MICA 2016

Milestones in Computer Algebra

Celebrating the research of Erich Kaltofen

July 16–18, 2016
University of Waterloo
Canada

All talks are in DC 1302, the Davis Centre.

Rooted in the boundary area between mathematics and computer science, computer algebra has evolved as a lively independent discipline and significantly influenced the research in many scientific fields.

This workshop surveys some major achievements of computer algebra and its connections to related scientific areas. Key focuses include both classical and emerging sub-disciplines of computer algebra, such as hybrid symbolic-numeric computation, exact linear algebra, algebraic complexity, polynomial factorization, and sparse interpolation. Besides presenting the latest results, the proposed workshop will assess these achievements and their impacts to other domains, in the hope of identifying promising future research directions.

We will take this occasion to acknowledge Erich Kaltofen's research accomplishments in computer algebra. Besides his many scientific contributions to computer algebra, number theory, and software systems, he has played a crucial role in the formation and development of many of the key emerging sub-disciplines represented here. Several of Kaltofen's key collaborators on these topics will present related results at this meeting.

Organizing Committee

Shaoshi Chen, Chinese Academy of Sciences, China
Mark Giesbrecht, University of Waterloo, Canada
Wen-shin Lee, University of Antwerp, Belgium
Austin A. Lobo, Washington College, USA
Sharon Moore, Baylor University, USA
Arne Storjohann, University of Waterloo, Canada
Stephen M. Watt, University of Waterloo, Canada
Zhengfeng Yang, East China Normal University, China
Lihong Zhi, Chinese Academy of Sciences, China

Webmaster

Andrew Arnold, North Carolina State University, USA

Sponsors

The Fields Institute
The University of Waterloo
Maplesoft

In-Cooperation with ACM, ACM SIGSAM

Saturday, July 16, 2016

8:00–9:30 (DC 1301)
Breakfast, registration

9:30–10:20
Joachim von zur Gathen
Universität Bonn, Germany

Algebraic complexity (survey)

10:20–10:45 (DC 1031)
Coffee break

10:45–11:10
Markus Hitz
University of North Georgia, USA

Integer division in residue number systems and log-space uniformity

Besides their use in algorithm design, Residue Number Systems (RNS) can be applied to signal processing, or arbitrary-precision integer computations. With the advent of powerful graphics processors, there has been renewed interest in RNS implementations. Residue arithmetic is closed under addition, subtraction, and multiplication. Therefore, it can exploit fine-grain parallelism provided by GPU architectures. Integer division, sign detection, and magnitude comparison cannot be directly performed in modular arithmetic. In our 1995 paper on RNS integer division, we devised a method based on Newton Iteration that stays close to RNS representation. It achieved logarithmic depth in terms of circuit implementation. We discuss its historic context, and the developments that lead to a log-space uniform NC^1 division algorithm in 2001.

11:10–11:35
George Labahn
University of Waterloo, Canada

Fast of computation of Hermite forms for matrices of polynomials

In this paper we present a deterministic algorithm for the fast computation of

the Hermite form of a matrix of polynomials. The algorithm has complexity $O\left(n^{\omega}s\right)$ where ω is the exponent of matrix multiplication and $s$is the average of the column degrees of our input matrix.

11:35–12:00
Eunice Y. S. Chan and **Rob M. Corless**
Western University, Canada

Narayana, Mandelbrot, and a new kind of companion matrix

We demonstrate a new kind of companion matrix, for polynomials of the form $c(\lambda) = \lambda a(\lambda)b(\lambda) + c_0$ where upper Hessenberg companions are known for the polynomials $a(\lambda)$ and $b(\lambda)$. This construction can generate companion matrices with smaller entries than the Fiedler or Frobenius forms. This generalizes Piers Lawrence's Mandelbrot companion matrix. We motivate the construction by use of Narayana-Mandelbrot polynomials, which are also new to this paper.

12:00–12:25
Laureano Gonzelez-Vega
Universidad de Cantabria, Spain

Resultants and subresultants through evaluation: formulae and applications

We show how resultants and subresultants can be described in terms of the evaluation of the considered two polynomials in any set of points not necessarily the roots of one of the considered polynomials and not necessarily different. We present the application of this formulae in the context of the so called "Polynomial Algebra by Values" and will show how to deal with intersection problems involving algebraic curves when their equations are presented "by values" (i.e., in the Lagrange, the Hermite or the Birkhoff basis).

12:25–14:00
Lunch break

14:00–14:50
Gilles Villard
French National Centre for Scientific Research (CNRS), France

Exact linear algebra (survey)

14:50–15:15 (DC 1301)
Coffee break

15:15–15:40
Jean-Guillaume Dumas
Université Grenoble Alpes, France

Efficient bootstrapping of sparse matrix-vector multiplication public verification

With the emergence of cloud computing services, computationally weak devices (clients) can delegate expensive tasks to more powerful entities (servers). This raises the question of verifying a result at a lower cost than that of recomputing it. This verification can be private, between the client and the server or public, when the result can be verified by any third party. We here present protocols for the verification of matrix-vector multiplications, that are secure against malicious servers. The obtained algorithms are essentially optimal in the amortized model: the overhead for the server is negligible, even in the sparse case; and the computational time for the public Verifier is linear in the dimension. Our protocols combine probabilistic checks and cryptographic operations, but minimize the latter to preserve practical efficiency.

15:40–16:05
Manuel Kauers
Johannes Kepler University, Austria

No news on matrix multiplication

Strassen's matrix multiplication algorithm relies on the fact that two 2×2 matrices over a (noncommutative) ring R can be multiplied using only 7 multiplications in R. Using his scheme recursively, two nxn matrices can be multiplied with $O(n^{\log_2(7)})$ operations in R. Faster matrix multiplication algorithms have been discovered since then, but Strassen's algorithm remains so far the only one that beats the classical algorithm not just in theory but also in practice. With the goal of finding an algorithm that may not beat the fastest known algorithms in theory but that is faster than Strassen's algorithm in practice, we tried to determine how many ring multiplications are needed for multiplying two 3×3 matrices. The classical algorithm needs 27, the best known

algorithm needs 23, it is known that at least 19 multiplications are necessary, and in order to be better than Strassen's scheme, we must use at most 21 multiplications, because $\log_3(21) < \log_2(7) < \log_3(22)$. We will report on our efforts to search for good 3×3-multiplication schemes using modern SAT solvers, although, until now, we haven't found any.

16:05–16:30
Christoph Koutschan
Johann Radon Institute (RICAM), Austria

Minimally rigid graphs

A graph is called rigid, if, after fixing the lengths of its edges, there are only finitely many ways, modulo rotations and translations, how it can be embedded in the plane. A rigid graph is called minimally rigid (or Laman) if omitting any single edge makes it non-rigid. There are many interesting questions concerning Laman graphs: How many Laman graphs exist with n vertices? Given a Laman graph, what is the number of its embeddings in the plane? What is the maximal number of embeddings that one can reach with a Laman graph of n vertices? We present some (partial) answers to these questions. This is joint and ongoing work of the Symbolic Computation Group at RICAM.

16:30–16:55 (DC 1301)
Coffee break

16:55–17:20
David Saunders
University of Delaware, USA

A brief history of matrix preconditioners in exact linear algebra

In 1986 a paper of Wiedemann spurred the development of blackbox linear algebra, the use of iterative methods to obtain exact results. Preconditioners have played a central role, expanding the range of problems solvable by blackbox methods while becoming increasingly efficient to use. I survey the evolution of preconditioners over the past 30 years, a process in which Erich Kaltofen has had a hand at every step of the way. Finally I discuss open problems concerning preconditioning and offer evidence in support of a promising new preconditioner candidate.

17:20–17:45
Wayne Eberly
University of Calgary, Canada

Black box linear algebra: extending Wiedemann's analysis of a sparse matrix preconditioner for computations over small fields

Wiedemann's paper, introducing his algorithm for sparse and structured matrix computations over arbitrary fields, also presented a pair of matrix preconditioners for computations over small fields. The analysis of the second of these is extended here in order to provide more explicit statements of the expected number of nonzero entries in the matrices obtained as well as bounds on the probability that the matrices being considered have maximal rank. It is hoped that this will make Wiedemann's second preconditioner of more practical use.

This is also part of ongoing work to establish that this matrix preconditioner can be used to bound the number of nontrivial nilpotent blocks in the Jordan normal form of a preconditioned matrix, in such a way that one can also sample uniformly from the null space of the originally given matrix. If successful this will result in a black box algorithm for the type of matrix computation required when using the number field sieve for integer factorization that is provably reliable (unlike some heuristics, presently in use) and—by a small factor—asymptotically more efficient than alternative provably reliable techniques that make use of other matrix preconditioners or require computations over field extensions.

17:45–18:10
George Yuhasz
Morehouse College, USA

Kaltofen's rank: computing matrix rank using Wiedemann methods

In 1986 Douglas Wiedemann published his method for solving a sparse linear system over a finite field by finding the minimal generator of a projection of the Krylov space. Since that time, many people have extended and improved this idea, with Erich Kaltofen and collaborators being among the foremost to do so. This presentation will give an overview of the basic method and relevant extensions made by Erich Kaltofen and others since that initial publication. An imporant application of the method is the computation of the rank of the matrix. In a work published in 1991 by Kaltofen and Saunders, a fast algorithm for rank using asymptotically fast preconditioners was described. Further improvements of Wiedemann's method include Coppersmith's block

version of the method, preconditioning the system to have various beneficial properties and implementations of fast methods for computing the minimal generator. An alternative approach to a portion of the rank computation using the block methods will be presented. This approach will use linear algebra to compute the degrees of the characteristic polynomial required by the rank computation instead of interpolation. The approach should as computationally fast or faster than the interpolation method and work over any finite field regardless of the field characteristic.

Sunday, July 17, 2016

8:00–9:30 (DC 1301)
Breakfast, registration

9:30–10:20
Lihong Zhi
Chinese Academy of Sciences, China

Hybrid symbolic-numeric computation (survey)

10:20–10:45 (DC 1301)
Coffee break

10:45–11:10
Didier Henrion[1], Simone Naldi [2], and **Mohab Safey El Din**[3]
Université de Toulouse, CNRS, France and Czech Techinical University in Prague, Czech Republic[1]
Technische Universität Dortmund, Germany[2]
Sorbonne Université, UPMC Univ Paris and INRIA, France[3]

Symbolic computation, sums of squares and linear matrix inequalities

Polynomial optimization appears in many applications of engineering sciences and is a challenging computational task. While it can be tackled through variants of algorithms for quantifier elimination over the reals, another approach based on Semi-Definite Programming (SDP), has been developed at the beginning of the millenium. Due to its efficiency, it has become popular. It consists in certifying lower bounds for global infima via sums-of-squares decompositions. This is done by noticing that a polynomial can be written as a sum of squares if some Linear Matrix Inequality has a non-empty feasible set.

The above approach makes use of numerical solvers for SDP yielding approximate certificates of positivity by means of sums of squares. In his joint work B. Li, Z. Yang and L. Zhi, Kaltofen provided some techniques that allow, in some cases, to reconstruct *exact* certificates of positivity assuming that such a certificate exists over the rationals. This contribution inspired several others works focusing on the computation of points with rational coordinates in convex semi-algebraic sets or feasible sets of Linear Matrix Inequalities.

Later on, Scheiderer proved that there exist non-negative polynomials with rational coefficients which are sums of squares of polynomials with coefficients in $\mathbb{R}$ but not sums of squares of polynomials with coefficients in $\mathbb{Q}$. This raised the question of designing exact algorithms for Linear Matrix Inequalities.

In this talk, we will describe recent algorithmic developments of exact algorithms for deciding the feasibility of Linear Matrix Inequalities. Up to some genericity assumptions on the input matrices, the algorithm computes an exact algebraic representation of at least one point in the feasible set, or decides that it is empty. The algorithm does not assume the existence of an interior point, and the computed point minimizes the rank of the pencil on the linear matrix inequality. The degree d of the algebraic representation of the point coincides experimentally with the algebraic degree of a generic semidefinite program associated to the pencil. Explicit bounds for the complexity of our algorithm are also given.

11:10–11:35
Kosaku Nagasaka
Kobe University, Japan

Approximate GCD and its implementations

Computing an approximate polynomial GCD of two polynomials with a priori errors on their coefficients, is one of interesting problems in Symbolic-Numeric Computations, and also one of topics connected to Erich Kaltofen's research literatures. In this talk, we give several implementation notes on these famous algorithms: QRGCD (and ExQRGCD), UVGCD and Fastgcd, mainly from the viewpoints of QR factorization and performance (timing, detected degree and tolerance). Any small extension, any effect by pivoting, any combination of sub-algorithms which may have less computational time (or complexity), and smaller tolerance are of interests. In summary, Fastgcd can find approximate GCD over reals, pivoting is not useful for 3 of those algorithms, there are more effective replacement of sub-algorithms (especially, ExQRGCD becomes competitive with UVGCD) and there are more theoretical and less complexity sub-algorithms but not better accuracy.

11:35–12:00
Daniel Lichtblau
Wolfram Research, USA

Computing approximate GCDs with approximate syzygies

I will show in brief how one can compute the GCD of a pair of multivariate polynomials by finding a syzygy. This is done by straightforward Grbner basis computation over a certain module (with theoretical underpinning related to work coauthored by Erich Kaltofen). I will then show how we can weaken this an create an "approximate syzygy" to find an approximate GCD.

12:00–12:25
Minjie Shen[1], Zhengfeng Yang[1], and **Zhenbing Zeng**[2]
East China Normal University, China[1]
Shanghai University, China[2]

Some applications of sparse interpolation via compressive sensing

In this talk, we present our investigation on using of the sparse interpolation based on compressive sensing method for formula regression from experimental data. The first one is the astronomy problem related to Kepler's Third Law for planets, that is, from the observed data about the period and the axis length of the elliptic orbit of the planets, the target is to find a simple relation between the period and the length. From the original data, sparse implicit equation interpolation based on compressive sensing method can succeed to recover the Kepler's Third Law for planets. The second one is about the asymptotic formula of the integer partition $p(n)$, viz, the number of the ways to write n as sums of different positive integers. To our knowledge, the best approximation is $p(n) = e^{(\pi\sqrt{2n/3})/(4\sqrt{3}n)}$, proved by Hardy and Ramanujan. We established a better approximation for $p(n)$ by using the approximate sparse interpolation of multivariate polynomials method. The third investigation is the equation of state(EOS) in gas thermodynamics. EOS is the empirical formula between state variables, which can be used to describe the relationship between two or more state functions associated with the matter, such as its pressure, volumes, temperature, or internal energy. From the same experimental data, P-V-T EOS can also be obtained by exploiting the sparse interpolation of multivariate implicit equations. From the above examples, sparse interpolation based on compressive sensing is a useful tool for discovering intrinsic relations hidden in complicated data from observation or experiments in mathematics and sciences. This is joint work with Minjie Shen and Zhengfeng Yang.

12:25–14:00
Lunch break

14:00–14:50

Mark Giesbrecht[1] and **John May**[1]
University of Waterloo, Canada[1]
Maplesoft, Canada[2]

Polynomial factorization (survey)

14:50–15:15 (DC 1301)
Coffee break

15:15–15:40
Anand Kumar Narayanan
California Institute of Technology, USA

Factoring polynomial over finite fields using Drinfeld modules with complex multiplication

We present novel algorithms to factor polynomials over a finite field $\mathbb{F}_q$ of odd characteristic using rank 2 Drinfeld modules with complex multiplication. The main idea is to compute a lift of the Hasse invariant (modulo the polynomial $f(x) \in \mathbb{F}_q[x]$ to be factored) with respect to a Drinfeld module ϕ with complex multiplication. Factors of $f(x)$ supported on prime ideals with supersingular reduction at ϕ have vanishing Hasse invariant and can be separated from the rest. A Drinfeld module analogue of Deligne's congruence plays a key role in computing the Hasse invariant lift. We present two algorithms based on this idea. The first algorithm chooses Drinfeld modules with complex multiplication at random and has a quadratic expected run time. The second is a deterministic algorithm with $O(\sqrt{p})$ run time dependence on the characteristic p of $\mathbb{F}_q$.

15:40–16:05
Takafumi Shibuta[1] and Shinichi Tajima[2]
Kyushu University, Japan[1]
University of Tsukuba, Japan[2]

An algorithm for computing the reduced standard bases of modules of finite colength

In this talk, an algorithm for computing the reduced standard basis of a submodule of a free module of finite colength is constructed based on the Matlis duality theorem.

16:05–16:30
Thomas Kaltofen
RISC Software GmbH, Austria

Biomechanical simulation of squint surgeries based on non-linear optimization

We present our software system SEE++, which implements a realistic biomechanical model of the human eye, its orbit and its extraocular muscles. The biomechanical model includes a geometrical representation of eye movements, a muscle force prediction model and a kinematic model that balances muscle forces by using non-linear optimization methods. Based on the model, the software offers an interactive simulation of eye motility disorders (like squinting) and their surgical correction with a "virtual patient". Moreover, the system allows the simulation of an increasing number of common clinical tests.

16:30–16:40 (DC 1301)
Coffee break

16:40–17:05
Lakshman
Google Inc., USA

17:05–18:05
Erich Kaltofen
North Carolina State University, USA

Remembrance of things past

I will review by way of items from my mail box and personal recollections my connection to the discipline of symbolic computation.

18:05–18:30
Walk to the Delta Hotel
110 Erb Street W
Waterloo, Ontario, N2L 0C6

18:30–23:00 (Delta Waterloo)
Banquet
Remarks by: **Keith Geddes**
Banquet speaker: **Stephen M. Watt**

Monday, July 18, 2016

8:00–9:30 (DC 1301)
Breakfast, registration

9:30–10:20
Wen-shin Lee
University of Antwerp, Belgium

Sparse interpolation (survey)

10:20–10:45 (DC 1301)
Coffee break

10:45–11:10
Zhengfeng Yang
East China Normal University, China

Sparse multivariate function recovery from values with noise and outlier errors

Error-correcting decoding is generalized to multivariate sparse rational function recovery from evaluations that can be numerically inaccurate and where several evaluations can have severe errors ("outliers"). Here we present an algorithm that can interpolate a sparse multivariate rational function from evaluations where the error rate is $1/q$ for any $q > 2$. Our multivariate polynomial and rational function interpolation algorithm combines Zippel's symbolic sparse polynomial interpolation technique with the numeric algorithm, and removes outliers ("cleans up data") through techniques from error correcting codes. Our multivariate algorithm can build a sparse model from a number of evaluations that is linear in the sparsity of the model. This is joint work with Erich L. Kaltofen.

11:10–11:35
Andrew Arnold
North Carolina State University, USA

Output-sensitive sparse polynomial multiplication, sparse interpolation, and early termination

A sparse representation of a polynomial f is a list comprised of its nonzero terms. We consider polynomial multiplication with integer coefficients, where the inputs and output are all in a sparse representation. To our knowledge, any known algorithm for this problem has a time cost factor that is quadratic in the combined bit size of the inputs and outputs. In this talk we present a probabilistic Monte Carlo algorithm for computing a sparse polynomial product, that reduces (but does not remove), this quadratic cost factor. This algorithm relies on techniques from sparse interpolation, and is joint work with Daniel S. Roche (ISSAC, 2015). A challenge of removing this aforementioned quadratic factor is that the size of the output is initially unknown, given the inputs. Lastly, we will show a subtle error in the original cost analysis of the algorithm, and how this may be repaired using the technique of early termination (Kaltofen and Lee, JSC, 2003).

11:35–12:00
Daniel Roche
United State Naval Academy, USA

Sparse interpolation of integer polynomials: Theory and Practice

We will briefly survey some of the most important results in how to perform fast evaluation and interpolation of integer polynomials, paying special attention to the slightly differing underlying model assumptions in each approach. We will also look at some recently-developed strategies and heuristics that may provide some improvements. Finally, we will see how these assumptions and theoretical complexities relate to practical performance in a modern implementation.

Sparse interpolation algorithms, which determine the coefficients and exponents of an unknown sparse polynomial from carefully-crafted evaluations, have numerous potential applications. The special case of integer coefficients and exponents is interesting and important, as any single evaluation (except at -1, 0, or 1) will generally be too computationally expensive even to write down. For this reason, fast algorithms must choose not only the evaluation points but also the domain(s) over which those evaluations are performed.

The first fully polynomial-time algorithm was discovered by Kaltofen in 1988 but was not published until 2010. Since then, numerous alternative approaches and heuristic tweaks have been proposed. After examining the key features and differences between the various options, we will see how they perform in practice. Understanding the interplay between theoretical bottlenecks and assumptions and practical results leads to some new and challenging questions.

12:00–12:25
Dai Numahata and Hiroshi Sekigawa
Tokyo University of Science, Japan

Degree estimate for black-box multivariate polynomials in symbolic-numeric sparse interpolation

We consider the problem of sparse interpolation of a multivariate black-box polynomial in floating-point arithmetic. More specifically, we assume that we are given a black-box polynomial $f(x_1, \ldots, x_n) = \sum_{j=1}^{t} c_j x_1^{d_{j,1}} \ldots x_n^{d_{j,n}} \in \mathbb{C}[x_1, \ldots, x_n]$ $(c_j \neq 0)$ and the number of terms t, and that we can evaluate the value of $f(x_1, \ldots, x_n)$ at any point in $\mathbb{C}^n$ in floating-point arithmetic. The problem is to find the coefficients $c_1, \ldots, c_t$ and the exponents $d_{1,1}, \ldots, d_{t,n}$. We propose an efficient algorithm which does not require degree bounds to solve the problem. Finally, we describe future directions: applying our ideas to early termination by E. Kaltofen et al., and constructing a more robust algorithm for the problem by using our ideas.

12:25–14:00
Lunch break

14:00–14:25
Michael Monagan and Alan Wong
Simon Fraser University, Canada

Fast parallel multi-point evaluation of sparse polynomials

We consider the problem of evaluating a sparse multivariate polynomial over a prime field at multiple points. We parallelize the asymptotically fast algorithm of Bostan, Lecerf, and Schost. We have implemented our algorithm in Cilk C. The algorithm is being used to compute multivariate polynomial GCDs using a sparse interpolation modulo a smooth prime.

14:25–14:50
Clément Pernet
Université Grenoble-Alps and LIP, France

Sparse interpolation and error correcting codes

Evaluation/Interpolation schemes are at the core of many of computation techniques, including signal processing, model fitting, computer algebra, cod-

ing theory, fault tolerant distributed computing... The interpolation of a dense polynomial from possibly erroneous evaluations is solved by the famous Reed-Solomon codes combining Fourier analysis and algebraic computation. A central tool there is Blahut's theorem, relating sparsity of a signal to the linear complexity of its discrete Fourier transform. Surprisingly, it also lies at the core of Prony/Ben-Or/Tiwari's algorithm for error-free sparse interpolation, showing a duality between these two problems. As a natural extension, Erich Kaltofen proposed to study the problem of performing sparse interpolation in the presence of errors in the evaluations. It happened to of a much different flavour, creating codes surprisingly hard to analyze: the few known decoding algorithms apply in settings where the worst case decoding radius is particularly small, although they perform well on average.

We will give an overview on the subject and present the best known unique and list decoding algorithms for these codes. In this process we shall see connections with the famous problem arising in additive combinatoric of the density of arithmetic progressions.

14:50–15:15 (DC 1301)
Coffee break

15:15–16:30
Panel Computer Algebra 1982 – 2016: reflection on the ways things have changed

Moderator:

Austin Lobo
Washington College, USA

Panel:

Wen-shin Lee
University of Antwerp, Belgium
Daniel Lichtblau
Wolfram Research, USA
John May
Maplesoft at JPL, Canada and USA
Gilles Villard
University of Lyons, France
Stephen M. Watt
University of Waterloo, Canada

16:30–16:55 (DC 1301)
Coffee break

16:55–17:20
Rui-Juan Jing, Chun-Ming Yuan, and **Xiao-Shan Gao**
Chinese Academy of Sciences, China

A polynomial-time algorithm to compute generalized Hermite normal forms of matrices over $Z[x]$

In this talk, we present a polynomial time algorithm to compute the generalized Hermite normal form for a matrix F over $Z[x]$, or equivalently, the reduced Groebner basis of the $Z[x]$-module generated by the column vectors of F. The algorithm has polynomial bit size computational complexities and is also shown to be practically more efficient than existing algorithms. The algorithm is based on three key ingredients. First, an F_4 style algorithm to compute the Groebner basis is adopted, where a novel prolongation is designed such that the sizes of coefficient matrices under consideration are nicely controlled. Second, the complexity bound of the algorithm is achieved by a nice estimation for the degree and height bounds of the polynomials in the generalized Hermite normal form. Third, fast algorithms to compute Hermite normal forms of matrices over $Z[x]$ are used as the computational tool.

17:20–17:45
Victor Pan
Lehman College, City University of New York, USA

Transformations of matrix structures and fast approximate computations with Cauchy matrices and polynomials

Matrices with the structures of Toeplitz, Hankel, Vandermonde and Cauchy types are omnipresent in modern computations in Sciences, Engineering, and Signal and Image Processing. These four matrix classes have distinct features, but in our 1990 paper in Mathematics of Computation we showed that Vandermonde and Hankel multipliers can be applied to transform each class into the others, and then we demonstrated how by using these transforms we can readily extend any successful matrix inversion algorithm from one of these classes to all the others. The power of this approach was widely recognized later, when novel numerically stable algorithms solved nonsingular Toeplitz linear systems of equations in quadratic (versus classical cubic) arithmetic

time based on transforming Toeplitz into Cauchy matrix structures. More recent papers combined the same transformation with a link of the Cauchy matrices to the Hierarchical Semiseparable matrix structure, which is a specialization of matrix representations employed by the Fast Multipole Method. This produced numerically stable algorithms that approximated the solution of a nonsingular Toeplitz linear system of equations in nearly linear arithmetic time. We first revisit the successful method of structure transformation, covering it comprehensively. Then we analyze the latter approximation algorithms for Toeplitz linear systems and extend them to approximate multiplication of Vandermonde and Cauchy matrices by a vector and to approximate solution of Vandermonde and Cauchy linear systems of equations provided that they are nonsingular and well-conditioned. We decrease the arithmetic cost of the known numerical approximation algorithms for these tasks from quadratic to nearly linear, and similarly for the computations with the matrices having structures that generalize the structures of Vandermonde and Cauchy matrices and for polynomial and rational evaluation and interpolation. We also accelerate a little further the known numerical approximation algorithms for a nonsingular Toeplitz or Toeplitz-like linear system by employing distinct transformations of matrix structures, and we briefly comment on some natural research challenges, particularly some promising applications of our techniques to high precision computations. An important implication of our work is the acceleration of the known numerical algorithms for multipoint polynomial evaluation and interpolation, which are fundamental for modern symbolic and numerical computing. The known algorithms solve both problems over any field of constants in nearly linear arithmetic time, but the cost grows to quadratic for numerical solution. We fix this discrepancy: our new numerical algorithms run in nearly linear arithmetic time. At first we restate the goals as the multiplication of an n-by-n Vandermonde matrix by a vector and the solution of a Vandermonde linear system of n equations. Then we combine our techniques of the transformation of matrix structures and Fast Multipole Method.

17:45–18:10
Shaoshi Chen
Chinese Academy of Sciences, China

The sixth dwarf of symbolic computation

In this talk, I will overview some fundamental algorithms and recent progress in symbolic integration. In particular, two historical notes of Kaltofen on symbolic integration will be recalled.

18:10–18:15
Closing remarks