Mathematics of Computer Algebra and Analysis
Mathématiques de l'algèbre et de l'analyse computationels
(Org: **Keith Geddes**, **Mark Giesbrecht**, **George Labahn** and/et **Arne Storjohann** (Waterloo))

JACQUES CARETTE, McMaster University, Hamilton, Canada
Functors, CPS and monads, or how to generate efficient algebraic code from abstract designs

Using monads and Ocaml's advanced module system in a generative context, it is possible to totally eliminate the overhead of abstraction. This lets one use extreme forms of *information hiding* at no run-time cost. Furthermore the typed nature of the generative context provide static guarantees about the generated code. The various aspects of the algorithms can be made completely orthogonal and compositional, even in the presence of name-generation for temporaries and other bindings as well as "interleaving" of aspects. We also show how to encode some domain-specific knowledge so that "clearly wrong" compositions can be statically rejected by the compiler. All our examples are drawn from numerical and symbolic linear algebra (Gaussian Elimination, LU Decomposition, *etc.*).

Joint work with Oleg Kiselyov.

FRED CHAPMAN, Waterloo
Hybrid Symbolic-Numeric Integration in Multiple Dimensions via Tensor Product Series

We present a new hybrid symbolic-numeric method for the fast and accurate evaluation of definite integrals in multiple dimensions. This method is well-suited for two classes of problems:

(1) analytic integrands over general regions in two dimensions, and

(2) families of analytic integrands with special algebraic structure over hyperrectangular regions in higher dimensions.

The algebraic theory of multivariate interpolation via natural tensor product series was developed in the doctoral thesis by Chapman, who named this broad new scheme of bilinear series expansions "Geddes series" in honour of his thesis supervisor. This talk describes an efficient adaptive algorithm for generating bilinear series of Geddes–Newton type and explores applications of this algorithm to multiple integration. We will present test results demonstrating that our new adaptive integration algorithm is effective both in high dimensions and with high accuracy. For example, Carvajal's Maple implementation of our algorithm has successfully computed nontrivial integrals with hundreds of dimensions to 10-digit accuracy, each in under 3 minutes on a desktop computer.

Current numerical multiple integration methods either become very slow or yield only low accuracy in high dimensions, due to the necessity to sample the integrand at a very large number of points. Our approach overcomes this difficulty by using a Geddes–Newton series with a modest number of terms to construct an accurate tensor-product approximation of the integrand. The partial separation of variables achieved in this way reduces the original integral to a manageable bilinear combination of integrals of essentially half the original dimension. We continue halving the dimensions recursively until obtaining one-dimensional integrals, which are then computed by standard numeric or symbolic techniques.

This talk presents joint research with Orlando Carvajal and Keith Geddes.

JÜRGEN GERHARD, Maplesoft Inc., Waterloo, Ontario
Recent developments in rational summation

The talk discusses recent algorithmic developments for the problem of rational summation: Given a univariate rational function $g(x)$, determine whether there exists a rational antidifference $f(x)$, such that $f(x+1) - f(x) = g(x)$, and the more general problem of extracting a maximal rationally summable part from $g(x)$. The emphasis is on improving the efficiency of rational summation algorithms. The techniques used are modular methods and shiftless decomposition: Modular methods lead to faster algorithms for all inputs. Shiftless decomposition reduces the number of worst case inputs with exponential running time behaviour.

This is joint work with Mark Giesbrecht, Arne Storjohann, and Eugene Zima.

PASCAL GIORGI, Laboratoire LIP, ENSL, Lyon, France, and Waterloo
On the use of polynomial matrix approximant in the block Wiedemann algorithm

The resolution of a linear system is one of the most studied problems in linear algebra. It is well known that by using Gaussian elimination one can solve a linear system with a cubic time complexity. However, when the matrix is sparse (only a few elements are non-zero) or structured (Toeplitz, ...) the use of iterative methods such as Krylov/Lanczos allows better time and space complexity. Nevertheless, these methods are probabilistic and the chances of success rely on randomness properties of the computation domain. In order to achieve better probability of success one can use blocking technique. One of the main concern in the Wiedemann algorithm is to compute the minimal generating polynomial of matrix. When we switch to the block Wiedemann algorithm the main concern becomes the computation of a matrix minimal generating polynomial. The use of the block Wiedemann algorithm leads us to deal with matrix polynomial operations instead of scalar polynomial operations.

In order to provide fast computation in the block Wiedemann algorithm, we use some recent reduction to matrix multiplication in polynomial matrix computation. In particular, we rely on polynomial matrix approximant (Pade Approximant) through minimal basis computation in order to obtain the block minimal polynomial of a matrix. In practice, the minimal basis allows us to use matrix multiplication and so to benefit from implementation based on hybrid numerical/symbolic computation. We present our work on the reduction of minimal basis computation to matrix multiplication and we present an adaptation of our algorithm to handle the computation of block minimal polynomial. We also shows some performances obtained within the Linbox library (`http://www.linalg.org`) for the block Wiedemann algorithm using minimal basis computation.

ILIAS KOTSIREAS, Wilfred Laurier University
Astronomical Bounds for finding inequivalent Hadamard Matrices

Hadamard matrices arise in Combinatorics and have a wide range of applications in Statistics, Coding Theory, Cryptography, Telecommunications and many other areas. For each permissible order (a multiple of 4) of Hadamard matrices there is only a finite number of Hadamard matrices of this order. The set of Hadamard matrices of a specific order is equipped with an equivalence relation and the representatives of the equivalence classes with respect to this relation are called inequivalent Hadamard matrices. The graph isomorphism criterion is a necessary and sufficient condition to test whether two given Hadamard matrices are inequivalent. The 4-profile criterion is a necessary, but not sufficient, condition to test whether two given Hadamard matrices are inequivalent. Both the graph isomorphism and the 4-profile criteria have been implemented in the Computer Algebra System Magma.

Using these and other criteria, various authors have established constructive lower bounds (of the order of a few hundreds) for the number of inequivalent matrices of many permissible orders. In this work we use the doubling construction for Hadamard matrices, in conjunction with the symmetric group (group of permutations) S_n, to construct millions on inequivalent Hadamard matrices of orders which are multiples of 8. Thus we establish constructively new lower bounds for many such orders, up to 100, by starting with some small initial sets of inequivalent, or equivalent, Hadamard matrices.

Joint work with G. Georgiou and C. Koukouvinos.

JOHN MAY, North Carolina State University
Solving Problems in Approximate Polynomial Algebra via SVD methods

Many problems in polynomial algebra can be formulated for polynomials which are given with inexact coefficients. When considered numerically many of these algebraic problems are ill-posed—small perturbations to coefficients lead to large changes in the answer. For example, very small random changes to a factorizatable multivariate polynomial typically result in an irreducible polynomial. Other examples of problems of this type are polynomial division, GCD computation and polynomial decomposition.

It is possible to find reasonable partial solutions for a number of problems in approximate algebra by linearizing and using singular value decomposition (SVD) methods. If the problem can be restated as a problem of computing null vectors of a given matrix, then we typically can do two things: first, given a polynomial without a given property, we can find a lower bound on the distance to the nearest polynomial with the property and second, we can compute a "nearby" polynomial which has the given property, though we cannot in general find the nearest such polynomial.

In this talk we will discuss the general technique, as well as the specific details for the GCD, and factorization problems.

MARC MORENO MAZA, University of Western Ontario
Equiprojectable decomposition of zero-dimensional varieties

Equidimensional decompositions of algebraic varieties, such as triangular decompositions, are used for many situations. However, even a zero-dimensional variety V may have several triangular decompositions. The *a priori* canonical choice, namely the irreducible decomposition of V, does not have good specialization properties.

Given a variable ordering, we introduce the equiprojectable decomposition of V. This is a canonical equidimensional decomposition of V with good computational properties. We show how to compute the equiprojectable decomposition of V from any triangular decomposition or primitive element representation of V.

Given a zero-dimensional polynomial system F over Q, we show that there exists an integer A whose height is softly in the order of the square of the Bezout number of F, such that any prime number not dividing A is a good prime for specializing the equiprojectable decomposition of F.

Using Hensel lifting techniques, we deduce a modular algorithm for computing the equiprojectable decomposition of zero-dimensional varieties over Q. We have realized a preliminary implementation with the Triade library developed in Maple by F. Lemaire. Our theoretical results are comforted by these experiments.

Joint work with Xavier Dahan, Eric Schost, Wenyuan Wu and Yuzhen Xie.

THOMAS WOLF, Brock University, Ontario
Partial and complete linearization of PDEs based on conservation laws

In the talk a method is described that, based on infinite parameter conservation laws, factors linear differential operators out of nonlinear partial differential equations (PDEs) or out of differential consequences of nonlinear PDEs. This includes a complete linearization to an equivalent linear PDE (-system) if that is possible. Comments are made concerning the computation of infinite parameter conservation with the computer algebra package ConLaw.

YANG ZHANG, Brandon University
Computing Valuation Popov Forms

Popov forms and weak Popov forms of matrices over noncommutative valuation domains are defined and discussed. Two new algorithms to construct these Popov forms are given, along with a description of some of their applications.

This is joint work with Mark Giesbrecht and George Labahn.