BIRS Workshop
Name of Workshop
Date of Workshop

MEALS

Breakfast (Continental): 7:00 - 9:00 am, 2nd floor lounge, Corbett Hall, Sunday - Thursday
*Lunch (Buffet): 11:30 am - 1:30 pm, Donald Cameron Hall, Sunday - Thursday
*Dinner (Buffet): 5:30 - 7:30 pm, Donald Cameron Hall, Saturday - Wednesday
Coffee Breaks: As per daily schedule, 2nd floor lounge, Corbett Hall
***Please remember to scan your meal card at the host/hostess station in the dining room for each lunch and dinner.**

MEETING ROOMS

All lectures are held in the main lecture hall, Max Bell 159. *Please note that the meeting space designated for BIRS is the lower level of Max Bell, Rooms 155-159. Please respect that all other space has been contracted to other Banff Centre guests, including any Food and Beverage in those areas.*

SCHEDULE

	Saturday	Sunday	Monday	Tuesday	Wednesday	Thursday
7:00-9:00	X	Continental Breakfast, 2nd floor lounge, Corbett Hall				
9:00-9:45	X	J. Demmel	P. Giorgi	L. Zhi	E. Hubert	SW discuss. II
9:45-10:30	X	E. Schost	F. Rouillier	H. Kai	F.-O. Schreyer	
10:30-11:00	X	Coffee Break, 2nd floor lounge, Corbett Hall				
11:00-11:45	X	M. van Hoeij	J.-G. Dumas	W.-S. Lee	G.-M. Greuel	X
11:45-12:00	X	X	X	Group Photo[1]	X	X
11:30-13:30	X	Buffet Lunch, Donald Cameron Hall				
13:00-14:00	X	Guided Tour[2]	X	free afternoon	X	X
14:30-15:15	X	von zur Gathen	D. Lazard	free afternoon	A. Steel	X
15:15-15:45	X	Coffee Break, 2nd floor lounge, Corbett Hall (except Tues.)				X
15:45-16:30	X	A. Sommese	SW discuss. I	free afternoon	M. Monagan	X
17:30-19:30	Buffet Dinner, Donald Cameron Hall					X

[1] A group photo will be taken on Tuesday at 11:45 am, directly after the last lecture of the morning. Please meet on the front steps of Corbett Hall.

[2] A free guided tour of The Banff Centre is offered to all participants and their guests on Sunday starting at 1:00 pm. The tour takes approximately 1 hour. Please meet in the 2nd floor lounge in Corbett Hall.

BIRS Workshop
Name of Workshop
Date of Workshop

ABSTRACTS
(in alphabetic order by speaker surname)

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 $\cdot$.

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.

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.

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 will 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 $n^{2.5}$.

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 will be given for the algorithm in "Factoring polynomials and the knapsack problem" (JNT 2002). A complexity result will also be given for factoring bivariate polynomials over finite fields. Specifically, to solve the combinatorial problem, it suffices to Hensel lift to accuracy min(p,n)*(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.

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 will 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.

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 will focus on sparse polynomials. I will discuss black box sparse interpolation and explore sparse representations of polynomials. The interplay between these problems and recent development will also be addressed.

Speaker: **Michael Monagan** (Simon Fraser University)
Title: *RECDEN, A data structure for multivariate polynomials over number fields*

Speaker: **Fabrice Rouillier** (INRIA France)

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;y)=0 with algebraic parameters as a family X → 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 will be given.

Speaker: **Allan Steel** (University of Syndey)
Title: *Linear and Polynomial Algebra in Magma: A Detailed Overview*
Abstract: I will 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 will be highlighted, particularly in the goal of practical implementations of asymptotically-fast algorithms.

Speaker: **Stephen Watt** (University of Western Ontario)

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.