MOCAA Project Meeting
Program

Room ICT 516, Information and Communication Technology Building, University of Calgary, Wed. May 11, 2005

8:30–9:15 Breakfast Reception, ICT 516

9:15 Opening remarks
9:20 Vahid Dabbaghian-Abdoly, Computing representations of the finite symplectic group Sp(4,q)
9:40 George Labahn, Symbolic Integration of Jacobi Elliptic Functions in Maple
10:00 John May, General Strategies for Problems in Approximate Algebra via STLS

10:20–10:50 Break

10:50 Ashley Pitcher, A numerical method for finding the roots of exponential polynomials
11:10 Yuzhen Xie, Lifting Techniques for Triangular Decompositions
11:30 Cosmin Oancea, Domains and Expressions: An interface between two approaches to computer algebra
11:50 Howard Cheng, Output-sensitive Modular Algorithms for Row Reduction of Matrices of Ore Polynomials

12:10–2:00 Lunch

2:00 Mike Monagan, Algorithms for the Non-monic case of the Sparse Modular GCD Algorithm
2:20 Sara Khodadad, Fast Rational Function Reconstruction
2:40 Marc Moreno Maza, On the Complexity of the D5 Principle
3:00 Simon Lo, Computing Characteristic Polynomials over Z

3:20-3:50 Break

3:50 Mhenni Benghorbal, A Unified Formula for Integer and Fractional Order Symbolic: Derivatives and Integrals of The Power-Exponential Class.
4:10 Bradford Hovinen, Analyzing blocked iterative linear system solvers
4:30 Ron Ferguson, Binary searches - the merit factor problem
4:50 Mahdad Khatirinejad, Title: A Graph Theory Package for Maple

Abstracts

Title: Computing representations of the finite symplectic group Sp(4,q)
Speaker: Vahid Dabbaghian-Abdoly
Abstract:

Let G be a finite group and c be an irreducible character of G. An efficient and simple method for computing representations of finite groups is applicable whenever G has a subgroup H such that c_H, the restriction of c on H, has a linear constituent with multiplicity one. In this paper we show that, when $G = Sp(4,q)$ where q is a power of a prime p and H is a Sylow p-subgroup of G, then c_H has a linear constituent with multiplicity one for every irreducible character c (with one exception). We also find a p-subgroup has this property for the exceptional character.

Title: Symbolic Integration of Jacobi Elliptic Functions in Maple
Speaker: George Labahn
Joint work with Thomas Humphries
Abstract:

In this talk we will describe the design and implementation of procedures for computing indefinite integrals of Jacobi Elliptic Functions in the computer algebra system Maple. The routines take advantage of Maple's ability to extend the *int* command and are careful to return answers having a minimal size whenever possible.

General Strategies for Problems in Approximate Algebra via STLS
Speaker: John May

Title: A numerical method for finding the roots of exponential polynomials
Speaker: Ashley B. Pitcher
Authors: Ashley B. Pitcher and Robert M. Corless
Abstract:

Exponential polynomials are sums of terms of the form$C * x^{\alpha} * y^{\beta}$ where $x = e^y$, alpha is a rational number, beta is a nonnegative integer, and C is a complex constant with rational coefficients. They arise in a number of applications, especially in areas involving delay differential equations. A new numerical homotopy (continuation) method has been developed for finding the roots of exponential polynomials and has been implemented in Maple. The concept and implementation of this method will be discussed. In particular, a system of delay differential equations arising in HIV modeling of CD4+ T-cells will be investigated using this newly developed numerical procedure.

Title: Lifting Techniques for Triangular Decompositions
Speaker: Yuzhen Xie
Authors: Xavier Dahan, Marc Moreno Maza, Eric Schost, Wenyuan Wu, Yuzhen Xie
Abstract:

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 which 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.

Title: Domains and Expressions: An interface between two approaches to computer algebra
Speaker: Cosmin Oancea
Authors: Cosmin Oancea and Stephen M. Watt
Abstract:
We described a method to use compiled, strongly typed Aldor domains in the interpreted, expression-oriented Maple environment. This represents a non-traditional approach to structuring computer algebra software: using an efficient, compiled language, designed for writing large complex mathematical libraries together with a top-level system based on user-interface priorities and ease of scripting.

Since the computational models of Maple and Aldor differ significantly, run-time code must implement a non-trivial semantic correspondence. This paper examines what is required to use Aldor libraries to extend Maple in an effective and natural way.

The Aldor functions run tightly coupled to the Maple environment, able to directly and efficiently manipulate Maple data objects. We call the overall system Alma.

Title: Output-sensitive Modular Algorithms for Row Reduction of Matrices of Ore Polynomials
Speaker: Howard Cheng
Joint work with George Labahn
Abstract:
We give an output-sensitive modular algorithm to perform row reduction of a matrix of Ore polynomials with coefficients in $Z[t]$. Both the transformation matrix and the transformed matrix are computed. The algorithm can be used for finding the rank and left nullspace of such matrices. In the special case of shift polynomials, we obtain algorithms for computing a weak Popov form and for computing a greatest common right divisor (GCRD) and a least common left multiple (LCLM) of matrices of shift polynomials. Our algorithms improve on existing fraction-free algorithms and can be viewed as generalizations of the work of Li and Nemes on GCRDs and LCLMs of Ore polynomials. We define lucky homomorphisms, determine the appropriate normalization, as well as bound the number of homomorphic images required. Our algorithm is output-sensitive, such that the number of homomorphic images required depends on the size of the output. Furthermore, there is no need to verify the result by trial division or multiplication. When our algorithm is used to compute a GCRD and a LCLM of shift polynomials, we obtain a new output-sensitive modular algorithm.

Title: Algorithms for the Non-monic case of the Sparse Modular GCD Algorithm
Speaker: Michael Monagan
Authors: Jennifer de Kleine, Michael Monagan, and Allan Wittkopf
Abstract:
Let $G = (4y^2 + 2z)x^2 + (10y^2 + 6z)$ be the greatest common divisor (GCD) of two polynomials A, B in

Z[x,y,z]. Because G is not monic in the main variable x, the sparse modular GCD algorithm of Richard Zippel cannot be applied directly as one is unable to scale univariate images of G in x consistently. We call this the normalization problem.

We present two new sparse modular GCD algorithms which solve this problem without requiring any factorizations. The first, LINZIP, a modification of Zippel's algorithm, treats the scaling factors as unknowns to be solved for. This leads to a structured coupled linear system for which an efficient solution is still possible. The second algorithm, RATZIP, reconstructs the monic GCD,

$$G/lc[x](G) = x^2 + (5y^2 + 3z)/(2y^2 + z),$$

from univariate images using a sparse variable-at-a-time rational function interpolation algorithm.

We present some "not so great" timing results comparing LINZIP with Maple's implementation of the EEZ-GCD algorithm of Wang. We have also implemented both algorithms in the "recden" data structure so that we can run the algorithm over number fields and finite fields as well as the integers. We will present some preliminary results comparing these two implementations of the algorithms. The bottleneck of the sparse modular GCD algorithms is the large number of evaluations of the inputs that need to be done. To reduce this we are working on an improvement in which we project down to bivariate images instead of univariate images.

Title: Fast Rational Function Reconstruction
Speaker: Sara Khodadad
Abstract:

Let F be a field, m, u in F[x] with n = deg m ¿ deg u ¿ 0, we want to find a rational function r/t in F(x) where r/t = u mod m. One way to do this is to use maximal quotient rational reconstruction which does not require degree bounds and uses one or two more points than the minimum necessary to reconstruct r/t. We have implemented the algorithm for F[x] = Zp[x], p a prime. To speed up the reconstruction algorithm, our implementation uses Karatsuba's algorithm for multiplication in Zp[x] and a fast extended Euclidean algorithm. We have modified Brown's modular GCD algorithm to use the maximal quotient algorithm. The modification reduces the number of primes and evaluation points needed by the algorithm.

Title: On the Complexity of the D5 Principle
Speaker: Marc Moreno Maza
Authors: Xavier Dahan, Marc Moreno Maza, Eric Schost, Wenyuan Wu, Yuzhen Xie
Abstract:

The standard approach for computing with an algebraic number is through the data of its irreducible minimal polynomial over some base field K. However, many algebraic numbers may appear when solving a polynomial system; applying them this approach requires possibly costly factorization algorithms. Della Dora, Dicrescenzo and Duval introduced "dynamic evaluation" techniques (also termed "D5 principle") as a means to compute with algebraic numbers, while avoiding factorization. Roughly speaking, this approach leads one to compute over direct products of field extensions of K, instead of only field extensions. In this talk, we address complexity issues for computations in such structures.

Title: Computing Characteristic Polynomials over Z
Speaker: Simon Lo
Joint work with Michael Monagan and Allan Wittkopf.
Abstract:

We present a modular algorithm for computing the characteristic polynomial of an integer matrix. The computation modulo each prime is done using the Hessenberg algorithm. It is implemented in C, and the rest of the algorithm is implemented in Maple. We also compare implementations for arithmetic modulo primes using 32-bit integers, 64-bit integers, and double precision floats. Using floats would give the best results.

———————————————————————————-

Title: A Unified Formula for Integer and Fractional Order Symbolic: Derivatives and Integrals of The Power-Exponential Class.
Speaker: Mhenni Benghorbal.
Abstract:

We give algorithms for finding integer and arbitrary order symbolic derivatives and integrals formulas of the power-exponential class order symbolic The theorems give a systematic way for deriving the nth derivatives and integrals formulas. The formulas, in general, are in terms of some special functions. A subclass of the power-exponential class has turned out to have the property that its integer order symbolic derivatives and integrals belongs to the same class. A theorem that gives a unified formula for integer and fractional order symbolic derivatives and integrals, in terms of the H-function, has been given.

———————————————————————————-

Title: Analyzing blocked iterative linear system solvers
Speaker: Bradford Hovinen
Abstract:

Blocked iterative algorithms for sampling from the nullspace of a matrix are an important part of index calculus techniques for solving discrete logarithm problems. Such algorithms are randomized, and it is useful to understand the probability of success on arbitrary input matrices. The study of randomly-generated linearly recurrent sequences and their associated block Hankel matrices has proved highly successful in obtaining very good bounds on these probabilities. This talk will discuss some of the theory and key results in this area.

——————————————————————————

Title: The Merit Factor Problem for Binary Sequences
Speaker: Ron Ferguson
Joint work with Peter Borwein and Josh Knauer
Abstract:

Two problem which have received considerable attention from both mathematicians and communications engineers regarding binary sequences are: 1. Do there exist Barker sequences of length ¿ 13? 2. Is the merit factor bounded? I will discuss both theoretical and algorithmic approaches to these problems, including our latest results obtained using methods of stochastic optimization.

———————————————————————————-

Title: A Graph Theory Package for Maple
Speaker: Mahdad Khatirinejad
Participants: J. Farr, S. Khodadad, M. Khatirinejad, M. Monagan
Abstract:

The Maple company asked us to develop a new graph theory package to replace the networks package. The package we are developing is intended for teaching and research usage, and expected to treat graphs of up to 1000 vertices in a reasonable time. Most of the standard operations for graphs, including a planarity test and chromatic number, are available in this package. The package also includes a drawing algorithm. We will demonstrate what we have done so far.