# Special Session on "Applications of Groebner Bases and Algebraic Computation"

Quoc-Nam Tran (Lamar) & Alexander Levin (CUA), Chairs

June 1, 2011

## 0.1 Andre Platzer, Carnegie Mellon University (CMU), aplatzer@cs.cmu.edu

- **TITLE:** Real Analysis for Complex Systems
- **ABSTRACT:** Formal verification techniques are used routinely in finite-state digital circuits. Theorem proving is also used successfully for infinite-state discrete systems. But many safety-critical computers are actually embedded in physical systems. Hybrid systems model complex physical systems as dynamical systems with interacting discrete transitions and continuous evolutions along differential equations. They arise frequently in many application domains, including aviation, automotive, railway, and robotics. There is a well-understood theory for proving programs. But what about complex physical systems? How can we prove that a hybrid system works as expected, e.g., an aircraft does not crash into another one?

  This talk illustrates the complexities and pitfalls of hybrid systems verification. It describes a theoretical and practical foundation for deductive verification of hybrid systems called differential dynamic logic. The proof calculus for this logic is interesting from a theoretical perspective, because it is a complete axiomatization of hybrid systems relative to differential equations. The approach is of considerable practical interest too. Its implementation in the theorem prover KeYmaera has been used successfully to verify collision avoidance properties in the European Train Control System and air traffic control systems. The number of dimensions and nonlinearities in the hybrid dynamics of these systems is surprisingly tricky such that they are still out of scope for other verification tools.

## 0.2 Takayuki Hibi, Hidefumi Ohsugi, Rikkyo University. hibi@math.sci.osaka-u.ac.jp, ohsugi@rikkyo.ac.jp

- **TITLE:** Toric rings and ideals of nested configurations arising in algebraic statistics.

- **ABSTRACT:** From a viewpoint of algebraic statistics, the concept of nested configurations (a generalization of Segre–Veronese configurations) is introduced by Aoki–Hibi–Ohsugi–Takemura in 2008. This is a survey on recent results on nested configurations.

  Let $K[\mathbf{t}] = K[t_1, \ldots, t_d]$ denote the polynomial ring in $d$ variables over a field $K$. Recall that a *configuration* of $K[\mathbf{t}]$ is a finite set $A$ of monomials belonging to $K[\mathbf{t}]$ such that there exists a vector $(w_1, \ldots, w_d) \in \mathbb{R}^d$ with $\sum_{i=1}^{d} w_i a_i = 1$ for all $t_1^{a_1} \cdots t_d^{a_d} \in A$. We will associate each configuration $A$ of $K[\mathbf{t}]$ with the homogeneous semigroup ring $K[A]$, called the *toric ring* of $A$, which is the subalgebra of $K[\mathbf{t}]$ generated by the monomials belonging to $A$. Let $K[X] = K[\{x_M \,|\, M \in A\}]$ denote the polynomial ring over $K$ in the variables $x_M$ with $M \in A$ with each $\deg(x_M) = 1$. The *toric ideal* $I_A$ of $A$ is the kernel of the surjective homomorphism $\pi : K[X] \to K[A]$ defined by setting $\pi(x_M) = M$ for all $M \in A$. It is known that the toric ideal $I_A$ is generated by those homogeneous binomials $u - v$, where $u$ and $v$ are monomials of $K[X]$, with $\pi(u) = \pi(v)$. Let $A$ be a configuration of $K[\mathbf{t}]$ with the properties that $\deg m = r$ for all $m \in A$ and that, for each $1 \leq i \leq d$, there exists $m \in A$ such that $m$ is divided by $t_i$. Assume that, for each $1 \leq i \leq d$, a configuration $B_i = \left\{m_1^{(i)}, \ldots, m_{\lambda_i}^{(i)}\right\}$ of a polynomial ring $K\left[\mathbf{u}^{(i)}\right] = K\left[u_1^{(i)}, \ldots, u_{\mu_i}^{(i)}\right]$ in $\mu_i$ variables over $K$ is given. Then the *nested configuration* arising from $A$ and $B_1, ..., B_d$ is the configuration

$$A(B_1, \ldots, B_d) := \left\{ m_{j_1}^{(i_1)} \cdots m_{j_r}^{(i_r)} \;\middle|\; t_{i_1} \cdots t_{i_r} \in A, \;\; 1 \leq j_k \leq \lambda_{i_k} \text{ for } 1 \leq k \leq r \right\}$$

  of the polynomial ring $K\left[\mathbf{u}^{(1)}, \ldots, \mathbf{u}^{(d)}\right]$ in $\sum_{i=1}^{d} \mu_i$ variables over $K$.

  In this talk, the normality of the toric ring together with Gröbner bases of the toric ideal arising from a nested configuration will be studied.

## 0.3 Christian Doench, Research Institute for Symbolic Computation, Johannes Kepler University. Linz, Austria. cdoench@risc.jku.at

- **TITLE:** Relative Reduction and Characterization of Relative Groebner Bases.

- **ABSTRACT:** Groebner bases are well-established as one of the main tools for the algorithmic treatment of commutative algebra. Levin introduced the notion of Groebner bases with respect to several orderings as an effective method for the

computation of dimension polynomials in multi-graded and multi-filtered modules over Ore polynomial rings. Zhou and Winkler introduced the notion of relative Groebner bases being closely related to Levin's notion of Groebner bases with respect to several orderings. We present some results on relative Groebner bases of polynomial ideals and point out their relation to similar results for Groebner bases. Furthermore, this allows us to achieve a characterization of relative Groebner bases.

## 0.4 Alexander Levin, The Catholic University of America. levin@cua.edu

- **TITLE:** Generalized Groebner bases and bivariate dimension polynomials of D-modules.

- **ABSTRACT:** In 1971 J. Bernstein introduced an analog of the Hilbert polynomial for a finitely generated filtered D-module, that is, a module over a Weyl algebra. Bernstein polynomials and their invariants (that is, characteristics of a finitely generated D-module M, which are carried by any its Bernstein polynomial and which do not depend on the system of generators of M this polynomial is associated with) play an important role in the theory of D-modules and its applications. In this talk we generalize the Gröbner basis method to the case of a finitely generated free D-module considered together with two natural term orderings. Then we apply the new technique to prove the existence, determine invariants and outline methods of computation of Bernstein-type dimension polynomials in two variables that carry more invariants than classical Bernstein polynomials.

## 0.5 Quoc-Nam Tran & Valentin Andreev, Lamar University, qntran@lamar.edu

- **TITLE:** Groebner Bases Computation in Boolean Rings for Model Checking and Their Applications in BioInformatics

- **ABSTRACT:** The theory of Groebner Bases has become a crucial building block to computer algebra, and is widely used in science, engineering, and computer science. It is well-known that Groebner bases computation is EXP-SPACE in a general setting. In this talk, we present some recent developments in this area including an algorithm to show that Groebner bases computation is actually P-SPACE in Boolean rings. We also show that with this discovery, the Groebner bases method can theoretically be as efficient as other methods for automated verification of hardware and software. Additionally, many useful and interesting properties of Groebner bases including the ability to efficiently convert the bases for different orders of variables making Groebner bases a promising method in automated verification.

In contrast to other known algebraic approaches, the degree of intermediate polynomials during the calculation of Groebner bases using our method will never grow resulted in a significant improvement in running time and memory space consumption. We also show how calculation in temporal logic for model checking can be done by means of our direct and efficient Groebner basis computation in Boolean rings. We present our experimental results in finding attractors and control strategies of Boolean networks to illustrate our theoretical arguments.

## 0.6 Christian Eder, University of Kaiserslautern, ederc@mathematik.uni-kl.de

- **TITLE:** Signature-based algorithms to compute Groebner bases.
- **ABSTRACT:** Recent algorithms to compute Groebner bases rely not on Buchberger's criteria, but on so-called signatures. Two important algorithms in this field are F5 and GGV: We concentrate on these two, reducing the difference between F5 and GGV subsequently to the choice of a rewritable criterion. We compare various possible variants of this criterion, both theoretically and practically. Moreover, we try to give some notes on optimizations and termination issues.

## 0.7 Zhou Meng, Beihang University, Beijing, China. zhoumeng6286@buaa.edu.cn

- **TITLE:** Groebner bases in difference-differential modules with coefficients in a commutative ring
- **ABSTRACT:** Insa and Pauer presented a basic theory of Gröbner basis for differential operators with coefficients in a commutative ring in 1998. Recently a improved version was giving by Xiaodong Ma et al.(2010). In this paper we present an algorithmic approach for computing Gröbner bases in difference-differential modules with coefficients in a commutative ring. We combine the generalized term order method of Zhou and Winkler(2006) with G-S-polynomial method of Insa and Pauer to deal with the problem. Our result is a generalization of theories of Insa and Pauer, Xiaodong Ma et al.,Zhou and Winkler and include them as special cases.

## 0.8 Margreta Kuijper, University of Melbourne VIC 3010, Australia. mkuijper@unimelb.edu.au

- **TITLE:** Groebner p-bases for applications in finite ring coding
- **ABSTRACT:** This presentation deals with modules of univariate vector polynomials over a finite ring of the type $Z_{p^r}$ (where $p$ is a prime integer and $r$ is an

integer $> 1$). Such modules are relevant in various coding applications, such as decoding algebraic codes over $Z_{p^r}$ and convolutional codes over $Z_{p^r}$. For the field case, minimal Groebner bases are the ideal tools to deal with the abovementioned applications. However, for the ring case minimal Groebner bases are less useful due to a lack of uniqueness. To help remove this obstacle, in an earlier recent work [1] the new concept of "minimal Groebner p-basis" was introduced. It allows us to still use powerful Groebner principles in the ring case. In this presentation we show how to use Groebner p-bases in a range of applications in finite ring coding. [1] M. Kuijper and K. Schindelar, "Minimal Groebner bases and the predictable leading monomial property", Linear Algebra and its Applications, vol. 434, pp. 104-116, 2011.

## 0.9 David Jeffrey, University of Western Ontario, djeffrey@uwo.ca, and Yosua Setyobudhi, New Frontier Solutions, Pte. Ltd, yosua@nfs-asia.com

- **TITLE:** Stirling numbers of complex arguments
- **ABSTRACT:** The late Phillipe Flajolet proposed a generalized definition for Stirling numbers, allowing them to be computed for complex arguments. We have implemented and explored this definition. We obtain some surprising results.

## 0.10 Jan Verschelde, University of Illinois at Chicago, jan@math.uic.edu, and Genady Yoffe, University of Illinois at Chicago, gyoffe@math.uic.edu

- **TITLE:** Quality Up in Polynomial Homotopy Continuation by Multithreaded Path Tracking
- **ABSTRACT:** Speedup measures how much faster we can solve the same problem using many cores. If we can afford to keep the execution time fixed, then quality up measures how much better the solution will be computed using many cores. In this presentation we describe our our multithreaded implementation to track one solution path defined by a polynomial homotopy. Limiting quality to accuracy and confusing accuracy with precision, we strive to offset the cost of multiprecision arithmetic running multithreaded code on many cores.

## 0.11 Danko Adrovic, University of Illinois at Chicago, adrovic@math.uic.edu, and Jan Verschelde, University of Illinois at Chicago, jan@math.uic.edu

- **TITLE:** Polyhedral Methods for Positive Dimensional Solution Sets

- **ABSTRACT:** We present a polyhedral algorithm to manipulate positive dimensional solution sets. Using facet normals to Newton polytopes as pretropisms, we focus on the first two terms of Puiseux series expansion. The leading powers of the series are computed via the tropical prevariety. This polyhedral algorithm is well suited for exploitation of symmetry when it arises in systems of polynomials. Initial form systems with pretropisms in the same group orbit are solved only once, allowing for a systematic filtration of redundant data. Computation with `cddlib` and `Sage` are illustrated on cyclic $n$-roots polynomial systems.