Gröbner Bases, Resultants and Linear Algebra

September 3 – 6, 2013

Research Institute for Symbolic Computation
Hagenberg, Austria

	Tuesday	Wednesday
9:00 – 9.30	Registration	
9:30 – 10:30	**Bruno Buchberger** Opening Talk	**Christian Eder** Introduction to F4, F5 Algorithms
10.30 – 11:00	***coffee break***	***coffee break***
11:00 – 12:00	**Elias Tsigaridas** Polynomial System Solving and Sparse Elimination: from Mixed Volume to Separation Bounds I	**Elias Tsigaridas** Polynomial System Solving and Sparse Elimination: from Mixed Volume to Separation Bounds II
12:00 – 14:30	***lunch***	***lunch***
14:30 – 15:00	**Manuel Kauers** Solving Linear Systems with Polynomial Coefficients in Sage	**Christian Eder** Signature-Based Gröbner Basis Algorithms
15:00 – 15:30	**Madalina Erascu** Synthesis of Optimal Numerical Algorithms by Real Quantifier Elimination	**Pierre-Jean Spaenlehauer** Complexity Bounds for Computing Critical Points with Gröbner Bases
15:30 – 16:00	***coffee break***	***coffee break***
16:00 – 16:30	**Matteo Gallet** Newton Polyhedra under Monomial Maps	**Milan Stehlik** Applications of Gröbner Bases In Statistics and Stochastics
16:30 – 17:00	**Ya-lun Tsai** Real Root Counting for Parametric Polynomial Systems and Applications	**Natalia Dück** Universal Gröbner Bases for a Binomial Ideal Associated to a Linear Code
17:00-17:30	**Manuela Wiesinger-Widi** Gröbner Bases Computation by Generalized Sylvester Matrices	**Christoph Fürst** Relative Gröbner Bases for Delta-Sigma-Modules
17:30 and on	*Discussion and open problems*	*Discussion and open problems*

	Thursday	Friday
9:30 – 10:30	**Laurent Busé** Introduction to the Classical Multivariate Resultant	**Laurent Busé** Linearization of Polynomial Systems via Fitting Ideals
10.30 – 11:00	***coffee break***	***coffee break***
11:00 – 12:00	**Carlos D'Andrea** Sparse Resultants	**Carlos D'Andrea** Sparse Resultants via Multiprojective Elimination
12:00 – 14:30	***lunch***	***lunch***
14:30 – 15:00	**Josef Schicho** Examples of Algebraic Systems of Equations Arising in Kinematics	**Christoph Koutschan** A Glimpse of Noncom-mutative Gröbner Bases
15:00 – 15:30	**Angelos Mantzaflaris** Computing Exact Matrices for Multihomogeneous Resultants	**Anders Nedergaard Jensen** Gröbner Fans and Tropical Resultants
15:30 – 16:00	**Adrien Poteaux** On the Complexity of Computations Modulo Zero-dimensional Triangular Sets	**Kinji Kimura** Computing the General Discriminant Formula of Degree 17
16:00 – 16:30	*Hike and dinner*	***coffee break***
16:30 and on	*Hike and dinner*	*Discussion and open problems*

Abstracts

Opening Talk
Bruno Buchberger

Introduction to the Classical Multivariate Resultant
Laurent Busé

Syllabus

- Definition the resultant of n homogeneous polynomials in n variables
- Geometric and algebraic points of view
- Main properties of resultants (multi-degree, multiplicativity, Bezout, ...)
- Matrix formulations (matrices of inertia forms essentially)

Linearization of Polynomial Systems via Fitting Ideals
Laurent Busé

Syllabus

- Elimination theorem, elimination ideals and annihilators
- The classical resultant revisited by means of the Koszul complex
- Application to the implicitization problem

Sparse Resultants
Carlos D'Andrea

Syllabus

- Monomial maps and toric varieties
- Definition of sparse resultants and basic properties
- Matrix formulations

Sparse Resultants via Multiprojective Elimination
Carlos D'Andrea

Syllabus

- Sparse resultants as multiprojective resultants
- Main properties: degree, intersection, Poisson formula
- Polynomial system solving via resultants: u-resultants and hidden variables

Universal Gröbner Bases for a Binomial Ideal Associated to a Linear Code

Natalia Dück

Digital data are exposed to errors when transmitted through a noisy channel. But as receiving correct data is indespensable in many applications, error-correcting codes are employed to tackle this problem. By adding redundancy to the messages, errors can be detected and corrected. Since the late 1940's the study of such codes is an ongoing and important task.

Gröbner bases, on the other hand, are a powerful tool that has originated from commutative algebra providing a uniform approach to grasp a wide range of problems such as solving algebraic systems of equations, ideal membership, and effective computation in residue class rings modulo polynomial ideals.

Both concepts can be linked by associating a linear code over a prime with a binomial ideal given as the sum of a toric ideal and a non-prime ideal which is termed the code ideal. In this way, several concepts from the rich theory of toric ideals can be translated into the setting of code ideals.

In this talk, results concerning the Gröbner basis structure of code ideals will be presented. This is important because Gröbner bases are the essential tool for utilizing ideals in computer algebra systems.

In particular, it will be shown that for binary codes the universal Gröbner basis consists of all binomials associated to codewords whose Hamming weight satisfies the Singleton bound and a particular rank condition. For the general case it will be shown that after some concepts in connection with toric ideals have been adapted the same techniques as for toric ideals can be applied in order to compute the universal Gröbner basis from the Graver basis.

Introduction to F4 and F5 Algorithms

Christian Eder

In this talk we introduce two new ideas for computing Groebner bases: F4 is an algorithm that uses linear algebra instead of usual polynomial reduction. We show how Gaussian Elimination of the Macaulay matrix coincides with doing several reduction steps at once. Moreover, reusing already computed results leads to further optimizations. F5, on the other hand, is the origin of all known signature-based Groebner basis algorithms. We show how F5 uses new criteria, based on these signatures, to discard useless steps during the computation of a Groebner basis. In this talk we present an easy variant of F5, the Matrix F5 Algorithm. We show that for the important class of regular sequences F5 computes no zero reduction at all.

Signature-Based Gröbner Basis Algorithms

Christian Eder

Over the last decade a new branch in Gröbner Basis theory evolved, so called signature-based attempts. Starting with Faugčre's F5 Algorithm, nowadays the number of variants seems to be vast. In this talk we present the general ideas of signature-based algorithms and show how all the efficient implementations can be deduced rather easily. Furthermore, with this attempt we are able to give an overview of current developments in this area.

Synthesis of Optimal Numerical Algorithms by Real Quantifier Elimination (Case Study: Square Root Computation)

Mădălina Eraşcu and Hoon Hong

(Sub)resultant computation is the main ingredient of quantifier elimination based on cylindrical algebraic decomposition. In this talk, we present an application of real quantifier elimination to the synthesis of optimal numerical algorithms. More precisely, we report a case study on a simple but fundamental numerical problem, namely square root computation: given a real number x and the error bound ε, find a real interval such that it contains $\sqrt{x}$ and its width is less than ε. We synthesized, semi-automatically, optimal algorithms, which are better than the well known Secant-Newton algorithm. The synthesis could have been done, in principle, as a single quantifier elimination process. However, it was infeasible for the current algorithms and the state-the-art software systems specialized on quantifier elimination. Hence, we carefully divided it into smaller quantifier elimination subproblems. After eliminating manually some of the quantifiers from these subproblems, by exploiting their structure, we were able to solve the synthesis problem using the quantifier elimination software QEPCAD-B and Reduce in Mathematica.

Relative Gröbner Bases for Δ-Σ-Modules

Christoph Fürst

Relative Gröbner bases are an attempt to lift Gröbner basis theory to the domain of an operator algebra. Going beyond the work of Ritt/Kolchin, we introduce difference-differential operators, and develop an according Gröbner basis theory. The practical value is shown by concrete applications, and by answering questions about dimension in difference-differential modules. Further, some open questions are posed, that are part of the authors Ph.D. research.

Newton Polyhedra under Monomial Maps

Matteo Gallet

Given an n-times-n integer-valued matrix A, this determines a morphism ϕ from the algebraic torus $(C^*)^n$ to itself, sending $t = (t_1, ..., t_n)$ to $(t_1^A, ..., t_n^A)$, where A_i are the columns of A. If X is a hypersurface in the torus, namely its ideal is principal, and generated by a Laurent polynomial f, then we can associate to it the Newton polyhedron P of f. We would like to investigate the relation between P and P', the Newton polyhedron of f', the equation of the Zariski closure of $\phi(X)$, if possible in terms of the matrix A. This might help determining the Newton polyhedron of rational surfaces arising from very particular parametrizations.

Gröbner Fans and Tropical Resultants

Anders Nedergaard Jensen

The Gröbner fan of a polynomial ideal was defined by Mora and Robbiano in 1988. Its maximal polyhedral cones are sets of weight-induced term orders for which Buchberger's algorithm produces the same reduced Gröbner basis. Gröbner fans can be computed by applying Gröbner walk techniques. In the field of tropical algebraic geometry Gröbner fans have received much attention recently. This is because one of the most important objects in tropical geometry, the tropical variety of an ideal, is a subfan of the Gröbner fan of the ideal. In this talk we define the tropical resultant variety of a set of Newton polytopes and present a theorem which says that the tropical resultant variety is the tropicalization of the (non-tropical) sparse mixed resultant variety. As a consequence we get improved polyhedral algorithms for computing the Newton polytope of the resultant without computing the resultant polynomial itself. Our algorithms have been implemented in the software Gfan.

This is joint work with Josephine Yu

Solving Linear Systems with Polynomial Coefficients in Sage

Manuel Kauers

In several algorithms for recurrences and differential equations, the runtime bottleneck is the computation of a nullspace vector for a matrix with polynomial entries. The matrices arising from such algorithms are not generic, but not very structured either. We present a Sage implementation of several algorithms for computing the nullspace of polynomial matrices and say some words on our experience with their respective performance on matrices we are interested in.

Computing the General Discriminant Formula of Degree 17

Kinji Kimura

We define the discriminant,

$$\text{discriminant}(f(x)) = (-1)^{\frac{1}{2}m(m-1)}\frac{1}{a_m}\text{resultant}(f(x), f'(x)),$$

where $f(x)$ is a polynomial of degree m. We try to compute the general discriminant formula for $f(x) = a_{17}x^{17} + a_{16}x^{16} + \cdots + a_0$ of degree 17 by using a modified multivariate Newton interpolation. The algorithm can be also used for the purpose of computing determinants with polynomials and resultants in general case. Our approach is not probabilistic but deterministic. Therefore, our result is clearly world-record in computing general discriminant formulas. As a computing environment, we use a super computer made by Cray Inc. The numbers of terms included in the discriminants are 2, 5, 16, 59, 246, 1103, 5247, 26059, 133881, 706799, 3815311, 20979619, 117178725, 663316190, 3798697446 and 21976689397 for $f(x)$ of degree 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16 and 17, respectively.

A Glimpse of Noncommutative Gröbner Bases

Christoph Koutschan

We give a short introduction to Gröbner bases in noncommutative polynomial rings. While many results and algorithms from the commutative world remain valid (with little changes), there are also some notable differences and surprising phenomena. Some applications in the context of holonomic functions will be mentioned.

Computing Exact Matrices for Multihomogeneous Resultants

Angelos Mantzaflaris

In this talk we present some techniques for deducing matrices that express the resultant of a system of multihomogeneous equations. This particular type of structured systems is among the few cases in which the resultant may have an exact expression as a matrix, without extraneous factors. We would like to identify those systems in the family of multihomogeneous supports that admit a, so called, determinantal formula, and ultimately to compute the resultant matrices and use them for approximating the roots of the system.

On the Complexity of Computations Modulo Zero-dimensional Triangular Sets

Adrien Poteaux

We study the complexity of some fundamental operations for triangular sets in dimension zero. Using Las-Vegas algorithms, we prove that one can perform such operations as change of order, equiprojectable decomposition, or quasi-inverse computation with a cost that is essentially that of modular composition. Over an abstract field, this leads to a subquadratic cost (with respect to the degree of the underlying algebraic set). Over a finite field, in a boolean RAM model, we obtain a quasi-linear running time using Kedlaya and Umans' algorithm for modular composition. Conversely, we also show how to reduce the problem of modular composition to change of order for triangular sets, so that all these problems are essentially equivalent.This is a work done in collaboration with Èric Schost (University of Western Ontario). Our algorithms are implemented in Maple; we present some experimental results.

Examples of Algebraic Systems of Equations Arising in Kinematics

Josef Schicho

We explain an attack of a famous open problem in kinematics, the classification of closed 6R linkages. The question is equivalent to finding the irreducible components of an algebraic set M in R^18. A system of equations is not known, but we can give a definition in terms of elimination theory.

Using bond theory, we can split up the conditions, i.e. we write M as a finite union of algebraic subsets. For each such subset M_r, we give some explicit equations that vanish on M_r. In some cases, we could find all the solution of these equations and show that they define M_r. There are other cases which we could not solve with the techniques available to us; maybe other participants of the workshop would be more lucky.

Complexity Bounds for Computing Critical Points with Gröbner Bases

Pierre-Jean Spaenlehauer

Let $f_1, \ldots, f_p$ and q be multivariate polynomials with rational coefficients. We consider the problem of computing the critical points of q restricted to the variety V associated to $f_1, \ldots, f_p$. Such computations are central in several algorithmic problems in real algebraic geometry and in optimization. These critical points lie in the intersection of V and of a special determinantal variety defined by the vanishing of the maximal minors of a Jacobian matrix. In practice, Gröbner bases algorithms are efficient methods to solve these highly structured systems. We will see how tools from commutative algebra (graded free resolutions of determinantal ideals) and from combinatorics (sets of non-intersecting paths) lead to an analysis of the underlying structure and to an explanation of the efficiency of Gröbner basis techniques for these systems. In particular, for several families of critical point systems, we show complexity bounds for the F4/F5 algorithms which are polynomial in the generic number of complex critical points.

Applications of Gröbner Bases in Statistics and Stochastics

Milan Stehlík

During the talk we will address several important interplays between Gröbner bases and statistics. To illustrate two important examples from statistics, we will discuss testing algebraic hypotheses (Drton et al. 2009) and algebraic structures in optimal design (Pistone et al. 2009). Several open problems will be formulated, mainly related to stochastic analysis and statistics. Also applications in ecological modelling will be provided (see Jordanova et al. 2013).

Real Root Cunting for Parametric Polynomial Systems and Applications

Ya-lun(Allen) Tsai

In this talk, I will present the problems about central configurations and Maxwell's conjecture. The former comes from the study of celestial mechanics and the latter is from the study of point charges. Both problems can be reduced to problems of solving parametric polynomial systems.

Solving here means to count the number of positive roots for all parameters. Using Groebner bases, Hermite quadratic forms, resultants, and subresultant sequences, we overcome some computation and complexity difficulties and successfully solve some problems form the two fields mentioned above.

Polynomial System Solving and Sparse Elimination: from Mixed Volume to Separation Bounds

Elias Tsigaridas

We present an introduction to sparse elimination techniques and mixed volume computation. We show the construction of matrices in sparse elimination and how to use linear algebra tools to compute the roots of polynomial systems. Finally, we use mixed volume and sparse resultants to deduce (exact and approximate) separation bounds for polynomial systems, and we show how to use them in some applications.

Gröbner Bases Computation by Generalized Sylvester Matrices

Manuela Wiesinger

We show how Groebner bases can be computed by triangularizing a Sylvester-like matrix generated from the input basis and give bounds for the size of this matrix for certain ideals.