutoring System) guiding algebraic calculation. Pen-based handwriting input enables an user enters mathematical expressions directly on an LCD pen tablet. Gestures enable an user executes ordinary editing operations (e.g. select, ovewrite, erase, move and paste) directly with a pen instead of keyboard and mouse. Expression editing include symbol editing and sub expression editing, which are applied to correct symbol recognition errors and calculation mistakes respectively. Therefore, a natural and convenient handwriting mathematical expression input/edit environement can be expected.

Requirements for Mobile Intellectual Collaboration

Nadya Belov, Colin Koeck, Werner Krandick, Joshua Shaffer
Drexel University
USA

Abstract

We present a scenario for the use of smartphones in improvised intellectual collaboration between two or more participants. The scenario results in a set of functional and non-functional requirements that smartphones must fulfill in order to support such collaboration. The Wireless Internet Collaboration System (WICS) implements some of the requirements for the domain of mathematics communication. A full implementation requires, in turn, support from software libraries such as the Java Micro Edition. We specify some of the features that are required from libraries for mobile devices. Finally, we discuss a distribution model for software that supports mobile intellectual collaboration.

Components for Pen-Based Mathematical Interfaces

Elena Smirnova, Clare So, Stephen Watt, Xiaofang Xie
Ontario Research Centre for Computer Algebra (ORCCA)
Department of Computer Science
University of Western Ontario
London, Ontario. Canada

Abstract

Any robust system for pen-based mathematical computation will comprise a number of components, many of which are sophisticated software systems in their own right. We present the components of our pen-based interface for mathematics, and describe the relationship among them. We present in some detail (i) our approach to recognition of characters from large sets of mathematical symbols, (ii) our use of empirical sub-expression frequency data, and (iii) our portable architecture for a pen-based component that may be embedded in Maple or Microsoft Office.

ACA '2005 List of Authors

- A -

Abe, Takayuki Niigata University, Japan

Adamchik V. Carnegie Mellon University, USA

Akritas, Alkiviadis G. University of Thessaly, Greece

Anai, Hirokazu FUJITSU LABORATOLIES LTD. / CREST, JST, Japan

Avis, David McGill University, Canada

- B -

Bates, Daniel University of Notre Dame, USA

Bayer, Thomas Technische Universit München, Germany

Beaudin, Michel École de technologie supérieure (ETS), Canada

Beaumont, James University of Bath, England

Belov, Nadya Drexel University, USA

Benghorbal, Mhenni M. Simon Fraser University, Canada

Berend, Daniel Ben-Gurion University of the Negev, Israel

Borges-Quintana Mijail Universidad de Oriente, Cuba

Borges-Trenard, M.Angel. Universidad de Oriente, Cuba

Botana, Francisco University of Vigo, Spain

Bradford, Russell University of Bath, England

Bretto, Alain Université de Caen, France

- C -

Cheng, Howard University of Lethbridge, Canada

Cheng, Jin-San Institute of Systems Science, AMSS Academia Sinica, China

Chibisov, Dmytro Technische Universit München, Germany

Ching, Wai-Ki The University of Hong Kong, HongKong

Corless, Rob University of Western Ontario, Canada

Coutsias, Evangelos A. University of New Mexico, USA

- D -

Dahan, Xavier École Polytechnique Palaiseau, France

Davenport, James H. University of Bath, England

Dimovski, Ivan Institute of Mathematics and Informatics, Bulgarian Academy of Sciences, Bulgaria

- E -

Ekaterina, Shemyakova Research Institute for Symbolic Computations (RISC), J. Kepler University, Austria

- F -

Feng, Xiang-Yang Venture Business Laboratory Saga University, Japan

Fujimoto, Mitsushi Fukuoka University of Education, Japan

- G -

Gao, Xiao-Shan Institute of Systems Science, AMSS, Academia Sinica, China

Gerdt, Vladimir P. Laboratory of Information Technologies, Joint Institute for Nuclear Research, Russia

Gillibert, Luc Université de Caen, France

Golan, Shahar University of the Negev, Israel

González Díaz, R. Universidad de Sevilla, Spain

- H -

Hara, Shinji University of Tokyo, Japan

Hashiba, Satoshi Kwansei Gakuin, Japan

Hashim, I. Universiti Kebangsaan Malaysia, Malaysia

Hespel,Christiane IRISA-INSA, France

Hong, Hoon North Carolina State University, USA

Hong, Myunghoon Fujitsu Hyper Software Technologies LTD., Japan

Horimoto, Katsuhisa University of Tokyo, Japan

Huguet, Guillem Universidad Pública de Navarra, Spain

Hyodo, Noriko AlphaOmega Inc., Japan

- I -

Ida, Tetsuo University of Tsukuba, Japan

Inaba, Daiju University of Tsukuba, Japan

Iriyama, Satoshi Tokyo University of Science, Japan

Iwama, Kazuo Kyoto University / ERATO, JST, Japan

Iwami, Maki University of Tsukuba, Japan

- J -

Jeffrey, David University of Western Ontario, Canada

Johnson, Jeremy Drexel University, USA

- K -

Kai, Hiroshi Ehime University, Japan

Kako, Fujio Nara Women's University, Japan

Kaltofen, Erich North Carolina State University, USA

Katamachi, Kentaro Iwate Prefectural University, Japan

Kawano, Yasuhito NTT Communication Science Laboratories, Japan

Keyser, John Texas AM University, USA

Koeck, Colin Drexel University, USA

Koshiba, Takeshi Saitama University, Japan

Kotsireas, Ilias Wilfrid Laurier University, Canada

Koukouvinos, C. National Technical University of Athens, Greece

Krandick, Werner Drexel University, USA

Kume, Masaki Ehime University, Japan

Kuwahara, Kosuke Kobe University, Japan

- L -

Labahn, George University of Waterloo, Canada

Laget, Bernard École Nationale d'Ingnieurs de Saint-Etienne, France

Lecerf, Grégoire Université de Versailles, France

Li, Bingyu Key Laboratory of Mathematics Mechanization, AMSS, China

Li, Hongbo Key Laboratory of Mathematics Mechanization, Chinese Academy of Sciences, China

Li, Ming Institute of Systems Science, AMSS, Academia Sinica, China

Li, Xin University of Western Ontario London, Canada

Lichtblau, Daniel Wolfram Research, USA

Lin, Long Key Lab of Mathematics Mechanization, Academy of Mathematics and Systems Sciences, China

Liska, Richard Czech Technical University, Czech Republic

Liu, Zhuojun Key Laboratory of Mathematics Mechanization, AMSS, China

- M -

Ma, Yujie Key Laboratory of Mathematics Mechanization, Chinese Academy of Sciences, China

Man, Yiu-Kwong The Hong Kong Institute of Education, HongKong

Marin, Mircea University of Tsukuba, Japan

Marino, Maria C. University of Messina, Italy

Martig, Cyrille IRISA-INSA, France

Martínez-Moro, E. Universidad de Valladolid, Spain

Maza, Marc Moreno University of Western, Canada

Medrano, B. Universidad de Sevilla, Spain

Minematsu, Daisuke Kwansei Gakuin, Japan

Mishra, Biswajit University of Southampton, England

Miyadera, Ryohei Kwansei Gakuin, Japan

Miyamoto, Atsushi Ehime University, Japan

Moldenhauer Wolfgang Thuringian Institute for In-service Teacher Training,Curriculum Development and Media (ThILLM), Germany

Mohamad-Fadzil, M. N. Universiti Kebangsaan Malaysia, Malaysia

Moritsugu, Shuichi University of Tsukuba, Japan

- N -

Nabeshima, Katsusuke Research Institute for Symbolic Computations (RISC-Linz),Johannes Kepler University, Austria

Nagasaka, Kosaku Kobe University, Japan

Nakajima, Yumi NTT Communication Science Laboratories, Japan

Nakamura, Yasuyuki Nagoya University, Japan

Nakayama, Hiromasa Kobe University, Japan

Nishimura, Harumichi ERATO Quantum Computation and Information Project, Japan Science and Technology Agency, Japan

Noda, Matu-Tarow Ehime University, Japan

- O -

Ohya, Masanori Tokyo University of Science, Japan

Orii, Shigeo FUJITSU LTD./ University of Tokyo, Japan

Ouchi, Koji Texas AM University, USA

- P -

Palacián, Jesús F. Universidad Pública de Navarra, Spain

Pan, Victor City University of New York, USA

Park, Hyungju Korea Institute for Advanced Study, Korea

Perry, John North Carolina State University, USA

Phisanbut, Nalina University of Bath, England

Pletsch, Bill Albuquerque Technical Vocational Institute, USA

Pope, Scott North Carolina State University, USA

- R -

Raymond, Rudy Kyoto University / ERATO, JST, Japan

Real, Pedro Universidad de Sevilla, Spain

Regensburger, Georg Johann Radon Institute for Computational and Applied Mathematics (RICAM), Austrian Academy of Sciences, Austria

Ruslanov, Anatole Drexel University, USA

Rutherford, Ian University of Waterloo, Canada

- S -

Sánchez Peláez, J. Universidad de Sevilla, Spain

Sangwin, Christopher J. University of Birmingham, England

Sasaki, Tateaki University of Tsukuba, Japan

Sato, Yosuke Tokyo University of Science, Japan

Schmidt, Karsten University of Applied Sciences (FH), Germany

Schost, Éric École polytechnique, France

Seidl, Andreas Universität Passau, Germany

Sekigawa, Hiroshi NTT Communication Science Laboratories, Japan

Severyanov, Vasily Laboratory of Information Technologies, Joint Institute for Nuclear Research, Russia

Shaffer, Joshua Drexel University, USA

Shirayanagi, Kiyoshi NTT Communication Science Laboratories, Japan

Shoji, Takumu Niigata University, Japan

Smirnova, Elena University of Western Ontario, Canada

So, Clare University of Western Ontario, Canada

Spiridonova, Margarita Institute of Mathematics and Informatics, Bulgarian Academy of Sciences, Bulgaria

Steinberg, Stanly University of New Mexico, USA

Strzeboński Adam Universität Passau, Germany

Sutner, K. Carnegie Mellon University, USA

Suzuki, Akira Kobe University, Japan

Suzuki, Masakazu Kyushu University, Japan

Szanto, Agnes North Carolina State University, USA

- T -

Tajima, Shinichi Niigata University, Japan

Takahashi, Hidekazu University of Tsukuba, Japan

- U -

Uhl, Jerry University of Illinois at Urbana-Champaign, USA

- V -

Vigklas, Panagiotis S. University of Thessaly, Greece

- W -

Wang, Dingkang Key Lab of Mathematics Mechanization, Academy of Mathematics and Systems Sciences, China

Watt, Stephen M. University of Western Ontario, Canada

Wester, Michael J. University of New Mexico, USA

Wilson, Peter University of Southampton, England

- X -

Xie, Xiaofang University of Western Ontario, Canada

- Y -

Yaacob, Yuzita International Islamic University Malaysia, Malaysia

Yanami, Hitoshi FUJITSU LABORATORIES LTD. / CREST, JST, Japan

Yanguas, Patricia Universidad Pública de Navarra, Spain

Yokoyama, Kazuhiro Rikkyo University, Japan

- Z -

Zhi, Lihong Key Laboratory of Mathematics Mechanization, AMSS, China

Zhou, Wenqin University of Western Ontario, Canda

ACA'2005, Nara Women's University, Japan