TABLE OF CONTENTS

Volume 49, Number 1, Issue 191, March 2015

Open Source Computer Algebra Systems (OSCAS):

1 The SDEval Benchmarking Toolkit – *A. Heinle, V. Levandovskyy*

10 The Computational Geometry Algorithms Library CGAL – *E. Fogel, M. Teillaud*

13 ACA-2014 Abstracts – *I. Kotsireas, R.H. Lewis, T. Shaska*

36 Abstracts of Recent Doctoral Dissertations in Computer Algebra

37 Recent and Upcoming Events

Association for
Computing Machinery

Advancing Computing as a Science & Profession

20th Conference on Applications of Computer Algebra, ACA-2014

Communicated by Ilias Kotsireas, Robert H. Lewis, and Tony Shaska

The ACA meetings are organized as a series of Special Sessions. There were eleven special sessions:

1. Computer Algebra Aspects of Finite Rings and Their Applications

Organizers: Edgar Martnez-Moro, Steve Szabo

Computer Algebra Challenges for Constructing Skew Cyclic Codes

Nuh Aydin
Kenyon College, Gambier, OH, USA
aydinn@kenyon.edu

One of the challenging problems of coding theory is to construct codes with best possible parameters. Computers and computer algebra systems are often used in achieving this goal. Since the computation of the minimum distance of a linear code is computationally intractable (NP-hard), it is necessary to focus on certain promising classes of codes with rich algebraic structures. Cyclic codes and their various generalizations, such as consta-cyclic, quasi-cyclic, and quasi-twisted codes have been subject to much research, both theoretical and computational, for decades. As a result, a large number of best-known codes come from these families. More recently, a new generalization of cyclic codes, called theta-cyclic codes or skew cyclic codes, have been introduced. The algebraic study of skew cyclic codes requires one to work in a non-commutative ring called skew polynomial ring. This introduces new computational challenges for computer algebra systems when it comes to implementing search algorithms for constructing skew cyclic and related codes over rings or fields. In this talk, we will describe some of these challenges.

A New Non-Associative Cryptosystem Based on NTOW Public Key Cryptosystem and Octonions Algebra

Kadijeh Bagheri, Mohammad-Reza Sadeghi
Amirkabir University of Technology (Iran)
msadeghi@aut.ac.ir

In this work, we present a public key cryptosystem, called OTWO, based on octonions algebra and NTWO cryptosystem which is a multivariate version of NTRU. Inherent security of this system relies on the difficulty of the shortest vector problem (SVP) in a certain type of lattices with a hybrid norm. Since the octonions are non-associative (power-associative) and alternative algebra, they do not have a matrix isomorphic representation. So, normally lattice attacks against this cryptosystem are impossible. The only way to cryptanalysis and to find the private key for decryption in this cryptosystem is to expand the equation of public key as a linear system of equations and form a non-circular lattice. However, this type of attack seems to has no chance to succeed.

We change the underlying algebraic structure of NTWO and use a different lattice for key generation and decryption that it increases complexity of decryption. Furthermore, the non-associativity of underlying algebraic structure and existence of different lattice for key generation and decryption improve the security of cryptosystem markedly.

Construction of codes for DNA computing by the Greedy Algorithm

Nabil Bennenni, Kenza Guenda;
University of Science and Technology, USTHB, (Algeria)

Aaron Gulliver; University of Victoria (Canada)
ken.guenda@gmail.com

In this paper we construct codes for DNA computing using the greedy algorithm over $\mathbb{Z}_4$. We obtain linear codes over $\mathbb{Z}_4$ with bounded GC content. We also consider the edit distance, we gave upper bounds for the edit distance and construct codes with bounded edit distance. This paper is organized as follows. In Section 2 we give some preliminaries. In Section 3 we give the greedy algorithm for bounded GC-content. In Section 4 we construct DNA lexicodes with edit distance criteria and we give upper bound on the edit distance. Several examples of DNA codes with bounded GC-content and edit distance criteria.

Exponents of Skew Polynomials

Ahmed Cherchem, LA3C, USTHB, Algiers (Algeria)
André Leroy, LML, Université de Lens (France)
ahmedcherchem@gmail.com

Let A be a finite ring and σ be a ring automorphism of A. Any polynomial $f(t) \in A[t;\sigma]$ which is monic and has a regular constant term is a right (resp. left) factor of a polynomial of the form $t^e - 1$ for some integer $e \geq 1$. The least such integer is called the right (resp. left) exponent of $f(t)$. This generalizes the classical definition of the exponent, also known as order or period. We compute the exponent for $f(t) \in \mathbb{F}_q[t;\theta]$, where θ is the Frobenius. We also give some properties and examples.

The Module Isomorphism Problem for Finite Rings and Related Results

Iuliana Ciocănea Teodorescu
Leiden University (Netherlands)
ciocaneai@math.leidenuniv.nl

Let R be a finite ring and let M, N be two finite left R-modules. We present two distinct deterministic algorithms that decide in polynomial time whether or not M and N are isomorphic, and if they are, exhibit an isomorphism. As by-products, we are able to determine the largest isomorphic common direct summand between two modules and the minimum number of generators of a module. By not requiring R to contain a field, avoiding computation of the Jacobson radical and not distinguishing between large and small characteristic, both algorithms constitute improvements to known results. We have not attempted to implement either of the two algorithms, but have no reason to believe they would not perform well in practice.

Moreover, the second algorithm represents an interesting object *per se*, due to its structure and the techniques it employs. A common approach to this type of problems is to reduce to the semisimple case and then "lift". In our algorithm, we work *as if* the ring were semisimple and we have a list, $S_1, \ldots, S_t$, of candidates for the isomorphism classes of simple modules composing it. During the running of the algorithm, we allow ourselves to be contradicted in our assumption about the simplicity of the S_i, in which case we update our list, quotient the ring by an appropriate two-sided nilpotent ideal and start again. If we are not contradicted, we may still draw conclusions. In this way, there is always a side-exit available and what forces an output in polynomial time is that we cannot take the side-exit too many times.

Codes over local rings of order 16 and their Gray maps

Steven T. Dougherty and Esengül Salturk
University of Scranton (USA)
prof.steven.dougherty@gmail.com

Weight preserving Gray maps are defined from any non-chain local ring of order 16 to the binary Hamming space. This is used to define the Lee weight for codes in this setting. MacWilliams relations for the weight enumerator with respect to the Lee weight are given. Self-dual codes are studied over these rings and they are used to study binary codes whose weight enumerators are held invariant by the action of the MacWilliams relations.

Codes Over Rings of Order 16

Steven Dougherty, Esengül Saltürk
University of Scranton (USA)
Steve Szabo
Eastern Kentucky University (USA)
`mathematicianesen@gmail.com`

We study codes over finite commutative local Frobenius rings of order 16. We define a standard form for the generator matrix for linear codes over these rings. Finally, we describe the generating characters for each ring which produce MacWilliams relations for codes over these rings.

Network Coding via Skew Polynomials

Felice Manganiello; Clemson University (USA)
`manganm@clemson.edu`

In 2003 it was proven independently by Kötter and Mérdard, and Li *et al.* that linear network coding over a suitable finite field can be used to achieve the capacity of multicast networks. After this result, networks were connected to matroids. In 2007 Dougherty *et al.* showed how matroids can be deployed to construct matroidal networks. Gadouleau and Goupil in 2011 proved the achievability of the capacity of a multicast network by means of matroids instead of linear spaces. As a consequence of this result together with the fact that matroids can be perceived as a generalization of linear spaces, one can obtain an increase in the size of the codebooks used for communication.

The ring of skew polynomials is a non commutative generalization of the classic univariate polynomial ring. The multiplication of the former obeys a non commutative multiplication rule between the variable and a scalar defined by an automorphism of the underlined field and a derivation map. The ring maintains the structure of a right Euclidean ring without zero divisors. At this point, one obtains a natural evaluation map for skew polynomials as the remainder of the right division by a monomial.

It can be proven that the set of the zero locus of all of the skew polynomials using the aforementioned evaluation map, forms a matroid. Focusing on the case of skew polynomial rings over finite fields with trivial derivation map, it is possible to characterize the flats of this matroid and their sets of generators using minimal skew polynomials. We are going to explore this matroid structure and connect it to multicast communication.

This is a joint work with Siyu Liu and Frank R. Kschischang.

Multivariable Codes in Principal Ideal Polynomial Quotient Rings

Edgar Martínez-Moro, Alejandro P. Nicolás
Universidad de Valladolid (Spain)
Ignacio F. Rúa
Universidad de Oviedo (Spain)
`edgar@maf.uva.es`

Multivariable codes over a finite field are a natural generalization of several classes of codes, including cyclic, negacyclic, constancyclic, polycyclic and abelian codes. Since these particular families have been also considered in the context of codes over a finite chain ring, we proposed constructions of multivariable codes over such a class of finite rings. As in the case of traditional cyclic codes over finite fields the modular case (i.e., codes with repeated roots) is much more difficult to handle than the semisimple case (i.e., codes with non-repeated roots). In this sense, different authors have dedicated their efforts to provide a better understanding of the properties of cyclic, negacyclic, constancylic and polycyclic modular codes over a finite chain ring. Among these codes, those contained in an ambient space which is a principal ideal ring admit a relatively simple description, quite close to that of semisimple. This feature has been recently used in the description of abelian codes over a finite field, and in the description of modular additive cyclic codes over $\mathbb{F}_4$. As a natural continuation of these works, in this paper we consider the structure of multivariable modular codes in an ambient space which is a principal ideal ring.

Linear Codes over $\frac{\mathbb{Z}_4[x]}{\langle x^2-2x\rangle}$: Dual Preserving Maps and Images as Codes over $\mathbb{Z}_4$

Edgar Martínez-Moro; Universidad de Valladolid (Spain)
Steve Szabo; Eastern Kentucky University (USA)

Bahattin Yildiz; Fatih University (Turkey)
Steve.Szabo@eku.edu

The most general class of rings to considered working on coding theory over are Frobenius rings. Since finite commutative Frobenius rings are isomorphic to a direct sum of local Frobenius rings, it is important to understand local Frobenius rings. Chain rings have been extensively studied which are examples of local Frobenius rings. There are however non-chain examples as well. These local Frobenius non-chain rings have not garnered much attention until recently. We consider linear codes over $\frac{\mathbb{Z}_4[x]}{\langle x^2+2x\rangle}$, which is one of the seven local Frobenius non-chain rings of order 16. Order 16 is of importance since there are no local Frobenius rings of smaller order that are not chain rings. A dual preserving map is presented along with a characterization of $\mathbb{Z}_4$ linear codes that are images of a codes over $\frac{\mathbb{Z}_4[x]}{\langle x^2+2x\rangle}$.

2. Computer Algebra in Coding Theory and Cryptography

Organizers: Edgar Martnez-Moro, Ilias Kotsireas, Steve Szabo

A Johnson-Type Bound for Group Codes and Lattices

Malihe Aliasgari, Mohammad-Reza Sadeghi;
Amirkabir University of Technology (Iran)

Daniel Panario; Carleton University (Canada)
ariyadokht@aut.ac.ir

Johnson-type bounds provide an upper bound on the number of codewords in a Hamming ball with a specified radius. In this work we give and analyze a Johnson-type bound for group codes considering the G-norm. Johnson bounds have been given for binary and q-ary codes with respect to the Hamming distance. We borrow the idea of the G-norm and define a new distance for codewords: the G-semidistance. We extend the Johnson-type bounds for binary and q-ary codes to the G-semidistance and give a relation between these bounds and our G-semidistance. By means of this, we present an upper bound on the number of codewords inside a G-ball and an l_1-ball, within a certain given radius, for both group codes and lattices.

Binomial Ideal Associated to a Lattice and Its Label Code

Malihe Aliasgari; Amirkabir University of Technology (Iran)
Daniel Panario; Carleton University (Canada)
Mohammad-Reza Sadeghi; Amirkabir University of Technology (Iran)
ariyadokht@aut.ac.ir

In coding theory the study of the binomial ideal derived from an arbitrary code is currently of great interest. This is mainly because of a known relation between binomial ideals and lattices or codes. Also, studying the relation between binomial ideals associated to a lattice and its label code helps to solve the closest vector problem in lattices as well as decoding binary and non-binary codes and finding a label code of a lattice, as we do in this work.

Every lattice Λ can be described in terms of a label code L and an orthogonal sublattice Λ' such that $\Lambda/\Lambda' \cong L$. We assign binomial ideals I_Λ and I_L to an integer lattice Λ and its label code L, respectively. In this work, we

identify the binomial ideal associated to an integer lattice and then establish the relation $I_\Lambda = I_{\Lambda'} + I_L$ between the ideal of the lattice and its label code.

Stickelberger's Congruences and Perfect Sequence constructions

K.T. Arasu; Wright State University (Dayton, Ohio)

k.arasu@wright.edu

Arrays whose two-dimensional auto-correlation functions having desirable correlation properties have found applications in spectrometry, acoustics and cryptography for encrypting two-dimensional arrays such as images. Their one-dimensional analog, known as perfect sequences, are equally interesting and useful. This talk will deal with some new constructions of such objects. We shall call them: perfect arrays/sequences. Several new families of these have been constructed by the speaker (joint work with John Dillon and Kevin Player in the binary/ternary case). The construction techniques heavily rely upon the Stickelberger's congruence on Gauss sums. The inequivalence of the new sequences follows by the p-rank calculations of the associated matrices.

On a class of difference set pairs

Ankita Bakshi and Deeksha;
Y.M.C.A. University of Science and Technology (India)
ankitabakshi02@gmail.com

Let $(G, +)$ be an abelian group of order v and let A and B be two subsets of G with $|A| = k$ and $|B| = k'$. If the list/multiset of differences $(x - y (\text{mod } v) | x \in A, y \in B)$ contains every nonzero element of G exactly λ times, then (A, B) is a (v, k, k', e, λ) difference set pair (DSP) in G where $e = |A \cap B|$.

The case $A = B$ reduces to the usual (v, k, λ) difference set.

In order for a difference set pair to exist, the parameters must clearly satisfy the relationship $kk' = \lambda(v - 1) + e$. This is a necessary, but not a sufficient condition.

For odd v, a difference set pair is said to be balanced if $k = \frac{v}{2}$.

A difference set pair is said to be ideal if $v - 2(k + k') + 4\lambda = -1$.

We provide a new construction technique for DSPs using group rings. One such theorem is given below:

Theorem: Let G be an abelian group of order v. Let (A, B) be a balanced and ideal difference set pair in G with $A \subseteq B$ and parameters $(v, \frac{(v+1)}{2}, 2\lambda, 2\lambda, \lambda)$. Let H be an abelian group of prime-power order $4m - 1$. Let E be a difference set in H with parameters $(4m-1, 2m, m)$. Define $C = EB$ and $D = EA + (H - E)(G - B)$. Then (C, D) is a balanced and ideal difference set pair in GxH with parameters $(v(4m - 1), \frac{(v(4m-1)+1)}{2}, 4m\lambda, 4m\lambda, 2m\lambda)$. Further new results and their connections to results of Peng, Xu, Arasu (2012) and Ke, Yu, Chang (2013) would be given. DSPs and their associated binary sequence pairs have applications in digital signal processing and cryptography.

Plaintext Recovery for One-Time Pads Used Twice

Gregory V. Bard; University of Wisconsin–Stout
Theodore McDonnough; University of Wisconsin—River Falls
bardg@uwstout.edu

The one-time pad is a very simple encryption scheme taught in most first-year cryptography courses. It consists of a pad $\vec{k} = (k_1, k_2, \ldots, k_\ell)$, a sequence of independently uniformly random elements of the integers mod n, in the possession of both the sender and the receiver. The sender encodes the plaintext $\vec{p} = (p_1, p_2, \ldots, p_\ell)$ as a sequence of symbols mod n. Encryption and decryption are simply addition and subtraction mod n. More precisely, $c_i = p_i + k_i \bmod n$.

The cipher is provably secure, but the classical proof makes explicit assumptions about the method of use. In particular, each pad (each $\vec{k}$) must be used only once—hence the name "one-time pad." It has been known for a long time that the cipher can be broken if a single pad is used twice. For example, if $\vec{c_1} = \vec{p_1} + \vec{k}$ and $\vec{c_2} = \vec{p_2} + \vec{k}$, and both $\vec{c_1}$ and $\vec{c_2}$ are intercepted, historical records indicate that it must be the case that it is computationally feasible to recover $\vec{p_1}$, $\vec{p_2}$, and $\vec{k}$. However, the method by which this is done is an open topic. Doing so can be called the "two-time pad problem." The authors propose a method, based on matrix computations mod n, which efficiently solves the "two-time pad problem" for plaintexts chosen from the English language, and working with $n = 29$. The method should be effective for other modern spoken languages and similar sized n.

This is joint work with Theodore McDonough, an undergraduate doing research under the McNair Program at the University of Wisconsin—River Falls.

A notion of multivariate BCH bounds and codes

José Joaquín Bernal, Juan Jacobo Simón; Universidad de Murcia (Spain)
Diana H. Bueno-Carreño; Pontificia Universidad Javeriana-Cali (Colombia)
josejoaquin.bernal@um.es, jsimon@um.es,
dhbueno@javerianacali.edu.co

In 1970, P. Camion [2] extended the study of the BCH bound to the family of abelian codes by introducing the notion of apparent distance of an abelian code. For cyclic codes, it coincides with *the* BCH bound (see[2, p. 22]). In [1] we gave an algorithm to compute the minimum apparent distance of a hypermatrix, and thereby to compute the apparent distance of an abelian code, based on hypermatrix manipulations that extends other methods. We use those techniques in [1] to develop a notion of BCH bound and BCH code in the multivariate case. We also extend the most classical results in BCH codes to our case. Finally, we show two different applications. The first one consists of constructing multivariate abelian codes from BCH cyclic codes, multiplying their dimension and preserving their BCH bounds. The second one consists of designing maximum dimensional abelian codes with respect to several bounds.

References

[1] D. H. Bueno-Carreño, J.J. Bernal and J.J. Simón, *Computing the Camion's multivariate BCH bound*, ITW-Sevilla 2013, pp. 355-359.

[2] P. Camion, *Abelian Codes*, MRC Tech. Sum. Rep. # 1059, University of Wisconsin, 1971.

Extending Construction X for Quantum Error-Correcting Codes

Akshay Degwekar; Indian Institute of Technology Madras
Kenza Guenda; University of Science and Technology of Algiers(Algeria)
T. Aaron Gulliver; University of Victoria(Canada)
ken.guenda@gmail.com

Quantum error correcting codes have been introduced as an alternative to classical codes for use in quantum communication channels. Since the landmark papers of Shor and Steane , this field of research has grown rapidly. Recently, Lisonek and Singh gave a variant of Construction X that produces binary stabilizer quantum codes from arbitrary linear codes. In their construction, the requirement on the duality of the linear codes was relaxed. In this paper, we extend their work on construction X to obtain quantum error-correcting codes over finite fields of order p^2 where p is a prime number. We apply our results to the dual of Hermitian repeated root cyclic codes to generate new quantum error-correcting codes.

quantum codes; construction X; optimal codes; cyclic codes

The degree compatible Gröbner Fan for Linear Codes

Natalia Dück; Hamburg University of Techology (Germany)
Irene Márquez-Corbella; INRIA Saclay - GRACE Project (France)
Edgar Martínez-Moro; University of Valladolid (Spain)
natalia.dueck@tuhh.de

The Gröbner fan of an ideal in the commutative polynomial ring consists of polyhedral cones indexing the different leading ideals and is thus the geometric collection of all reduced Gröbner bases for this ideal. One application of the Gröbner fan is the so-called Gröbner walk which is the conversion of Gröbner bases.

With the software system TiGERS (Toric Gröbner bases Enumeration by Reverse Search) an efficient alternative for computing the Gröbner fan has been provided for the special case of toric ideals. Indeed, by identifying a reverse search tree on the cones of the Gröbner fan, a memoryless combinatorial Gröbner walk can be established that furthermore, requires no cost weight vectors.

Linear codes, on the other hand, can be linked to this whole subject by associating to each linear code a binomial ideal that encodes the information about the code in the exponents. This correspondence proved to be very beneficial as it provided new approaches to several well-known problems in coding theory. Almost all applications, however, require the computation of a degree compatible Gröbner basis.

In this talk, it will be shown how methods from the software system TiGERS can be modified in order to compute all reduced Gröbner bases with respect to a degree compatible ordering for code ideals – even though these binomial ideals are not toric. To this end, the correspondence of linear codes and binomial ideals will be briefly described as well as their resemblance to toric ideals. Finally, we will hint at applications of the degree compatible Gröbner fan to the code equivalence problem.

Some applications of idempotent semirings in Public Key Cryptography

Mariana Durcheva
Technical University of Sofia (Bulgaria)
mdurcheva66@gmail.com

In the present work we show how to apply different dual pairs of idempotent semirings for constructing new cryptographic protocols. We employ four idempotent semirings: **Max-plus semiring**, **Min-plus semiring**, **Max-time semiring**, **Min-time semiring**. The suggested protocols are generalization of the Diffie-Hellman key exchange protocol, to the context of semiring actions. Our protocols in its most general form consist of the following: two commutative semirings S_1, S_2 act on a set X i.e. $((S_1 \times S_2) \times X) \to X$.

We propose two practical realizations of this scheme, based on different dual pairs of idempotent semirings. For the semirings S_1 and S_2 we suggest commutative semirings generated by two given matrices M and N. These semirings are semirings of polynomials of the matrices M and N whose entries are selected from two dual pairs of idempotent semirings. Set X should be selected carefully with respect to the chosen pairs of semirings.

HIMMO: A collusion-resistant identity-based scheme for symmetric key generation

Oscar García-Morchón, Ronald Rietman, Ludo Tolhuizen
Philips Research, Eindhoven, The Netherlands
Domingo Gómez, Jaime Gutiérrez
University of Cantabria, Santander, Spain
jaime.gutierrez@unican.es

We describe HIMMO, a new scheme for identity-based symmetric key generation. Like the scheme of Blundo et al, HIMMO employs symmetric polynomials, which lead to very efficient implementations, but it is much less vulnerable against collusion attacks. HIMMO employs mixing modular operations over different rings and hiding part of the result of polynomial evaluation by only considering its least significant bits. We discuss the collusion resistance properties of HIMMO based on lattice-based cryptanalysis.

An overview on algebraic invariants and the main parameters of some parameterized codes

Manuel González Sarabia; Instituto Politécnico Nacional, UPIITA (México)
mgonzalezsa@ipn.mx

The main goal of this work is to describe the parameters of some evaluation codes known as parameterized codes by using the relationships with the algebraic invariants of a quotient ring. We use some tools of algebraic geometry and commutative algebra to do this description. Some results in the case of codes parameterized by the edges of a graph or a clutter are given.

Let $K = \mathbb{F}_q$ be a finite field with q elements. Let $L = K[Z_1, \ldots, Z_n]$ be a polynomial ring over the field K and let $Z^{a_1}, \ldots, Z^{a_m}$ be a finite set of monomials. As usual if $a_i = (a_{i1}, \ldots, a_{in}) \in \mathbb{N}^n$, where $\mathbb{N}$ stands for the non–negative integers, then we set $Z^{a_i} = Z_1^{a_{i1}} \cdots Z_n^{a_{in}}$ for all $i = 1, \ldots, m$. In this situation we say that the following set X, which is a multiplicative group under componentwise multiplication, is the toric set parameterized by these monomials.

$$X = \{[(t_1^{a_{11}} \cdots t_n^{a_{1n}}, t_1^{a_{21}} \cdots t_n^{a_{2n}}, \ldots, t_1^{a_{m1}} \cdots t_n^{a_{mn}})] \in \mathbb{P}^{m-1} : t_i \in K^*\}, \tag{1}$$

where $K^* = K \setminus \{0\}$ and $\mathbb{P}^{m-1}$ is a projective space over the field K.

Let $S = K[X_1, \ldots, X_m] = \bigoplus_{d=0}^{\infty} S_d$ be a polynomial ring over the field K with the standard grading and let $X = \{[P_1], \ldots, [P_{|X|}]\}$. The evaluation map

$$\begin{gathered} \mathrm{ev}_d : S_d \to K^{|X|}, \\ f \to \left(\frac{f(P_1)}{X_1^d(P_1)}, \ldots, \frac{f(P_{|X|})}{X_1^d(P_{|X|})} \right) \end{gathered}$$

defines a linear map of K–linear spaces. The image of this map is denoted by $C_X(d)$ and it will be called a parameterized code of order d associated to the toric set (1). The vanishing ideal of X, denoted by I_X, is the ideal of S generated by the homogeneous polynomials of S that vanish on X. We relate some of the algebraic invariants of the ring S/I_X with the main characteristics of the code $C_X(d)$.

Some results on finite fields

James Hufford; Wright State University (Dayton, Ohio)

hufford.12@wright.edu

In the study of perfect sequences, use of trace functions in finite fields has been a common technique, dating back to Singer's classical examples of m- sequences. Many variations of Singer's theme have been the topic of research by many mathematicians during the last few decades. In all these investigations, expressing the underlying function as a polynomial whose coefficients are from the prime subfield has been a main problem. Explicit answers require the use of Stickelberger's congruence of Gauss sums. Using elementary methods, we provide a simple result along these lines.

The following is well-known:

Let $f : \mathbb{F}_{p^d}^* \to \mathbb{F}_{p^d}$ be any function. Then $f(x) = \sum_{k=0}^{p^d-2} \alpha_k x^k \in \mathbb{F}_{p^d}[x]$

We prove a finer version of the above result:

Let p be an odd prime. Let $f(x) \in \mathbb{F}_{p^d}[x]$. Let $degf(x) = r$. Suppose $r < p^d - 1$ and $f(\alpha) \in \mathbb{F}_p$ for each $\alpha \in \mathbb{F}_p^*$. Then $f(x) \in \mathbb{F}_p[x]$.

Edge-weighted Cayley graphs, monotonicity and bent functions

David Joyner U. S. Naval Academy

wdj@usna.edu

This is an abstract for a talk summarizing joint work of mine with several different authors on bent functions.

We discuss various results on monotone Boolean functions. In particular, that there are no monotone bent Boolean functions. This is joint with Claude Carlet and Pante Stanica.

Let $f : GF(p)^n \to GF(p)$. When $p = 2$, Bernasconi et al. have shown that there is a correspondence between certain properties of f (e.g., if it is bent) and properties of its associated Cayley graph. Analogously, but much earlier, Dillon showed that f is bent if and only if the "level curves" of f have certain combinatorial properties (again, only when $p = 2$). We discuss an analogous theory when $p > 2$. Which graph-theoretical properties of the Cayley graph Γ_f can be characterized in terms of function-theoretic properties of f? Which function-theoretic properties of f correspond to combinatorial properties of the set of "level curves" $f^{-1}(a)$ $(a \in GF(p))$? Are there natural generalizations of the Bernasconi correspondence and Dillon correspondence? We discuss a partial classification, in a combinatorial way, of even bent functions $f : GF(p)^n \to GF(p)$ with $f(0) = 0$ for $(p, n) = (3, 2)$, $(3, 3)$, and

$(5, 2)$. Our main conjecture extends this classification, and we end with a series of open questions on amorphic bent functions. This is joint with Caroline Melles, Charles Celerier, David Philips, and Steven Walsh.

The extended and generalized rank weight enumerator of a code

Relinde Jurrius; Free University of Brussels
Ruud Pellikaan; Eindhoven University of Technology
g.r.pellikaan@tue.nl

This paper investigates the rank weight enumerator of a code over L, where L is a finite extension of a field K. This is a generalization of the case where $K = \mathbb{F}_q$ and $L = \mathbb{F}_{q^m}$ of Gabidulin codes to arbitrary characteristic. We use the notion of counting polynomials, to define the (extended) rank weight enumerator, since in this generality the set of codewords of a given rank weight is no longer finite. Also the extended and generalized rank weight enumerator are studied in analogy with previous work on codes with respect to the Hamming metric.

Error-correcting pairs: a new approach to code-based cryptography

Irene Márquez-Corbella; INRIA, École Polytechnique

Ruud Pellikaan; Eindhoven University of Technology
irene.marquez-corbella@inria.fr

McEliece proposed the first public-key cryptosystem based on linear error-correcting codes. A code with an efficient bounded distance decoding algorithm is chosen as secret key. It is assumed that the chosen code looks like a random code. The known efficient bounded distance decoding algorithms of the families of codes proposed for code-based cryptography, like Reed-Solomon codes, Goppa codes, alternant codes or algebraic geometry codes, can be described in terms of error-correcting pairs (ECP). That means that, the McEliece cryptosystem is not only based on the intractability of bounded distance decoding but also on the problem of retrieving an error-correcting pair from the public code. In this article we propose the class of codes with a t-ECP whose error-correcting pair that is not easily reconstructed from of a given generator matrix.

McEliece Cryptosystem Based on Punctured Convolutional Codes and the Pseudo-Random Generators

Hamza Moufek and Kenza Guenda; University of Science and Technology (Algeria)
ken.guenda@gmail.com

In 1978 Robert J. McEliece invented the first cryptosystem based on algebraic coding theory. Since then different variants have been proposed.

Different attacks were made against these schemes. Among them, we mention the attack on the original McEliece system by Canteaut and Sendrier and the attack on the cryptosystem based on convolutional codes by Landais and Tillich.

The purpose of this paper is to present a new version of the McEliece cryptosystem based on punctured convolutional codes and the pseudo-random generators. We use the modified self-shrinking generator to fill the punctured pattern. More precisely we propose to fill out the pattern punctured by the bits generated using a pseudo random generator LFSR. We also show that our new variant is secure against several attacks.

Some new almost difference sets via finite fields

Bo Phillips and Jace Robinson; Wright State University (Dayton, Ohio)
robinson.329@wright.edu

Several investigations on antenna arrays focus on the “thinning problem” wherein one would like to reduce the number of array elements with respect to the original filled layouts. The rationale to do so is to economize costs, weight, consumption of power etc. But this typically would result in the loss of SLL (sidelobe level) control and gain when compared to the filled arrangements. Caorsi, S., Lommi, A., Massa, A. and Pastorino, M. [2004] have successfully used the so-called "difference sets" (DS), a rich class of combinatorial objects in thinned-array design procedures, to synthesize thinned arrays with controlled sidelobes. Oliveri,G., Donelli, M., and Massa, A [2009] go a step further and exploit the use of a more general class of combinatorial objects known as "almost difference sets" (ADS) since the admissible array configurations embrace a much larger terrain in their generalization. Several construction techniques based on finite fields and cyclotomy are obtained during the last decade providing infinite classes of ADS. We obtain some new examples of such objects using a finite field of order 31, thereby obtaining an almost perfect sequence of length 62 whose existence status was previously open. Further such examples are likely and are being investigated in our REU project supported by NSF.

Evaluation Codes and Weierstrass Semigroups

Emma Previato; Boston University
ep@bu.edu

We report on a construction of modified evaluation codes by Dias and Neves [1]. Evaluation codes are a type of Reed-Muller code, where the code is the image of a space of polynomial functions under the evaluation map on a given set of points in affine space, cf. [2]. In their work, Dias and Neves assign weights to the coordinates, namely a finite sequence of natural numbers. The goal is to compute the parameters of the code, especially aiming at the Minimum-Distance-Separable property. Even with the simplest choice of points on which to evaluate, however, the problem is difficult, as it is related to the Frobenius problem [3]. In collaboration with Neves, we propose to establish a connection between the spaces of functions and sections of line bundles on algebraic curves when the chosen sequence generates the Weierstrass semigroup of a point on the curve. The prospective application is to compute the parameters of the code in some cases by using Riemann-Roch arguments.

References

[1] [DN] E. Dias and J.S. Neves, *Codes over a weighted torus*, http://arxiv.org/abs/1307.6380.

[2] [G] O. Geil *Evaluation Codes from an Affine Variety Code Perspective*, in Advances in algebraic geometry codes, Ser. Coding Theory Cryptol., 5, World Sci. Publ., Hackensack, NJ, 2008, Eds.: E. Martinez-Moro, C. Munuera, D. Ruano, pp. 153-180.

[3] [R] J. Ramírez Alfonsín, The Diophantine Frobenius problem. Oxford Univ. Press, 2005.

Optimum Shortened Cyclic Codes for Multiple Burst-Error Correction

Ana Lucila Sandoval Orozco, Luis Javier García Villalba
and Mario Blaum; University Complutense of Madrid (Spain)
asandoval@fdi.ucm.es

On channels with memory, the noise is not independent from transmission to transmission. As a consequence, transmission errors occur in clusters or bursts, and channels with memory are called burst-error channels. Examples of burst-error channels are mobile telephony channels, where the error bursts are caused by signal fading owing to multipath transmission; cable transmission, which is affected by impulsive switching noise and crosstalk; and magnetic recording, which is subject to dropouts caused by surface defects and dust particles. Codes designed to correct burst errors are called burst-error correcting codes.

Hence, burst-correcting codes are of interest for some applications in which errors tend to occur in clusters. With higher transmission rates or higher storage densities this may even be more so in the future. The problem of correcting bursts of errors is a difficult one. In practice, Reed-Solomon codes, either interleaved or not, are used for correcting multiple bursts. However, it is of interest to find efficient multiple burst-correcting codes that are optimal in terms of redundancy.

In addition to the familiar Hamming distance, it is well known that there is also a burst distance and a burst weight. The codes considered in this talk are all binary and linear. Codes meeting the Singleton bound with equality are called Maximum Distance Separable (MDS). Other bounds can also be obtained using the burst distance, like for instance, the Hamming bound. Another well known bound for burst-correcting codes is the Gallager bound. The Gallager bound is more general than the Reiger bound, since it applies to both block and convolutional codes, while

the Reiger bound applies only to block codes. Even if we restrict only to block codes, the Gallager bound seems to be more general than the Reiger bound, since it connects the burst length with the guard space. However, the Reiger bound contains implicitly the guard space, although this does not look very clear from the bound itself. In fact, for block codes, both bounds are equivalent.

Finally, shortened cyclic codes that are capable of correcting multiple bursts of errors are considered, together with tables of generator polynomials.

3. Computational Differential and Difference Algebra

Organizer: Alexey Ovchinnikov

Computing differential Galois groups of parameterized second-order linear differential equations

Carlos E. Arreche; The CUNY Graduate Center (USA)
carreche@gc.cuny.edu

We describe recent algorithms to compute the differential Galois group G associated to a parameterized second-order homogeneous linear differential equation of the form

$$\frac{\partial^2}{\partial x^2}Y + r_1\frac{\partial}{\partial x}Y + r_0 Y = 0,$$

where the coefficients $r_1, r_0 \in F(x)$ are rational functions in x with coefficients in a partial differential field F of characteristic zero. As an application of these algorithms, we describe a set of criteria to decide the differential transcendence of the solutions with respect to the parametric derivations on F.

A Direct Algorithm for Computing k-Simple Forms of First-Order Linear Differential Systems

Moulay A. Barkatou; University of Limoges (France)
moulay.barkatou@unilim.fr

Most algorithms for computing solutions of linear ordinary differential equations proceed by investigating the singularities of the coefficients to obtain information on the singularities of the solutions. For systems, this is more difficult than for scalar equations and a main tool for computing the local exponents and the non-ramified local exponential parts in this case is Moser- and super-reduction. From super-reduced forms, one can compute all the integer slopes of the Newton-polygon and determine the corresponding Newton polynomials. Moser- and super-reduced forms are also used in the computation of the formal solutions of the system around a singularity and in the computation of the global solutions such as the rational solutions and the exponential solutions.

However, solving some of these problems requires only weaker forms than super-reduced forms. In this talk, we present a direct (i.e., without computing first a super-reduced form) algorithm for computing k-simple forms of first-order differential systems at $x = 0$ with coefficients from $C((x))$, where C is a field of constants. We give the arithmetic complexity of our algorithm which has been implemented in Maple and we illustrate it with some examples. Finally, we show how using this algorithm one can find the formal invariants of the system at $x = 0$.

This is a joint work with Carole El Bacha, Lebanese University (Lebanon).

Bounding the size of a finite differential algebraic variety

James Freitag; University of California at Berkeley (USA)
freitag@math.berkeley.edu

Given a collection of differential polynomials, $f_1, \ldots, f_n$, suppose that their common solution set is finite. In the ordinary case, Hrushovski and Pillay showed how to get effective bounds for the size of this finite solution set in terms of the orders and degrees of the differential polynomials. This result is at the differential algebraic heart of various applications of differential algebra to problems in diophantine geometry (due to Hrushovski, Pillay and recent results of Freitag and Scanlon). The proof of the upper bound is algorithmic, and reveals how the problem is related to so-called geometric axioms for differentially closed fields. The upper bound eventually comes from intersection theory in arc spaces. We will explain how to extend this work to the partial case, which is more involved, essentially due to the coherence condition for differential polynomials. If time permits, recent diophantine applications related to the the André-Oort conjecture will be given.

This is joint work with Omar Leon Sanchez.

Binomial Difference Ideal and Toric Difference Variety

Xiao-Shan Gao; Academy of Mathematics and Systems Science,
Chinese Academy of Sciences (China)
{xgao,cmyuan}@mmrc.iss.ac.cn

In this talk, the concepts of binomial difference ideals and toric difference varieties are defined and their properties are proved. Two canonical representations for Laurent binomial difference ideals are given using the reduced Gröbner basis of $\mathbb{Z}[x]$ lattices and regular and coherent difference ascending chains, respectively. Criteria for a Laurent binomial difference ideal to be reflexive, prime, perfect, and toric are given in terms of their support lattices which are $\mathbb{Z}[x]$ lattices. The reflexive and perfect closures of a Laurent binomial difference ideal are shown to be binomial. Four equivalent definitions for toric difference varieties are presented in terms of rational parametrization, implicit ideals, coordinate rings, and group actions. Finally, algorithms are given to check whether a given Laurent binomial difference ideal I is reflexive, prime, perfect, or toric, and in the negative case, to compute the reflexive and perfect closures of I. An algorithm is given to decompose a finitely generated perfect binomial difference ideal as the intersection of reflexive prime binomial difference ideals.

This is a joint work with Zhang Huang and Chun-Ming Yuan.

Towards a non-commutative Picard-Vessiot theory

Florian Heiderich; RWTH Aachen (Germany)
florian@heiderich.org

André unified the Galois theories of linear differential equations and of linear difference equations. In this talk we present a more general Galois theory of linear functional equations, which can involve operators from a wide class not only containing derivations and automorphisms, but also skew-derivations. The Galois groups are no longer affine group schemes, but quantum groups instead. We illustrate this theory by means of an easy example.

Radicals of Ore Polynomials

Maximilian Jaroschek; Johannes Kepler University Linz (Austria) - RISC;
Max-Planck-Institute for Informatics (Germany)
mjarosch@risc.jku.at

We give a comprehensible algorithm to compute the radical of an Ore operator. Given an operator P, we find another operator L and a positive integer k such that P is the kth power of L and k is maximal among all integers for which such an operator L exists. Furthermore we discuss possible extensions of this procedure to identify operators of the form $A \cdot P$ where P is the kth power of some operator L and to derive a reduced operator $A \cdot L$.

Effective differential Lüroth theorem

Gabriela Jeronimo; University of Buenos Aires (Argentina)
jeronimo@dm.uba.ar

Let $\mathcal{F}$ be a differential field of characteristic 0 and $\mathcal{F}\langle u \rangle$ the field of differential rational functions in a single indeterminate u. The differential Lüroth theorem proved by Ritt and extended by Kolchin states that for any differential subfield $\mathcal{G}$ of $\mathcal{F}\langle u \rangle$ there exists $v \in \mathcal{G}$ such that $\mathcal{G} = \mathcal{F}\langle v \rangle$.

The talk will focus on effectivity aspects of this result. More precisely: given non-constant rational functions $v_1, \ldots, v_n \in \mathcal{F}\langle u \rangle$ such that $\mathcal{G} = \mathcal{F}\langle v_1, \ldots, v_n \rangle$, we will give upper bounds for the total order and degree of a Lüroth generator v of the extension $\mathcal{G}/\mathcal{F}$ in terms of the number and the maximum order and degree of the given generators of $\mathcal{G}$.

Our approach combines elements of Ritt's and Kolchin's proofs with estimations concerning the order and the differentiation index of differential ideals. As a byproduct, we will show that our techniques enable the computation of a Lüroth generator by dealing with a polynomial ideal in a polynomial ring in finitely many variables.

This is a joint work with Lisi D'Alfonso and Pablo Solernó.

On the integration of algebraic functions: computing the logarithmic part

Lourdes Juan; Texas Tech University (USA)
lourdes.juan@ttu.edu

Bronstein developed a complete algorithm to compute the logarithmic part of an integral of a function that lies in a tower of transcendental elementary extensions. However, computing the logarithmic part in an algebraic extension has remained difficult and challenging. In his Ph.D. dissertation, Brian Miller, building on the work of Manuel Kauers, developed a method to compute the logarithmic part when the function lies in a tower of transcendental elementary extensions followed by an algebraic extension. The method uses Gröbner bases and primary decomposition. In this talk we will discuss Miller's work and work in progress to produce a complete algorithm for some particular cases of algebraic functions.

Differential algebra of invariants and invariant variational calculus

Irina A. Kogan; North Carolina State University (USA)
iakogan@ncsu.edu

Systems of differential equations and variational problems arising in geometry and physics often admit a group of symmetries. As was first recognized by S. Lie, these problems can be rewritten in terms of group-invariant objects: differential invariants, invariant differential forms, and invariant differential operators. Differential invariants and invariant differential operators constitute a differential algebra with often non-trivial but computable structure. It is desirable from both computational and theoretical points of view to study invariant problems in terms of invariant differential algebra. In this talk, we will describe how differential algebra of invariants can be constructed and show applications to variational calculus.

Dynamical Systems and Scaling Invariants

George Labahn; University of Waterloo (Canada)
glabahn@uwaterloo.ca

In this talk we study the field of rational invariants of the scalings along with their use in reducing dynamical systems. Scalings are group actions which are nicely described by an integer matrix of exponents. Making use of integer linear algebra we show how to compute a minimal generating set of invariants along with the substitution to rewrite any invariant in terms of this generating set. When applied to dynamical and polynomial systems one obtains new systems with reduced variables and simpler solution systems.

This is joint work with Evelyne Hubert (INRIA Méditerranée, France)

Counting Solutions of Differential Equations

Markus Lange-Hegermann; RWTH Aachen (Germany)
markus.lange.hegermann@rwth-aachen.de

The aim of this talk is a quantitative analysis of the solution set of a system of differential equations. We generalize Kolchin's differential dimension polynomial and its properties from prime differential ideals to characterizable differential ideals. This makes the dimension polynomial more accessible for algorithms. In certain applications, an even more detailed quantitative description of differential equations is needed. Therefore, we introduce the differential counting polynomial, a generalization of the differential dimension polynomial. The tools used in this talk are the decomposition algorithms by J.M. Thomas.

New development and application of integration of differential fractions

François Lemaire, Université des Sciences et Technologies de Lille (France)
Francois.Lemaire@lifl.fr

The publication "On the Integration of Differential Fractions" published at ISSAC'13 (Boulier, Lemaire, Regensburger, Rosenkranz) introduces the differential fractions (which are quotients of differential polynomials) and presents algorithms for representing such fractions. In particular, a differential fraction F can be decomposed into $F = G + dH/dx$ (where G and H are differential fractions and d/dx designates the total derivative w.r.t. x). I will present recent developments concerning the canonicity of such a decomposition, as well as numerical applications of the decomposition in the context of parameters estimation.

Parametrized logarithmic equations and their Galois theory

Omar León Sánchez; McMaster University (Canada)
oleonsan@math.mcmaster.ca

I will talk about (parametrized) differential D-groups which are not necessarily defined over a field of constants. Then, I will present the foundational results on the Galois theory of logarithmic differential equations in such groups. I will also discuss two natural non-linear examples of such equations which are not defined over the constants.

Generalized Gröbner bases and dimension polynomials of modules over some finitely generated noncommutative algebras

Alexander Levin; Catholic University of America (USA)
levin@cua.edu

We present a generalized Gröbner basis method in free modules over finitely generated noncommutative algebras that arise as a natural generalization of algebras of solvable type studied by A. Kandri-Rody and V. Weispfenning. The considered class of algebras includes, in particular, algebras of differential, difference and difference-differential operators, Ore algebras, quantized (and classical) Weyl algebras. We prove the existence and give methods of computation of univariate and multivariate Hilbert-type dimension polynomials associated with systems of generators of finitely generated modules over such algebras.

We also determine invariants of the dimension polynomials, that is, numerical characteristics carried by these polynomials that do not depend on the choice of the corresponding systems of module generators. Finally, we will show how the obtained results can be applied to the computation of difference-differential dimension polynomials associated with finitely generated extensions of difference-differential fields and systems of algebraic difference-differential equations.

Formal Solutions of Completely Integrable Pfaffian Systems with Normal Crossings

Suzy S. Maddah; University of Limoges (France)
suzy.maddah@etu.unilim.fr

In this talk, we are interested in the formal reduction of the so-called completely integrable Pfaffian systems with normal crossings, i.e. the class of linear systems of partial differential equations. Pfaffian systems arise in many applications including the studies of aerospace and celestial mechanics. By far the most important for applications are those with normal crossings. We tackle the question of formal reduction, i.e. the algorithmic procedure that computes the transformation which takes the system into its canonical form so that formal solutions can be constructed. Clearly, the particular univariate case corresponds to singular linear systems of ordinary differential equations which have been studied extensively. Moreover, unlike the multivariate case, algorithms to related problems leading to the construction of the formal solutions have been widely developed.

We present an algorithm, based on a joint work with Moulay Barkatou, to construct a fundamental matrix of formal solutions of completely integrable Pfaffian systems with normal crossings in two variables. Our algorithm is based on associating to the Pfaffian system a singular linear system of ordinary differential equations from which its formal invariants can be efficiently derived. We then discuss the extension of this algorithm to the multivariate case. Our algorithm builds upon the package ISOLDE and is implemented in the computer algebra system Maple.

Parameterized Differential Equations and Patching

Annette Maier; RWTH Aachen University (Germany)
annette.maier@mathA.rwth-aachen.de

We consider linear parameterized differential equations over $k((t))(x)$ with parameter t such as

$$\partial_x(y) = \frac{t}{x} \cdot y.$$

The parameterized Galois group of such an equation is a linear differential algebraic group over $k((t))$, i.e., a subgroup of GL_n given by differential ∂_t-algebraic equations. In the example above, the parameterized Galois group equals

$$G = \{c \in \mathrm{GL}_1 \mid \partial_t^2(c)c - \partial_t(c)^2 = 0\}.$$

The inverse problem asks which linear differential algebraic groups occur as parameterized Galois groups. In the talk, I will explain how algebraic patching methods (developed by David Harbater and Julia Hartmann) can be applied in this context to realize a certain class of groups as parameterized Galois groups over $k((t))(x)$.

Dimensions of difference-algebraic groups

Alice Medvedev; CUNY City College (USA)
amedvedev@ccny.cuny.edu

Model-theoretic dimensions (Lascar rank, Morley rank) of groups defined by difference equations of the form $x \in G$ and $\sigma^m(x) = \Phi(x)$ for some algebraic group G and some algebraic group morphism $\Phi : G \to \sigma^m(G)$ are relatively easy to compute. I will discuss two interesting and useful notions of the limit of these dimensions as m tends to infinity.

Undecidability of the uniqueness testing problem for analytic solutions of PLDE with boundary conditions

Sergey Paramonov; Moscow State University (Russia)
s.v.paramonov@yandex.ru

We consider linear partial differential equations with polynomial coefficients and prove algorithmic undecidability of the following problem: to test whether a given equation of considered form has no more than one solution that is analytic on an open region and that satisfies some fixed boundary conditions. It is assumed that a polynomial which vanishes at each point of the region boundary is known.

Galois groups of difference equations on elliptic curves

Julien Roques; Université Grenoble Alpes (France)
Julien.Roques@ujf-grenoble.fr

We will give some general results about the Galois groups of difference equations of order two on elliptic curves. We will compute the Galois groups of some equations of order two, such as discrete Lamé equations.

This is a joint work with Thomas Dreyfus (Université Paris Diderot, France).

A Jordan–Hölder theorem for difference algebraic groups

Michael Wibmer; RWTH Aachen University (Germany)
michael.wibmer@matha.rwth-aachen.de

Difference algebraic groups, i.e., groups defined by algebraic difference equations occur as the Galois groups of linear differential and difference equations depending on a discrete parameter. In this talk I will introduce difference algebraic groups and explain some of their basic properties. In particular, I will present an analog of the Jordan–Hölder theorem for difference algebraic groups.

On the termination of algorithm for computing relative Gröbner bases

Guanli Huang, Meng Zhou; Beihang University (China)
zhoumeng1613@hotmail.com

Relative Gröbner bases were introduced by Zhou and Winkler (2008) in order to compute bivariate dimension polynomials in difference-differential modules. The algorithm for computing relative Gröbner bases and bivariate dimension polynomials also were presented in Zhou and Winkler(2008). Christian Dönch (2010) give a Maple software of the algorithm. By now it is used as the main tool for the algorithmic computation of bivariate dimension polynomials in difference-differential modules.

Recently Christian Dönch (2013) presented an example pointing out the algorithm does not terminate in some case. From the counterexample Dönch pointed out that it is questionable whether a relative Gröbner basis always exists. Also it is uncertain whether the algorithm for computing bivariate dimension polynomials in difference-differential modules terminates.

In this paper we improve the results of Zhou and Winkler (2008) about relative Gröbner bases. We introduce the concept of difference-differential degree compatibility on generalized term orders. Then we prove that in the process of the algorithm the polynomials with higher and higher degree wouldn't be produced, if the term orders "$\prec$" and "$\prec'$" are difference-differential degree compatibility. So we present a condition on the generalized orders and prove that under the condition the algorithm for computing relative Gröbner bases will terminate. Also the relative Gröbner bases exist under the condition. Finally we prove the algorithm for computation of the bivariate dimension polynomials in difference-differential modules terminates.

---

4. Algebraic and Algorithmic Aspects of Differential and Integral Operators

Organizers: Moulay Barkatou, Thomas Cluzeau, Georg Regensburger, and Markus Rosenkranz

---

Differential (Lie) algebras from a functorial point of view

Laurent Poinsot
LIPN - UMR CNRS 7030
University Paris 13, Sorbonne Paris Cité (France)
laurent.poinsot@lipn.univ-paris13.fr

It is well-known that any associative algebra becomes a Lie algebra under the commutator bracket. This relation is actually functorial, and this functor, as any algebraic functor, is known to admit a left adjoint, namely the universal enveloping algebra of a Lie algebra. In the differential context a similar, but somewhat different, correspondence holds. Indeed any commutative differential algebra becomes a Lie algebra under the Wronskian bracket $W(a, b) = ab' - a'b$.

I will prove that this correspondence again is functorial, and also the existence of a left adjoint, namely the differential enveloping (commutative) algebra of a Lie algebra. I will also show in this talk that it actually defines an adjoint pair from the category of commutative differential algebras to the category of differential Lie algebras. Contrary to the non-differential usual case, when the differential algebra is not commutative the Wronskian bracket does not provide a Lie bracket anymore because it is not alternating. Nevertheless in this talk we will see that it gives rise to the so-called non-commutative version of a Lie algebra, namely a Leibniz algebra. I will then present the construction of the free differential algebra over a (differential) Leibniz algebra, and also discuss several other functorial relations and open problems.

Differential elimination by differential specialization of Sylvester style matrices

Sonia L. Rueda; Universidad Politécnica de Madrid (Spain)
sonialuisa.rueda@upm.es

Differential resultant formulas are defined, for a system $\mathcal{P}$ of n ordinary Laurent differential polynomials in $n-1$ differential variables. These are determinants of coefficient matrices of an extended system of polynomials obtained from $\mathcal{P}$ through derivations and multiplications by Laurent monomials. To start, through derivations, a system $\mathsf{ps}(\mathcal{P})$ of L polynomials in $L-1$ algebraic variables is obtained, which is non sparse in the order of derivation. This enables the use of existing formulas for the computation of algebraic resultants, of the multivariate sparse algebraic polynomials in $\mathsf{ps}(\mathcal{P})$, to obtain polynomials in the differential elimination ideal generated by $\mathcal{P}$. The formulas obtained provide order and degree bounds for a polynomial in the differential elimination ideal.

Acknowledgments: This work was developed, and partially supported, under the research project MTM2011-25816-C02-01. The author belongs to the Research Group ASYNACS (Ref. CCEE2011/R34).

Local Stability of Cubic Differential Systems

Dahira Dali, Jugurta Mahrez
University of science and technology Houari Boumediene (Algeria)
Faculty of mathematics
dddahira@gmail.com

The qualitative study of differential equations, introduced in the early 19th century by Henri Poincare [2] allowed us to determine the properties of solutions, the number and nature of singularities, the behavior of solutions of these equations without solving the differential equations. The qualitative theory of differential equations is a new issue for the study of these differential equations which can't be solved explicitly. Then at the end of the 19th century invariant theory introduced by Hilbert [1] allowed the evolution of the qualitative theory of differential equations. This qualitative theory becomes a powerful tool in the qualitative study of polynomial differential systems when Sibirskii [3] had the idea to write the coefficients of these systems as tensorial coefficients.

In the case of autonomous linear differential systems the stability of a singular point or its trajectory is known. In the case of non-linear differential systems, in particular polynomial differential systems, the problem of their stabilty can be reduced in some cases to the study of a stability of a linear differential system defined from this nonlinear differential system.In general, the study of the stability in an equilibrium point for a given differential equation is determined using a function called Lyapunov function. This function is not easy to find. In this work, using Gröbner bases our idea is to develop an algorithmic method to compute singularities of a given cubic differential system and characterise their nature with the help of algebraic invariants.

[1] D. Hilbert, Invariant Theory, Cambridge University Press, 1993.

[2] H. Poincaré, Sur les courbes définies par les équations différentielles, J. Math. Pures Appl. 1(1985), 167–244.

[3] C. S. Sibirskii, Introduction to the Algebraic Theory of Invariants of Differential Equations, Nonlinear Science, Theory and Applications, Manchester University Press, 1988.

Differential algebraic aspect of orthogonal polynomials and modular forms

Emma Previato, Boston University
ep@bu.edu

The purpose of this talk is to investigate the positive-characteristic version of classical objects related to differential operators. An application of the study would be the use of algorithms for CAS such as *Maple* and Magma; another, the novel use of those objects in coding theory and cryptography.

We focus on Orthogonal Polynomials (OPs) and Modular Forms.

A program of classification of differential equations satisfied by OPs was begun in 1929, when S. Bochner answered the question of classifying all differential equations of the form

$$\sum_{i=1}^{2n}\sum_{j=0}^{i}\ell_{ij}x^i y^{(j)}(x)=\lambda_m y(x),\ n\geq 1$$

having a sequence $(\phi_m(x))_{m=0}^{\infty}$ of polynomial solutions, for $n=1$ (cf. [L1]). The classification of all second-order PDEs (in two variables) having orthogonal polynomial solutions was achieved by H.L. Krall and I.M. Sheffer in 1967 (cf. [L2] for a survey and further questions). More recently, sequences of OPs were found to be related by "Darboux transformation". To give a brief illustration, in the difference-operator case this is worked out in [GH]: Let a set of polynomials $\{p_0=1, p_n(k)\}$ satisfy a recursion relation $a_np_{n-1}+b_{n+1}p_n+p_{n+1}=kp_n,\ p_n=0$ for $n<0$, and write this in matrix form $Lp=kp$. Write the tridiagonal matrix L as the product, $L=UV$, of two tridiagonal matrices $U=(u_{ij}),\ V=(v_{ij})$, with the non-zero entries $u_{ii}=\alpha_{i+1},\ u_{i,i+1}=1,\ v_{ii}=1,\ v_{i+1,i}=\beta_{i+1},\ i\geq 0$. Then the tridiagonal matrix $M=VU$ is the Darboux transform of L. Applying the Darboux transform to the Laguerre or Jacobi polynomials generates orthogonal polynomials that are eigenfunctions of a fourth-order differential operator. Over the complex numbers, this observation makes it possible to write an explicit expression for the polynomials in terms of theta functions for the spectral curve associated to the matrix L. In turn, theta is associated to another "special function", known as "Sato's tau function", and there is a Painlevé-type ODE which governs this specific tau function, whose relation with Bochner's equation does not appear to have been investigated and this will be posed a question during the talk. More pertinently, a proposal will be made to establish analogues over finite fields, with sums replacing the integrals. Toward this goal, we will present the Kleinian sigma function, also associated to the theta function, and some of its (remarkably) characteristic-free identities, based on *Maple* work [P].

The sigma function associated to a curve is a modular function; modular forms, and modular curves, have been widely studied in positive characteristic, but less so their differential aspect: we focus on the "Rankin-Cohen bracket", brought to light by Zagier [Z]. On the other hand, in [R], the author considers Weierstrass points on curves of arithmetic interest, such as the Fermat curves $x^N+y^N+z^N=0$ and the modular curves $\Gamma(N)$ and $\Gamma_0(N)$. The problem of determining the precise set of Weierstrass points on these curves remains largely unsolved. In order to find new Weierstrass points, the author considers the Wronskian from the viewpoint of modular forms: indeed, if $\{f_1,...,f_g\}$ is a basis for the space of cusp forms of weight two for a subgroup Γ of finite index in $\mathrm{Sp}(2,\mathbb{Z})$, then the zeros of their Wronskian, a modular form of weight $g(g+1)$ for Γ, are the Weierstrass points (with multiplicities) of the modular curve determined by Γ. The proposal of this part is therefore to compute the Wronskian for the reduction of the modular curves mod p, construct the Rankin-Cohen operators where the Wronskian acts on another modular form, and write Zagier's identities as differential equations. The differential-Galois algebraic aspects of such equations are unexplored and clearly promising (cf. [SU]), since the curves carry large automorphism groups.

References

[GH] F. Alberto Grünbaum and Luc Haine, *Orthogonal polynomials satisfying differential equations: the role of the Darboux transformation*, in: Symmetries and integrability of difference equations (Estérel, PQ, 1994), 143-154, CRM Proc. Lecture Notes, 9, Amer. Math. Soc., Providence, RI, 1996.

[L1] Lance L. Littlejohn, *On the classification of differential equations having orthogonal polynomial solutions*, Ann. Mat. Pura Appl. (4) 138 (1984), 35-53.

[L2] L.L. Littlejohn, *Orthogonal polynomial solutions to ordinary and partial differential equations*, in: Orthogonal polynomials and their applications (Segovia, 1986), 98-124, Lecture Notes in Math., 1329, Springer, Berlin, 1988.

[P] E. Previato, *Sigma function and dispersionless hierarchies*, in: XXIX Workshop on Geometric Methods in Physics, 140-156, AIP Conf. Proc., 1307, Amer. Inst. Phys., Melville, NY, 2010.

[R] D.E. Rohrlich, *Some remarks on Weierstrass points*, in: Number theory related to Fermat's last theorem (Cambridge, Mass., 1981), pp. 71-78, Progr. Math., **26**, Birkhäuser, Boston, Mass., 1982.

[SU] M.F. Singer and F. Ulmer, *On a third order differential equation whose differential Galois group is the simple group of* 168 *elements*, in: Applied algebra, algebraic algorithms and error-correcting codes (San Juan, PR, 1993), Lecture Notes in Comput. Sci., Springer, Berlin, 316–324, 673, 1993.

[Z] D. Zagier, *Modular forms and differential operators*, in': K. G. Ramanathan memorial issue. Proc. Indian Acad. Sci. Math. Sci. 104 (1994), no. 1, 57-75. (Reviewer: Jannis A. Antoniadis) 11F25 (11F11).

On the Formal Reduction of Singularly-Perturbed Linear Differential Systems

Suzy S. Maddah; University of Limoges (France)
suzy.maddah@etu.unilim.fr

We consider the singularly-perturbed linear differential system of the form

$$\epsilon \frac{dY}{dx} = A(x,\epsilon)Y = \epsilon^{-h} x^{-p} \sum_{k=0}^{\infty} A_k(x)\epsilon^k Y. \tag{2}$$

where x is a complex variable, ϵ is a small parameter, h, p are integers, and the entries of $A(x,\epsilon)$ lie in $\mathbb{C}[[x,\epsilon]]$, the ring of formal power series in x and ϵ over the field of complex numbers.

Such systems have countless applications traced back to the year 1817 and their study encompasses a vast body of literature. However, their symbolic resolution is still open to investigation.

Clearly, system (2) is a singular perturbation of the widely studied linear singular system of differential equations given by

$$x \frac{dY}{dx} = A(x)Y = x^{-p} \sum_{k=0}^{\infty} A_k x^k Y. \tag{3}$$

The methods proposed in the literature of system (2) either exclude its *turning points* or are not algorithmic throughout. Moreover, they make an essential use of the so-called Arnold-Wasow form. On the other hand, for system (3), the research advanced profoundly in the last two decades making use of methods of modern algebra. The former classical approach is substituted by efficient algorithms giving rise to the Maple package ISOLDE. It was the hope of Wasow, in his 1985 treatise summing up contemporary research directions and results on system (2), that techniques of system (3) be generalized to tackle the problems of system (2). This is the interest of this talk which presents a joint work with Moulay Barkatou.

Endomorphisms of quantum generalized Weyl algebras

Stephane Launois; University of Kent (England)
S.Launois@kent.ac.uk

We study quantum generalized Weyl algebras $A(a,q)$ over a Laurent polynomial ring, where $q \in K^*$ is not a root of unity and $\sigma(h) = qh$. We give a complete answer to the classification of endomorphisms of $A(a,q)$. In the case where these algebras are simple, our classification shows that every endomorphism is an automorphism. This applies in particular to several quantizations of the first Weyl algebra.

Differential Equations and Hurwitz Series

William F. Keigher; Rutgers University (USA)
V. Ravi Srinivasan; IISER Mohali (INDIA)
keigher@rutgers.edu

In this talk, we consider the study of linear differential equations over a field of any characteristic using Hurwitz series. We first obtain explicit recursive expressions for solutions of such equations and study the group of differential automorphisms of the solutions. Moreover, we give explicit formulas that compute the group of differential automorphisms. The notion of intertwining of sequences is shown to have applications to the solution of such linear differential equations. We do not require that the field of constants of the underlying field be algebraically closed.

Rational Invariants of Finite Abelian Groups

George Labahn
University of Waterloo (Canada)
glabahn@uwaterloo.ca

In this talk we study the field of rational invariants of the linear action of a finite abelian group in the non modular case. By diagonalization, the group is accurately described by an integer matrix of exponents. Making use of integer linear algebra we show how to compute a minimal generating set of invariants along with the substitution to rewrite any invariant in terms of this generating set. This generating set can be chosen to consist of polynomial invariants.

As an application, we provide a symmetry reduction scheme for dynamical and polynomial systems whose solution set is invariant by the group action. In addition we provide an algorithm to find such symmetries given a dynamical or polynomial system.

This is joint work with Evelyne Hubert (INRIA Méditerranée, France)

Gelfand-Kirillov dimension of differential difference algebras

Yang Zhang and Xiangui Zhao
University of Manitoba (Canada)
xian.zhao@umanitoba.ca

Differential difference algebras, introduced by Mansfield and Szanto, arose naturally from differential difference equations. We investigate the Gelfand-Kirillov dimension of differential difference algebras. We give a lower bound of the Gelfand-Kirillov dimension of a differential difference algebra and a sufficient condition under which the lower bound is reached; we also find an upper bound of this Gelfand-Kirillov dimension under some specific conditions and construct an example to show that this upper bound can not be sharpened any more.

The generalized multiplicative operator of differentiation for the construction of analytic solitary solutions to nonlinear differential equations

Minvydas Ragulskis
Kaunas University of Technology (Lithuania)
minvydas.ragulskis@ktu.lt

Many different methods for the construction of analytic solutions of nonlinear evolutions in mathematical physics have been established and developed during the last decades. A number of semi-automatic methods based on the extensive use of symbolic computations have been used to construct solutions to different nonlinear ordinary differential equations. Homogeneous balance method, the Exp-function method, the tanh-function method and its various extensions, the (G'/G) expansion method, the auxiliary ordinary differential equation method are successfully used to solve high-dimensional nonlinear evolutions in mathematical physics with the help of symbolic computation. The key idea of most of these methods is that the traveling wave solution of a complicated nonlinear evolution equation can be guessed (supposed) as a polynomial (or a ratio of polynomials) of standard functions whose argument is the traveling wave term. The degree of the polynomial can be determined by considering homogeneous balance between the highest derivatives and nonlinear terms in the nonlinear evolution equation considered. Nevertheless, it can be noted that a straightforward application of these methods has attracted a considerable amount of criticism.

The main objective of this presentation is to propose an alternative approach for the construction of analytic solutions to nonlinear ordinary differential equations. It is based on the generalized operator of differentiation for the generation of algebraic structures representing analytic solutions to differential equations. We derive an analytical criterion based on the concept of H-ranks and the properties of the generalized operator of differentiation − and determine if a solution can be expressed in an analytical form comprising standard functions. The employment of this criterion does not only give an answer to the above-stated question but gives the structure of the solution − so that one does not have to guess what the form of the solution is. The load of symbolic calculations is brought before the structure of the solution is identified. This is in contrary to the previously mentioned semi-automatic methods based on symbolic computations (Exp-function, tanh-function, etc. methods) where the structure of the solution is first proposed, and then symbolic calculations are exploited for the identification of parameters.

The proposed concept is illustrated by using the generalized multiplicative operator techniques for the construction of analytic solutions to Riccati, Liouville, KdV equations. The concept of the generalized multiplicative operator provides the insight into the algebraic structure of solutions to nonlinear ordinary differential equations and enables automatic generation of the existence conditions in the space of system parameters and initial conditions.

Rota-Baxter Type Operators, Rewriting Systems And Gröbner-Shirshov Bases

Li Guo; Rutgers University at Newark (U. S. A.)
William Sit; The City College of The City University of New York (U. S. A.)
Xing Gao, Shanghua Zheng; Lanzhou University (China)
wyscc@sci.ccny.cuny.edu

In this talk, we apply the methods of rewriting systems and Gröbner-Shirshov bases to give a unified approach to study a class of linear operators on associative algebras. These operators resemble the classic Rota-Baxter operator, and we call them Rota-Baxter type operators. We show that all Rota-Baxter type operators may be characterized by the convergence of their corresponding rewriting systems that we associate uniformly to the operators. We also associate to each Rota-Baxter type operator a Gröbner-Shirshov basis, by which we obtain a canonical basis for the free objects in the category of associative algebras equipped with such an operator. This uniform construction of free objects include as special cases several previously known constructions such as certain ones for free Rota-Baxter algebras and for free Nijenhuis algebras.

On Factoring Differential and Difference Operators in n Variables

Mark Giesbrecht, Albert Heinle
University of Waterloo (Canada)
Viktor Levandovskyy
RWTH Aachen University (Germany)
aheinle@uwaterloo.ca

Factoring in non-commutative polynomial algebras is generally more involved than in commutative polynomial algebras, since factors of a given element are unique only up to a weak notion of similarity.

For operator algebras like the Weyl algebras, research until now mostly constrained itself by assuming a certain number of variables or a specific maximal degree when dealing with the factorization problem.

For the polynomial first Weyl algebra A_1, we have developed and implemented algorithms to factor its elements (`ncfactor.lib` in Singular). Our methods make use of the $\mathbb{Z}$-graded structure that is given on A_1. Recently, we generalized the underlying methodology to extend those algorithms to factor polynomials in the nth Weyl, the nth shift and homogeneous polynomials in the nth q-Weyl algebra. In contrast to other approaches for factoring that were developed in the past, the generalization is elegant and unexpectedly requires only a minor extension of the underlying theory.

We will present our factorization technique for the nth Weyl algebra A_n and its implementation, combined with some interesting and counterintuitive examples. Furthermore, we will show how the graded structure of the mentioned algebras can be applied to approach problems other than factorization.

Multi-parameter Laser Modes in Paraxial Optics

Christoph Koutschan
Johann Radon Institute for Computational and Applied Mathematics
Austrian Academy of Sciences, Austria

Erwin Suazo, School of Mathematical Sciences
University of Puerto Rico, Mayaguez, Puerto Rico

Sergei K. Suslov, School of Mathematical and Statistical Sciences
Arizona State University, USA
sergei@asu.edu

By computer algebra methods we study multi-parameter solutions of the inhomogeneous paraxial wave equation in a linear and quadratic approximation which include oscillating laser beams in a parabolic waveguide and spiral light beams in weakly varying media. A similar effect of superfocusing of particle beams in a thin monocrystal film is also discussed.

Method of generalized characteristic sets and multivariate dimension polynomials of differential field extensions with a group action

Alexander Levin, Department of Mathematics
The Catholic University of America Washington, D. C. 20064, USA
E-mail: levin@cua.edu

We present a method of characteristic sets with respect to several term orderings in the ring of differential G-polynomials over a differential field with a finitely generated commutative group G-action. In the case of a partition of the basic set of derivations and representation of the group G as the direct product of its subgroups, we use this method to prove the existence and obtain a method of computation of multivariate Hilbert-type dimension polynomials of differential field extensions with a group action. We also consider applications of the obtained results to the study of algebraic differential equations with a group action.

5. Integration: Implementation and Applications

Organizers: David Jeffrey, Michael Wester and Michel Beaudin

RUBI and integration as term re-writing: integrals containing tangent

David Jeffrey, Albert Rich, Junrui Hu; University of Western Ontario (Canada)
djeffrey@uwo.ca

Recent progress in the long-term project RUBI is presented. We describe, as a case study, how a large class of integrands containing tangent functions can be integrated using RUBI's term-rewriting rules.

Rewrite rules for nested integrals

Clemens G. Raab; Deutsches Elektronen-Synchrotron, Zeuthen (Germany)
clemens.raab@desy.de

Parameter integrals naturally arise as integral transforms or related convolution integrals, for instance. We consider the special case where such integrals originate from expressions involving nested integrals. More precisely, we deal with integrals where the integrand is given by a nested integral multiplied by a parameter-dependent factor. The aim is to compute those parameter integrals, or at least rewrite them in simpler form, using rewrite rules. The main feature of these rules is that they reduce the original integral to one of a similar type which has lower nested depth. A general principle to construct rewrite rules for this purpose will be discussed. Examples for Mellin transforms and Mellin convolutions originating from applications in perturbative quantum chromodynamics will be shown. Based on these rules also general properties of Mellin transforms and Mellin convolutions involving nested integrals can be proven.

Piecewise Functions and Convolution Integrals (Part I, Part II)

Michel Beaudin, Frédéric Henri; École de technologie supérieure,
Montréal, Québec (Canada)
michel.beaudin@etsmtl.ca

In most calculus textbooks, piecewise continuous functions do not constitute an important subject: students are rarely asked to use the fundamental theorem of calculus with a piecewise continuous integrand! But in signal analysis courses, engineering students have to deal with integrals of piecewise continuous functions, especially in the study of a (continuous) linear time invariant system, the so-called LTI system. Here is the reason: if $x(t)$ is the input signal, then the output signal $y(t)$ is the convolution of $x(t)$ with the system impulse response $h(t)$. In other words: $y(t) = \int_{-\infty}^{\infty} x(\tau)h(t-\tau)\,d\tau$. Usually, the signals are piecewise continuous and have compact support in order to avoid convergence problems with the improper integral. The talk will show how easy it can be to perform a convolution for any compact support signal using the CAS DERIVE and its built-in indicator function (if one signal is an impulse, we can take a limit of indicator function). Then we will try to do the same using the templates of TI-Nspire CAS for piecewise continuous functions. This will require conversions from piecewise to indicator functions. Some results presented at ACA 2013 will be used and extended.

The Hazards of Symbolic Definite Integration (a Continuing Saga)

Daniel Lichtblau; Wolfram Research (U.S.A.)
danl@wolfram.com

This talk is an update to ongoing work to improve symbolic definite integration. Various sticky points we will cover include convergence testing, checking a path for singularities, and more. In the event that we reach infinity during this talk I will provide a guided tour of the things that can go wrong there, and possibly also a light snack.

Combinatorial integration (Part I, Part II)

Gilbert Labelle;
LaCIM and Department of Mathematics, UQAM (Canada)
labelle.gilbert@uqam.ca

Let X be a formal indeterminate. A *combinatorial power* of X is an expression of the form X^n/H, where H is a subgroup of the symmetric group S_n. More generally, a *combinatorial power series* in X (CPS, for short) is of the form,

$$\sum_{n,H} c_{n,H} X^n/H \ , \quad c_{n,H} \in \mathbb{C} \ . \tag{4}$$

Many operations have been defined on such series and implemented in computational algebra systems. In particular, CPS form a differential ring, denoted $\mathbb{C}\|X\|$, equipped with a substitution operation, which contains the ring $\mathbb{C}[[X]]$ of classical power series in X. The main reason to study CPS is that they "encode" classes (species) of combinatorial structures, according to their automorphisms groups, together with the combinatorial operations between them. In the present talk, we put emphasis on computational techniques for combinatorial integration in $\mathbb{C}\|X\|$, the inverse of combinatorial differentiation. It turns out that integrals are no longer defined up to a constant. One integral of the class of total orders is the class of oriented cycles; one integral of the class of forests of rooted trees is the class of trees, etc. Integration techniques for families of combinatorial differential equations are also presented and illustrated on explicit examples, including "combinatorial liftings" to $\mathbb{C}\|X\|$ of the Lambert W function. Various tables computed using Maple and GAP softwares are also included.

Unwinding paths on the Riemann sphere for continuous integrals of rational functions

Robert H. C. Moir, Robert M. Corless, David J. Jeffrey;
University of Western Ontario (Canada)
robert@moir.net

We consider the problem of obtaining integrals of rational functions on domains of maximum extent. We show that for integrals of real rational functions that can be expressed in elementary finite terms, the expressions returned by the Risch algorithm and its variants can have their spurious discontinuities removed using a generalized unwinding number that accounts for both the usual winding of complex functions around 0 in the complex plane as well as windings through the point at infinity on the Riemann sphere. This latter sort of winding occurs where arguments of the arctangent function have poles of odd order. We show that both sorts of windings can be accounted for by introducing, in addition to an angular unwinding number that accounts for logarithmic branch cut crossings, a second radial unwinding number to account for pole-type singularities, which converts expressions of integrals with spurious discontinuities into correct continuous expressions for the integral. We also discuss the status of an early implementation of the approach in BPAS (basic polynomial algebra subprograms, bpaslib.org), an open source, efficient, low-level polynomial algebra software package written in CilkPlus targeting multicore architectures.

Abstracts of Recent Doctoral Dissertations in Computer Algebra

Each quarter we are pleased to present abstracts of recent doctoral dissertations in Computer Algebra and Symbolic Computation. We encourage all recent Ph.D. graduates who have defended in the past two years (and their supervisors), to submit their abstracts for publication in CCA.
Please send abstracts to the CCA editors `<editors_SIGSAM@acm.org>` *for consideration.*

Author: Anen Lakhal
Title: Elimination in Operator Algebras
School: Institute of Mathematics, University of Kassel, Kassel, Germany
Thesis Advisor: Wolfram Koepf and Werner Seiler
Defended: July 2014

A large class of special functions are solutions of systems of linear difference and differential equations with polynomial coefficients. For a given function, these equations considered as operator polynomials generate a left ideal in a noncommutative algebra called Ore algebra. This ideal with finitely many conditions characterizes the function uniquely so that Gröbner basis techniques can be applied.
Many problems related to special functions which can be described by such ideals can be solved by performing elimination of appropriate noncommutative variables in these ideals.
In this work, we mainly achieve the following:

1. We give an overview of the theoretical algebraic background as well as the algorithmic aspects of different methods using noncommutative Gröbner elimination techniques in Ore algebras in order to solve problems related to special functions.

2. We describe in detail algorithms which are based on Gröbner elimination techniques and perform the creative telescoping method for sums and integrals of special functions.

3. We investigate and compare these algorithms by illustrative examples which are performed by the computer algebra system *Maple*. This investigation has the objective to test how far noncommutative Gröbner elimination techniques may be efficiently applied to perform creative telescoping.

Recent and Upcoming Events

July 6–9, 2015
40th International Symposium on Symbolic and Algebraic Computation (ISSAC'15)
Bath, UK

Organizers: Steve Linton (General Chair), Kazuhiro Yokoyama (PC Chair)
Dates: Submission: January 5, 2015 (abstracts) and January 12, 2015 (full papers), Notification: March 20, 2015, Final Version: April 20, 2015
Website: `http://www.issac-symposium.org/2015`

July 10–12, 2015
The 7th International Workshop on Parallel Symbolic Computation (PASCO'15)
Bath, UK

Organizers: Clément Pernet (General Chair), Jean-Guillaume Dumas and Erich L. Kaltofen (PC Chairs)
Dates: Submission: April 2015, Notification: end of May, 2015
Website: `http://pasco2015.imag.fr/index.php`

July 20–23, 2015
Applications of Computer Algebra (ACA 2015)
Kalamata, Greece

Organizers: Ilias Kotsireas (General Chair), Edgar Martínez-Moro (PC Chair)
Dates: Session proposals: January 16, 2015, Talk Submission deadline: May 15, 2015
Website: `http://www.singacom.uva.es/ACA2015/index.html`

July 27-31, 2015
The second summer school "Algorithmic and Enumerative Combinatorics" (AEC 2015)
Linz, Austria

Organizers: Carsten Schneider
Dates: Submission of contributed talks: June 1, 2015
Website: `https://www.risc.jku.at/conferences/aec2015/`

August 10-14, 2015
The Third Workshop on Hybrid Methodologies for Symbolic-Numeric Computation
Beijing, China

Organizers: Lihong Zhi (Organizing Chair)
Website: `http://mmrc.iss.ac.cn/HMSNC2015/`

July – December, 2015
Fields Institute: Thematic Program on Computer Algebra
Toronto, Canada

Organizers: Stephen Watt (Lead Organizer)
Website: `http://www.fields.utoronto.ca/programs/scientific/15-16/computeralgebra/`
