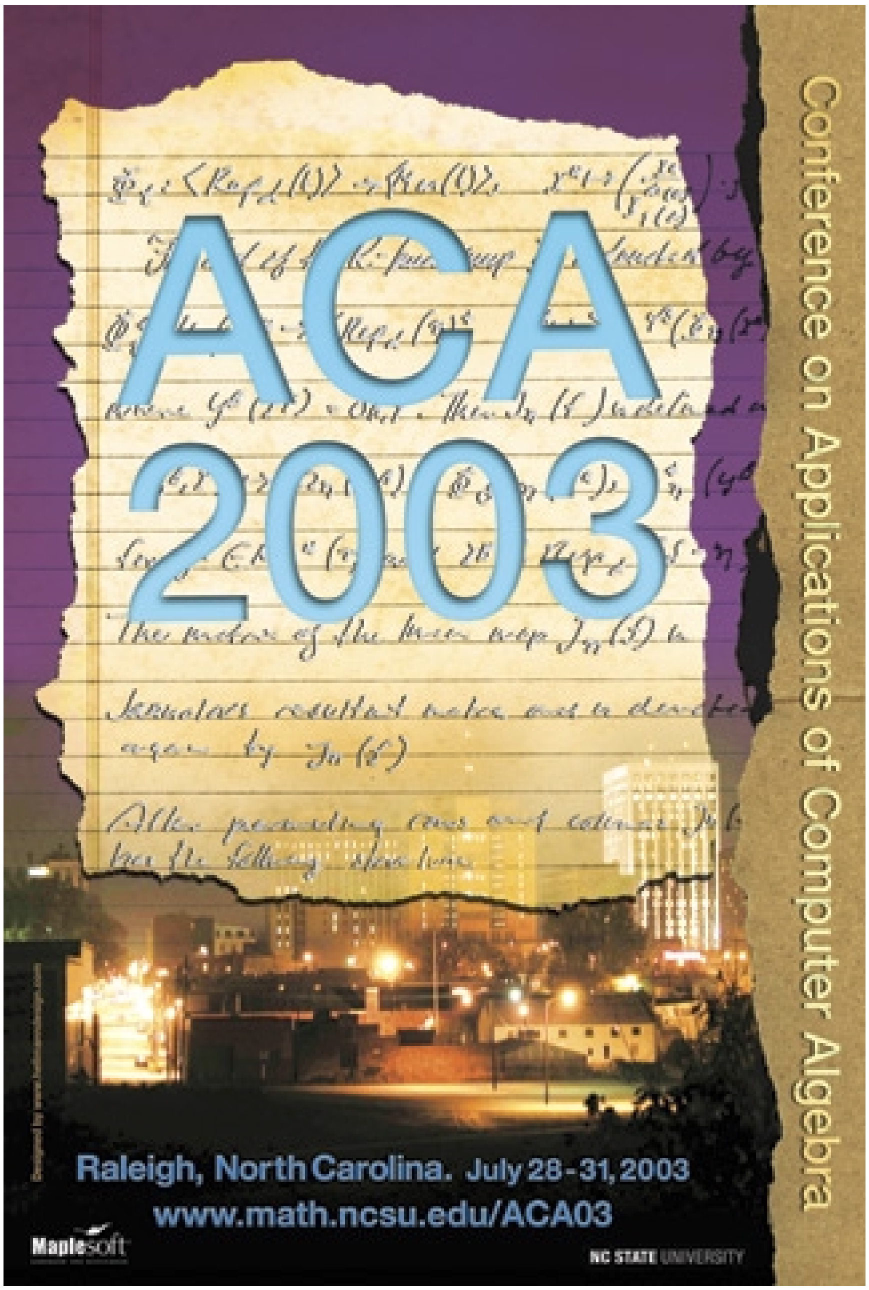
Conference on the Applications of Computer Algebra (ACA'2003)

July 28–30, 2003 North Carolina State University

Conference Schedule and Submitted Abstracts



ACA'2003

July 28-31, 2003

9th International Conference on Applications of Computer Algebra

North Carolina State University Raleigh, North Carolina, USA

General Chairs: Hoon Hong (NCSU), Erich Kaltofen (NCSU), Agnes Szanto (NCSU)

Program Chair: Mark Giesbrecht (University of Waterloo)

Organizing Committee: Stanly Steinberg (University of New Mexico), Michael Wester (Cotopaxi).

ACA'2003 conference e-mail: aca2003@math.unm.edu
ACA'2003 conference web site: http://math.unm.edu/ACA/2003

Conference Theme

The ACA series of conferences is devoted to promoting the applications and development of Computer Algebra and Symbolic Computation. Topics include Computer Algebra and Symbolic Computation in engineering, the sciences, medicine, pure and applied mathematics, education, communication and computer science.

Scientific Committee: ACA WORKING GROUP

Alkiviadis G. Akritas	Greece	Victor Edneral	Russia
Jacques Calmet	Germany	Richard Liska	Czech Republic
Victor Ganzha	Germany	Bill Pletsch	USA
Vladimir Gerdt	Russia	Eugenio Roanes-Lozano	Spain
Mark Giesbrecht	Canada	Stanly Steinberg	USA
Hoon Hong	USA	Quoc-Nam Tran	USA
Erich Kaltofen	USA	Nikolay Vassiliev	Russia
Ilias S. Kotsireas	Canada	Michael Wester	USA

ACA 2003: Schedule of Sessions and Talks
(Last Updated July 22, 2003)

Session Number	Session Name	Organizers	# of Talks in Session
T1	Computational aspects of algebraic curves	Tony Shaska (UC Irvine)	11
T2	Symbolic Summation	Sergei A. Abramov (Moscow), Marko Petkovsek (Ljubljana), Eugene V. Zima (Waterloo)	7
T3	Computer Algebra in Education	Alkis Akritas (Thessaly, Greece), Michael Wester (New Mexico), Bill Pletsch (New Mexico)	7
T4	Computer Algebra in Science and Technology	Laurent Bernardin (Maplesoft), David Jeffrey (Western Ontario)	4
T5	Groebner Bases and Applications	Quoc-Nam Tran (Lamar University, USA) and Alexander Levin (Catholic University of America)	10
T6	Interval Computation	Ned Nedialkov (McMaster) and George Corliss (Marquette)	8
T8	Elimination Theory	Amit Khetan and Carlos D'Andrea (UC Berkeley, USA)	9
T9	Computer Algebra and Polynomial Systems in Chemistry	Karin Gatermann (Berlin)	5
T10	Symbolic Linear Algebra	B. David Saunders (Delaware) and Gilles Villard (ENS Lyon)	8
T11	Mathematics on the Internet	Mike Dewar (NAG, UK)	8
T12	Symbolic-Numeric methods for Curves and Surfaces	J. Schicho and Mohamed Shalaby (RISC Linz, Austria)	9
T13	Young Investigators	Mark Giesbrecht (Waterloo) and Stanly Steinberg (New Mexico)	7

Conference Overall Schedule

Date	July 28, 2003 Monday			July 29, 2003 Tuesday			July 30, 2003 Wednesday			July 31, 2003 Thursday
Start Time	**A**	**B**	**C**	**A**	**B**	**C**	**A**	**B**	**C**	
9:00	Official Opening			T5	T6	T8	RedHat Tour			Panel Discussion
9:30	T1	T2	T3	T5	T6	T8				
10:00	T1	T2	T3	T5	T6	T8				
10:30	Break			Break						Trip to Wrightsville Beach
11:00	T1	T2	T3	T5	T6	T8	T12	T10	T11	
11:30	T1	T2	T3	T5	T6	T8	T12	T10	T11	
12:00	T1	T2	T3	T5	T6	T8	T12	T10	T11	
12:30	Lunch			Lunch			Lunch			
1:00										
1:30										
2:00	T1	T2	T3	T9	T6	T8	T12	T10	T11	
2:30	T1	T2	T3	T9	T6	T8	T12	T10	T11	
3:00	T1			T9	T4	T8	T12	T10	T11	
3:30	Break			Break			Break			
4:00	T1	T13	T4	T9	T5	T13	T12	T10	T11	
4:30	T1	T13	T4	T9	T5	T13	T12	T10	T11	
5:00	T1	T13	T4	T9	T5	T13	T12	T10		
5:30					T5	T13	ACA Business meeting			
	Activity			Activity (Banquet)			Activity			End of Conference

Monday July 28, 2003

Start Time	A	B	C
9:00	Official Opening		
9:30	B. Brock: *Moments associated to the moduli space of hyperelliptic curves over a finite field*	Juergen Gerhard, Ha Le *Symbolic summation in Maple*	Jerry Uhl, *Raising the Level of Precalculus Mathematics*
10:00	Burhanuddin, *On computing discrete logarithms in Formal groups and it's applications*	Burkhard Zimmermann, *Summation in DifferenceDifferential Rings*	Eugenio Roanes-Lozano & Eugenio Roanes-Macias, *Symbolic Manipulation in Projective Geometry through the Cooperation of Dynamic Geometry Systems and Computer Algebra Systems*
10:30	Break		
11:00	J. Wolper, *Theta Vanishings and Automorphism Groups of Riemann Surfaces of Genus Three*	Sergei A. Abramov, Marko Petkovsek *Gosper's and Zeilberger's algorithms revisited*	Laurent Bernardin, *A Look at the New Student Packages in Maple*
11:30	T. Shaska, *Computational Aspects of Algebraic Curves, a survey*	Daniel Lichtblau*, Issues in Symbolic Definite Integration*	Michel Beaudin, *Give Mathematics a Chance!*
12:00	C. Yin, *Special Loci in Moduli of Curves*	Carsten Schneider, *Symbolic Summation in #- #Fields*	Karsten Schmidt & Wolfgang Moldenhauer, *Using the TI-89 in Math Education - What are the Students' Views?*
12:30	Lunch		
2:00	M. Seppala, *Numerical uniformization of algebraic curves*	Victor Adamchik, *Symbolic Computation of Series and Products in Terms of the Multiple Gamma and Related Functions*	Bill Pletsch, *A CAS Lecture for the Calculus Students: The Riemann Product*
2:30	D. Mills, *Some Questions Regarding Avoidable Families of Sets*	Mark van Hoeij, *Rational definite summation*	Giovanna Albano & Matteo Desiderio, *An Effective Learning using CAS*
3:00	G. Cardona, *Curves of genus 2 over arbitrary fields*		
3:30	Break		
4:00	C. Hurlburt, *Computational Aspects of Differential Algebraic Geometry*	Young Investigator: Howard Cheng, *Algorithms for Normal Forms for Matrices of Ore Polynomials*	Paulina Chin, *Automatic Code Generation*
4:30	M. van Hoeij, *Reparametrizing rational algebraic curves*	Young Investigator: Yang Zhang, *Popov forms of Ore matrices*	Cecelia Laurie, *The Use of Maple in Computing DNA Match Probabilities.*
5:00	T. Yamauchi, *On Q-simple factors of J_0(N)*	Young Investigator: Alin Bostan, *Tellegen's principle into practice.*	Brian Moore, *Symofros: A symbolic modeling and simulation tool for mechanical system*
	Activity		

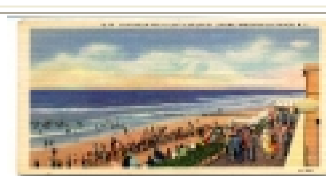
Tuesday July 29, 2003

Start Time	A	B	C
9:00	Yosuke Sato, *ACGB on Varities*	Ned Nedialkov, *Introduction to Interval Numerical Methods*	Agnes Szanto, *Elimination theory of non-commutative algebras of differential invariants*
9:30	Alexander Levin, *Groebner Bases w.r.t. Several Orderings and Difference Dimension Polynomials*	John Pryce, *Mapping Expressions to Functions in Cset Interval Arithmetic*	John Nahey, *Differential Resolvents of Minimal Order and Weight*
10:00	V. Mityunin, Pankratev, *Comparison of the parallellization quality of algorithms for computing Groebner and involutive bases*	Nathalie Revol, *Multiple Precision Interval Arithmetic and Application to Linear Systems*	Arthur Chtcherba, *Sylvester-type matrices via the Dixon resultant formulation and their optimizations*
10:30	Break		
11:00	Quoc-Nam Tran, *Efficient Groebner Basis Computation for Finding Implicit Representations of Geometric Objects*	Markus Neher, *From Intervals to Taylor Models: A Numeric Symbolic Approach to Validated Computation*	Manfred Minimair, *Developments in resultants of composed polynomials*
11:30	Martinez-Moro, *Using Groebner basis for determining the equivalence of linear codes.*	Jeff Tupper, *Pictures from Proofs: Sound Graphing Algorithms*	Amit Khetan, *Implicitization of rational surfaces using toric varieties*
12:00	Ekaterina Shemyakova, *Graphs of involutive divisions*	Ekaterina Auer, *Interval Arithmetic in the Multibody Modeling System MOBILE*	Laurent Busé, *Implicitizing rational hypersurfaces using approximation complexes*
12:30	Lunch		
2:00	Anke Sensse, *Electrocatalytic oxidation of formic acid*	Yves Papegay, *ALIAS: A Library Mixing Interval Analysis and Computer Algebra*	Marc Moreno Maza, *Recent advances in triangular decomposition methods*
2:30	Brandilyn Stigler, *Polynomial Models for Gene Regulatory Networks*	Stan Wagon, *The Role of Symbolic Computation in the SIAM/Oxford 100-Digit Challenge*	Ilias Kotsireas, *Recent advances in polynomial system solving and an application in Chaos Theory*
3:00	Karin Gatermann, *Positive solutions of systems with mass action kinetics*	Joseph Schicho, *Improving the element pre-conditioning method by symbolic computation*	Ming Zhang, *An Approximation Approach to Molecular Conformational Search*
3:30	Break		
4:00	Carsten Conradi, *Model Discrimination using Algebraic Geometry and Computer Algebra Systems*	Jeff Farr, Shuhong. Gao, *Computing Groebner Bases for Vanishing Ideals of Finite Sets of Points*	Young Investigator: Alexey Ovchinnikov, Moscow State University, *Characterizable Radical Differential Ideals and Characteristic Sets*
4:30	David M. Malonza, *Groebner basis methods in Symbolic Computation of Invariants and Equivariants applied to Normal forms of Non linear Systems with Nilpotent linear part*	Aleksandra Slavkovic: *An Application of Algebraic Geometry in Statistical Disclosure Limitation*	Young Investigator: Hirokazu Anai, *On Solving Real Algebraic Constraints in System and Control Theory*
5:00	Bill Pletsch, *Investigating Young Group Double Cosets with Computer Algebra: Latest Advances with Some Proofs*	Quoc-Nam Tran, *A Maple package for fast conversion of Groebner bases*	Young Investigator: Virginia Rodrigues, *Grobner Basis Structure of Finite Sets of Points.*
5:30		Éric Schost, Erwan Le Pennec, *Computing foveal wavelets*	Young Investigator: Ana Gonzalez-Uriel, *Expert System for House Layout Selection*
	Activity: Banquet Dinner Speaker: Eugenio Roanes-Lozano		

Wednesday July 30, 2003

Start Time	A	B	C
9:00	**Redhat Tour**		
9:30			
10:00			
10:30			
11:00	Rida Farouki, *Minkowski geometric algebra of complex sets.*	Bradford Hovinen, *On Montgomery's Block Lanczos Algorithm*	Laurent Bernardin, *Maple on the Web*
11:30	Lihong Zhi, *A complete symbolic-numeric linear method for camera pose determination.*	Victor Pan, *Nearly Optimal Toeplitz/Hankel Computations*	Stephen Buswell, *MathML, OpenMath and the Evolution of Maths on the Web*
12:00	John May, *Bounding the Radius of Irreducibility of Multivariate Polynomials.*	Shuhong Gao, *Random Krylov spaces over finite fields*	Olga Caprotti, *Mathematical Services Registration and Discovery*
12:30	Lunch		
2:00	Mohamed Shalaby, *Spline Implicitization of Planar Curves*	Wayne Eberly, *On the Reliability of Block Lanczos Algorithms*	James Davenport, *Mathematical Knowledge Management.*
2:30	Wen-shin Lee, *Symbolic-Numeric Sparse Interpolation of Multivariate Polynomials.*	Pascal Giorgi, *From BLAS routine to finite field exact linear algebra solution*	Mike Dewar, *OpenMath and Web Services.*
3:00	Bohumir Bastl, *Symbolic-numeric method for computing surface self-intersection.*	Keith Geddes, *Exploiting Fast Hardware Floating Point in High Precision Computation*	Mika Seppälä, *Advanced Learning Technologies Project.*
3:30	Break		
4:00	Ilias S. Kotsireas, *Implicit Polynomial Support Optimized for Sparseness.*	B. David Saunders, *Rank and Smith Form of extremely sparse matrices*	Clare M. So and Stephen M. Watt, *Conversion Between Content MathML and OpenMath*
4:30	Elisabeth Malsch, *A symbolic method for defining test functions which satisfy ellipticity, boundary conditions lower order field behaviors exactly.*	Robert Lewis, *Using the Dixon Resultant on Big Problems*	Tom Wickham-Jones, *Math on the Web with Mathematica Technology.*
5:00	Daniel Lichtblau, *Computational algebra visits number theory: Trigonometric polynomials, planar extremal packings, and Groebner bases.*	Arne Storjohann, *Effective reductions to matrix multiplication*	
5:30	ACA Business Meeting		

Thursday July 31, 2003

Start Time	
9:00	**Panel Discussion**
9:30	
10:00	
10:30	**Trip to Wrightsville Beach (see Events Page)** 

Session T1: Computational aspects of algebraic curves

Organizer: Tony Shaska (University of California at Irvine).

Overview

Problem:

Algebraic curves have been studied for a long time, however there are still many problems left unanswered some of which with a long history. The goal of this session is to look at some of these problems from a computational point of view. Furthermore, we want to explore how new computational techniques can be used to study algebraic curves.

Motivation and Importance:

The development of new computational techniques has made it possible to attack some classical problems of algebraic geometry. The goal of this session is to highlight such computational techniques related to algebraic curves. Especially, we would like to explore how computational algebra packages can be used to study the geometry of algebraic curves. Topics of the session include, but are not limited to:

- Algebraic curves and their automorphisms, Hurwitz curves,
- Jacobians of algebraic curves, curves with split Jacobian, rational torsion points in the Jacobian etc.
- Computational Number Theory, rational points on curves,
- Minimal field of definition of an algebraic curve,
- Covering of the Riemann sphere by a generic curve of genus g, solvable monodromy groups,
- Interaction between computational group theory and algebraic curves,
- Groups acting on surfaces, loci of curves with prescribed automorphism group,
- Hurwitz spaces, braid action

Speakers and Abstracts

T1.1 B. Brock (Center for Communications Research). *Moments associated to the moduli space of hyperelliptic curves over a finite field*

On average there are $q^r + O(q^{(r-1)/2+\varepsilon})$ $\mathbf{F}_q$-rational points on a curve of genus g defined over $\mathbf{F}_q$ if r is odd or $r > 2g$, but if r is even and $r \leq 2g$ there are $q^r + q^{r/2} + O(q^{(r-1)/2+\varepsilon})$ $\mathbf{F}_q$-rational points on average. Of course these facts can be interpreted as statements about the moments of the roots of the Weil polynomial. Based on computations we conjecture precise formulas for the moments and product moments associated to the submoduli of hyperelliptic curves. In some cases we can prove our formulas. (The work is joint with Andrew Granville.)

T1.2 I. Burhanuddin (University of Southern California), *On computing discrete logarithms in Formal groups and it's applications*

Given $x, y \in G$ an (additive) abelian group and $y \in \langle x \rangle$ to compute $n \in \mathbf{Z}$ such that $y = [n]x$ is called the discrete logarithm problem. The supposed computational intractability of this problem in certain groups forms the core of many cryptographic systems. We provide efficient algorithms to compute discrete logarithms in certain formal groups and show how in particular this helps us to compute discrete logarithms in elliptic curves over local fields. Finally we provide some cryptographic applications.

T1.3 J. Wolper (Idaho State University), *Theta Vanishings and Automorphism Groups of Riemann Surfaces of Genus Three.*

The existence of a non-trivial automorphism group on a compact Riemann surface leads to vanishings of Riemann's theta function. Accola showed that in some cases the converse is true. In particular, certain vanishings of θ at quarter-periods imply the existence of an involution in the automorphism group. This talk will discuss these vanishings, with special attention to the case when the existence of two or more involutions is known. It will show how to use the vanishings to determine the order of the dihedral group generated by two corresponding involutions; this is topological in nature. Then, group-theoretic arguments show how to use theta-vanishings to find equations for the locus of surfaces of genus three with *given* automorphism group, in the case when the group is nonabelian and generated by its involutions.

T1.4 T. Shaska (University of California at Irvine), *Computational Aspects of Algebraic Curves, a survey.*

Let X be a genus g algebraic curve defined over an algebraically closed field k of characteristic zero. Determining the automorphism group $\mathrm{Aut}(X)$ of this curve, the field of moduli, and the minimal field of definition are some of the problems of classical algebraic geometry. We will give a survey of some of the techniques used in studying these problems. Further, we will discuss some of these problems from a computational viewpoint and show how GAP, MAGMA, MAPLE are used in the study of these problems.

T1.5 C. Yin (University of Pennsylvania), *Special Loci in Moduli of Curves.*

The talk will considers special loci in moduli space of curves of genus g with n marked points. Special loci in this space parameterize marked curves with extra automorphisms. A typical curve with marked points has no automorphisms; but some do, depending upon the choice of curves and position of marked points. This gives us certain subvarieties in the moduli space. For Riemann surfaces, these subvarieties are characterized by specifying a finite group of mapping-classes whose action on a curve is fixed topologically. Schneps considered the situation of genus 0 with n marked points, and genus 1 with $n = 1$ or 2 marked points, corresponding to the curves having a cyclic group in its automorphism group, over the complex numbers. After reviewing that work, the talk will discuss more general cases in higher genus and in characteristic p.

T1.6 M. Seppala (Florida State University), *Numerical uniformization of algebraic curves*

A smooth projective algebraic curve C is a Riemann surface, and hence can be represented as $C = D/G$ where D is an open set in the finite complex plane, and G is a group of Möbius transformations acting on D. We will discuss algorithms and their implementations which allow one to approximate the domain D and the generators of G once C is given. We will also discuss the extensions of these algorithms to the case of stable curves (with double points).

T1.7 D. Mills (Southern Illinois University), *Some Questions Regarding Avoidable Families of Sets.*

Let $\mathbb{N}$ denote the set of natural numbers. A set $S \subset \mathbb{N}$ is said to be *avoidable* if there exists a partition of $\mathbb{N}$ into two (nonempty) disjoint sets A and B such that no element of S is the sum of two distinct elements of either A or B. While avoidable sets in $\mathbb{N}$ have been studied for some time, not many families of such sets are known. To date, the Fibonacci and Tribonacci sequences have been categorized.

We define the following function. Given k, $n \geq 3$ with $n \geq k$, let $U(k,n)$ denote the number of sets $S \subset \{1,2,\ldots,n\}$ with $|S| = k$ that are unavoidable. We restrict k and n to be at least three because all singleton and size-two sets are avoidable. In this talk, we shall present a recursion algorithm to calculate $U(3,n)$ efficiently, and we shall give a nontrivial lower bound for $U(k,n)$ when $k \geq 4$.

We shall also discuss the following problem. Given an avoidable set

$$S = \{u_1, u_2, ..., u_m\} \subset \mathbb{N}$$

with $u_i u_m$ such that $\{u_1, u_2, ..., u_m, b_m(S)\}$ is also avoidable? Beyond the trivial bounds $u_m + 1 \leq b_m(S) \leq 2u_m - 3$, it is not clear what values $b_m(S)$ can take on in general.

T1.8 G. Cardona (Universitat de les Illes Ballears), *Curves of genus 2 over arbitrary fields*

In this talk we will treat the classification of curves of genus 2 over arbitrary fields of any characteristic, including the case of characteristic 2. We will start by considering the moduli space M_2 that classifies curves of genus 2 up to isomorphisms defined over an algebraically closed field, in order to show the relationship between field of definition and field of moduli. We will give explicit representatives for moduli points corresponding to curves with non-trivial reduced group of automorphisms. Then, we will show how one can obtain the classification modulo isomorphisms over an arbitrary field via the study of certain cohomology sets. This will allow us to describe the isomorphism classes of curves of genus 2 in terms of field extensions. As an application, we will give formulas for the number of curves of genus 2 over arbitrary finite fields.

T1.9 C. Hurlburt (Northern Illinois University), *Computational Aspects of Differential Algebraic Geometry.*

The field of differential algebraic geometry results from the expansion of classical algebraic geometry to include algebraic differential equations and arithmetic analogs of algebraic differential equations. Specifically, given an algebraic variety X/R and a differential operator $\delta : R \to R$, it is possible to construct a prolongation sequence of varieties $... \to \hat{X}^2 \to \hat{X}^1 \to \hat{X}^0 = \hat{X}$ compatible with the differential operator. We will discuss the explicit computation of some key objects connected with this construction.

T1.10 M. van Hoeij (Florida State University), *Reparameterizing rational algebraic curves.*

If an algebraic curve over Q is birationally equivalent over Q to the projective line, then such equivalence (a parametrization) can be found with existing computer implementations. However, the rational number coefficients in this parametrization often have much more digits than necessary. The problem we study is how to find a Moebius transformation that turns this parametrization into one with smaller coefficients.

T1.10 T. Yamauchi (Hiroshima University), *On Q-simple factors of* $J_0(N)$.

Let X be a proper, smooth, geometrically connected curve over any field k and $J(X)$ be the jacobian variety of X. We say that $J(X)$ is completely decomposable over k if $J(X)$ is isogenous to the product of elliptic curves over k. In general, it seems to be difficult to find precise informations of factors of $J(X)$. Therefore, we restrict our attention to modular curves of type $X_0(N)$. Then as a result, we give all positive integers N for which $J_0(N)$ is completely decomposable over the rational number field. Let H is a subgroup of the group generated by Atkin-Lehner involutions with respect to N. We can determine all pairs (N,H) for which the jacobian variety of a quotient modular curve $X_0(N)/H$ is completely decomposable. Furthermore we explore some open problems and conjectures in this area.

Session T2: Symbolic Summation

Organizers: Sergei A. Abramov (Russian Academy of Sciences), Marko Petkovsek (University of Ljubljana), Eugene V. Zima (University of Waterloo).

Overview

Problem:
Finding sums in closed form.

Motivation and Importance:
The problem of finding closed-form expressions for various sums is among the most ancient and attractive mathematical problems. While formulas for sums with polynomial and exponential summands have been known for a long time, systematic search for algorithms dealing with more general classes of summands began only rather recently. Some notable early achievements were Abramov's algorithms for indefinite rational summation (1971) and minimal rational-sum decomposition (1975), as well as Gosper's algorithm for indefinite hypergeometric summation (1978). A general algorithm for indefinite summation in the so-called Pi-Sigma fields was designed by Karr (1981, 1985). In the early nineties, symbolic summation received a dramatic boost with the creation of Zeilberger's algorithm for definite hypergeometric summation, and its various offspring. Since then this area of research has experienced steady and solid growth. To mention just a few of the numerous results, the efficiency of Zeilberger's algorithm has been significantly improved by various strategies and algorithmic results such as automatic filtering, creative substituting, creative symmetrizing, greatest factorial factorization, complete algorithmic characterization of applicability of the algorithm, nontrivial lower bounds for the order of the minimal telescopers, and even a direct computation of this order in the case of rational input. The Wilf-Zeilberger conjecture about holonomic hypergeometric functions has been resolved. Creative telescoping based on Karr's algorithm, as well as for Abel-type sums has been developed. More generally, the creation of a successful Galois theory of difference equations opened the way to solutions of many related problems, such as finding all Liouvillian solutions of difference equations.
The purpose of this session is to present some recent developments in the area of symbolic summation, to highlight some current directions of research, and also to identify important problems to be investigated in the future. Reports on the research in symbolic solution of difference equations and related fields are also most welcome.
Topics of the session include, but are not limited to:

- rational summation
- hypergeometric summation
- holonomic summation
- Abel-type sums
- summation of special functions
- summation by means of integral representations
- asymptotics of sums
- exact solution of recurrences
- solution of recurrences by means of generating functions
- Galois theory of difference equations

Speakers and Abstracts

T2.1 Jürgen Gerhard (Maplesoft), Ha Le (University of Waterloo), *Symbolic summation in Maple.*

The talk gives an overview of the symbolic summation capabilities and recent developments in Maple. Feedback is very much appreciated.

T2.2 Burkhard Zimmermann (RISC, Linz), *Summation in Difference-Differential Rings.*

We present summation algorithms for a certain class of summands, which we call the "level2-sequences". They include (q-)hypergeometric sequences, P-finite sequences, and many sequences involving special functions from mathematical physics.

The algorithms of Sister Celine and Kurt Wegschaider are generalized for computing (multiple) sums of level-2-sequences. In the single sum case, F. Chyzak's extension of Zeilberger's algorithm can be adapted to level-2-sequences in a straightforward way.

All algorithms presented are implemented in Mathematica.

T2.3 Sergei A. Abramov (Russian Academy of Sciences), Marko Petkovsek (University of Ljubljana), *Gosper's and Zeilberger's algorithms revisited.*

Gosper's algorithm takes as input a univariate hypergeometric term t_k and computes, if possible, a rational function $R(k)$ such that $s_k = R(k)t_k$ satisfies the recurrence $s_k + 1 - s_k = t_k$. However, $R(k)$ can have integer poles and hence this recurrence need not be valid for all integer k. Similarly, Zeilberger's algorithm takes as input a bivariate hypergeometric term $F(n,k)$ and computes, if possible, a rational function $R(n,k)$, and a linear recurrence operator L with polynomial coefficients (depending only on n), such that $G(n,k) = R(n,k)F(n,k)$ satisfies the recurrence $G(n,k+1) - G(n,k) = LF(n,k)$. Again, $R(n,k)$ can have integer singularities and hence this recurrence need not be valid for all integer n and k. In this talk, we discuss this phenomenon and its influence on the correctness of the final result.

T2.4 Carsten Schneider (RISC, Linz), *Symbolic Summation in* $\Pi - \Sigma$ *-Fields.*

`Sigma` is a summation package, implemented in the computer algebra system Mathematica, that enables to discover and prove nested multisum identities. Based on Karr's difference field theory (1981) this package allows to find all solutions of parameterized linear difference equations in a very general difference field setting, so called $\Pi - \Sigma$ -fields. With a refined version of this difference field machinery indefinite multisums can be simplified by minimizing the depth of nested sum-quantifiers. In addition, `Sigma` provides several algorithms in order to discover closed form evaluations of definite nested multisums. Here one first tries to compute a recurrence for a given definite sum by applying Zeilberger's creative telescoping idea in the difference field setting. Second one attempts to solve this recurrence in terms of d'Alembertian solutions, a subclass of Liouvillian solutions. As it turns out, our indefinite summation algorithm plays a major role in order to simplify those solutions further. Combining these simplified solutions one finally may find a closed form evaluation of a definite multisum. All these aspects will be illustrated by various examples.

T2.5 Victor Adamchik (Carnegie Mellon University), *Symbolic Computation of Series and Products in Terms of the Multiple Gamma and Related Functions.*

The multiple gamma function, defined by a recurrence-functional equation as a generalization of the Euler gamma function, was originally introduced by Kinkelin, Glaisher, and Barnes around 1900. Today, due to the pioneer work of Conrey, Katz and Sarnak, interest in this function has been revived. In this talk I will discuss some theoretical aspects of the multiple gamma function and its applications to summation of series and infinite products.

T2.6 Mark van Hoeij (Florida State University), *Rational definite summation.* Let $F(n,k)$ be a rational function in two variables. For positive integers n, let $R(n)$ be the sum of $F(n,k)$ for k from 0 to n. We present a method, that we conjecture to be a complete algorithm, to compute $R(n)$ if $R(n)$ is a rational function in n.

T2.7 Daniel Lichtblau (Wolfram Research Inc.), *Issues in symbolic definite integration.* The computation of definite integrals presents one with a variety of choices. There are various methods such as Newton-Leibniz or Slater's convolution method. There are issues such as whether to split or merge sums, how to search for singularities on the path of integration, when to issue conditional results, how to assess (possibly conditional) convergence, and more. These various considerations moreover interact with one another in ways that are not necessarily comfortable.

This talk will discuss these various issues, with examples. I will describe some of the successful strategies and some of the open areas (read: not terribly successful to date) for further work. The focus is not technical in regard to the specifics of integration methods, but rather is on illustrating some of the problems one faces in constructing a practical implementation. It is based on my work on Mathematica's definite integration over the past year and a half.

Session T3: Computer Algebra in Education

Organizers: Alkis Akritas (University of Thessaly), Michael Wester (Cotopaxi, USA), Bill Pletsch (Albuquerque Technical Vocational Institute).

Overview

Education has become one of the fastest growing application areas for computers in general and computer algebra in particular. Computer algebra tools such as TI-92/89, Axiom, Derive, Macsyma, Maple, Mathematica, MuPAD or Reduce, make powerful teaching tools in mathematics, physics, chemistry, biology, economy.

The goal of this session is to exchange ideas and experiences, to hear about classroom experiments, and to discuss all issues related with the use of computer algebra tools in classroom (such as assessment, change of curricula, new support material, ...)

Speakers and Abstracts

T3.1 Jerry Uhl (University of Illinois at Urbana-Champaign), *Raising the Level of Precalculus Mathematics.*

The Problems in Mathematics Education Addressed by College Prep Math (CPMath).

Today, largely because of technology, math permeates more of university education and life outside the university than ever before. In almost every field of study, math is strikingly more important than it was even twenty years ago. Many fields of study place demands on math that were not even thought about twenty years ago. Today's culture is both math needy and math hungry. But most students arrive at the university poorly prepared for the math they will use in their university education and their work. They may be prepared for the math their parents and grandparents had to learn, but this is not adequate preparation for the math they will actually use in today's world of technology. In fact, most of the students who score at the top on standardized tests are poorly prepared. Some can even manipulate x's and y's with reckless abandon, but have little understanding of how those skills relate to their university courses and their work beyond the university. They do not realize that because of technology such skills are not as valuable today as they were even twenty years ago. With wise use of technology, the CPMath students move from symbol pushing to understanding and see mathematics as worthy of serious attention. On the other side of this problem is that many of the most creative students have been turned off with math courses in algebra and trigonometry that emphasize drill on rote manipulations of seemingly meaningless symbols. These are often the students who continually ask, "What's this stuff good for?" only to be told (often incorrectly) that they will need it later on. This group needs a new way of learning with content appropriate for answering the question "What's this stuff good for in today's world?"

College Prep Math (CPMath) is designed to address both issues. For students who have been enjoying their school math, the course is an opportunity to learn what is important at the university level before they get to the university. For students who have been turned off by school math, this course is an opportunity for a new start and a fast track to the math (in context) that actually arises in science, engineering, technology and in the workplace.

Why CPMath is a recommended alternative to conventional courses called "Pre-Calculus?"

Conventional precalculus courses spend the most of the students' time rehashing the techniques that the students have taken previously. What's worse is that conventional precalculus courses give almost no hint of what calculus is. These courses look backward and not forward. CPMath looks both ways.

CPMath students deal with almost all underlying calculus and engineering concepts through approximate numerical calculations instead of the exact formula manipulation found in calculus. These include the studies of growth and change as well as approximate area measurements and approximate tangent lines. CPMath students experience all the underlying calculus ideas (but not all calculus techniques) and are not blind-sided as they step into university calculus and mathematics.

How learning in CPMath differs from learning in conventional mathematics courses.

When you want a youngster to learn about cats, do you give a lecture telling them that a cat is a small carnivorous mammal with rectile claws and distinctive sonic output? Instead, you put a kitty in front of the youngster and let the youngster see, feel and play with the kitty. CPMath students use the CPMath computer courseware to play with the math kitty through dazzling interactive computer graphics (of a quality and a quantity impossible in a conventional textbook), instant calculation and experimentation. (One student called the CPMath format "a mathematical chemistry set.") CPMath students have the freedom to experiment and inspect the results. The interactive visualizations and experiments in CPMath set up the ideas giving students instant access to the ideas. Students in conventional courses attempt to learn the material through a maze of unfamiliar words. They are forced to memorize because they don't always have an idea about what the words mean. In CPMath, the understanding students get through visualization and experimentation minimizes the need for memorization. In CPMath, only after an issue has been set up visually do the words go on. And when the words go on, they are in standard American and not in the stilted language usually associated with conventional mathematics text books. Professional studies show that random learners and sequential learners do equally well in the CPMath format; they use the computer-based courseware in different ways as they see fit. Anecdotal information from University of Illinois at Urbana-Champaign and The Ohio State University indicates that dyslexic, ADD, autistic and brain-damaged students have done well in the CPMath format. Perhaps Lynn Arthur Steen, past president of the Mathematical Association of America, summed it up best when he wrote: "Most students take only one or two terms of college mathematics,and quickly forget what little they learned of memorized methods for calculation. Innovative instruction using a new symbiosis of machine calculation and human thinking can shift the balance of mathematical learning to understanding, insight, and mathematical intuition." CPMath is the first course at the precollege level that delivers on Steen's vision.

T3.2 Eugenio Roanes-Lozano (Universidad Complutense de Madrid), Eugenio Roanes-Macias (Universidad Complutense de Madrid), *Symbolic Manipulation in Projective Geometry through the Cooperation of Dynamic Geometry Systems and Computer Algebra Systems.*

Dynamic Geometry Systems (DGS) were developed with the intention of allowing the user to "explore" (plane) Euclidean Geometry the same way he would proceed with (graduated) rule and compass. The adjective "dynamic" comes from the fact that, once the sketch is finished, the first objects drawn (points) can be dragged and dropped with the mouse, consequently changing the whole sketch.

Unfortunately, Computer Algebra Systems (CAS) and DGS have evolved independently. Some CAS, like Maple, include powerful packages devoted to Euclidean Geometry, but no one includes dynamic capabilities.

On the other hand, DGS cannot deal with non-assigned variables. This fact prevents the use of DGS in any process involving non-assigned variables, like mechanical theorem proving in Geometry (where it is standard and necessary to consider parameters as certain coordinates of the initial points).

Other authors have solved these lacks in different ways, but all the approaches we know are based in implementing new software (whole DGS and/or CAS): The Algebraic Geometer, GDI (unifying the former Lugares, Discovery and Rex), Geometry Expert and MathXP.

Our strategy is completely different: software reuse. Another difference is that we do not try to produce a system that exceeds in a certain task (e.g. mechanical theorem proving in Geometry) but a kind of dynamic Graphic User Interface (GUI) with diverse applications.

We have developed a bridge between existing DGS and CAS: GSP v.3 & v.4 and Maple 8 and Derive 5 that is published elsewhere. Now a new adaptation to the projective case is presented.

T3.3 Laurent Bernardin (Maplesoft), *A Look at the New Student Package in Maple.*

Maple's new student package provides tools for supporting the teaching and learning of concepts in first year calculus, linear algebra as well as precalculus. The packages allow computations (like integration, differentiation, limits, Gaussian elimination and others) to be performed step by step such that the solution process is exposed. Visualization routines illustrate key concepts in the material being taught. Interactive tutors (using the Maplets technology) provide an environment for exploring the mathematical concepts in an interactive way. Educators can use all of this material to enhance the delivery of a course. Students will be able to use the package to reinforce what they have learned in class.

T3.4 Michel Beaudin, (École de Technologie Supérieure Montréal), *Give Mathematics a Chance!*

Why is technology (CAS) dividing mathematics teachers into (at least) two groups? Those (this is our case) who love to use it and think that software like Derive and the TI-92 Plus/Voyage 200 are very good tools for teaching and learning mathematics and those who think that students should learn to do everything by hand, first, before using Computer Algebra Systems. We don't know the answer but we are going to give examples of how both (use of a CAS and paper/pencil techniques) can be happily joined. There is no magic way to teaching but trying to convince our (engineering) students that mathematics are useful comes easier with a good use of technology. Live examples will be performed, originating from students' questions.

T3.5 Karsten Schmidt (University of Applied Sciences, Schmalkalden), Wolfgang Moldenhauer (ThILLM, Bad Berka), *Using the TI-89 in Math Education - What are the Students' Views?*

Authorities in the German state of Thuringia are considering allowing the use of CAS technology in math education in schools. Therefore, a project in 8 grammar schools is being carried out to investigate which effects the use of the Texas Instruments TI-89 in math classes has on math skills. As from grade 10, these calculators are provided free of charge to all students in the project schools for use in math courses (and examinations).

In November 2002 a survey was carried out to find out which views all (about 1000) grade 11 and 12 students in the project schools have on using the TI-89 in math and science. Students of three different levels are in the project: each student has at least to attend a math "Grundkurs", a course that is offered in every grade and communicates the basic math competence. Students with more interest in math opt to attend the math "Leistungskurs" which imparts more advanced material (in more hours per week). Two of the project schools have special classes open only to the most talented math students in Thuringia.

The main part of the one-page questionnaire comprised 8 statements - 7 related to the effects of using the TI-89 in math and science lessons and one general statement about math lessons. Students were asked to mark on a scale how strong they agree or disagree with each statement. In the paper it will also be analyzed how certain characteristics of the students (e.g., which type of course they are in; which grade they got in math in their last report) influenced their answers.

T3.6 Bill Pletsch (Albuquerque Technical Vocational Institute), *A CAS Lecture for the Calculus Students: The Riemann Product.*

The use of computer algebra in the mathematics classroom will be discussed. As an example, a specific computer classroom lecture will be demonstrated, that of the behavior of the Riemann Product.

Last year in Volos, Greece, the tangent exponential was discussed. (A tangent exponential is an exponential function that is tangent to a curve.) This year the same technique used to develop the tangent exponential is turned on integration. The result is the Riemann Product.

Computer algebra is in a unique position to aid students in learning the Riemann Product. A graphing calculator is not enough, since symbol manipulation is required to do the necessary limits. Simultaneously, the presentation will demonstrate by example, the modern methods of presenting a mathematical concept from the numerical, graphical, and symbolic points of view.

T3.7 Giovannina Albano and Matteo Desiderio (University of Salerno), *Effective Learning using CAS.*

It is well known that differential equations represent a fundamental tool in the mathematical modeling in many applied fields such as physics, astronomy, economic sciences and others.

During our courses of mathematical analyses, we often use differential equations linked to the daily life problem, discovering in such a way, the real adhesion between experience and mathematical environment and giving motivation to the students for the study of the subject.

In such cases, we have noted that students were used to learning just some techniques, which make them able to solve some equations and when they get the results, they do not relate them to the initial problem or they elaborate some restrictions in order to avoid nonsense solutions. They were used to seeing mathematics as a tool, so they were used to learning just some techniques without “thinking”.

We believe that teaching should not be a pure transfer of notions and techniques, but it has to stimulate learning that is reasoning, induction and so on. Thus it is important to change methods, and techniques of learning and teaching. This is more and more true, because otherwise we will have just people able to do standard computations or solve standard problems, but not people able to face new problems.

We believe that the computer support allows to interpret more deeply the mathematical results that in the case of classical approaches we didn’t do. We want to stimulate the student to have a more critical attitude towards the solution of the problem described by a differential equation. We are not concentrating on “how to solve a differential equation or a Cauchy problem”, but indeed on what is the meaning of some results, stimulating students to be active asking themselves questions, not to accept passively the results they have from their own calculations.

In this work, we propose to research how the CAS can foster a more critical, significant and effective learning.

Session T4: Computer Algebra in Science and Technology

Organizers: David Jeffrey (University of Western Ontario) and Laurent Bernardin (Maplesoft).

Overview

The goal of this session is to increase the interaction between those who apply computer algebra to science and technology and specialists in the systems. We hope that developers of computer algebra systems will learn about new applications of their products and we hope that the users will be able to discuss their computational problems with experts. Talks by those who use computer algebra while studying other problems in science, technology or industry are welcome.

Speakers and Abstracts

T4.1 Paulina Chin (Maplesoft), *Automatic Code Generation*

Automatic code generation facilities within a computer algebra system allow users to work within a symbolic environment while producing code that can be incorporated into numeric systems for scientific applications.

We will show how Maple's code generation tools fit into the process of modeling scientific problems and prototyping algorithms. Furthermore, we will show how the tools may be customized for specific target languages and environments. Finally, we will discuss issues and challenges related to source-to-source translation in this context.

T4.2 Cecelia Laurie (University of Alabama), *The Use of Maple in Computing DNA Match Probabilities.*

This is joint work with B. S. Weir, Bioinformatics Research Center, North Carolina State University.

It is common practice to compute match probabilities of genotypes from two individuals at several loci by assuming independence of the loci, i.e. multiplying together one-locus match probabilities. For finite populations, differences in individual histories can cause between-locus allelic dependencies even for unlinked loci. The main motivation for this study was to quantify the effect of such dependencies on genotypic match probabilities. The match probabilities can be computed in terms of identity-by-descent probabilities, i.e. probabilities that various combinations of alleles are identical. In order to compute two-locus match probabilities, one must take into account the effects of recombination (of alleles across loci) as well as those of mutation and sampling with replacement from a finite population. These computations are highly combinatorial in nature. This talk will give a flavor of the nature of the computations and will discuss how Maple was used.

T4.3 Brian Moore (Canadian Space Agency), *Symofros: A symbolic modeling and simulation tool for mechanical system.*

Software tools for design, modeling, analysis, and simulation can greatly improve the performance and efficiency of mechanical systems. Symofros, an environment for modeling and simulation, is used for all robots and experimental systems at the Canadian Space Agency R& D Robotics Laboratory. In particular, Symofros is the core of the SPDM (Special Purpose Dextrous Manipulator) Tasks Verification Facilities[1] where a ground robot is used to emulate the contact task of a space manipulator (here the Space Station manipulator SPDM). In SMP[2], a generic simulator for astronauts training has been developed based on Symofros and other tools. SMP is used to develop situation awareness, provides kinematics and dynamics understandings of robotic systems and increases the dexterity of the operator. SMP is now on board of the International Space Station.

Symofros is composed of several modules for mechanical system description, modeling and simulation. The modeling module of Symofros, the Symbolic Model Generator, is built within Maple.

This module is composed of several Maple modules: topology, preprocessing, kinematics, non-linear dynamics, linear dynamics and dynamics identification. It automatically derives a set of over 90 functions, called basic functions, which represent the kinematics and dynamics. These functions are symbolic expressions written in terms of variables (time dependent) and parameters (constant with time). Variables comprise positions, velocities, accelerations and system inputs while parameters can be the mass and the length of the links. The functions are translated into C for simulation purposes.

T4.4 Ulrich Langer (University of Linz), Stefan Reitzinger(University of Linz), Josef Schicho(University of Linz), *Improving the element pre-conditioning method by symbolic computation.*

Recently, element preconditioning has been proposed as an improvement for the algebraic multigrid method (AGM) for solving elliptic boundary value problems (see [1]). One exploits the well-known fact that the AGM works fine when the stiffness matrix K_h is an M-matrix. Typically, K_h is not an M-matrix, but one can construct an M-matrix regularisator by assembling suitable M-matrices corresponding to the local elements. Here “suitable” means that the local M-matrix should be as close as possible – in the spectral sense – to the local element stiffness matrix.

The sub-problem of finding the closest M-matrix to a given symmetric and positive matrix has to be solved for many instances (namely, for each element). The numerical solution of all these optimization problems can be very expensive. We achieve a speed-up by solving the optimization problem once and for all symbolically, and then instantiating the solution by the local data.

Theoretically, it is possible to give a closed form solution in terms of field operations and square roots, and – in one particular case – roots of higher degree polynomials. Such a closed form would be too large to be useful, so we prefer to give a “formula” consisting of a program with arithmetic or square root (and in one case higher order root) assignments and **if the else** branches, but no loops. Using these formula, we can compute the optimal preconditioners faster and more accurately than by standard numerical optimization techniques (see [2] for a comparison).

The optimization problem can be reduced to a quantifier elimination problem over real closed fields. However, the problem is too complex for a solution by a general method like Gröbner bases, resultants, or cylindrical algebraic decomposition. It is necessary to exploit the specific structure of the problem. We use some techniques from linear algebra and geometry.

[1] Hasse G., Langer, U. Reitzinger, S., and Schöberl, J. Algebraic multigrid methods based on element preconditioning. *International Journal of Computer Mathematics 78*, 4 (2001), 575–598.

[2] Langer, U., Reitzinger S., and Schicho, J. Symbolic methods for the element precondition technique. In *Proc. SNSC Hagenberg 2001 (2002)*, U. Langer and F. Winkler, Eds., Springer.

Session T5: Gröbner Bases and Applications

Organizers: Quoc-Nam Tran (Lamar University) and Alexander Levin (Catholic University of America).

Overview

This session is a continuation of a series of sessions on the theory of Groebner bases and its applications organized at previous ACA conferences and other workshops. The method of Groebner bases has become one of the most important techniques in providing exact solutions of nonlinear problems in multivariate polynomial ideal theory, in computational commutative algebra, in elimination theory, in solving systems of algebraic equations, and in many other related areas. It is also being used fruitfully in a variety of seemingly unrelated research areas such as geometrical theorem proving, integer programming, solid modeling and engineering. The method is implemented in all major computer algebra systems.

Nevertheless, the field is still under active development both in the direction of improving the method by new theoretical insights and in finding new applications. This time we will concentrate on efforts to improve the method including:

(a) enlarged criteria for detecting useless zero reductions,
(b) basis conversion,
(c) involutive algorithms and Janet bases,
(d) nontrivial applications of the method of Groebner bases in computer aided design, modeling, mathematics, sciences, engineering, logic, education and other research areas.

Speakers and Abstracts

T5.1 Yosuke Sato (Tokyo University of Science), Akira Suzuki (Kobe University), Katsusuke Nabeshima (Ritsumeikan University). *ACGB on Varieties.*

In construction of parametric Gröbner bases, we usually assume that parameters can take arbitrary values. In case, however, there exist some constraints among parameters, it is more natural to construct parametric Gröbner bases for only parameters satisfying such constraints. Using this idea, we formalized parametric Gröbner bases in terms of ACGB (Alternative Comprehensive Gröbner Bases) which we proposed in ISSAC2002. This natural formalization leads us to an interesting and desirable fact that is discrete comprehensive Gröbner bases studied by us can be naturally defined and generalized as special instances of ACGB.

T5.2 Alexander Levin (Catholic University of America), *Gröbner Bases with respect to Several Orderings and Difference Dimension Polynomials*

Let K be a partial difference field with a basic set σ and let a partition of σ into p disjoint subsets be fixed. We consider a generalization of the Grobner basis method to free difference modules and apply the new technique to the study of difference dimension. In particular, we generalize the author's theorems on difference dimension polynomials and obtain new invariants of a finitely generated difference field extension.

T5.3 V.A. Mityunin (Moscow State University), *Comparison of the parallelization quality of algorithms for computing Gröbner and involutive bases.*

T5.4 Quoc-Nam Tran (Lamar University), *Efficient Groebner Basis Computation for Finding Implicit Representations of Geometric Objects.*

The author uses new results and techniques from the method of Groebner bases to devise an efficient and reliable algorithm for finding implicit representations of geometric objects. The process of finding implicit representations is also known as implicitization. Implicitization is an “established” research topic, which is studied in several research areas such as computer aided geometric design (CAGD), visualization and solid modeling. However, until now there is no method for implicitization that is both reliable and efficient. The implicitization method using Groebner bases is reliable but not efficient and the other two main approaches, namely Dixon’s resultants and moving surfaces, are more efficient but not reliable. In the context of this research, a reliable method is a method that theoretically never fails to give a correct answer. An efficient method is a method that has a better complexity or a more reasonable running time and consumes less memory space in order to support interaction between the designer/user and the computer.

In this paper, the author investigates the use of the deterministic Groebner walk method to convert a parametric representation of a surface into its implicit form. For rational parametric surfaces, the author uses a different approach to deal with base points in that the calculation of a Groebner basis for the starting cone is no longer needed. This approach will help to improve the efficiency of the algorithms because the usual calculation of the implicit representation, which often consumes a lot of time and memory space, is replaced by a sequence of small calculations along the walking path and then lift the results using linear transformations.

Another important task of this research is to reduce the number of terms of the intermediate polynomials and find criteria for detecting unnecessary reduction. Experimental results with the deterministic Groebner walk conversion method show that most of the time for implicitization is used for reducing the minimal bases after lifting. Obviously, not all of the polynomials need to be reduced; for example, at the last cone most of the polynomials do not need to be reduced. Therefore, detecting all unnecessary reductions would be a leap in improving the efficiency of algorithms for implicitization. This will also significantly reduce the memory space needed for the calculation.

This research will hopefully produce improved algorithms for implicitization, which will never fails, faster and consume less memory space. Such an efficient and reliable algorithm will make an impact on research areas dealing with designing curves and surfaces. For example, it can be used for finding the intersection of surfaces, to verify whether or not a point lies on a surface, etc. The author expects that results from this research project will be presented at international conferences on symbolic computation as well as some publications on peer-review journals. Additionally, the author also hopes that this research will give some insight for finding extra criteria for detecting unnecessary reduction for Groebner basis computation in general.

T5.5 Edgar Martinez-Moro (Universidad de Valladolid), *Using Groebner basis for determining the equivalence of linear codes.*

Two linear codes are permutation-equivalent if they are equal up to a permutation on the codeword coordinates. We present an invariant for the class of linear codes, i.e. a mapping such that any two permutation equivalent codes take the same value. This mapping is closely related to the ideas behind FGLM (Faugere, Gianni, Lazard and Mora 1993), mainly to the presence of linear algebra techniques into the framework of some Groebner bases tools. We show how these Groebner basis tools can be used to determine if two linear codes are equivalent or not.

T5.6 Ekaterina S. Shemyakova (Moscow State University), *Projections and graphs of involutive divisions.*

In this article the definitions of projections of involutive divisions and graphs are formulated. With their help, series of new examples of involutive divisions are constructed. The criteria of completeness and globalness of involutive divisions in the language of the graphs are formulated and proved. It is obtained and proved the criterion of noetherian global involutive division corresponds to the given graph.

T5.7 Jeff Farr (Clemson), Shuhong Gao (Clemson), *Computing Groebner Bases for Vanishing Ideals of Finite Sets of Points.*

We present an algorithm that incrementally computes a Gröbner basis for the vanishing ideal of any finite set of points in $\mathbb{F}^m$ under any given monomial order, and we apply this algorithm to multivariate polynomial interpolation and rational function interpolation. Our algorithm is polynomial in the dimension, m, and the number of points, n. This approach is completely different from the several forms which rely on Gauss elimination and is, in fact, a natural generalization of univariate Newton interpolation.

T5.8 Aleksandra Slavkovic (Carnegie Mellon University), *An Application of Algebraic Geometry in Statistical Disclosure Limitation.*

Statistical disclosure limitation applies statistical tools to address the problem of limiting sensitive information releases about individuals/groups while maintaining proper statistical inferences. Within this context, Dobra and Fienberg (2000,2002) have recently employed Gröbner bases in connection with graphical models given a set of marginal counts to establish bounds and distributions for cell entries in contingency tables. Building on their work and that of Garcia et. al. (2003), we explore the applicability of Gröbner bases in connection with Bayesian networks to address the issue of data confidentiality when the released information is in the form of an arbitrary collection of conditional and marginal distributions.

T5.9 Quoc-Nam Tran, *A Maple package for fast conversion of Groebner bases.*

In this talk, the author will present a new Maple package that uses the deterministic Groebner walk method for fast conversion of Groebner bases. Previous efforts to implement the Groebner walk method encountered some technical problems, which resulted in packages with many limitations. This new package overcame most of the known technical difficulties in dealing with term orders and big weight vectors. Comparison with Maple's implementation of the traditional Buchberger's algorithm and FGLM conversion will be given to illustrate the efficiency of the Groebner walk method.

T5.10 Éric Schost, Erwan Le Pennec, *Computing foveal wavelets.*

Session T6: Interval Computation

Organizers: Ned Nedialkov (McMaster University) and George Corliss (Marquette University)

Overview

Symbolic and interval validated techniques are natural allies. Symbolic techniques attempt to compute exact answers. When exact answers are not available, a symbolic environment must resort to numerical techniques. It would seem that the guarantees of interval techniques are more philosophically satisfying than more standard approximate techniques. Further, interval techniques tend to draw more heavily than approximate techniques on the tools of symbolic computations.

This session attempts to build bridges between symbolic and interval researchers. We provide a survey of interval techniques and present some recent developments in interval computing we think may be useful in the context of symbolic algorithms. We present some interval research challenges for which symbolic techniques may provide the answers. Our goal is to facilitate interactions between symbolic and interval researchers.

Speakers and Abstracts

T6.1 Ned Nedialkov (McMaster University), *Introduction to Interval Numerical Methods.*

Interval methods produce bounds that are guaranteed to contain mathematically correct results. Such bounds enclose truncation, rounding, and often modeling errors. Simply replacing reals by intervals in a point numerical method usually leads to a "naive" interval method, which computes bounds that are generally too wide to be useful. To compute sufficiently tight bounds, an interval method normally involves specific "interval" machinery. This talk presents interval arithmetic and techniques commonly used in interval methods.

We discuss interval arithmetic and some of its properties. Bounding ranges of functions is central to interval computing. We illustrate popular approaches, such as the mean-value form, the slope form, and Taylor series, for bounding ranges of functions.

A contractive mapping theorem is frequently the basis of an efficient interval algorithm. We show how contractive mapping (and other approaches) are employed when enclosing the solution of a nonlinear system of equations, using an interval Newton method, and when enclosing the solution of a linear system of equations.

We also discuss briefly several popular interval-arithmetic packages.

T6.2 John D. Pryce (Cranfield University, RMCS Shrivenham), *Mapping Expressions to Functions in Cset Interval Arithmetic.*

Csets (containment-sets) are a way of giving expressions a value even at arguments that give rise to division by zero or other "illegal" operation. The definition for evaluation over the reals is that, if $f(x)$ is a function of n variables (so $x = (x_1, \ldots, x_n)$) then its cset at a point $x = a$ is the set of all limits, in the extended reals $[-\infty, +\infty]$ of sequences of values $y_j = f(x_j)$ where the sequence (x_j) converges to a. Thus, regarding $1/0$ as the value of x/y at $x = 1$, and $y = 0$ one has in the cset sense $1/0 = \{-\infty, +\infty\}$, similarly $\sin(+\infty) = [-1, +1]$, and so on. This leads to an arithmetic system in which exceptions do not occur, but where point inputs can produce set outputs.

There are subtle difficulties associated with this programme. How are set-valued constants to be interpreted? For instance, does it make sense to define a function $f(x)$ by $f(x) = \frac{[1,2]}{x+[1,2]}$? When we see the expression $1/0$, how do we know to interpret it as the function $f(x,y) = x/y$ evaluated at $x = 1$, and $y = 0$?

T6.3 Nathalie Revol (INRIA, LIP, École Normale Supérieure de Lyon) *Multiple Precision Interval Arithmetic and Application to Linear Systems.*

Introduction to MPFI. Interval arithmetic provides guaranteed results: it encloses every value or result in an interval, and it computes with these intervals. However, the resulting intervals may grow as the computations proceed. To obviate this swelling, contracting iterative methods are favoured. With such methods, the computing precision becomes a limiting factor. This observation led us to propose a library for arbitrary precision interval arithmetic, Multiple Precision Floating-point Interval (MPFI) arithmetic library, built upon Multiple Precision Floating-point Reliable arithmetic (MPFR, `www.mpfr.org`). MPFI is developed by N. Revol and F. Rouillier in C and can be freely downloaded from `www.ens-lyon.fr/~nrevol/`.

Applications. Some algorithms have been developed using MPFI. A first algorithm isolates the real roots of a polynomial using a multiple precision interval arithmetic in the Uspensky (or rather Vincent) algorithm to avoid time-consuming exact computations. A second one is the adaptation of the interval Newton algorithm to this arithmetic. The Interval Newton algorithm encloses the real roots of a function and may also determine the existence and uniqueness of these roots in the returned enclosing intervals. The proposed algorithm additionally allows to enclose the roots with arbitrary accuracy.

Linear systems. Solving a linear system $\boldsymbol{A}x = \boldsymbol{b}$ with a matrix $\boldsymbol{A}$ and a vector $\boldsymbol{b}$, both with interval components, amounts to determining an enclosure of $\{x : \exists A \in \boldsymbol{A} \text{ and } \exists b \in \boldsymbol{b} \text{ such that } Ax = b\}$. Gauss-Seidel iteration, applied to the pre-processed system $C\boldsymbol{A}x = C\boldsymbol{b}$ with C a point matrix, is often used. This method is called the Hansen-Sengupta algorithm. When this iteration can be made contracting, it is a method of choice for interval arithmetic and also for arbitrary precision interval arithmetic. Another linear system comes from signal processing: determine the dynamics of an IIR filter. This problem can be written as an iteration similar to Gauss-Seidel. We will present some preliminary results on this problem.

This type of iteration may be comparable with the technique of elimination of division as presented in Strassen, 1973, which is classical in symbolic computations.

T6.4 Markus Neher (Universität Karlsruhe), *From Intervals to Taylor Models: A Numeric-Symbolic Approach to Validated Computation.*

Interval arithmetic has been widely used in enclosure methods for almost 40 years. It is a well established tool for the calculation of rigorous error bounds for many problems in numerical analysis. However, interval arithmetic suffers from two drawbacks: the dependency problem and the wrapping effect. Both can cause an overestimation of the solution set of a given problem, so that the computed error bounds may become over-pessimistic in practical calculations.

To reduce the overestimation of the true error, Taylor models have been developed by Berz and his group since the 1980s. A Taylor model of a function f on an interval X consists of the Taylor polynomial p_n of order n of f and an interval remainder term I_n, which encloses the approximation error $|f - p_n|$ on X. In computations that involve f, the function is then replaced by $p_n + I_n$. The polynomial part is propagated by symbolic calculations, whereas the interval remainder term encloses all truncation and roundoff errors that appear in the computation. Thus, Taylor models can be regarded as a symbiosis of a computer algebra method and interval arithmetic.

Software implementations of Taylor models have been applied to a variety of problems, such as global optimization problems, validated multidimensional integration, or the solution of ODEs and DAEs.

Our talk will present an introduction to Taylor models and discuss some open problems.

T6.5 Jeff Tupper (University of Toronto), *Pictures from Proofs: Sound Graphing Algorithms.*

Given just a picture of a relation, what can we deduce about the relation? If the picture was produced by a typical equation graphing program then almost nothing can be deduced as such pictures contain, by themselves, very little useful information. This clearly could be improved upon. I begin by offering some simple semantics for pictures of relations. After discussing some of the limitations of these semantics, I will outline some algorithms. Much of this work is embodied in GrafEq, which is available from `www.peda.com/grafeq`.

T6.6 Ekaterina Auer (University of Duisburg-Essen), *Interval Arithmetic in the Multibody Modeling System MOBILE.*

We show how a variety of interval algorithms found their use in an important area of applied physics, multibody systems' modeling, and in particular, in the multibody modeling program MOBILE. The talk acquaints the audience with the key features of this open source software (e.g. its object-oriented approach resulting in usage of state objects and transmission elements for modeling of arbitrary mechanical systems), outlines the main advantages of applying interval arithmetic concepts to it (e.g. an opportunity to implement new kinds of transmission elements), and concentrates on interval modeling of dynamics, which is an inherent part of almost all multibody simulations. In the latter case, the strategies to overcome difficulties with integration of an interval initial value problem solver into MOBILE are described and as a result, its interval extension enhanced with such a solver (based on VNODE) is presented. The functionality of the above ways of intervals' application is shown on some examples. We provide insight into techniques used to enhance already existing modeling software with interval arithmetic concepts.

T6.7 Yves Papegay (INRIA Sophia Antipolia), *ALIAS: A Library Mixing Interval Analysis and Computer Algebra.*

ALIAS is a C++ library of algorithms that deal with systems of equations and inequalities. Most of these algorithms are based on interval analysis, but some of them are related to constraint programming methods, and a few others perform symbolic computations. The scope of ALIAS includes algebraic expressions and also expressions involving intervals. The library provides tools for a wide range of problems including finding an approximation of the real roots of a 0-dimensional system, giving bounds of the roots of an univariate polynomial, and performing global optimization of a function with interval coefficients.

T6.8 Stan Wagon (Macalester College), *The Role of Symbolic Computation in the SIAM/Oxford 100-Digit Challenge*

The challenge of the title consisted of ten computing problems (available from `www.siam.org/siamnews/01-02/challenge.pdf`) posed by L. N. Trefethen, who offered a cash prize for the best solutions. The event attracted 94 teams from 25 countries. The problems were numerical in nature, but symbolic computing was able to play an important, and sometimes surprising, role in about half of them. Interval arithmetic provides both an algorithm and verification for the global optimization problem of problem 4; intervals are also useful for problem 2, as a way to control the exposure to excessive rounding error. For problem 9, computer integration plays a surprising role. Symbolic work yielded interesting results in several of the other problems too, such as 6, 7, and 10. The important moral is that symbolic computation and interval methods can be very important in work on problems that are ostensibly purely numerical.

Session T8: Session on Elimination Theory

Organizers: Carlos D'Andrea, Amit Khetan (UC Berkeley).

Overview

Problem:
Elimination Theory is the study of eliminating unknowns from equations (polynomial or differential). Some of the typical computational tools in this area are

- Groebner bases
- resultants
- characteristic sets

It is our intention to invite researchers working currently in this area in order to have a general overview of recent developments, applications and future directions.

Motivation and Importance:
Elimination theory is classical topic that has been studied for hundreds of years. Recent extentions to the realm of symbolic computation has led to numerous applications such as solving algebraic equations, geometric theorem proving, computational algebraic geometry and Computer Aided Graphic Design. In this session we investigate how modern techniques in symbolic computation can be used to effectively solve a variety of problems from different domains that fall under the general heading of elimination theory.

Speakers and Abstracts

T8.1 E.L. Mansfield (University of Kent) and A. Szanto (North Carolina State University), *Elimination theory of non-commutative algebras of differential invariants.*

We consider non-commutative algebras comprising of non-linear invariantized differential equations with invariant differential operators acting on them. The structure differs from standard differential algebras in that the application of the invariant differential operators introduces error terms. By close inspection of the error terms we are able to prove that an extended non-commutative version of the differential Gr"obner basis algorithm terminates in algebras of differential invariants. Applications include classical invariant theory, geometric integration and invariant numerical schemes.

T8.2 John Nahey, *Differential Resolvents of Minimal Order and Weight.*

Any univariate polynomial whose coefficients lie in a differential field of characteristic zero possesses an associated nonzero linear ordinary differential equation called an alpha-resolvent of the polynomial. In the case that the distinct roots of the polynomial are differentially independent over constants, we will determine the minimal number of powers of alpha that appear with nonzero coefficient in a resolvent of smallest possible order. We will then give an upper bound on the weight of a resolvent of smallest possible weight. The difficult part of calculating this upper bound was generalizing the known case of simple roots to multiple roots. I will present the various ways I eliminated the roots with the help of computer algebra before figuring out the proper symbolic formula.

The material from this talk comes from my paper, "Differential Resolvents of Minimal Order and Weight", currently under review by the Journal of Symbolic Computation (JSC3359), and online at the preprint server at

`http://www.mathpreprints.com/math/Preprint/resolvent`

This work is a "prequel" to the poster I presented at ECCAD2002 in which I used partial differential equations to factor terms of the alpharesolvent given by the Powersum Formula.

T8.3 Arthur Chtcherba (University of Wyoming), *Sylvester-type matrices via the Dixon resultant formulation and their optimizations.*

The computation of a resultant of a polynomial system is one of the fundamental problems in computer algebra. The significance of the resultants rapidly grows with advancement of technology as well as the efficiency of methods to compute them. Since most efficient methods reduce resultant computation to the computation of the determinant of a symbolic matrix, the matrix size is a major bottleneck in the computation of the resultant of a polynomial system. In this talk we outline a new construction of Sylvester type resultant matrices which is derived from the Dixon/Bezout formulation. We show that in practice these matrices are usually much smaller than the Sylvester-type resultant matrix based on other constructions. Consequently, a resultant method based on such matrices is of lower overall complexity. Moreover, it is possible to select certain construction parameters based on the support structure of an input polynomial system to minimize the size of these matrices. The method has been implemented, tried on a variety of examples and compared with other resultant methods.

T8.4 Manfred Minimair (Seton Hall University), *Developments in Resultants of Composed Polynomials.*

We give a survey on toric (sparse) resultants of composed polynomials. By the toric (sparse) resultant, we mean an irreducible polynomial in the coefficients of a set of given polynomials that vanishes if the given polynomials have a common zero. By a composed polynomial we mean the polynomial obtained from a given polynomial by replacing each variable by a polynomial. We give an overview of previous findings as well as of a recent one, all providing the irreducible factors of resultants of various composed polynomials. Furthermore, we discuss open questions. This line of research is motivated by the need for efficiently eliminating variables from composed polynomials.

T8.5 Amit Khetan and Carlos D'Andrea (UC Berkeley), *Implicitization of Rational Surfaces with Toric Varieties.*

Implicitization of parametric surfaces in P 3 is an important problem in CAGD and there have been a number of new techniques in recent years. Following a suggestion by Bernd Sturmfels, we reduce the computation of the implicit equation to the computation of the Chow form of a certain toric surface which projects onto our rational surface. Exact formulas for the latter were found by the first author in his Ph.D. thesis. In many cases this leads to an exact determinantal formula for the implicit equation, for example in the case of no base points or more generally if the basepoints are isolated local complete intersections. Projection from a toric variety often leads to far fewer basepoints and smaller matrices then previously studied methods.

T8.6 Laurent Busé (Mathematical Sciences Research Institute, Berkeley), *Implicitizing rational hypersurfaces using approximation complexes.*

The implicitization problem asks for an implicit equation of a rational hypersurface given by a parameterization map $\phi : \mathbb{P}^{n-1} \to \mathbb{P}^n$, with $n \geq 2$. This problem received recently a particular interest, especially in the cases $n = 2$ and $n = 3$, corresponding respectively to curves and surfaces implicitization,because it is a key-point in computer aided geometric design and modeling. In this talk I will report on joint works with Marc Chardin (University of ParisIV) and Jean-Pierre Jouanolou (University of Strasbourg) using approximation complexes to solve this problem when the base points of the parameterization map ϕ are isolated and locally a complete intersection. I will also try to show theclose link with the so-called method of moving surfaces for curves and surfaces implicitization.

T8.7 Marc Moreno Maza (University of Western Ontario), *Recent advances in triangular decomposition methods.*

Like Gröbner bases of polynomial ideals, triangular decompositions of algebraic varieties are computed by means of rewriting techniques and offer important features such as canonicity. The drawback is their theoretical complexity which is superior to that of probabilistic methods for solving polynomial systems.

Most of the effort in the area of triangular decompositions was devoted in the recent years to the design of algorithms for processing arbitrary systems of algebraic or differential equations. However, many systems of equations arising in practice have structural properties.

We will present new developments based on this observation (and others) leading to algorithms for triangular decompositions whose practical complexity is far improved.

T8.8 Ilias S. Kotsireas (Wilfrid Laurier University), *Recent advances in polynomial system solving and an application in Chaos Theory.*

Polynomial systems of equations arise ubiquitously in Mathematics (Differential Equations, Graph Theory, Topology etc), Physics, Chemistry and many other branches of Science. Often the polynomial systems arising naturally in these areas exhibit some sort of symmetry that can be accounted for rigorously using group theoretic ideas such as representations and invariant theory of finite groups. I will discuss some aspects of a joint work with R. Corless (UWO, Canada) and K. Gatermann (ZIB-Berlin, Germany) on solving efficiently polynomial systems with symmetries. To illustrate the method I will discuss an application from Chaos Theory, namely the determination of bifurcation points of the logistic map. The logistic map is the prototype of one-dimensional mappings of the interval and although it is the simplest example of a nonlinear dynamical system, it captures remarkably many features of more general nonlinear systems. The global structure of the bifurcation diagram for instance, is a universal property.

T8.9 Ming Zhang (University of Texas), *An Approximation Approach to Molecular Conformational Search.*

Searching for molecular conformations with respect to geometric and energy constraints is frequent in computational biology and chemistry. The conformational search often can be reduced to solving systems of polynomial equations. These equations, however, have number of unknowns and degree beyond the scope of the available algebraic systems.

Realizing solving for the exact solutions is a too difficult task, we turn to seek the approximations. I will present two methods that we have investigated to find the real solutions of the polynomial equations.

The first method computes the number of solutions in regions of the parameter space. By subdividing the regions into smaller and smaller sizes, we get closer and closer approximations to the solutions. This method uses bilinear mappings induced by the polynomials defining the boundaries of the regions, and obtains the solution counts from the positive and negative eigenvalues of the bilinear mappings. The mappings, however, are computed using Groebner bases or resultant matrices. We experienced very big computational complexities from them. This method thus still remains theoretical.

The second method focuses on eliminating regions that contain no solutions in the parameter space instead of obtaining number of solutions within the regions. This method also carries a subdivision process. With enough steps, the regions become so small that the values of the original polynomials can be approximated by evaluating at any point inside the regions. The final small regions after the subdivision process are reported as the approximations of the solutions. This method, with an initial implementation, has “solved” systems of six polynomials equations (degree 10) rising from the docking problems in computer-assisted drug design. To our knowledge, no other deterministic algebraic methods have solved these equations.

Session T9: Computer Algebra and Polynomial Systems in Chemistry

Organizer: Karin Gatermann (Konrad-Zuse-Zentrum, Germany)

Overview

Problem:

In the recent years there has been progress in applications of computational algebra to chemistry including the related areas of biophysics, biochemistry, geosciences, and others. The session will center around the new applications of symbolic and algebraic computations in this area. In stoichiometric network analysis systems with mass action kinetics are investigated which are polynomial differential equations. The main progress is due to the application of toric geometry to steady state analysis. This includes multistationarity and results on the dynamical behavior. A different, but related, approach is the time series analysis of biochemical models over discrete fields. Another approach to the investigation of dynamical systems is that of normal forms which requires computational invariant theory.

Motivation and Importance:

Various phenomena in chemistry, biophysics and mathematical biology are modeled by differential equations or discrete dynamical systems. Mass action kinetics is to most common and most basic model available. Computer algebra enables the exploitation of structure and gives new insights. In particular the presence of multistationarity is important since this is the basis for other dynamical phenomena such as Hopf bifurcation, bistability and reaction-diffusion waves. This theory enables to exclude already in the creation process models with unwanted properties, the so-called model discrimination. The time series analysis of biochemical systems gives insight which chemical species is influencing others and thus can be viewed as the main species.

Speakers and Abstracts

T9.1 Anke Sensse (Fritz Haber Institut, Berlin), *Electrocatalytic oxidation of formic acid*

Modeling the dynamics of a chemical reaction systems is an interesting topic where the application of convex and toric geometry can be of great advantage. As an illustrative example a model for the electrocatalytic oxidation of formic acid will be presented. It will be shown how a realistic system involving different rate laws like mass action kinetics and Butler-Volmer kinetics can be described by a set of purely polynomial ordinary differential equations. The property of the set of positive stationary solutions of such systems as an intersection set of a convex cone and the variety of a toric ideal will be explained in details. It allows to reduce this high dimensional set to a curve and leads to a new parameterization of the steady state. The stability analysis can then be executed with the usual theorems stemming from the theory of dynamical systems. Of special interest are bistability and oscillatory instabilities. The consideration of this problem under the light of toric geometry allows to make justified conclusions about the occurrence of such dynamical phenomena and about the parameter range in which they are to be expected.

T9.2 Brandilyn Stigler (VBI Virginia), *Polynomial Models for Gene Regulatory Networks.*

Several different approaches to modeling of gene regulatory networks have been used in recent years, in particular ODE-based models and Boolean networks. In this talk we propose a modeling approach that can be thought of interpolating between these two frameworks. It is based on the concept of a dynamic network represented by polynomial functions on finite, but arbitrarily large state sets. Applications contain the reverse-engineering of gene regulatory networks from data, as well as the reverse-engineering of dynamics. The polynomial framework makes it possible to bring to bear the powerful machinery of algorithmic polynomial algebra.:

T9.3 Karin Gatermann (Konrad-Zuse-Zentrum), *Positive solutions of systems with mass action kinetics.*

The behavior of the concentrations of chemical species in a system of chemical reactions is given by a polynomial differential system. We are interested in the stationary solutions and thus the positive solutions of a system of sparse polynomial equations. The system comes with a rich structure given by two graphs, a directed graph describing the chemical reactions and a bipartite graph for the stoichiometric coefficients. The polynomials depend on many unknown parameter. We show the existence of special solutions of type complex balancing with the Cayley trick. The existence of several positive solutions is shown by a variation of the Viro method. This is based on the approach to intersect a deformed toric variety with a convex polyhedral cone. The generators of this cone are known as extreme fluxes or extreme currents. The so-called stoichoimetric generators are central for multistationarity. Our result gives the parameter region where multistationarity is expected to occur.

T9.4 Carsten Conradi (Otto-von-Guericke Universitt Magdeburg), Jörg Stelling (Max Planck Institut, Magdeburg), Jörg Raisch (Max Planck Institut, Magdeburg). *Model Discrimination using Algebraic Geometry and Computer Algebra Systems.*

Model discrimination is concerned with the ability to make distinctions between different reaction networks (i.e. directed graphs) based on available experimental data and qualitative properties of the reaction networks and their associated dynamical models. Whereas it is a straithforward procedure to translate a network structure into a set of ordinary differential equations (ODEs) with yet unknown parameters (i.e. a dynamical model), it is not a-priori clear, which network structure will yield a dynamical model that is compatatible with the available experimental data. We suggest to use qualitative properties, such as the number of steady states, to discriminate between different network structures. The solution set of a system of sparse polynomial equations is identical to the staedy states of a system of ODEs derived from a (bio)chemical reaction network. Since the unknowns represent chemcial concentrations we are only interested in real nonnegative solutions. Our contribution show how results from [1] can be applied to model discrimination.

Two simplified, yet realistic network structures describing the transition between two phases in the cell of Saccharomyces cerevisiae (budding yeast) are examined: Under the assumed conditions the qualitative behavior of the system is primarily characterized by the existence of two staedy states, one corresponding to the G1-phase and one to S-pahse and Mitasis. For model discrimination it is sufficient to show that the ODE system corresponding to one of those network structures will never exhibit two steady states, regardless of the parameter values, whereas for some parameter values the system associated with the second network structure indeed admits two steady states.

Thus two sets of sparse polynomial equations are investigated by using certain triangulations of the Newton polytopes associated with those sets. Each triangulation defines a subnetwork of the original reaction network and thus a set of polynomial equations involving less terms. Based on results from [1] the existence of two nonnegative solutions for these sets of polynomial equations is explored. Extension to the complete set of polynomial equations and thus to the complete network is then possible by again using results from [1].

[1] Karin Gatermann and Matthias Wolfrum. Bernstein's 2. theorem and Viro's method for sparse polynomial systems in chemistry.

T9.5 David M. Malonza (Iowa State University), *Groebner basis methods in Symbolic Computation of Invariants and Equivariants applied to Normal forms of Non-linear Systems with Nilpotent linear part.*

The set of systems of differential equations that are in normal form with respect to a particular linear part has the structure of a module of equivariants, and it is best described by giving a Stanley decomposition of that module. Groeber basis methods(implementable in a computer algebra system) are used to determine the Stanley decomposition of the ring of invariants, that arise in normal forms for systems with nilpotent linear part consisting of repeated 2x2 Jordan blocks. An efficient algorithm developed by Murdock is then used to produce a Stanley decomposition of the module of the equivariants from the Stanley decomposition of the ring of invariants.

T9.6 Bill Pletsch (Albuquerque Technical Vocational Institute, USA). *Investigating Young Group Double Cosets with Computer Algebra: Latest Advances with Some Proofs.*

Consider a deuteron colliding with another deuteron ignoring charge and spin. In the case where after the collision two deuterons are returned, there are only two possible reactions. Either nothing happened or a particle was exchanged. Generalizing this simple problem from scattering theory results in an excursion into Polya's theory of counting and the theory of double cosets. 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 generated double cosets, we will see just how valuable Computer Algebra can be. Some surprising and stimulating patterns emerge after a just few computer algebra experiments. The results presented last year will be extended and expanded. Some proofs will be sketched.

Session T10: Symbolic Linear Algebra

Organizer: David Saunders and Gilles Villard

Overview

Problem:
Symbolic linear algebra has seen significant progress in recent years with developments for dense matrices and for sparse and structured matrices, faster methods both in elimination based techniques and in black box algorithms.

Motivation and Importance:
The purpose of this session is to bring together users and developers: those who need effective exact linear algebra solutions with developers of algorithms and implementations.

Speakers and Abstracts

T10.1 Bradford Hovinen (University of Waterloo), *On Montgomery's Block Lanczos Algorithm*

Montgomery's block Lanczos algorithm is a blocked extension to the scalar Lanczos iteration for solving linear systems over finite fields. It facilitates parallelization and allegedly improves the probability of success over small finite fields. This talk examines the algorithm on theoretical and empirical levels, examining how the probability of success depends on the blocking factor and the characteristics of the input matrix. It also shows how block Lanczos and Coppersmith's block Wiedemann algorithm are related.

T10.2 Victor Pan (Lehman College, CUNY), *Nearly Optimal Toeplitz/Hankel Computations.*

he classical and intensively studied problem of solving a Toeplitz/Hankel linear system of equations is omnipresent in computations in sciences, engineering and signal processing. We study this subject as a computer algebra problem assuming a nonsingular integer input and rely on Hensel's p-adic lifting to improve the current fastest divide-and-conquer algorithm by Morf 1974/1980 and Bitmead and Anderson 1980. With randomization, lifting enables solution of a nonsingular Toeplitz/Hankel linear system of n equations by using $O(m(n)n\mu(\log n))$ bit operations (versus the information lower bound of $n2\log n$), where $m(n)$ and $\mu(d)$ bound the arithmetic and Boolean cost of multiplying polynomials of degree n and integers modulo 2^d+1, respectively, and the input coefficients are integers in $n^{O(1)}$. Furthermore, we extend our algorithms and cost bound to q-adic lifting for a fixed integer q, in particular $q = 2^g$ allowing computations in binary form. This enhances practical value of our study. In Pan (2002) the algorithms and the bit cost estimates are extended to solving nonsingular and consistent singular Toeplitz/Hankel-like linear systems and computing the rank and a vector from or a basis for the null space of a Toeplitz/Hankel-like matrix as well as the resultant, gcd and lcm of two polynomials of bounded degrees, a fixed entry of a Padé approximation table, and the Berlekamp-Massey linear recurrence coefficients provided that the input values are some bounded integers. To yield this extension, Hensel's lifting is combined with the Morf-Bitmead-Anderson's divide-and-conquer algorithm, where again we allow computations both modulo a random prime and a fixed prime power, in particular a power of 2.

T10.3 Shuhong Gao (Clemson University) *Random Krylov spaces over finite fields.*

Iterative methods for solving linear systems are based on Krylov subspaces generated by a fixed linear mapping and a set of elements in a vector space. We consider the probability that a random Krylov subspace in a vector space over a finite field equals the whole space itself. We present an exact formula for this probability, and from it we derive good lower bounds that approach 1 exponentially fast as the size of the set increases. Joint work with Richard P. Brent and Alan G. B. Lauder.

T10.3 Wayne Eberly (University of Calgary), *The Reliability of Block Lanczos Algorithms.*

Block Lanczos algorithms have recently been used to sample from the nullspace of sparse matrices over small fields, as part of number-theoretic computations. While experimental evidence suggests that these computations are reliable, considerable work remains to be done in order to prove that this is generally the case.

This talk includes prelimary work to investigate the worst-case expected behaviour of randomized versions of a block Lanczos algorithm to sample from the nullspace or estimate the rank of a given matrix, and to determine the consistency of a given sparse system of equations.

In particular, it will be shown that these methods are provably unreliable in the worst case, when they are applied to solve problems that include sparse matrices over small fields, unless the input matrix is also conditioned in some way. A sparse conditioner that addresses the problems, suggested above, will also be proposed.

T10.4 Pascal Giorgi (ENS Lyon), *From BLAS routine to finite field exact linear algebra solution.*

Numerical libraries provide fast routines for floating point arithmetic. We know that using such libraries allows for faster matrix mutliplication over finite fields. In particular, there exists a fast matrix multiplication routine based on BLAS. Using this work, we go further by providing fast routines for solving basic exact linear algebra problems such as LSP factorization and triangular system solving. In this talk we describe these routines and their application to computing the minimal matrix polynomial. More generally, these routines should be useful for other algorithms that incorporate matrix multiplication. This work is part of the LinBox project. (See http://www.linalg.org).

T10.6 Keith Geddes (U. Waterloo), *Exploiting Fast Hardware Floating Point in High Precision Computation.*

We present an iterative refinement method based on a linear Newton iteration for solving a particular group of high precision computation problems. Our method generates an initial solution at hardware floating point precision using a traditional method and then repeatedly refines this solution to higher precision, exploiting hardware floating point computation in each iteration. This is in contrast to direct solution of the high precision problem completely in software floating point. Theoretical cost analysis, as well as experimental evidence, shows a significant reduction in computational cost is achieved by the iterative refinement method on this group of problems.

T10.7 Robert Lewis (Fordham University), *Using the Dixon Resultant on Big Problems.*

The Bezout-Cayley-Dixon resultant is a useful and efficient way to solve systems of polynomial equations. This has been known since at least the 1994 paper by Kapur, Saxena, and Yang [KSY]. Their key idea was proven correct in great generality by the 2000 paper of Buse, Elkadi, and Mourrain [BEM]. I will summarize some of the large problems I have solved with it, in which it has routinely bested Groebner basis techniques by several orders of magnitude.

I will discuss:

- The Cayley-Dixon-Bezout-KSY Resultant Method
- The spurious factor problem
- Various problems motivated by geometry, signal processing, and biochemistry.
- How I attack the spurious factor problem

[BEM] L. Buse, M. Elkadi, and B. Mourrain, Generalized resultants over unirational algebraic varieties. J. Symbolic Comp. 29 (2000), p. 515-526.

[KSY] D. Kapur, T. Saxena, and L. Yang, Algebraic and geometric reasoning using Dixon resultants. In: Proc. of the International Symposium on Symbolic and Algebraic Computation. A.C.M. Press (1994).

T10.8 B. David Saunders (University of Delaware), *Rank and Smith Form of extremely sparse matrices.*

Blackbox algorithms for sparse and structured matrices have proven very effective and are the core of LinBox. In this talk, we consider matrices in which the storage of matrix elements is a small multiple of the matrix dimension. Blackbox methods are particularly useful in this situation, especially for large problems where memory is at a premium. However, Gaussian elimination based methods are generally faster for small matrices and cases where fill-in is sufficiently low. It is hard to predict a priori which method will be best for many matrices. We discuss topics related to the design of hybrid algorithms that adapt to the properties of the matrix at hand.

Saunders will discuss the situation for matrices with just 2 nonzero elements per row and mention some situations in which these arise. In this situation, fill-in may be avoided but elimination must be done with care for optimal performance.

Wan will describe a hybrid of sparse elimination, SuperLU, and Wiedemann's blackbox approach. Included will be a report on the latest optimization of field arithmetic in prime fields for these algorithms.

Lobo will report on the status of implementation of blackboxes for Toeplitz and other structured matrices using fast, FFT based, polynomial arithmetic. Comparisons showing the cutoff threshold between this and dense matrix elimination will be presented.

T10.9 Arne Storjohann (University of Waterloo), *Effective reductions to matrix multiplication*

The effectiveness of adapting highly optimized numerical BLAS routines to the task of exact matrix multiplication over finite fields has been established by project F.F.L.A.S. (Finite field linear algebra subroutines) from Dumas, Pernet, Brassel, and Gautier. Some of the ideas from that project, in particular a fast matrix multiplication algorithm for small prime fields, are now incorporated into the Maple computer algebra system. In this talk we describe a Maple implementation of an algorithm for computing the echelon transform. This single routine gives effective reductions to matrix multiplication for many other tasks, such as computation of rank, rank profile, determinant, inverse, nullspace, and solution of a linear system. To evaluate our implementation we use a ratio test, e.g. we plot the ratio of time taken to compute the determinant of an $n \times n$ matrix and the time taken to multiply two $n \times n$ matrices. The goal is a ratio of less than one. Joint work with Zhuliang Chen.

Session T11: Mathematics On The Internet

Organizer: Mike Dewar (NAG Ltd.)

Overview

The aim of this session is to bring together groups and individuals who are building web-based mathematical applications. Topics will include semantic markup systems such as OpenMath and Content MathML, the use of web and grid service infrastructures, and semantic web technologies for identifying and describing web-based mathematical resources.

Speakers and Abstracts

T11.1 Laurent Bernardin (Maplesoft), *Maple on the Web.*

T11.2 Stephen Buswell (Stilo Technology Ltd.) *MathML, OpenMath and the Evolution of Maths on the Web.*

MathML, the W3C recommendation for mathematics on the Web, has its fifth birthday this year and is now seeing widespread adoption. The CEC-supported OpenMath initiative on the exchange of semantically rich mathematical objects has been running for a similar length of time. These technologies have achieved a considerable degree of synergy and interoperability and underpin a number of current initiatives, including the MONET and MathBroker projects concerned wih mathematical web services.

T11.3 Olga Caprotti (RISC, Linz), *Mathematical Services Registration and Discovery.*

Web Services technologies such as ebXML, UDDI, WSDL are not enough for describing the details concerning the functionality of a web service performing a mathematical computation. They lack the accuracy that allows for "intelligent" discovery by clients. In this talk we will present the ongoing developments within the European project MONET and the Austrian FWF Mathbroker project to overcome those limitations. We illustrate how registration of a mathematical service via the MONET mathematical service description language at the MONET broker subsequently supports queries about multiple aspects of a computational problem. Because mathematical service discovery is essentially problem solving, it is easy to envision the development of "specialised" (intelligent) brokers dealing with queries of a certain form. The Mathbroker project is an example of one such extension to MONET.

T11.4 James Davenport (University Of Bath), *Mathematical Knowledge Management.*

T11.5 Mike Dewar (NAG Ltd.) *OpenMath and Web Services.*

T11.6 Mika Seppälä (Florida State University and University of Helsinki), *Advanced Learning Technologies Project.*

T11.7 Clare M. So and Stephen M. Watt (University of Western Ontario). *Conversion Between Content MathML and OpenMath.*

OpenMath and Content MathML use XML formats to encode the semantics of mathematical expressions. We examine the relationship between these two formats with a view to identifying any advisable adjustment of the standards. To do this, we develop a bijection between Content MathML and Openmath, implemented as a set of XSLT stylesheets. We see that while most of the conversions are straight-forward, some are difficult or impossible because of the subtle differences between the basic concepts in Content MathML and OpenMath. Finally, we demonstrate the possibility of converting OpenMath to "Simplified" Content MathML, which is valid Content MathML not making use of pre-defined functions.

T11.8 Tom Wickham-Jones (Wolfram Research Inc.) *Math on the Web with Mathematica Technology.*

This talk will give an overview of the use of Mathematica technology for mathematical presentation, computation, and visualization over the web. It will focus on the support in Mathematica for MathML and show how to use this in combination with webMathematica to build MathML based web sites for computation. It will also show how SVG can be used in conjunction with XHTML and MathML to add visualization features. Finally it will show how to deploy these features with SOAP based web services.

Session T12: Symbolic-Numeric methods for Curves and Surfaces

Organizers: Josef Schicho (RISC Linz), Mohamed Shalaby (RISC Linz).

Overview

Problem:

This session aims to present some up-to-date symbolic-numerical methods for curves and surfaces and theirs applications to Computer Aided Geometric Design (CAGD), Solid Modeling and Visualization. Topics of the session include, but are not limited to :

- Symbolic-Numerical methods for curves/surfaces parameterization.
- Symbolic-Numerical methods for curves/surfaces implicitization.
- Symbolic-Numerical methods for resolution of singularities for curves/surfaces.
- Mathematical methods for CAGD.
- Methods for evaluation and visualization of offsets and intersections of surfaces.
- Symbolic-Numerical methods for polynomial solving.
- Intersection of Bezier and B-spline curves and surfaces.
- Bernstein bases versus monomial bases.
- Gröbner Bases and CAGD.
- Industrial application.

Motivation and Importance:

The combination of symbolic and numerical methods has lead to various interesting new applications in CAGD. Several new algorithms/methods have been developed in the recent years. In this special session, we want to bring together as many as possible of these various approaches, in the hope to inspire fruitful discussions and interactions.

Speakers and Abstracts

T12.1 Rida Farouki (UC Davis), *Minkowski geometric algebra of complex sets.*

Algebraic operations on sets of complex numbers produce remarkably rich geometrical structures, with diverse applications and connections to science and engineering. For "simple" operands, such as circular disks, precise descriptions of their algebraic combinations are available in terms of the Cartesian and Cassini ovals, and higher-order generalizations. Algorithms can be formulated to approximate algebraic operations on complex sets with general (piecewise-smooth) boundaries to a given precision. This "Minkowski algebra of complex sets" is the natural generalization of (real) interval arithmetic to sets of complex numbers. It provides a versatile two-dimensional "shape operator" language, with connections to mathematical morphology, geometrical optics, and stability analysis of dynamic systems.

T12.2 Greg Reid (University of Western Ontario), Jianliang Tang (Chinese Academy of Sciences), Lihong Zhi (Chinese Academy of Sciences), *A complete symbolic-numeric linear method for camera pose determination.*

Camera pose estimation is the problem of determining the position and orientation of an internally calibrated camera from known 3D reference points and their images. We briefly survey several existing methods for pose estimation, then introduce our new complete linear method, which is based on a symbolic-numeric method form the geometric (Jet) theory of partial differential equation. The method is stable and robust. In particular, it can deal with the points near critical configurations. Numerical experiments are given to show the performance of the new method.

T12.3 Erich Kaltofen (North Carolina State University), John May (North Carolina State University), *Bounding the Radius of Irreducibility of Multivariate Polynomials.*

Given an irreducible polynomial in two or more variable with complex floating point coefficients we find a lower bound on its distance to a reducible polynomial of the same degrees. This is accomplished by using generalizations of an irreducibility test of Ruppert together with theory of bounding matrices away from those with lower ranks which involves singular value decompositions, and psuedo-inverses. We compare a couple different ways of computing these bounds.

T12.4 Bert Jüttler (Johannes Kepler University), Josef Schicho (Johannes Kepler University), Mohamed Shalaby (Johannes Kepler University), *Spline Implicitization of Planar Curves and Applications.*

We present a new method for constructing a low degree C1 implicit spline representation of a given parametric planar curve. To ensure the low degree condition, quadratic B-splines are used to approximate the given curve via orthogonal projection in Sobolev spaces. Adaptive knot removal, which is based on spline wavelets, is used to reduce the number of segments. The B-spline segments are implicitized. After multiplying the implicit B–spline segments by suitable polynomial factors the resulting bivariate functions are joined along suitable transversal lines. This yields to a globally C1 bivariate function. Some applications of the proposed method is presented.

T12.5 Wen-shin Lee (University of Waterloo), *Symbolic-Numeric Sparse Interpolation of Multivariate Polynomials.*

We consider the problem of interpolating a multivariate polynomial that is given as a black box. When the target polynomial is sparse, there are efficient algorithms taking advantage of this situation, such as Zippel's probabilistic algorithm and the Ben-Or/Tiwari algorithm. These methods are developed for exact arithmetic environments. Interestingly, the method of Ben-Or and Tiwari is similar to that of Prony's from 1795 for interpolating a sum of exponential functions. Recent work by Golub, Milanfar, and Varah recasting Prony's method as a generalized eigenvalue problem may provide the key to a numerically sound symbolic-numeric sparse polynomial interpolation. This method avoids explicitly constructing and solving the generating polynomial in the interpolation process. Furthermore, in the finite precision arithmetic, evaluating the black box at appropriate primitive roots of unity may not only improve the condition embedded in the interpolation steps, but also provide a numeric method for recovering all variables at once in the target polynomial. In addition to the standard power basis, our approach can be applied to polynomials represented in some non-standard bases. We discuss general issues and a framework for sparse, black-box, approximate polynomial interpolation, our algorithm for solving this problem, and details of our numerical experiments.

This is joint work with Mark Giesbrecht (University of Waterloo) and George Labahn (University of Waterloo).

T12.6 Bohumir Bastl (University of West Bohemia, Czech Republic), *Symbolic-numeric method for computing surface self-intersection.*

This talk presents a new symbolic-numeric method for computing self-intersection of surface with arbitrary rational parameterization. The problem of finding surface self-intersection can be stated as a problem of solving system of non-linear algebraic equations (for surface with rational parameterization). Symbolic part of this method uses Groebner bases method for solving given system of non-linear algebraic equations which can be easily replaced by resultant method. Any of these elimination methods gives on the output one-dimensional algebraic set represented by the polynomial $P(u,v) = 0$. Every algebraic set of this type consist of open and closed components. The algorithm computes start points on all components which correspond to surface self-intersection. Then component splitting is used to partition the domain such that each resulting region contains only one component. Finally, tracing is used to evaluate the curve on the given region and to obtain appropriate part of the surface self-intersection. The technique to handle singularities is also presented. The algorithm has been implemented in MathWorks Matlab 6.1 and CoCoA 4.2 is used for reduced Groebner basis computations.

T12.7 Ilias S. Kotsireas (Wilfrid Laurier University), Ioannis Z. Emiris (INRIA Sophia-Antipolis, France), *Implicit Polynomial Support Optimized for Sparseness.*

We propose the use of various tools from algebraic geometry, with an emphasis on toric (or sparse) elimination theory, in order to predict the support of the implicit equation of a parametric hypersurface. The problem of implicitization lies at the heart of several algorithms in geometric modeling and computer-aided design. In the case of two specific implicitization algorithms IPSOS results in tremendous efficiency improvements. Other implicitization methods shall probably be able to benefit from our work. More specifically, we use information on the support of the toric resultant, and degree bounds, formulated in terms of the mixed volume of Newton polytopes. The computed support of the implicit equation depends on the sparseness of the parametric expressions and is much tighter than the one predicted by degree arguments. Our Maple implementation illustrates many examples in which we always obtain the exact support.

T12.8 Elisabeth Malsch (Columbia University), *A symbolic method for defining test functions which satisfy ellipticity, boundary conditions lower order field behaviors exactly.*

Given a set of nodal points which define a polygonal geometry, such as the vertices of a convex or concave polygon, a smooth and bounded test function can be constructed in explicit algebraic form. It smoothly distributes the given values at the nodes over the interior of the domain. The closed form representation is constructed by combining simple geometric descriptions, such as boundary edge length and area. The smooth test function on a convex polygon can be constructed as the rational combination of the product of areas. Accordingly the representation is rational polynomial. The test function on a concave or multiply-connected polygon is constructed as the function of areas and edge lengths. Accordingly, a square root term enters the representation. Computer algebra is a uniquely suited for developing such test functions which satisfy required geometric conditions exactly, such as boundary conditions, and approximates unknown behavior reasonably, such as domain behavior. A method for constructing linear edged test functions satisfying constant and linear field conditions will be presented.

T12.9 Daniel Lichtblau (Wolfram Research), *Computational algebra visits number theory: Trigonometric polynomials, planar extremal packings, and Groebner bases.*

A few years ago S-H Kim investigated some problems at the boundary of number theory, optimization, and geometry. One question regarded an optimal packing of certain “triangular oval” planar curves and another looked at some related transformations of $\mathbb{R}^2$ to $\mathbb{R}^2$. While these were cast using trigonometric functions in a calculus setting, it turns out that a tool from computational polynomial algebra, Groebner bases, may be used to advantage. The goal is to convey some sense of where and how computational technology can be of use in approaching and illustrating the theory behind that work.

Session T13: Young Researchers Invitational Session

Organizers: Mark Giesbrecht and Stanly Steinberg and the ACA Working Group.

Overview

The purpose of this session is to have young researchers that are doing excellent work on important problems present their latest results. The speakers are choosen by the Working Group of the ACA.

Speakers and Abstracts

T13.1 Howard Cheng (University of Waterloo), *Algorithms for Normal Forms for Matrices of Ore Polynomials*

In this talk we study algorithms for computing normal forms for matrices of Ore polynomials while controlling coefficient growth. By formulating row reduction as a linear algebra problem, we obtain a fraction-free algorithm for row reduction for matrices of Ore polynomials. The algorithm allows us to compute the rank and a basis of the left nullspace of the input matrix. When the input is restricted to matrices of shift polynomials and ordinary polynomials, we obtain fraction-free algorithms for computing row-reduced forms and weak Popov forms. These algorithms can be used to compute a greatest common right divisor and a least common left multiple of such matrices. Our fraction-free row reduction algorithm can be viewed as a generalization of subresultant algorithms. The linear algebra formulation allows us to obtain bounds on the size of the intermediate results and to analyze the complexity of our algorithms.

We then make use of the fraction-free algorithm as a basis to formulate modular algorithms for computing a row-reduced form, a weak Popov form, and the Popov form of a polynomial matrix. By examining the linear algebra formulation, we develop criteria for detecting unlucky homomorphisms and determining the number of homomorphic images required.

Parts of this work have been done jointly with George Labahn (University of Waterloo) and Bernhard Beckermann (Université des Sciences et Technologies de Lille).

T13.2 Yang Zhang (University of Western Ontario). *Popov forms of Ore matrices.*

Let A be a matrix over a polynomial ring $R[x]$. It is known that we can compute some normal forms of A, for example, the Smith form, Jordan form and Hermite form. But in many cases the degrees of entries in these normal forms are much bigger those in A. Popov forms avoid this disadvantage and play an important role in control theory. We define and discuss Popov forms of a matrix whose entries are skew polynomials and make some progress in their computation:

- algorithms for (weak) Popov forms. These will be used to get short vectors and applied in lifting algorithms.
- applying differential Popov forms as a rewite rule for a differential system of differential polynomials.
- valuation based (weak) Popov forms.

This is joint work with Mark Giesbrecht (U. Waterloo) and George Labahn (U. Waterloo).

T13.3 Alin Bostan, *Tellegen's principle into practice.*

The transposition principle, sometimes referred to as Tellegen's theorem, is a set of transformation rules for linear programs, originating from linear circuit design and analysis in the 50s.

In computer algebra, despite a recurrent need for transposed algorithms, Tellegen's principle is not used systematically, specific algorithms being often developed to circumvent its use; moreover, few practical implementations rely on it.

The primary goal of this talk is to demonstrate that the transposition principle can, and should, be strictly complied with in practice. We will describe explicit transposed versions of basic polynomial algorithms and report on their successful implementation in the NTL C++ library. This is joint work with G. Lecerf and É. Schost.

We will also discuss a range of applications of Tellegen's principle in designing fast algorithms for computing with algebraic numbers and for solving polynomial systems. This is joint work with Ph. Flajolet, B. Salvy and É. Schost.

T13.4 Alexey Ovchinnikov, *Characterizable Radical Differential Ideals and Characteristic Sets.*

We consider the property of a radical differential ideal to be characterizable and give a criterion of characterizablility. This criterion is based on the known algorithms for decomposing radical differential ideals into characterizable components. The Ritt problem and its restriction to our particular case are discussed. Furthermore, we discuss differential algebraic properties of reducible to zero elements of radical ideals and present some sufficient conditions for an autoreduced set to be a characteristic set of a radical differential ideal in Kolchin's sense. We discuss the method of computation of characteristic sets in ordinary case developed by Brahim Sadik. We also introduce and investigate a special class of definable radical differential ideals.

T13.5 Hirokazu Anai (Fujitsu Laboratories Ltd.) *On Solving Real Algebraic Constraints in System and Control Theory.*

The design problems in system and control theory require determining feasible values of certain parameters satisfying the given design specifications. Ideally, it is desired to obtain the feasible regions of the parameters which satisfy the given specifications in a parameter space. The methods to obtain such feasible regions in a parameter space is referred to a parameter space approach. In the last decade it has been shown that a parameter space approach accomplished by quantifier elimination (QE) is effective for the problems such as robust control synthesis, multi-objective design problems, and hybrid dynamical system design that are difficult to solve by using numerical methods.

In this talk, we show how various control system design problems are solved by a parameter space approach based on QE and how we achieve efficiency of the QE based method with concrete control design examples. The examples show that combining reduction of control problems to particular formulas and usage of QE algorithms specialized to such particular formulas works in an efficient way for the practical control design problems.

We also report the present state of the development of our maple-package for real algebraic constraints called "SyNRAC". SyNRAC includes the implementation of specialized QE algorithms used to solve the control problems.

Parts of this work have been done jointly with Prof. Shinji Hara (University of Tokyo) and Prof. Volker Weispfenning (University of Passau).

T13.6 Virginia M. Rodrigues (Clemson University), *Gröbner Basis Structure of Finite Sets of Points.*

We study the structure of Grobner bases for zero-dimensional radical ideals. These ideals correspond to vanishing ideals of finite sets of points in an affine n-dimensional space. We are interested in monomial orders that "eliminate" one variable, say z, which correponds to the projection map of points in the n-space to $(n-1)$-space where the z-coordinate is projected out. We show that any minimal Grobner basis of an ideal under an elimination order exhibits the geometric structure of the variety defined by the ideal. Particularly, the degrees in z of the polynomials in the Grobner basis match the fibre sizes of the projection map, and the leading coefficients of z with given degrees give Grobner bases for the projected points with corresponding fibre sizes.

Joint work with Shuhong Gao and Jeff Stroomer.

T13.7 Ana Gonzalez-Uriel (Universidad Complutense de Madrid), *Expert System for House Layout Selection.*

Automatic reasoning is applied to building design problems with a big number of highly standardized conditions, such as non-singular housing.

PRELIMINARIES

During the XXth century, several studies and experiences regarding mass-produced houses, industrialization and prefabricated elements, have been carried out.

These antecedents were studied prior to designing this system, in order to determine a big (but finite) number of house layout schemes that could form the set of possible proposals. A modular structure was adopted. It uses modules that are all based on a 3.60 meter span bay. It considers the inclusion of a set of predefined service rooms (bathrooms, kitchen, storage spaces, boiler room...) and the adoption of compatible wall panels and closing systems. The schemes were developed for (isolated) house typology (for houses of one or more floors).

DESCRIPTION OF THE SYSTEM

The schemes have been grouped in basic types, the relative position of the rooms (aligned, around a court, around the service rooms...) being the basic criterion for the classification.

Each scheme implies a set of characteristics: area occupied by the building, number of usable square meters (discounting the width of walls), number of floors, total built area.

For each "basic type", a matrix of data has been prepared. In this matrix the data are organized by rows and columns. Each row represents a certain house layout scheme. Each column contains the different values of a certain characteristic of the houses for the different kind of houses considered.

A matrix-based approach has been chosen because there are many possible different schemes and very many data involved. Moreover there is no really deep extraction of knowledge or interference among types (that could provoke any inconsistency problems). A similar system that takes into account the town planning laws of Madrid was developed using GB-based inference engine. It was the same kind of approach and the inference engine was infra-used.

Maple was chosen because it is a user-friendly system that provides comfortable and complete programming and matrix-handling features.

The first data the user has to introduce are those related to the climate and the specific plot (dimensions, hours of direct sunlight, views, noise sources...).

Based on these data, the system selects a "best" basic type (and, consequently, one of the prepared data matrices).

Afterwards, the user has to introduce information about the number of members and special needs of the family group. There are some other few technical data required (that can be provided by a smart user or an architect), such as building regulations concerning the plot.

All these data are processed in order to select the specific house layout scheme, i.e., row of the matrix, that fits best. The process can be iterated in order to obtain other appropriate schemes.

If the user didn't like the basic type or no scheme could be found in the "best" basic type, a "second option" basic type is used instead.

ACKNOWLEDGMENTS

Partially supported by research project TIC-2000-1368-C03-03, Ministry of Science and Technology (MCYT), Spain.

CONCLUSIONS

Expert systems for choosing mass-produced house models allows the buyer to be involved in the designing process (for instance to easily compare different alternatives) in order to obtain a tailor-made house, at a reasonable price. As far as we know no similar systems exist.

Although the system is simple from the computational point of view, a very important part of this work consisted in the previous organization of the architectural knowledge.