CHALLENGES IN LINEAR AND POLYNOMIAL ALGEBRA IN SYMBOLIC COMPUTATION SOFTWARE

Wolfram Decker (University of the Saarland)
Keith Geddes (University of Waterloo)
Erich Kaltofen (North Carolina State University)
Stephen M. Watt (University of Western Ontario)

October 1, 2005–October 6, 2005

1 Summary

1.1 Overview of area covered

The subject of the workshop was innovation in algorithms and software addressing key bottlenecks in symbolic mathematical computation software. By symbolic mathematical computation software we mean software like Maple (represented by several participants including Jürgen Gerhard from Maplesoft), Mathematica, Macaulay 2 (represented by Michael Stillman), Magma (represented by Allan Steele), MuPAD, NTL, SINGULAR (represented by Gert-Martin Greuel) etc., whose purpose it is to aid a mathematician, scientist, engineer, or educator to solve mathematical problems on a computer. The specific area of focus for this workshop was challenges arising from linear and polynomial algebra at the core of these systems.

Symbolic computation software implements many sophisticated algorithms on polynomials, matrices, combinatorial structures and other mathematical objects in a multitude of different dense, sparse, or implicit (black box) representations. Several of the algorithms are well-known: Buchberger's Gröbner basis reduction algorithm in all its flavors, lattice bases reduction algorithms (LLL, PSLQ) [addressed by M. van Hoeij's presentation], Wiedemann's sparse linear system solver for scalars from a finite field [addressed by P. Giorgi's and J.-G. Dumas's presentations], polynomial factorization algorithms [addressed by M. van Hoeij's presentation], algorithms for solving in closed form differential and difference equations [addressed by E. Hubert's presentation], sparse interpolation algorithms [addressed by W.-s. Lee's presentation], and many more. These algorithms form the backbone of any symbolic computation software, and their improvement is the continuous effort of researchers.

In addition, several categories of algorithms for new basic problems are the subject of vigorous current investigation: diophantine linear system solution, algorithms for approximate data, e.g., floating point scalars, such as approximate polynomial greatest common divisors [addressed by L. Zhi's and H. Kai's presentations], factorization and non-linear system solving via homotopical deformation [addressed by A. Sommese's presentation], manipulation of polynomials over non-commutative domains, and more.

We estimate that the company-based systems Maple and Mathematica together are licensed to over five million users. We note that the Research & Development divisions in these companies are quite small. One objective subject of the workshop was how academia and industry can provide the users an ever-increasing speedup in the known algorithmic solutions on platforms designed with modern computer science principles.

This entails the discovery of completely new algorithms, such as the ones in the new problem categories mentioned above, the change of existent algorithms for efficient computer implementation [addressed by A. Steele's presentation], and the computer science of meshing the individually implemented algorithms into a large symbolic computing environment [see the section on the two software discussions].

1.2 Overview of achieved objectives

Our workshop brought together algorithm designers and symbolic computation software builders from industry and academia. Our first objective was to review the status of the problems in the core area whose solution has the greatest impact in systems for symbolic mathematical computation. Our second objective was to design an approach that can achieve fast transfer of new mathematical algorithmic advances and new computer science concepts into the available software. We invited for discussion those who make the new mathematics for the discipline and those who make the computer programs, in particular those who are engaged in both activities.

The software builder is faced with a mammoth task: the involved mathematical analysis in current algorithms can be highly sophisticated, using deep mathematical ideas. We give as an example the computation of sparse resultant formulas via exterior algebras and Chow forms or F.-O. Schreyer's presentation.

The underlying system for programming these algorithms is highly complex, combining techniques from reusable object-oriented design with entirely original data structures and standards. For example, the LinBox group, which is developing a symbolic linear algebra library in analogy to numerical libraries such as LinPack and MatLab, had to revise the basic generic archetype for a black box matrix three times, thus requiring a re-programming of the entire library. The revisions were necessitated when new concepts such as non-native garbage collection and BLAS (basic linear algebra subprograms) were introduced. J.-G. Dumas presentation addressed several of those issues. In general, our experience is that efficient delivery of effective symbolic computation software requires ongoing and often original computer science research.

Clearly, given the proliferation of algorithmic ideas and the complexity of a modern computer environment, innovative design principles and linkages are required to bring the new breakthroughs quickly into the software that the users, including our own community, need.

This workshop provided a forum for focused discussion among the experts in industry and academia, and among algorithm designers and algorithm implementors. The goal was to understand a framework which will foster the evolution of new algorithmic ideas into usable software in a timely fashion. The pressures on being able to faster compute more are great. In some cases, the difference can be the proof or disproval of a mathematical conjecture [addressed in part in D. Lazard's talk on the Solotareff problem]. In others, the yield can be a better FFT (fast Fourier transform) algorithm.

2 Titles and abstracts of presentations

SCHEDULE

	Sunday	**Monday**	**Tuesday**	**Wednesday**	**Thursday**
Session chairs	M. Dewar	A. Storjohann	C. Brown	M. Stillman	
9:00-9:45	J. Demmel	P. Giorgi	L. Zhi	E. Hubert‡	SW disc.† II
9:45-10:30	E. Schost	F. Rouillier	H. Kai	F.-O. Schreyer	
11:00-11:45	M. van Hoeij	J.-G. Dumas	W.-s. Lee	G.-M. Greuel	
Session chairs	T. Lange	F. Winkler		J. Gerhard	
14:30-15:15	von zur Gathen	D. Lazard	Hike at Lake Luise/	A. Steel	
15:45-16:30	A. Sommese	SW disc.† I	Moraine Lake	M. Monagan	

†Software group discussion

‡Hubert's talk was recorded

Speaker: **James Demmel** (University of California at Berkeley)
Title: *Toward accurate polynomial evaluation in rounded arithmetic*
Abstract: Given a multivariate real (or complex) polynomial p and a domain $\mathcal{D}$, we would like to decide whether

an algorithm exists to evaluate $p(x)$ accurately for all $x \in \mathcal{D}$ using rounded real (or complex) arithmetic. Here "accurately" means with relative error less than 1, i.e., with some correct leading digits. The answer depends on the model of rounded arithmetic: We assume that for any arithmetic operator $op(a, b)$, for example $a + b$ or $a \cdot b$, its computed value is $op(a, b) \cdot (1 + \delta)$, where $|\delta|$ is bounded by some constant ϵ where $0 < \epsilon \ll 1$, but δ is otherwise arbitrary. This model is the traditional one used to analyze the accuracy of floating point algorithms. Our ultimate goal is to establish a decision procedure that, for any p and $\mathcal{D}$, either exhibits an accurate algorithm or proves that none exists. In contrast to the case where numbers are stored and manipulated as finite bit strings (e.g., as floating point numbers or rational numbers) we show that some polynomials p are impossible to evaluate accurately. The existence of an accurate algorithm will depend not just on p and $\mathcal{D}$, but on which arithmetic operators and which constants are are available and whether branching is permitted. Toward this goal, we present necessary conditions on p for it to be accurately evaluable on open real or complex domains $\mathcal{D}$. We also give sufficient conditions, and describe progress toward a complete decision procedure. We do present a complete decision procedure for homogeneous polynomials p with integer coefficients, $\mathcal{D} = \mathbb{C}^n$, and using only the arithmetic operations $+$, $-$ and $\cdot$. Reference: [1].

Speaker: **Jean-Guillaume Dumas** (Université de Grenoble, France)
Title: *LinBox-1.0*
Abstract: Three major threads have come together to form the linear algebra library LinBox. The first is the use of modular algorithms when solving integer or rational matrix problems. The second thread and original motive for LinBox is the implementation of black box algorithms for sparse/structured matrices. Finally, it has proven valuable to introduce elimination techniques that exploit the floating point BLAS libraries even when our domains are finite fields. The latter is useful for dense problems and for block iterative methods. Black box techniques are enabling exact linear algebra computations of a scale well beyond anything previously possible. The development of new and interesting algorithms has proceeded apace for the past two decades. It is time for the dissemination of these algorithms in an easily used software library so that the mathematical community may readily take advantage of their power. LinBox is that library. In this talk, we sketch the current range of capabilities, describe the design and give several examples of use. Reference: `http://www.linalg.org`.

Speaker: **Joachim von zur Gathen** (B-IT, University of Bonn, Germany)
Title: *High-performance computer algebra*
Abstract: There are two scenarios for putting the asymptotically fast algorithms of computer algebra to work: in software and in hardware. The first is exemplified by polynomial arithmetic, in particular factorization, on sequential and parallel machines. The size of cutting edge problems is measured in megabits. The second one deals with a few hundred bits and yields fast cryptographic coprocessors at the size of current key lengths. Reference: [4].

Speaker: **Pascal Giorgi** (University of Waterloo)
Title: *Integer Linear System Solving*
Abstract: Recent implementations of algorithms for integer linear system solving can compute solutions of systems with around $2,000$ equations over word size numbers in about a minute. These performances are achieved for dense matrices using the highly optimized BLAS library. Currently we are exploiting the same approach to provide practical implementations for large sparse systems. In our talk we describe our prototype implementation of an experimental algorithm for sparse solving which reduces much of the computation to level 2 and 3 BLAS and seems to improve the bit complexity from n^3 to $n^{2.5}$. Reference: [3].

Speaker: **Gert-Martin Greuel** (University of Kaiserslautern Germany)
Title: *Computing equisingularity strata of plane curve sigularities*
Abstract: Equisingular families of plane curve singularities, starting from Zariski's pioneering 'Studies in Equisingularity I–III' have been of constant interest ever since. The theory was basically topologically motivated and so far it was only considered in characteristic 0. We develop a new theory for equisingularity in any characteristic which gives even new insight in characteristic 0. Moreover, it is algorithmic and the algorithms for computing equisingularity strata have been implemented in Singular.

Speaker: **Mark van Hoeij** (Florida State University)
Title: *Complexity results for factoring univariate polynomials over the rationals and bivariate polynomials over finite fields*
Abstract: In this talk, a polynomial time complexity bound is given for the algorithm in "Factoring polynomials and the knapsack problem" [6]. A complexity result is also given for factoring bivariate polynomials over finite fields. Specifically, to solve the combinatorial problem, it suffices to Hensel lift to accuracy $min(p, n) \cdot (n - 1) + 1$ where p is the characteristic of the finite field and n is the total degree.

Speaker: **Evelyne Hubert** (INRIA Sophia Antipolis)
Title: *Rational and Replacement Invariants of a Group Action*
Abstract: Group actions are ubiquitous in mathematics. They arise in diverse areas of applications, from classical mechanics to computer vision. A classical but central problem is to compute a generating set of invariants. The proposed presentation is based on a joint article with I. Kogan, North Carolina State Universtity, and is part of a bigger project for differential systems invariant under a Lie group that was started with E. Mansfield, University of Kent at Canterburry.

We consider a rational group action on the affine space and propose a construction of a finite set of rational invariants and a simple algorithm to rewrite any rational invariant in terms of those generators.

The rewriting of any rational invariant in terms of the computed generating set becomes a trivial replacement. For the general case we introduce a finite set of replacement invariants that are algebraic functions of the rational invariants. They are the algebraic analogues of the normalized invariants in Cartan's moving frame construction. The construction generalizes to the computation of a fundamental set of differential invariants.

Speaker: **Hiroshi Kai** (Ehime University)
Title: *Reliable rational interpolation by symbolic-numeric computation*
Abstract: A rational interpolation is computed by simultaneous linear equations numerically. But, if the linear equations are solved by fixed precision floating point arithmetic, there appear a pathological feature such as undesired pole and zero. An algorithm is presented to eliminate the feature and then give a reliable rational interpolation with the help from stabilization theory and computer assisted proof. Reference: [7].

Speaker: **Daniel Lazard** (INRIA France)
Title: *New challenges in polynomial computation and real algebraic geometry: Example of Solotareff approximation problem*
Abstract: Most of the computations related to polynomial equations and inegalities are done either by numeric computation, either by using Gröbner bases, Collin's cylindrical decomposition or triangular systems. With the progress of all these methods, the main algorithmic challenge becomes to select well specified classes of problems which may be solved by using appropriately several of these methods.

Examples of such an approach may be found in global optimization or parametric systems (see Rouillier's talk).

We illustrate this with Solotareff approximation problem (Kaltofen's challenge 2) for which CAD fails in degree 6, while a complete solution in degrees up to 10 may be obtained by mixing theoretical considerations on quantifier elimination and with well choosen operations of localization and projection done through Gröbner bases. Reference [10].

Speaker: **Wen-shin Lee** (University of Antwerp, Belgium)
Title: *Sparse Polynomial Interpolation and Representation*
Abstract: As polynomials are one of the fundamental objects in symbolic computation, being able to represent and manipulate them efficiently can have dramatic effects on the cost of many algorithms.

This talk focuses on sparse polynomials. I discuss black box sparse interpolation and explore sparse representations of polynomials. The interplay between these problems and recent development [5] are also addressed.

Speaker: **Michael Monagan** (Simon Fraser University)
The talk was on sparse rational interpolation.

Speaker: **Fabrice Rouillier** (INRIA France)
The talk was on parametric system solving.

Speaker: **Éric Schost** (Ecole Polytechnique France)
Title: *Point counting in genus 2, and some of the problems it raises*
Abstract: Computing the number of points in the Jacobian of a hyperelliptic curve is a basic question for hyperelliptic cryptosystem design. For curves of genus 2 over prime fields, present solutions rely on a variety of tasks: polynomial system solving, root finding, computation with algebraic numbers, ...

This talk (given from a computer algebraist point-of-view) aims at describing problems met when trying to reach "cryptographic size", some solutions, and how they meet, or can motivate, research in symbolic computation. This is joint work with Pierrick Gaudry.

Speaker: **Frank-Olaf Schreyer** (Universität des Saarlandes, Germany)
Title: *Computing the higher direct image complex of coherent sheaves*
Abstract: The higher direct image complex of a coherent sheaf (or finite complex of coherent sheaves) under a projective morphism is a fundamental construction that can be defined via a Cech complex or an injective resolution, both inherently infinite constructions. Using exterior algebras and relative versions of theorems of Beilinson and Bernstein-Gel'fand-Gel'fand, we give an alternate description in finite terms.

Using this description we can give explicit descriptions of the loci in the base spaces of flat families of sheaves in which some cohomological conditions are satisfied—for example, the loci where vector bundles on projective space split in a certain way, or the loci where a projective morphism has higher dimensional fibers.

Our approach is so explicit that it yields an algorithm suited for computer algebra systems.

Speaker: **Andrew Sommese** (University of Notre Dame)
Title: *Exceptional Sets and Fiber Products*
Abstract: Regard the solution set of a polynomial system $f(x\colon y) = 0$ with algebraic parameters as a family $X \to Y$ of algebraic sets. A symbolic/numeric algorithm based on fiber products is given to compute the subsets of X consisting of points where the fiber dimension of X is greater than it is for generic values of the parameters. A discussion of motivating problems from engineering is given.

Speaker: **Allan Steel** (University of Syndey)
Title: *Linear and Polynomial Algebra in Magma: A Detailed Overview*
Abstract: I give a detailed overview of the many structures and algorithms in the Magma Computer Algebra system for computing in Linear and Polynomial Algebra. The key challenges and successes are highlighted, particularly in the goal of practical implementations of asymptotically-fast algorithms.

Speaker: **Lihong Zhi** (Key Lab of Mathematics Mechanization, AMSS Beijing China)
Title: *Structured Low Rank Approximation of a Sylvester Matrix*
Abstract: The task of determining the approximate greatest common divisor (GCD) of polynomials with inexact coefficients can be formulated as computing for a given Sylvester matrix a new Sylvester matrix of lower rank whose entries are near the corresponding entries of that input matrix. We solve the approximate GCD problem by new methods: one is based on structured total least norm algorithm, another is based on structured total least squares algorithm, in our case for matrices with Sylvester structure. We present iterative algorithms that compute a minimum approximate GCD and that can certify an approximate ϵ-GCD when a tolerance ϵ is given on input. Each single iteration is carried out with a number of floating point operations that is of cubic order in the input degrees. In the univariate GCD case, we explore the displacement structure and reduce the complexity of each single iteration to be of only quadratic with respect to the degrees of the input polynomials. We also demonstrate the practical performance of our algorithms on a diverse set of univariate and multivariate pairs of polynomials. This is joint work with Erich Kaltofen, Bingyu Li and Zhengfeng Yang [11, 9, 8].

3 Summary of the two discussions on software

Both discussions were moderated by Stephen M. Watt.

The first discussion on Monday afternoon covered two topics, one given by Gert-Martin Greuel on the *Oberwolfach References on Mathematical Software (ORMS)* project [`http://orms.mfo.de`], and one by James Demmel on plans for the next release of LAPACK `http://www.netlib.org/` and ScaLAPACK `http://www.netlib.org/scalapack/`, including arbitrary precision versions, [joint work with Jack Dongarra et al.]. In particular, arbitrary precision, was discussed. One approach is to use F90 operator overloading so that one can produce fixed precision versions of any precision, calling someone else's arbitrary precision package. A web site to enter opinions was `http://icl.cs.utk.edu/lapack-forum/survey/`, which now has the survey's results.

The second discussion on Thursday morning addressed problems in transferring algorithms into systems. The use of generic algorithm techniques either by templates in C++ or by types in Aldor was promoted. The philosophical difference between opensource free software and commercial products was noted. For purpose of comparing implementations, the creation of a standard repository for tests and specific versions of software was deemed to be useful. E. Kaltofen pointed out that many symbolic computation problems require parallel computation like those done in ScaLAPACK. He suggested that more parallel symbolic computation algorithms and implementations should be developed in the next five years.

4 Assessment

This workshop provided a unique opportunity for leading researchers and developing younger investigators to exchange ideas on current challenges in several important areas of computer algebra. The areas of concentration of the workshop were:

- Linear algebra, both for exact methods (Dumas's and Giorgi's talk) and numerical methods (Demmel's presentation in the first discussion on software).
- Polynomial algebra. Polynomial factorization was covered by three speakers (von zur Gathen, van Hoeij and Steel), sparse polynomial interpolation by Monagan and problems in commutative algebra and polynomial systems by Greuel, Lazard, Roullier and Schreyer.
- Applications of symbolic computation to cryptography were presented by Schost.
- Hybrid symbolic-numeric algorithms were a focus, covered by Kai, Lee, Sommese and Zhi.
- Differential equations were addressed by Hubert, the talk which we chose to record.

We feel the workshop was valuable for several reasons: First, many speakers chose to discuss new ongoing work. Second, Demmel's numerical computation point-of-view made it apparent that numerical methods must be an integral part of symbolic computation software. One of the questions Demmel raised, that of the difference of structured vs. unstructured condition numbers in the case of the Sylvester matrices has subsequently been addressed [8]. Third, there was participation from the software industry, namely Gerhard from Waterloo Maplesoft and Dewar from the Numerical Algorithms Group (NAG).

5 Acknowledgement

The organizers would like to thank the Banff International Research Station for financial and logistic support to host this workshop. In particular, we would like to thank Barbara Dempsey, Natalia Gartley, Jacqueline Kler, Jewel Peters, and Kathryn Wood for their assistance in coordination of the invitees and to Brent Kearney and Brenda Shakotko for help during the workshop. We are grateful to the BIRS scientific directors Nassif Ghoussoub and Robert Moody for the appreciation and support for our workshop and discipline.

References

[1] James Demmel, Ioana Dumitriu, and Olga Holtz. Toward accurate polynomial evaluation in rounded arithmetic. In Luis M. Pardo, Allan Pinkus, Endre Süli, and Michael J. Todd, editors, *Foundations of Computational Mathematics, Santander 2005*, volume 331 of *London Mathematical Society Lecture Note Series*, pages 36–105. Cambridge Univ. Press, Cambridge, United Kingdom, 2006.

[2] Jean-Guillaume Dumas, editor. *ISSAC MMVI Proc. 2006 Internat. Symp. Symbolic Algebraic Comput.*, New York, N. Y., 2006. ACM Press.

[3] Wayne Eberly, Mark Giesbrecht, Pascal Giorgi, Arne Storjohann, and Gilles Villard. Solving sparse rational linear systems. In Dumas [2], pages 63–70.

[4] Joachim von zur Gathen and J. Gerhard. *Modern Computer Algebra*. Cambridge University Press, Cambridge, New York, Melbourne, 1999. Second edition 2003.

[5] Mark Giesbrecht, George Labahn, and Wen shin Lee. Symbolic-numeric sparse interpolation of multivariate polynomials. In Dumas [2], pages 116–123.

[6] Mark van Hoeij. Factoring polynomials and the knapsack problem. *J. Number Theory*, 95:167–189, 2002. Implementation available at `http://web.math.fsu.edu/~hoeij/`.

[7] Hiroshi Kai. Rational function approximation and its ill-conditioned property. In Wang and Zhi [12], pages 62–64.

[8] Erich Kaltofen, Zhengfeng Yang, and Lihong Zhi. Approximate greatest common divisors of several polynomials with linearly constrained coefficients and singular polynomials. In Dumas [2], pages 169–176.

[9] Erich Kaltofen, Zhengfeng Yang, and Lihong Zhi. Structured low rank approximation of a Sylvester matrix. In Dongming Wang and Lihong Zhi, editors, *Symbolic-Numeric Computation*. Birkhäuser, submitted Oct. 2005; revised June 2006. To appear, 15 pages. Preliminary version in [12], pp. 188–201.

[10] Daniel Lazard. Solving Kaltofen's challenge on Zolotarev's approximation problem. In Dumas [2], pages 196–203.

[11] Bingyu Li, Zhengfeng Yang, and Lihong Zhi. Fast low rank approximation of a Sylvester matrix by structured total least norm. *J. JSSAC (Japan Society for Symbolic and Algebraic Computation)*, 11(3,4):165–174, 2005.

[12] Dongming Wang and Lihong Zhi, editors. *Internat. Workshop on Symbolic-Numeric Comput. SNC 2005 Proc.*, distributed at the Workshop in Xi'an, China, July 19–21, 2005.