06271 Abstracts Collection
Challenges in Symbolic Computation Software
— Dagstuhl Seminar —

Wolfram Decker[1], Mike Dewar[2], Erich Kaltofen[3] and Stephen M. Watt[4]

[1] Universität Saarbrücken, DE
decker@math.uni-sb.de
[2] NAG Ltd. - Oxford, GB
miked@nag.co.uk
[3] North Carolina State University, US
kaltofen@math.mit.edu
[4] University of Western Ontario, CA
Stephen.Watt@uwo.ca

Abstract. From 02.07.06 to 07.07.06, the Dagstuhl Seminar 06271 "Challenges in Symbolic Computation Software" was held in the International Conference and Research Center (IBFI), Schloss Dagstuhl. During the seminar, several participants presented their current research, and ongoing work and open problems were discussed. Abstracts of the presentations given during the seminar as well as abstracts of seminar results and ideas are put together in this paper. The first section describes the seminar topics and goals in general. Links to extended abstracts or full papers are provided, if available.

Keywords. Symbolic computation, computer algebra, computational algebraic geometry, combinatorial methods in algebra, hybrid symbolic-numerical methods, algorithm design, symbolic computation languages, systems and user interfaces

06271 Executive Summary - Challenges in Symbolic Computation Software

Symbolic computation software allows mathematicians, scientists, engineers, or educators to deal with elaborate calculations using a computer. The applications range from introducing the experimental method in fields of pure mathematics to practical applications, for instance, in cryptology, robotics, or signal theory. The software includes mainstream commercial products such as Maple or Mathematica and highly specialized, public domain systems such as CoCoa, Macaulay2, or Singular.

Symbolic computation software implements a variety of sophisticated algorithms on polynomials, matrices, combinatorial structures, and other mathematical objects in a multitude of different dense, sparse, or implicit (black box) representations.

The subject of the seminar was innovation in algorithms and software, bringing algorithm designers, software builders, and software users together.

Keywords: Symbolic computation, computer algebra, computational algebraic geometry, combinatorial methods in algebra, hybrid symbolic-numerical methods, algorithm design, symbolic computation languages, systems and user interfaces

Joint work of: Decker, Wolfram; Dewar, Mike; Kaltofen, Erich; Watt, Stephen M.

Extended Abstract: http://drops.dagstuhl.de/opus/volltexte/2006/777

CoCoALib and computational commutative algebra

John Abbott (University of Genova, I)

CoCoaLib is a C++ library for COmputations in COmmutative Algebra. The design of the library has been developed in tandem with the book by Robbiano & Kreuzer - this approach ensures the solidity of the (mathematical) foundations of the software while also forcing a thorough check of the mathematical details. The development proved surprisingly taxing despite the expertise and experience of the authors, but produced results (book & software) of notable quality.

The production of CoCoALib is a gamble: the costs of writing high quality code are high yer the effort and outcome receive only scant recognition in the computer algebra community. Without recognition of the work involved, those who do implement risk being penalized for "insufficient academic production"

There is a need of a mechanism of assessing software and for publishing it (provided it is deemed to be of sufficiently high quality). The obstacles to achieving this goal are plenty: the reviewing process appears to be more difficult than for normal mathematical papers, published programs need to evolve with time (at least for debugging), code relying on commercial software posses problems. Another development we anticipate is the birth of specialized servers which intercommunicate (e.g. via OpenMath) in the course of a computation. This means existing interactive systems must make their capabilities available via a "server interface". In some cases making the software available as a library may be desirable: tighter integration, no communications overhead...

Access to CoCoALib will eventually be posible in all three ways: library, server & interactive system.

Challenges in Computational Commutative Algebra

John Abbott (University of Genova, I)

In this paper we consider a number of challenges from the point of view of the CoCoA project one of whose tasks is to develop software specialized for computations in commutative algebra. Some of the challenges extend considerably beyond the boundary of commutative algebra, and are addressed to the computer algebra community as a whole.

Keywords: Academic recognition implementation OpenMath CoCoA

Extended Abstract: http://drops.dagstuhl.de/opus/volltexte/2006/768

Coxeter Lattice Paths

Thomas Ashby (University of Edinburgh, GB)

This talk concerns generating code for running computationally intensive numerical lattice QCD simulations on large parallel computers, using an approach based on the theory of Coxeter groups. Many physical systems have inherent symmetry, and this is usually implicit in the calculations needed to simulate them using discrete approximations, and thus in the associated code. By reversing this and basing the generation of code on the symmetry group of the lattice in question, we arrive at a very natural way of generating and reasoning about programs. The principal aim is a formal way of representing lattices and the paths on these lattices that correspond to the required calculations. This foundation allows the creation and manipulation of lattices and paths to be automated, obviating what can be a labour-intensive and errorprone task.

In more detail, a method will be given for representing the points of a regular lattice as elements of the translation subgroup of an affine Coxeter group, by finding the subgroup generators starting from the Coxeter graph of the affine group. Similarly, step sequences are derived as words in the free group generated by the translation subgroup generators themselves. We introduce code generation techniques and the automation of two code optimisations; the grouping of paths into equivalence classes, and the factoring out of common path segments. The latter technique reduces the amount of communication necessary between nodes, and is thus likely to be important in practice.

Keywords: Parallel computing, code generation, Coxeter groups, regular lattices, lattice paths, path optimisation

Joint work of: Ashby, Thomas J.; Kennedy, Anthony D.; Watt, Stephen M.

Extended Abstract: http://drops.dagstuhl.de/opus/volltexte/2006/769

Change of order for regular chains in positive dimension

Xavier Dahan (Ecole Polytechnique - Palaiseau, F)

We present a new algorithm to change the lexicographic order of a *regular chain* (a triangular polynomial system, whith initials having nice properties) in *positive dimension*.

The computations are reduced to changing of order in dimension zero only (such an algorithm in dimension zero is taken as a blackbox in this work), using the "specialize then lift" paradigm, relying on the Newton-Hensel operator.

Several calls to change of orders in dimension zero are required, and they are conducted by combinatorial informations readable through a linearization of the problem on a relevant tangent space. Complexity anf probability analyses are given.

Keywords: Change of order, Regular Chain, Newton operator, Matroids

Joint work of: Dahan, Xavier; Jin, Xin; Moreno Maza, Marc; Schost, Eric

Adaptive Triangular System Solving

Jean-Guillaume Dumas (LMC-IMAG - Grenoble, F)

Large-scale applications and software systems are getting increasingly complex. To deal with this complexity, those systems must manage themselves in accordance with high-level guidance from humans. Adaptive and hybrid algorithms enable this self-management of resources and structured inputs.

In this talk, we first propose a classification of the different notions of adaptivity. For us, an algorithm is adaptive (or a poly-algorithm) when there is a choice at a high level between at least two distinct algorithms, each of which could solve the same problem. The choice is strategic, not tactical. It is motivated by an increase of the performance of the execution, depending on both input/output data and computing resources.

Then we propose a new adaptive algorithm for the exact simultaneous resolution of several triangular systems over finite fields. The resolution of such systems is e.g. one of the two main operations in block Gaussian elimination. For solving triangular systems over finite fields, the block algorithm reduces to matrix multiplication and achieves the best known algebraic complexity. Exact matrix multiplication, together with matrix factorizations, over finite fields can now be performed at the speed of the highly optimized numerical BLAS routines. This has been established by the FFLAS and FFPACK libraries. In this talk we propose several practicable variants solving these systems: a pure recursive version, a reduction to the numerical dtrsm routine and a delaying of the modulus operation. Then a cascading scheme is proposed to merge these variants into an adaptive sequential algorithm.

We then propose a parallelization of this resolution. The adaptive sequential algorithm is not the best parallel algorithm since its recursion induces a dependancy. A better parallel algorithm would be to first invert the matrix and then to multiply this inverse by the right hand side. Unfortunately the latter requires more total operations than the adaptive algorithm. We thus propose a coupling of the sequential algorithm and of the parallel one in order to get the best performances on any number of processors. The resulting cascading is then an adaptation to resources.

This shows that the same process has been used both for adaptation to data and to resources. We thus propose a generic framework for the automatic adaptation of algorithms using recursive cascading.

Keywords: Adaptive and hybrid algorithms, triangular system solving, parallel and sequential degenerations

Joint work of: Dumas, Jean-Guillaume; Pernet, Clément; Roch, Jean-Louis

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2006/770

Computational Aspects of the Resolution of Singularities

Anne Frühbis-Krüger (TU Kaiserslautern, D)

The task of resolution of singularities has been one of the central topics in Algebraic Geometry for many decades. After results in low dimension in the first half of the 20th century, it was Hironaka's monumental article in 1964 which solved the porblem in the general case in chareacteristic zero. The case of characteristic $p > 0$ is still unsolved except in partial results in low dimension.

But Hironaka's proof did not put an end to the interest in characteric zero, instead it shifted the focus toward the task of finding a more constructive approach. Such algorithmic approaches appeared at the end of the 1980's independently by Villamayor and by Bierstone and Milman. In this talk we consider the computational tasks arising from Villamayor's algorithm and present an implementation.

Keywords: Resolution of Singularities, algorithmic desingularization

Extended Abstract: http://drops.dagstuhl.de/opus/volltexte/2006/771

Decomposition of Differential and Difference Polynomials

Xiao-Shan Gao (MMRC - Beijing, PRC)

We propose algorithms to reduce the decomposition of nonlinear univariate ordinary differential polynomials and ordinary difference polynomials to the decomposition of univariate linear ordinary differential polynomials and linear ordinary difference polynomials, respectively.

The algorithms are of exponential complexity in the worst case, but seem practically effective for a large class of problems.

In the differential case, we first find the right decomposition factor by reducing the problem in the general case to the decomposition of differential polynomials whose left decomposition factor is pseudo linear. Then the pseudo linear case is solved by decomposition of linear differential polynomials and solution of systems of linear equations. After the right decomposition factor is found, it is easy to find the left decomposition factor.

In the difference case, we find the right decomposition factor by reducing the problem in the general case to the decomposition of total degree homogeneous difference polynomials, which in turn is reduced to finding the linear left decomposition factors of total degree homogeneous difference polynomials. Finally, the linear left decomposition factor can be found by decomposing a newly constructed linear difference polynomial.

Keywords: Decomposition, Differential polynomials, difference polynomials

Decomposition of Differential Polynomials

Xiao-Shan Gao (MMRC - Beijing, PRC)

We present an algorithm to decompose nonlinear differential polynomials in one variable and with rational functions as coefficients. The algorithm is implemented in Maple for the *constant field* case. The program can be used to decompose differential polynomials with more than one thousand terms effectively.

Keywords: Decomposition, differential polynomial, difference polynomial

Joint work of: Gao, Xiao-Shan; Zhang, Mingbo

Extended Abstract: http://drops.dagstuhl.de/opus/volltexte/2006/772

Generating Symmetric FFT Algorithms

Jeremy Johnson (Drexel University, USA)

This talk is centered around two challanges for symbolic mathematical software and is organized into two parts. The first challenge is to use mathematical structure and symbolic mathematical computation to generate high-performance code - the challenge is to produce adaptable code that is competetive with highly tuned vendor implementations. The second challenge is to provide a high-level interface where mathematical algorithms, denoted in the appropriate mathematical abstraction, are easily specified and the details automatically derived.

The first part presents an overview of the SPIRAL system (www.spiral.net) for generating, optimizing, and automatically adapting to different platforms high-performance implementations of fast signal transforms such as the Fast

Fourier Transform (FFT), discrete trigonometric transforms, fast wavelet transform, and filtering. Algorithms are represented as mathematical formulas and algorithms are derived and manipulated using rewrite rules. The selection of algorithm and implementation strategy are guided by a feedback loop which uses intelligent search to find the best implementation on a given platform. Performance data for the FFT is shown illustrating that the code generated is competitive with vendor supplied code (Intel's MKL and IPP libraries) and alternative approaches such as FFTW. In cases where the vendor was unable to spend sufficient time tuning, the SPIRAL generated code is significantly faster.

The second part presents a new algorithm, generalizing the real FFT, for computing the multi-dimensional discrete Fourier transform of an input vector having symmetric data. The algorithm uses a divide and conquer approach similar to the standard FFT, but improves the constant by avoiding the redundant computation presented by the symmetric data. This algorithm is most naturally stated and derived abstractly using FFTs of finite Abelian groups. The symmetries of a function defined on the group A, are described by a subgroup of the semi-direct product of the automorphism group of A and the Heisenberg group of A, and the algorithm is obtained from the action of the affine part of this group on the indexing set given by A. This level of abstraction makes the algorithm easy to describe and derive, but difficult to implement due to the many details the abstraction hides. We present, preliminary software, written in the computer algebra system GAP, designed to build on top of SPIRAL, for generating concrete symmetric FFT algorithms, described by matrix factorizations, from the abstract formulation.

Keywords: FFT, Symmetric FFT, Heisenberg group, SPIRAL, GAP, automated performance tuning, code generation, algorithm generation

Finding Small Degree Factors of Multivariate Supersparse (Lacunary) Polynomials Over Algebraic Number Fields

Erich Kaltofen (MIT - Cambridge, USA)

We present algorithms that compute all irreducible factors of degree $\leq d$ of supersparse (lacunary) multivariate polynomials in n variables over an algebraic number field in deterministic polynomial-time in $(l+d)^n$, where l is the size of the input polynomial. In supersparse polynomials, the term degrees enter logarithmically as their numbers of binary digits into the size measure l. The factors are again represented as supersparse polynomials. Our approach follows that by H. W. Lenstra, Jr., on computing factors of univariate supersparse polynomials over algebraic number fields. Our generalization appeals to recent lower bounds on the height of algebraic numbers and to a special case of the former Lang conjecture.

By example we show how our algorithm applies to Stephen Watt's symbolic polynomials (first talk of this seminar).

Keywords: Sparse polynomials, lacunary polynomials, multivariate polynomials, polynomial factorization, polynomial-time complexity, algebraic numbers, height, Lang conjecture

Joint work of: Kaltofen, Erich; Koiran, Pascal

Full Paper:
http://www4.ncsu.edu/~kaltofen/bibliography/06/KaKoi06.pdf

See also: Proc. ISSAC 2006, ACM Press

Experiments with a pen-based math system

George Labahn (University of Waterloo, CA)

Pen-based devices such as Tablet PCs have gained a significant following of users in the past few years. However there still does not seem to be any outstanding applications for such devices. We view mathematics as being the one application that can change the current state. Of course by mathematics we mean both writing and working with mathematical expressions. In particular mathematics used with Tablet PCs need to take advantage of not only pen input but also of todays powerful computer algebra systems.

In this talk discuss many of the issues that make doing mathematics on pen-bsed devices a hard task. We also give a preliminary description of an experimental system, currently named MathBrush, for working with mathematics using pen-based devices. The system allows a user to enter mathematical expressions with a pen and to then do mathematical computation using a computer algebra system.

The system provides a simple and easy way for users to verify the correctness of their handwritten expressions and, if needed, to correct any errors in recognition. Choosing mathematical operations is done making use of context menus, both with input and output expressions.

Keywords: Pen-math, coputer algebra systemsm

MathBrush: An Experimental Pen-Based Math System

George Labahn (University of Waterloo, CA)

It is widely believed that mathematics will be one of the major applications for Tablet PCs and other pen-based devices. In this paper we discuss many of the issues that make doing mathematics on such pen-based devices a hard task.

We give a preliminary description of an experimental system, currently named MathBrush, for working with mathematics using pen-based devices. The system

allows a user to enter mathematical expressions with a pen and to then do mathematical computation using a computer algebra system. The system provides a simple and easy way for users to verify the correctness of their handwritten expressions and, if needed, to correct any errors in recognition. Choosing mathematical operations is done making use of context menus, both with input and output expressions.

Keywords: PC Tablets, pen-based devices, computer algebra systems

Joint work of: Labahn, George; MacLean, Scott; Marzouk Mirette; Rutherford, Ian; Tausky, David

Extended Abstract: http://drops.dagstuhl.de/opus/volltexte/2006/773

Computation of the Minimal Associated Primes

Santiago Laplagne (University of Buenos Aires, RA)

Solving systems of polynomial equations is a main task in Computer Algebra, although the precise meaning of what is an acceptable solution depends on the context.

In this talk, we interpret it as finding the minimal associated primes of the ideal generated by the polynomials. Geometrically, this is equivalent to decompose the set of solutions into its irreducible components.

We study the existing algorithms, and propose some modifications. A common technique used is to reduce the problem to the zero dimensional case. In a paper by Gianni, Trager and Zacharias they use this technique, combined with the splitting tool $I = (I : h^\infty) \cap \langle I, h^m \rangle$ for some specific polynomial h and integer m. This splitting introduces a number of redundant components that are not part of the original ideal. In the algorithm we present here, we use the reduction to the zero dimensional case, but we avoid working with the ideal $\langle I, h^m \rangle$. As a result, when the ideal has components of different dimensions, our algorithm is usually more efficient.

Keywords: Minimal associated primes, groebner basis, polynomail equations, radical

Extended Abstract: http://drops.dagstuhl.de/opus/volltexte/2006/774

Voronoi Diagram of Three Lines in 3D space

Daniel Lazard (Univ. Paris VI, F)

Voronoi diagrams are widely used in various fields or applications of computational geometry. Most of previous work is devoted to 2D Voronoi diagrams.

Voronoi diagrams of isolated points are delimited by the mediator planes of the pairs of points, and are therefore theoretically simple, even if the combinatoric complexity may make the computation difficult, if there are many points. Beside this, the simplest case is the Voronoi diagram of lines. For 2 lines, it is delimited by the bisector, which is a hyperbolic paraboloid (HP) if the two lines are not coplanar, two orthogonal planes if they intersect and a single plane if they are parallel. For 3 lines, the Voronoi diagram is easy to study if two of them are coplanar or if they are parallel to a plane (althought there are 13 different cases). We say that the 3 lines are in general position if they are not parallel to the same plane and no pair of line is coplanar. We show that the Voronoi diagram of 3 lines in general position is topologically independent of the particular choice of the lines. Especially, the trisector (curve of the points which are at the same distance of the 3 lines) is the intersection of two HP and has always 4 infinite smooth branches, which together are either a quartic of genus one or the union of a line and the 3 branches of a skew cubic which do not intersect it. Althought it looks very simple, this result needs the full power of the software state-of-the-art and involves algorithmic developments in real algorithmic geometry (due to Mohab Safey el Din) which are not yet published. The touch stones are to prove that a polynomial in 6 variables is never negative and the computation of the real part of the singular locus of an hypersurface in the 5D space, defined by a one page equation.

This illustrates the thesis already presented last year in Banff: The present challenge in real (algebraic) geometry is to develop efficient algorithms using as basic operations the efficient geometric operations like zero-dimensional solving, elimination, saturation and computation of the dimension and the degree of a variety?

Keywords: Voronoi diagram, positive multivariate polynomial, effective real algebraic geometry

Probabilistically Stable Numerical Sparse Polynomial Interpolation

Wen-Shin Lee (University of Antwerp, B)

We consider the problem of sparse interpolation of a multivariate black-box polynomial in floating-point arithmetic. That is, both the inputs and outputs of the black-box polynomial have some error, and all values are represented in standard, fixed-precision, floating-point arithmetic. By interpolating the black box evaluated at random primitive roots of unity, we give an efficient and numerically robust solution with high probability. We outline the numerical stability of our algorithm, as well as the expected conditioning achieved through randomization. Finally, we demonstrate the effectiveness of our techniques through numerical experiments.

Keywords: Symbolic-numeric computing, multivariate interpolation, sparse polynomial

Joint work of: Giesbrecht, Mark; Labahn, George; Lee, Wen-Shin

Extended Abstract: http://drops.dagstuhl.de/opus/volltexte/2006/775

Bounds and algebraic algorithms for ordinary differential characteristic sets

Marc Moreno Maza (University of Western Ontario, CA)

Consider the Rosenfeld-Groebner algorithm for computing a regular decomposition of a radical differential ideal generated by a set of ordinary differential polynomials. This algorithm inputs a system of differential polynomials and a ranking on derivatives and constructs finitely many regular systems equivalent to the original one. The property of regularity allows to check consistency of the systems and membership to the corresponding differential ideals.

We propose a bound on the orders of derivatives occurring in all intermediate and final systems computed by the Rosenfeld-Groebner algorithm and outline its proof.

We also reduce the problem of conversion of a regular decomposition of a radical differential ideal from one ranking to another to a purely algebraic problem. For the algebraic case, efficient modular and parallel algorithms are currently being developed and implemented.

Keywords: Differential algebra, maximal orders of derivatives, ranking conversions

Joint work of: Golubitsky, Oleg; Kondratieva, Marina; Moreno Maza, Marc; Ovchinnikov, Alexey

Toward efficient and reliable Groebner basis computation

Masayuki Noro (Kobe University, J)

Buchberger algorithm is the most general one for computing Groebner basis for general input polynomial set, but its naive implementation is not at all practical and various techniques have been applied for gaining efficiency in actual implementations. Among such techniques, trace algorithms and F4 algorithm with modular technique is considered to be efficient over the field of rationals, but for then latter one, only a few implementations succeed in achieving the expected efficiency.

I have been trying to find an efficient implementation of F4, and recently I have found a relatively satisfactory one. Exactly speaking the method is an F4-flavored Buchberger algorithm, similar to 'slimgb' in Singular. The same idea can be applied to Buchberger algorithm itself, which makes the existing Buchberger algorithm implementation faster for many examples.

We also consider the reliability of outputs from computer algebra systems. In some applications the correctness of an output is crucial and it is desirable to give some data for verification if possible. In Buchberger algorithm, a history of the computation of the non-zero intermediate bases is reasonably small and is sufficient for verification. In our (pseudo-)F4 implementation, in addition to the similar history for Buchberger algorithm part, we only have to give a prime number for each step of the row echelon form computation for checking the rank.

Keywords: Groebner basis, modular computation, F4 algorithm, reliability

Quartics, Log-Concavity and Computer Algebra

Peter Paule (University of Linz, A)

Victor Moll begins his article "The evaluation of integrals: A personal story" (Notices of the AMS, 2002) with the remark, "... It was even more a surprise to discover that new things can still be said today about the mundane subject of integration of rational functions of a single variable and that this subject has connections with branches of contemporary mathematics as diverse as combinatorics, special functions, elliptic curves, and dynamical systems." In this talk I will add another ingredient to his story, namely computer algebra. I will show how recently developed procedures can be used to retrieve observations which in Moll's original approach were derived with classical methods, like the positivity of the coefficients of a specialized family of Jacobi polynomials. In addition, as a result from a recent cooperation with Manuel Kauers (RISC), I will demonstrate that computer algebra can do even more, namely by proving Moll's longstanding log-concavity conjecture with a combination of various algorithms. These applications will lead to a variety of questions in connection with the general theme of the Dagstuhl Seminar ("Challenges in Symbolic Computation Software").

Keywords: Definite integrals, positivity, symbolic summation, log-concavity

FoCal A Framework for Effective Mathematics

Renaud Rioboo (Université Pierre et Marie Curie, F)

The talks presents the FoCaL framework which is a set of tools that helps building software systems. It is developped by French's Universite Pierre et Marie Curie, Conservatoire National des Arts et Metiers and Institut National de la Recherche en Informatique et Automatique. FoCaL enables to specify and implement programs but also to state and ensure correctness of properties about those programs.

The heart of the FoCaL framework is the FoCaL language which has object oriented features and enables to share specifications and properties between different components of a software system. The language also enable to share and resue definition and proofs of properties. Components of the FoCaL language are called species which have multiple inheritance and allows late binding. FoCaL is made of a compiler producing Ocaml code which is intended to be executed, running code compares favourabily with the best computer algebra packages available. Certification is achieved by producing Coq code with the help of an automatic prover which we call Zenon. Running examples covering computer algebra, effective mathmatics and also general software security programs are presented which illustrate the expressive and computational power of FoCaL.

The framework also has tools which enable to provide MathML documentation acting as Doxygen or JavaDOC emhance with methematical capabilities which can be viewed using current Web browsers technologies. Somme program analysis and XML conversion tools are also presented.

Keywords: FoCaL, Ocaml, Coq, Object Oriented Languages, Certification, Compiling, Semantics

Using fast matrix multiplication to solve structured linear systems

Eric Schost (University of Western Ontario, CA)

Structured linear algebra techniques are a versatile set of tools; they enable one to deal at once with various types of matrices, with features such as Toeplitz-, Hankel-, Vandermonde- or Cauchy-likeness.

Following Kailath, Kung and Morf (1979), the usual way of measuring to what extent a matrix possesses one such structure is through its displacement rank, that is, the rank of its image through a suitable displacement operator. Then, for the families of matrices given above, the results of Bitmead-Anderson, Morf, Kaltofen, Gohberg-Olshevsky, Pan (among others) provide algorithm of complexity $O(\alpha^2 n)$, up to logarithmic factors, where n is the matrix size and α its displacement rank.

We show that for Toeplitz- Vandermonde-like matrices, this cost can be reduced to $O(\alpha^{(}\omega - 1)n)$, where ω is an exponent for linear algebra. We present consequences for Hermite-Padé approximation and bivariate interpolation.

Keywords: Structured matrices, matrix multiplication, Hermite-Pade, bivariate interpolation

Joint work of: Schost, Eric; Bostan, Alin; Jeannerod, Claude-Pierre

Extended Abstract: http://drops.dagstuhl.de/opus/volltexte/2006/778

Optimizing linear algebra computations

Arne Storjohann (University of Waterloo, CA)

Highly optimized software libraries exit for multiplying matrices modulo word size primes. By using a recursive reduction all the standard problems can be solved in about the same time as matrix multiplication: rank, inverse, determinant, nullspace, linear solving. Implementations are now available in numerous software libraries as well as becoming standard in computer algebra systems.

Recently, nearly optimal reductions to matrix multiplication have been discovered for problems over integer matrices such as determinant and linear system solving. Integer matrices are more challenging to deal with because of the growth in bitlength of the integers in the output.

In this talk I will discuss the optimized implementation of an algorithm for solving linear systems over the integers.

Keywords: Integer matrices, linear system solving, implementation

Notes on computing minimal approximant bases

Arne Storjohann (University of Waterloo, CA)

We show how to transform the problem of computing solutions to a classical Hermite Pade approximation problem for an input vector of dimension $m \times 1$, arbitrary degree constraints $(n_1, n_2, \ldots, n_m)$, and order $N := (n_1 + 1) + \cdots + (n_m + 1) - 1$, to that of computing a minimal approximant basis for a matrix of dimension $O(m) \times O(m)$, uniform degree constraint $\Theta(N/m)$, and order $\Theta(N/m)$.

Keywords: Hermite Pade approximation, minimal approximant bases

Extended Abstract: http://drops.dagstuhl.de/opus/volltexte/2006/776

Two Families of Algorithms for Symbolic Polynomials

Stephen Watt (University of Western Ontario, CA)

We wish to work with polynomials where the exponents are not known in advance, such as $x^{2n} - 1$. There are various operations we will want to be able to do, such as squaring the value to get $x^{4n} - 2x^{2n} + 1$, or differentiating it to get $2nx^{2n-1}$. Expressions of this sort arise frequently in practice, for example in the analysis of algorithms, and it is very difficult to work with them effectively in current computer algebra systems.

We consider the case where multivariate polynomials can have exponents which are themselves integer-valued multivariate polynomials, and we present

algorithms to compute their GCD and factorization. The algorithms fall into two families: algebraic extension methods and interpolation methods.

The first family of algorithms uses the algebraic independence of x, x^n, x^{n^2}, x^{nm}, etc, to solve related problems with more indeterminates.

Some subtlety is needed to avoid problems with fixed divisors of the exponent polynomials. The second family of algorithms uses evaluation and interpolation of the exponent polynomials. While these methods can run into unlucky evaluation points, in many cases they can be more appealing. Additionally, we also treat the case of symbolic exponents on rational coefficients (e.g. $4^{n^2+n} - 81$) and show how to avoid integer factorization.

Keywords: Computer algebra, symbolic computation, factorization, gcd, symbolic exponents

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2006/793

Pivot-Free Block Matrix Inversion

Stephen Watt (University of Western Ontario, CA)

We present a pivot-free deterministic algorithm for the inversion of block matrices. The method is based on the Moore-Penrose inverse and is applicable over certain general classes of rings. This improves on previous methods that required at least one invertible on-diagonal block, and that otherwise required row- or column-based pivoting, disrupting the block structure. Our method is applicable to any invertible matrix and does not require any particular blocks to invertible. This is achieved at the cost of two additional specialized matrix multiplications and, in some cases, requires the inversion to be performed in an extended ring.

Keywords: Linear algebra, block matrices, matrix inverse

Extended Abstract: http://drops.dagstuhl.de/opus/volltexte/2006/780

See also: Proc. 8th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing, 26-29 September 2006, Timisoara, Romania

Approximate Greatest Common Divisors of Polynomials

Lihong Zhi (MMRC - Beijing, PRC)

We consider the problem of computing minimal real or complex deformations to the coefficients in a list of relatively prime real or complex multivariate polynomials such that the deformed polynomials have a greatest common divisor (GCD) of at least a given degree k.

In addition, we restrict the deformed coefficients by a given set of linear constraints, thus introducing the linearly constrained approximate GCD problem. We present an algorithm based on a version of the structured total least norm (STLN) method and demonstrate on a diverse set of benchmark polynomials that the algorithm in practice computes globally minimal approximations. As an application of the linearly constrained approximate GCD problem we present an STLN-based method that computes a real or complex polynomial the nearest real or complex polynomial that has a root of multiplicity at least k. We demonstrate that the algorithm in practice computes on the benchmark polynomials given in the literature the known globally optimal nearest singular polynomials. Our algorithms can handle, via randomized preconditioning, the difficult case when the nearest solution to a list of real input polynomials actually has non-real complex coefficients.

Keywords: Multivariate polynomial, gcd, approximate polynomial gcd, singular polynomial, approximate multiple root, linear constraint, symbolic and numeric hybrid method

Joint work of: Kaltofen, Erich; Yang, Zhengfeng; Zhi, Lihong

GNU TeXmacs

Joris van der Hoeven (Université Paris Sud, F)

GNU TeXmacs is a free scientific editing platform with special features for mathematicians.

The editor can be used to produce documents with a professional typesetting quality (better than TeX/LaTeX) via a user-friendly front-end. The editor can be used as a front-end to several computer algebra systems and includes a lot of additional facilities, like a presentation mode, a technical picture editor, a typed linking tool, etc.

The editor can be extended by users in several ways: using style files, plug-ins or via the Scheme extension language. Converters exist for LaTeX, Xhtml and MathML.

Keywords: Scientific text editor, Mathematics, Computer algebra system, Front-end

Extended Abstract: http://drops.dagstuhl.de/opus/volltexte/2006/767

Full Paper:
http://www.texmacs.org