Letter from the SIGSAM Chair

Emil Volcheck

Dear readers and SIGSAM members,

Thank you for reading this issue. If you are seeing this as a printed copy, then let me welcome you to our first printed double issue of the "ACM Communications in Computer Algebra" (CCA). Allow me to tell you about this change. Printing and distribution of our quarterly publication is a major expense. In order to save money, we have decided to combine printing and publish two printed double issues each year while continuing to publish quarterly on the web. We hope that this arrangement will retain most of the benefits of a printed publication with the same electronic access as before. Now, I would like to report to you on a few issues.

Dues Increase

The SIGSAM Executive Committee voted to increase dues from 29 to 30 USD per year and to leave the student rate unchanged at 9 USD. The last dues increase was in 2003, from 23 to 29 USD.

Viability Review and Finances

At the February 5, 2007 meeting of the SIG Governing Board (SGB), SIGSAM was approved to continue for another two years, meaning that our next Viability Review will be in early 2009. The SGB resolution reads as follows: "The SGB congratulates SIGSAM for making progress on its financial performance and finds it viable to continue its status for the next 2 years." You can view my presentation to the SGB here:

`http://sigsam.org/officers/Viability_Review/2007/Slides.pdf` .

SIGSAM has indeed made progress towards more stable finances. SIGSAM has profited from a larger distribution of revenue from the ACM Digital Library. Printing two double issues of CCA will save us at least 1800 USD per year. ISSAC 2006 was financially successful, returning about 1500 USD, which SIGSAM shares evenly with the ISSAC Steering Committee. SIGSAM also saved money by no longer offering complimentary memberships to those who register for ISSAC at the higher nonmember rate. The dues increase will bring in a small amount of additional revenue each year. ACM Finance projects our balance to grow by about 8000 USD in Fiscal Year 2008 to finish with over 17000 USD.

Elections

The current officers will finish their terms of office at the end of June 2007. Elections for new officers will be held soon through the ACM online election service. The Nomination Committee consisting of Bob Caviness, Rob Corless (chair), and Erich Kaltofen submitted the following slate of candidates to ACM:

For Chair:	Mark Giesbrecht	Jeremy Johnson
For Vice Chair:	Peter Paule	Kiyoshi Shirayanagi
For Treasurer:	Dan Lichtblau	Markus Hitz
For Secretary:	Wen-shin Lee	Howard Cheng

Please congratulate the nominees and be sure to vote!

Anthony Hearn Named ACM Fellow

Please join me in congratulating Anthony ("Tony") Hearn for being named an ACM Fellow for his contributions to computer algebra and symbolic computation. Hearn is well known as the architect and lead developer of the REDUCE computer algebra system and also for his contributions to the application of computer algebra to physics. I am proud to say that SIGSAM submitted the nomination which resulted in his selection. For more information on the ACM Fellows program, please visit

`http://fellows.acm.org/` .

Hearn is a former ACM National Lecturer and helped develop the CSNet in the early 1980s. He is a long-time member of SIGSAM and served as chair from 1981-83.

Call for Nominations for ACM Dissertation Award

Please consider nominating a student for the ACM Doctoral Dissertation Award. There is so much good research being done by doctoral students in computer algebra and symbolic computation that we as a community should strive to gain broader recognition for their work. Nominations must be made by the thesis advisor and endorsed by the head of the department. While SIGSAM has no formal role in this process, we are eager to help facilitate the nomination by providing supporting letters. For more information, see

`http://www.acm.org/awards/ddainfo.html` .

Although there is an English language requirement, this is an international award. The deadline for submissions is August 31, 2007.

SIGSAM Supports More Conferences

SIGSAM has been asked to give scientific support to three conferences this year, which is a new milestone for our service to the community. I am delighted to say that SIGSAM is in cooperation with Symbolic-Numeric Computation (SNC) 2007, Parallel Symbolic Computation (PASCO) 2007, and the (US) East Coast Computer Algebra Day (ECCAD) 2007. When SIGSAM cooperates with a conference or workshop, that means the ACM endorses its scientific program. This allows the conference to use the ACM logo in its publicity and to place its proceedings in the ACM Digital Library. SIGSAM members have access to the proceedings as a benefit of membership.

Special Interest Groups of the ACM can support conferences in two ways: through sponsorship or cooperation. Sponsorship of an event indicates that ACM gives its scientific endorsement to and takes financial responsibility for the event. For instance, SIGSAM often sponsors ISSAC. Cooperation indicates scientific endorsement but without financial responsibility. If you are planning an event for which you would like SIGSAM support, please contact me at `chair_SIGSAM@acm.org` or `volcheck@acm.org` .

Thank you for your attention.

Sincerely,

Emil Volcheck

Computing Gröbner Bases of Ideals of Few Points in High Dimensions

Winfried Just[1] and Brandilyn Stigler[2]

[1]Department of Mathematics, Ohio University, Athens, OH 45701
[2]Mathematical Biosciences Institute, The Ohio State University, Columbus, OH 43210

Abstract

A contemporary and exciting application of Gröbner bases is their use in computational biology, particularly in the reverse engineering of gene regulatory networks from experimental data. In this setting, the data are typically limited to tens of points, while the number of genes or variables is potentially in the thousands. As such data sets vastly underdetermine the biological network, many models may fit the same data and reverse engineering programs often require the use of methods for choosing parsimonious models. Gröbner bases have recently been employed as a selection tool for polynomial dynamical systems that are characterized by maps in a vector space over a finite field.

While there are numerous existing algorithms to compute Gröbner bases, to date none has been specifically designed to cope with large numbers of variables and few distinct data points. In this paper, we present an algorithm for computing Gröbner bases of zero-dimensional ideals that is optimized for the case when the number m of points is much smaller than the number n of indeterminates. The algorithm identifies those variables that are *essential*, that is, in the support of the standard monomials associated to a polynomial ideal, and computes the relations in the Gröbner basis in terms of these variables. When n is much larger than m, the complexity is dominated by nm^3. The algorithm has been implemented and tested in the computer algebra system *Macaulay 2*. We provide a comparison of its performance to the Buchberger-Möller algorithm, as built into the system.

Keywords: Gröbner bases, Buchberger-Möller algorithm, essential variables, run-time complexity, computational biology applications

1 Introduction

The theory of Gröbner bases has been an active field of study in the last four decades, beginning with the seminal work of Buchberger [6]. A problem of particular interest has been the development of algorithms for computing Gröbner bases. The first algorithm, proposed by Buchberger, has time complexity that is doubly exponential in the number of variables [7]. Since then, several improvements to Buchberger's algorithm have been proposed, as well as a number of alternative methods for certain classes of ideals.

Many of the improvements focus on two aspects. The first is coefficient growth when computing Gröbner bases in a field of characteristic 0 (for example, see [5]). The second is Buchberger's Criterion, which states that

> "A set $G = \{g_1, \ldots, g_r\} \subset I$ is a Gröbner basis for I if and only if the S-polynomial $\overline{S(g_i, g_j)}^G$ is 0 for all $1 \leq i, j \leq r$."

The Optimized Buchberger Algorithm [9] proposed by Caboara *et al.* and Faugére's $F4$ and $F5$ [13, 14] are instances of methods that seek to minimize the number of S-polynomials to be computed. While they still have exponential complexity in the worst case, in practice their performance renders them efficient alternatives to the original Buchberger algorithm.

For zero-dimensional ideals, several methods have been described and implemented. In [8], the authors presented the Buchberger-Möller algorithm (BMA) for computing the reduced Gröbner basis for the vanishing ideal of a variety V over a field. This algorithm eliminates the need to compute

S-polynomials and instead performs Gaussian elimination on a generalized Vandermonde matrix. Its complexity is quadratic in the number of variables and cubic in the number of points in V (for details, see [1, 20, 21, 22]). It has been implemented in publicly available computer algebra systems such as CoCoA [10] and *Macaulay 2* [15]. The BMA was later generalized to noncommutative rings [4]. Abbott *et al.* [1] described a modular version of the BMA for the case when $k = \mathbb{Q}$.

There are other algorithms for zero-dimensional ideals which have been developed for particular settings. Farr and Gao presented an algorithm based on a generalization of Newton interpolation in [12]. While the complexity is exponential in the number n of variables, the algorithm has been optimized for the case in which n is small as compared to the number of points. Lederer proposed a method for lexicographic term orders which gives insight into the structure of the Gröbner basis [19].

A recent and exciting development in the theory of Gröbner bases is their use in computational biology. For instance they have been used in the identification of critical points of maximum likelihood functions in phylogenetic-tree reconstruction [16]. Gröbner bases have also been employed as a selection tool for polynomial dynamical systems (PDSs) in the study of gene regulatory networks [18] and protein signal transduction networks [3].

In applications to molecular biology, networks often consist of n biochemicals, such as gene products or metabolites, with changing concentration levels. In [18] a method was proposed to reverse engineer biochemical networks, where the levels are mapped to a finite field $k = \mathbb{F}_p$ for some prime p. In this setting, networks are modeled as PDSs, which generalize the widely studied Boolean networks (see [17] for an introduction). Concentration levels are recorded in a vector in k^n, and the data consists of input-output pairs $(s_i, s_{i+1}) \in k^n \times k^n$, where s_i is a vector describing the state of the network at time i, for $i = 1, \ldots, m$. The input vectors can be viewed as an affine variety $V \subset k^n$, and a family of models represented as PDSs is constructed in terms of the vanishing ideal of V. Gröbner bases are then used to select the most parsimonious PDS from this collection. In these applications, the number n is typically in the hundreds to thousands, whereas the number m is at best on the order of tens of measurements.

Below we describe an algorithm for computing Gröbner bases for zero-dimensional ideals (*i.e.*, vanishing ideals) in a polynomial ring R. This algorithm is specialized for the case when the number m of distinct points is much smaller than the number n of variables. In this setting, there are few relations in terms of *essential* variables, that is, variables that are in the support of the standard monomials associated to an ideal. The remaining ones are of the type $x_i - g$ where the leading term x_i is not an essential variable and the support of g has only essential variables. Therefore computation of a Gröbner basis can be restricted to a proper subring of R containing only essential variables. The algorithm identifies these variables and computes relations of the first type using the BMA. The relations of type $x_i - g$ are computed using standard linear algebra techniques. We have implemented the algorithm, which we call EssBM, in *Macaulay 2*.

The paper is organized as follows. First we describe the EssBM algorithm. In Section 3, we provide the theoretical support for the algorithm and include a complexity analysis. In Section 4, we compare its performance to the BMA, as implemented in *Macaulay 2*. We conclude our paper with a discussion of future directions.

2 The EssBM Algorithm

Let $R = k[x_1, \ldots, x_n]$ where k is a field, and $\succeq$ be a fixed term order on R. Consider a variety $V \subset k^n$ of points with multiplicity one and $|V| = m < \infty$. Here we are primarily interested in finite fields, where these conditions will automatically be satisfied for all varieties. The goal of the EssBM algorithm is to construct the reduced Gröbner basis G with respect to $\succeq$ for the ideal $\mathbf{I}(V)$ of points in V and the set $\mathfrak{B}(G)$ of standard monomials associated to G, which forms a basis for the k-vector space $R/\mathbf{I}(V)$. The algorithm constructs a set $EV \subset \{x_1, \ldots, x_n\}$ of *essential variables*, a set SM of monomials on $\{x_1, \ldots, x_n\}$, and subsets GB and Rel of the ring R. We will see below that G will be given by $GB \cup Rel$ and $\mathfrak{B}(G)$ by the set SM. The *support* (defined in the next section) of the elements in SM is the set EV. We let EV_i, SM_i, GB_i, and Rel_i denote the i-th approximations of the corresponding sets.

Initialize each set as follows: $EV_0 = \{\}$, $SM_0 = \{1_R\}$, $GB_0 = \{\}$, and $Rel_0 = \{\}$. Let $[n]$ denote the set $\{1, \ldots, n\}$ and x^a the monomial $x_1^{a_1} \cdots x_n^{a_n}$. For each $i \in [n]$, do the following. Find the i-th smallest variable, say x_i. Suppose there are r monomials $x^{a_1}, \ldots, x^{a_r}$ in SM_{i-1} that are smaller than

x_i in the given ordering. Try to write x_i as a k-linear combination of these monomials. That is, find (if they exist) $c_1, \ldots, c_r \in k$, where

$$\begin{aligned} x_i(1) &= \sum_{j=1}^{r} c_j x^{a_j}(1) \\ x_i(2) &= \sum_{j=1}^{r} c_j x^{a_j}(2) \\ &\cdots \\ x_i(m) &= \sum_{j=1}^{r} c_j x^{a_j}(m) \end{aligned} \tag{1}$$

and $x^a(t)$ is the evaluation of x^a at the t-th point in V for $t \in [m]$. If there are such coefficients, then

$$x_i(t) - \sum_{j=1}^{r} c_j x^{a_j}(t) = 0$$

for every $t \in [m]$ and it follows that $h := x_i - \sum_{j=1}^{r} c_j x^{a_j} \in \mathbf{I}(V) \cap k[EV_{i-1} \cup \{x_i\}]$, where $k[EV_{i-1} \cup \{x_i\}]$ is the polynomial ring in the variables in $EV_{i-1} \cup \{x_i\}$. Since the monomials x^{a_j} were chosen so that $x_i \succeq x^{a_j}$, it follows that x_i is the leading term of an element of $\mathbf{I}(V)$ and so is not a standard monomial. In this case let $Rel_i = Rel_{i-1} \cup \{h\}$. If there is no solution to the system in (1), then x_i is a standard monomial. In this case let $EV_i = EV_{i-1} \cup \{x_i\}$, and compute the Gröbner basis GB_i and the set SM_i of standard monomials for the ideal $\mathbf{I}(V) \cap k[EV_i]$ of the points projected onto the variables in EV_i. When $i = n$, return the sets $G := GB_n \cup Rel_n$ and $\mathfrak{B}(G) := SM_n$.

Below we give pseudo-code for the complete algorithm, which has been implemented in *Macaulay 2*. While the BMA computes *separators* for the points in V in addition to the Gröbner basis and the set of standard monomials, the implementation in *Macaulay 2* does not. In order to appropriately compare the two implementations, we do not include separators in this version of EssBM. However, our algorithm can easily be modified to return the separators at an additional cost of $O(m)$.

For simplicity, let $[x_j(t)]_{t=1}^{m}$ denote the $(m \times 1)$-column vector

$$\begin{pmatrix} x_j(1) \\ x_j(2) \\ \vdots \\ x_j(m) \end{pmatrix}.$$

The EssBM Algorithm

Input: V a variety; $\succeq$ a term order
Output: G the reduced Gröbner basis for $\mathbf{I}(V)$ with respect to $\succeq$;
$\mathfrak{B}(G)$ the set of standard monomials for G

---

1. Initialize: $EV_0 := \{\}$; $SM_0 := \{1_R\}$; $GB_0 := \{\}$; $Rel_0 := \{\}$.
2. For i from 1 to n do
3. $\quad x_i :=$ i-th smallest variable
4. $\quad S := k[EV_{i-1} \cup \{x_i\}]$ with term order $\succeq_S$ induced by $\succeq$
5. $\quad r := |SM_{i-1}|$ and $LM_i := \{x^{a_j} \preceq_S x_i : x^{a_j} \in SM_{i-1}, 1 \leq j \leq r\}$ the standard monomials less than x_i

6. $A_i := (m \times (s+1))$-matrix with $s = |EV_{i-1}|$
   first column $[x_i(t)]_{t=1}^m$ and s columns $[x_j(t)]_{t=1}^m$ for all $x_j \in EV_{i-1}$
7. $Eval_i := (m \times r)$-matrix $(x^{a_j}(p_t))$, where $x^{a_j} \in LM_i$ is evaluated on p_t, the point in row t of A_i
8. If there is a solution $c = (c_1, \ldots, c_r)^T$ to the system of linear equations $Eval_i \cdot c = [x_i(t)]_{t=1}^m$
9. then $Rel_i := Rel_{i-1} \cup \{x_i - \sum c_j x^{a_j}\}$ where $x^{a_j} \in LM_i$
10. else $EV_i := EV_{i-1} \cup \{x_i\}$ and compute GB_i and SM_i in $k[EV_i]$ using the BMA on A_i
11. Return $G = GB_n \cup Rel_n$ and $\mathfrak{B}(G) = SM_n$

The variables in EV_n are called *essential*. The polynomial $x_i - \sum c_j x^{a_j}$ computed in the i-th step of the algorithm has x_i as its leading term since the monomials x^{a_j} were chosen to be smaller than x_i. The variables x_i are called *inessential* since they can be written in terms of essential variables.

3 Theoretical Background

In this section, we provide a detailed proof of the correctness and worst-case time complexity of the EssBM algorithm. Before stating and proving the main results, namely Theorems 5, 7 and 8, we begin with some preliminaries.

Recall that the matrix A_i has rows corresponding to the points in V projected onto the coordinates defined by $EV_i = EV_{i-1} \cup \{x_i\}$. Let P_i be this set of projected points.

For the remainder of this paper, we use the shorthand notation I for the ideal $\mathbf{I}(V)$ and $k[EV_i]$ for the polynomial ring in the variables in the set EV_i. Also, we let $G = GB_n \cup Rel_n$ and $\mathfrak{B}(G)$ the set of standard monomials for G.

Lemma 1. *The equality $\mathbf{I}(P_i) = I \cap k[EV_i]$ holds.*

Proof. This follows immediately from the construction of the ideal $\mathbf{I}(P_i)$. □

Corollary 2. *The set GB_i is the reduced Gröbner basis for the ideal $I \cap k[EV_i]$ with respect to $\succeq$ and SM_i is the set of standard monomials for $I \cap k[EV_i]$ with respect to GB_i. In particular, the statement holds for $i = n$.*

Proof. The sets GB_i and SM_i are the reduced Gröbner basis and the set of standard monomials, respectively, for the ideal $\mathbf{I}(P_i)$ in $k[EV_i]$. From the previous lemma, we have that $\mathbf{I}(P_i) = I \cap k[EV_i]$. Hence the result follows. □

Let $f \in R$ be a polynomial. We define the *support* of f, denoted by $supp(f)$, to be the set of variables that appear in f. By construction, $supp(f)$ is the smallest set $X \subset \{x_1, \ldots, x_n\}$ such that $f \in k[X]$. The *support* of a set of polynomials S is the union over the support of each polynomial $g \in S$. Let $LT(f)$ denote the leading term of f with respect to a given term order. The *tail* of f is the polynomial $tail(f) := f - LT(f)$.

Lemma 3. *Let $f \in R$ be such that $supp(f) \subset EV_n \cup \{x_{\beta_1}, \ldots, x_{\beta_s}\}$ where $x_{\beta_1} \prec \cdots \prec x_{\beta_s}$ are inessential variables. Suppose that $supp(LT(f)) \subset EV_n$. Then there is $f^* \in R$ such that $supp(f^*) \subset EV_n \cup \{x_{\beta_1}, \ldots, x_{\beta_{s-1}}\}$, the polynomial f^* has the same leading term as f, and $f - f^* \in I$.*

Proof. Consider the largest inessential variable x_{β_s}. We can write

$$f = LT(f) + \sum_{i=0}^{r} (x_{\beta_s})^i h_i$$

where $supp(h_i) \subset EV_n \cup \{x_{\beta_1}, \ldots, x_{\beta_{s-1}}\}$. As x_{β_s} is an inessential variable, there is an element $x_{\beta_s} + g$ of Rel_n with leading term x_{β_s}. Note that $supp(g) \subset EV_n$. Define the polynomial f' from f by replacing each $(x_{\beta_s})^i$ with $-(x_{\beta_s})^{i-1} g$:

$$f' = LT(f) - \sum_{i=0}^{r} (x_{\beta_s})^{i-1} g h_i.$$

Then

$$f - f' = \sum_{i=0}^{r} \left((x_{\beta_s})^i + (x_{\beta_s})^{i-1} g \right) h_i \in I$$

since $(x_{\beta_s})^i + (x_{\beta_s})^{i-1} g = (x_{\beta_s})^{i-1}(x_{\beta_s} + g) \in I$. As $LT(f) \succ x_{\beta_s} \succ LT(g)$, we have that $LT(f') = LT(f)$. Let f^* be the polynomial obtained after r replacements of x_{β_s}. Note that we have $f - f^* \in I$ and $LT(f^*) = LT(f)$. Since we have replaced all occurrences of x_{β_s}, it follows that $supp(f^*) \subset EV_n \cup \{x_{\beta_1}, \ldots, x_{\beta_{s-1}}\}$. □

This lemma gives us a way of removing inessential variables from a polynomial in I without affecting its leading term, which will be useful for proving the correctness of EssBM (Theorems 5 and 7). In fact, we can remove *all* inessential variables. We emphasize this fact with the following corollary.

Corollary 4. *Let $f \in R$. Then there is $f^* \in R$ such that $supp(f^*) \subset EV_n$, $LT(f^*) = LT(f)$, and $f - f^* \in I$.*

Theorem 5. *The set G is the reduced Gröbner basis for I with respect to $\succeq$.*

Proof. We first show that $G \subset I$. Consider $g \in G$. If $g \in GB_n$, then $g \in I$. Suppose that $g \in Rel_n$. Then g is of the form $x_i - \sum c_j x^{a_j}$ for some $c_j \in k$ and $x^{a_j} \in R = k[x_1, \ldots, x_n]$. The coefficients c_j were chosen so that $x_i(t) = \sum c_j x^{a_j}(t)$ for all $t \in [m]$. Therefore by construction $g \in I$.

Now let $f \in I$. We must show that there is some $g \in G$ such that $LT(g) \mid LT(f)$. We distinguish two cases.

Case 1: $supp(LT(f)) \not\subset EV_n$.
Suppose that $LT(f)$ contains an inessential variable x_i. By construction of the set Rel_n, there is an element g of $Rel_n \subset G$ with leading term x_i. It follows that $LT(g)$ divides the leading term of f.

Case 2: $supp(LT(f)) \subset EV_n$.
Recall that the set GB_n is a Gröbner basis of the projection of I onto the variables in EV_n (see Corollary 2). If $supp(tail(f))$ is also contained in EV_n, then $f \in k[EV_n]$ and there is a $g \in GB_n \subset G$ whose leading term divides $LT(f)$.
Assume that $supp(tail(f)) \not\subset EV_n$. Using Corollary 4, we can find $h \in I$ such that $supp(f - h) \subset EV_n$ and $LT(f - h) = LT(f)$. Since $f - h \in k[EV_n]$, there is a $g \in GB_n \subset G$ whose leading term divides $LT(f - h) = LT(f)$.

To prove that G is reduced, let $g \neq h \in G$. We wish to show that g and h satisfy the following criterion:

$$LT(g) \text{ does not divide any monomial in } h. \tag{2}$$

We consider the following four cases.

Case 1: $g, h \in GB_n$.
As GB_n is the reduced Gröbner basis for the ideal I projected onto the essential variables, then g, h satisfy (2).

Case 2: $g, h \in Rel_n$.
Let $LT(g) = x_i$ and $h = x_j - \sum_i c_i x^{a_i}$ for $i \neq j$. Note that $supp(h) \subset EV_{j-1} \cup \{x_j\}$. Clearly x_i does not divide x_j. As $supp(tail(h)) \subset EV_n$ and $x_i \notin EV_n$, then x_i does not divide any monomials in $tail(h)$.

Case 3: $g \in GB_n$ and $h \in Rel_n$.
Let $LT(h) = x_i$ for some inessential variable. This will not be divisible by $LT(g)$, which contains at least one essential variable. All other terms x^a of h are standard monomials for the projection of I onto the variables in EV_i; in particular, $supp(x^a) \subset EV_i$. It follows that if $supp(g) \subseteq EV_i$, then $LT(g)$ does not divide any term of h. By Corollary 2, $supp(g)$ contains only essential variables. Thus if $supp(g)$ is not contained in EV_i, then $supp(g)$ must contain a variable x_j with $x_i \prec x_j$. This x_j divides some term x^b of g, and it follows that if $LT(g)$ divides some term x^a of h, then $x_j \preceq x^b \preceq LM(g) \preceq x^a \preceq x_i$, which contradicts the assumption that $x_i \prec x_j$.

Case 4: $g \in Rel_n$ and $h \in GB_n$.
Then $LT(g)$ is some inessential variable, say x_i. However, $supp(h) \subset EV_n$ and so g, h satisfy criterion (2).

□

Next we compute the number of elements in $\mathfrak{B}(G)$ and show the relationship between $\mathfrak{B}(G)$ and the set SM_n.

Lemma 6. *The set $\mathfrak{B}(G)$ has $|V|$ elements.*

The previous lemma is usually stated for algebraically closed fields k and proved with the help of the Strong Hilbert Nullstellensatz (see [11]). We include a proof of the statement for the case where all points have multiplicity one, as is being assumed throughout the paper.

Proof. Suppose $V = \{a_1, \ldots, a_m\}$ and define $I_i := \mathbf{I}(\{a_i\})$. Then $I = \mathbf{I}(\bigcup_{i=1}^m \{a_i\}) = \bigcap_{i=1}^m I_i$, since each point a_i has multiplicity one. Note that each of the ideals I_i is maximal and it follows that they are pairwise comaximal. Consider the quotient ring R/I. By the Chinese Remainder Theorem, there is a ring homomorphism such that

$$R/I \cong R/I_1 \times \cdots \times R/I_m.$$

As each I_i is maximal, then each $R/I_i \cong k$ and it follows that $R/I \cong k^m$, as rings. Further, the quotient ring and k^m can be viewed as k-vector spaces, and the isomorphism can be extended to an isomorphism of vector spaces. Hence, the dimension of R/I as a vector space is $dim_k(R/I) = m$. Since $\mathfrak{B}(G)$ forms a basis for the vector space R/I (Proposition 2.1.6 in [2]), we conclude that $|\mathfrak{B}(G)| = m = |V|$. □

Theorem 7. *The set SM_n is the set of standard monomials for I with respect to G.*

Proof. By Corollary 2, we have that SM_n is the set of standard monomials for the ideal $I \cap k[EV_n]$ with respect to the Gröbner basis GB_n. As V has finitely many points, then $|\mathfrak{B}(G)| = |V|$. Consider a monomial $x^a \in \mathfrak{B}(G)$. If $x^a \notin k[EV_n]$, then it contains an inessential variable, say x_i. As x_i is the leading term of an element in $Rel_n \subset I$, it is not a standard monomial for G, contradicting the assumption that $x^a \notin \mathfrak{B}(G)$. Therefore $x^a \in k[EV_n]$.

By construction, $x^a \notin LT(I)$. Using the set-containment relation

$$LT\left(I \cap k[EV_n]\right) \subset LT(I),$$

it follows that $x^a \notin LT(I \cap k[EV_n])$ and so $\mathfrak{B}(G) \subset SM_n$. To see equality, note that the set P_n of projected points defined by EV_n has at most as many points as V. Then $|SM_n| = |P_n| \leq |V| = m$. Since $\mathfrak{B}(G) \subset SM_n$, it follows that $m = |\mathfrak{B}(G)| \leq |SM_n| \leq m$. Hence $\mathfrak{B}(G) = SM_n$; that is, SM_n is the set of standard monomials for I with respect to G. □

We conclude this section with a complexity analysis of EssBM.

Theorem 8. *The EssBM algorithm terminates and has worst-time complexity $O(nm^3) + O(m^5)$, which is dominated by $O(nm^3)$ when $m \ll n$.*

Proof. We compute the complexity of each step and then provide a summary at the end. Step 1 has complexity $O(1)$. In Step 2, the algorithm enters a loop of length n. Steps 3-8 are executed in each iteration of the loop. They have the following complexities:

Step 3. $O(1)$: Executing this step requires constant time since the variable order, given as part of the declaration of the term order, is maintained in one array.

Step 4. $O(m^2)$: This step may not even be required by all implementations; if required, it involves passing $O(m^2)$ variables to a new object of size $O(m^2)$.

Step 5. $O(m^3)$: As term orders are typically stored as matrices, in this case the term order $\preceq_S$ is a matrix of dimension $O(m^2)$. Determining the order between two monomials of S requires multiplication of a vector of length $O(m)$ by this matrix. So for each monomial $x^a \in SM_{i-1}$, there are at most m^2 operations required for comparing x_i to x^a and there are at most m such monomials.

Step 6. $O(m)$: An $(m \times 1)$-column vector is added to a matrix with columns corresponding to the variables in EV_{i-1}.

Step 7. $O(m^3)$: As there are at most m variables in each monomial and at most m^2 entries in the matrix, the cost of executing this step is $O(m^3)$.

Step 8. $O(m^3)$: Solving a linear system of m equations in $r \leq m$ unknowns requires $O(m^3)$ time.

Step 9 has complexity $O(1)$ and will be executed at most n times.

Since there can be at most m essential variables, Step 10 will be executed at most m times. The complexity of each execution of Step 10 is $O(m^4)$: Updating EV_i is a constant operation. However, computing GB_i and SM_i for the matrix A_i is associated to the cost of calling the BMA, which is $O(nm^3 + n^2m^2)$ ([20]; for a synopsis, see [1, 21, 22]). In this case, the numbers of points and required variables are given by the dimensions of A_i. Since both row and column dimensions are bounded above by m, it follows that the complexity of executing this step is $O(m^4)$.

Step 11 has complexity $O(n + m^2)$: Note that there are $O(m^2)$ elements in GB_n (see [20]), $O(n)$ relations in Rel_n, and m monomials in SM_n. So returning these sets requires $O(n+m^2+m)$ operations.

Hence, we can calculate the total complexity $C(EssBM)$ of the algorithm as follows:

$$\begin{aligned} C(EssBM) &= O(1) + O(n)\left[O(1 + m^2 + m^3 + m + m^3 + m^3 + 1)\right] + O(m)O(m^4) + O(n + m^2 + m) \\ &= O(nm^3) + O(m^5). \end{aligned}$$

When $m \ll n$, then $O(nm^3)$ becomes the dominating term and the above estimate reduces to

$$C(EssBM) = O(nm^3).$$

□

4 Performance of the EssBM Algorithm

To test the performance of our algorithm, we compared its run-time to that of the BMA[1], as implemented in *Macaulay 2*, on randomly generated varieties in k^n. For this analysis, we let the field k be $\mathbb{F}_p$ for $p \in \{3, 17\}$. Since the complexities of the two algorithms depend on m and n, we chose a range of values for these parameters, namely, $m \in \{5, 10, 15\}$ and $n \in \{100, 150, 200, 250, 300\}$. For each set of parameters p, m, and n, we generated 10 varieties using a built-in random number generator in *Macaulay 2*, without specifying prior constraints on the relative position of the points in the variety. We performed this experiment using two term orders: a lexicographic order (*lex*) and a graded reverse lexicographic order (*grevlex*), each with the same variable order.

Figures 1 and 2 show the run-times for the two algorithms for $p = 3$ and $m = 5, 15$. As the run-times for $m = 10$ fall between the $m = 5$ and $m = 15$ settings, we omitted them from the plots. We display the results for all parameters settings in the appendix. The run-times for $p = 17$ are similar.

As a measure of the stability of the run-time data, we computed the *coefficient of variation*, defined to be the ratio of the standard deviation to the mean of the data. For the *grevlex* experiments, this coefficient ranges from 0.004 to 0.2, whereas for the *lex* experiments it ranges from 0.01 to 0.1. Since this implies very low variability of the run-times for fixed p, n, and m, we displayed only mean values in Figures 1 and 2.

The empirical results corroborate our theoretical prediction that for $m \ll n$, the EssBM algorithm outperforms the BMA. For small n, however, we observe that EssBM is slower, which we attribute to the overhead costs associated to multiple calls to the BMA.

5 Discussion

Recently, applications of Gröbner bases as a promising model selection tool in molecular biology have been proposed [3, 18]. These applications require computation of a Gröbner basis for a zero-dimensional

[1]The Buchberger-Möller algorithm has been implemented as the function *points* in the "Points" package of *Macaulay 2* distribution version 0.9.8.

ideal $\mathbf{I}(V)$ in a polynomial ring $k[x_1, \ldots, x_n]$, where $|V| = m \ll n$. Previously, no algorithms for computing Gröbner bases optimized for $m \ll n$ had been available. The run-time of the existing implementations was a bottleneck in applications of the methods in [3] and [18] to data sets whose size is of the order typical for biochemical data sets such as microarray data.

The EssBM algorithm presented here goes some way towards alleviating this problem in that it reduces the worst-case complexity, which is $O(nm^3+n^2m^2)$ for the standard Buchberger-Möller algorithm, to $O(nm^3)$ for $m \ll n$. Our implementation and testing indicate that for a small number of distinct points in general position, EssBM starts outperforming a standard implementation of the BMA when the number of variables exceeds 200. This should make it possible to use the methods of [3] and [18] for analysis of larger data sets than was hitherto possible. Unfortunately, the worst-time complexity estimate $O(nm^3 + m^5)$ of the EssBM algorithm suggests that it may still be infeasible for moderately large m. We are currently working on a related algorithm that would further reduce this complexity.

6 Acknowledgements

We wish to thank Luis García-Puente and an anonymous reviewer for their valuable comments.

This research was done during the visit of WJ to the Mathematical Biosciences Institute in the academic year 2006/2007 and supported by the National Science Foundation under Agreement No. 0112050.

References

[1] J. Abbott, A. Bigatti, M. Kreuzer, and L. Robbiano, *Computing ideals of points*, Journal of Symbolic Computation **30** (2000), no. 4, 341–356.

[2] W. Adams and P. Loustaunau, *An introduction to Gröbner bases*, Graduate Studies in Mathematics, vol. 3, American Mathematical Society, 1994.

[3] E. Allen, J. Fetrow, L. Daniel, S. Thomas, and D. John, *Algebraic dependency models of protein signal transduction networks from time-series data*, Journal of Theoretical Biology **238** (2006), 317–330.

[4] M. Alonso, M. Marinari, and T. Mora, *The big mother of all dualities: Möller Algorithm*, Communications in Algebra **31** (2003), no. 2, 783–818.

[5] E. Arnold, *Modular algorithms for computing Gröbner bases*, Journal of Symbolic Computation **35** (2003), no. 4, 403–419.

[6] B. Buchberger, *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenrings nach einem nulldimensionalen Polynomideal*, PhD thesis, Universität Innsbruck, 1965.

[7] ———, *A note on the complexity of constructing Groebner-Bases*, Computer Algebra: Proceedings of EUROCAL 83 (J. von Hulzen, ed.), Lecture Notes in Computer Science, vol. 162, Springer Berlin, 1983, pp. 137–145.

[8] B. Buchberger and H.M. Möller, *The construction of multivariate polynomials with preassigned zeroes*, Computer Algebra: EUROCAM '82 (J. Calmet, ed.), Lecture Notes in Computer Science, vol. 144, Springer Berlin, 1982, pp. 24–31.

[9] M. Caboara, M. Kreuzer, and L. Robbiano, *Efficiently computing minimal sets of critical pairs*, Journal of Symbolic Computation **38** (2004), no. 4, 1169–1190.

[10] CoCoATeam, CoCoA*: A system for doing Computations in Commutative Algebra*, Available at `http://cocoa.dima.unige.it`, 2006.

[11] D. Cox, J. Little, and D. O'Shea, *Using algebraic geometry*, 2nd ed., Springer Verlag, New York, 2005.

[12] J. Farr and S. Gao, *Computing Gröbner bases for vanishing ideals of finite sets of points*, Applied Algebra, Algebraic Algorithms and Error-Correcting Codes: 16th International Symposium, AAECC-16 (M. Fossorier, H. Imai, S. Lin, and A. Poli, eds.), Lecture Notes in Computer Science, vol. 3857, Springer Berlin, 2006, pp. 118–127.

[13] J.-C. Faugére, *A new efficient algorithm for computing Gröbner bases (F4)*, Journal of Pure and Applied Algebra **139** (1999), 61–88.

[14] ———, *A new efficient algorithm for computing Gröbner bases without reduction to zero (F5)*, Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation (Lille, France), ACM Press, 2002, pp. 75–83.

[15] D. Grayson and M. Stillman, *Macaulay 2, a software system for research in algebraic geometry*, Available at `http://www.math.uiuc.edu/Macaulay2`, 2006.

[16] S. Hoşten, A. Khetan, and B. Sturmfels, *Solving the likelihood equations*, Foundations of Computational Mathematics **5** (2005), 389–407.

[17] S. Kauffman, *Origins of order: Self-organization and selection in evolution*, Oxford University Press, 1993.

[18] R. Laubenbacher and B. Stigler, *A computational algebra approach to the reverse engineering of gene regulatory networks*, Journal of Theoretical Biology **229** (2004), 523–537.

[19] M. Lederer, *The vanishing ideal of a finite set of closed points in affine space*, Available at `http://arxiv.org/abs/math/0604133`, 2006.

[20] M. Marinari, H.M. Möller, and T. Mora, *Gröbner bases of ideals defined by functionals with an application to ideals of projective points*, Applicable Algebra in Engineering, Communication and Computing **4** (1993), 103–145.

[21] T. Mora and L. Robbiano, *Points in affine and projective spaces*, Computational Algebraic Geometry and Commutative Algebra, Cortona-91 (D. Eisenbud and L. Robbiano, eds.), Symposia Mathematica, vol. 34, Cambridge University Press, 1993, pp. 106–150.

[22] L. Robbiano, *Gröbner bases and statistics*, Gröbner Bases and Applications (New York) (B. Buchberger and F. Winkler, eds.), London Mathematical Society Lecture Notes Series, vol. 251, Cambridge University Press, 1998, pp. 179–204.

Appendix

Figure 1: Run-times averaged over 10 randomly generated varieties for $p = 3$ and *lex*.

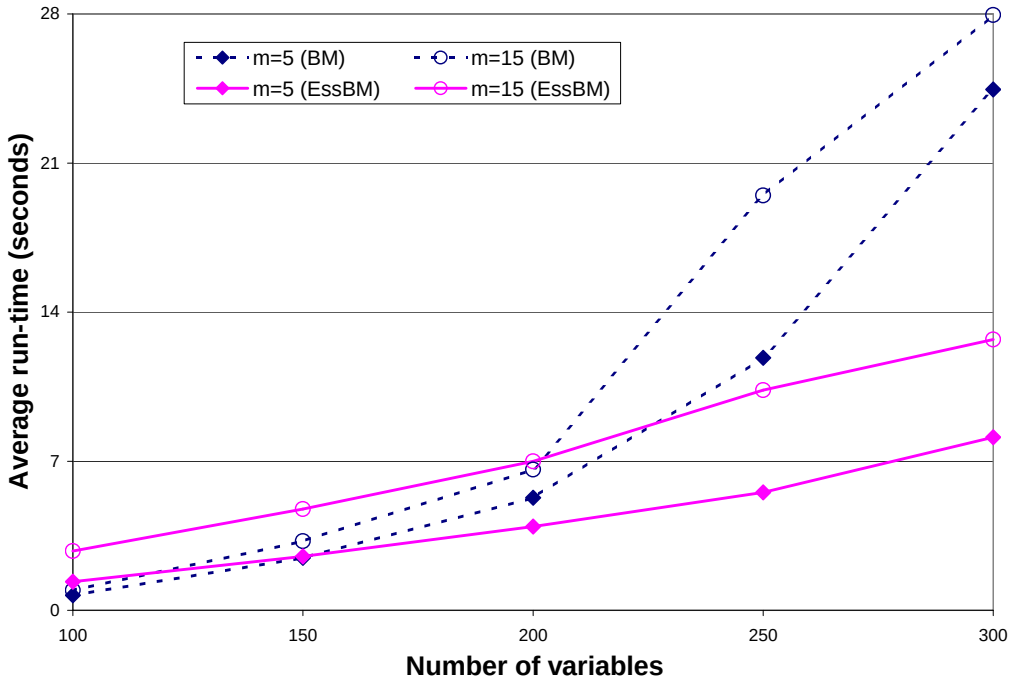


Figure 2: Run-times averaged over 10 randomly generated varieties for $p = 3$ and *grevlex*.

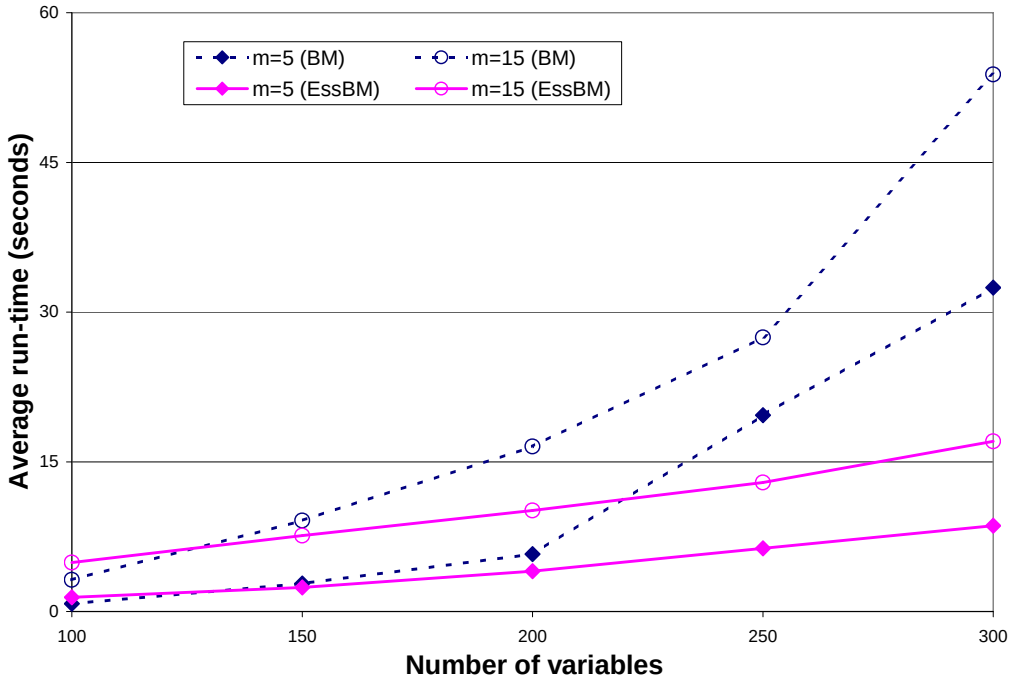


Figure 3: Run-times for 10 randomly generated varieties and *lex*.

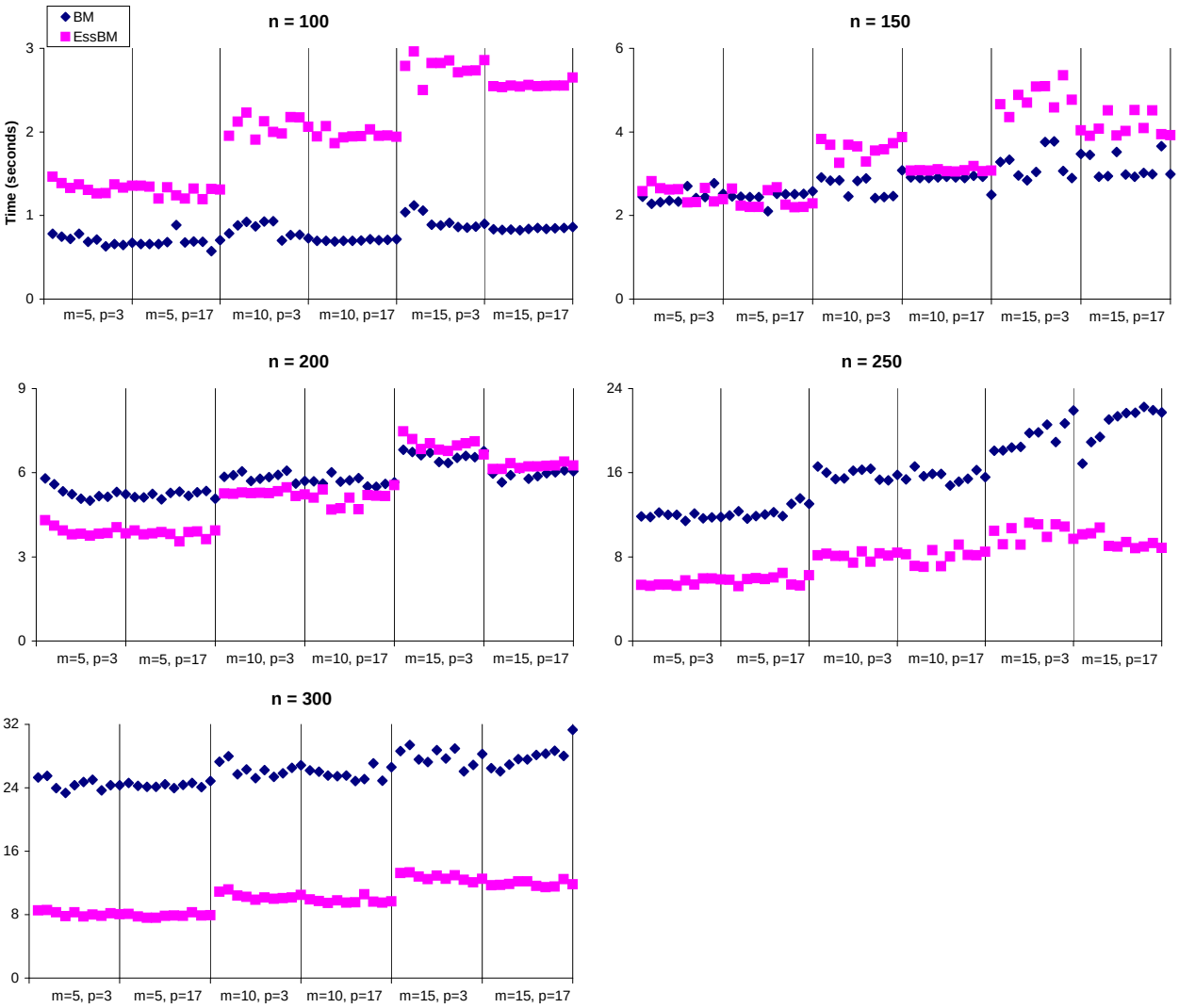
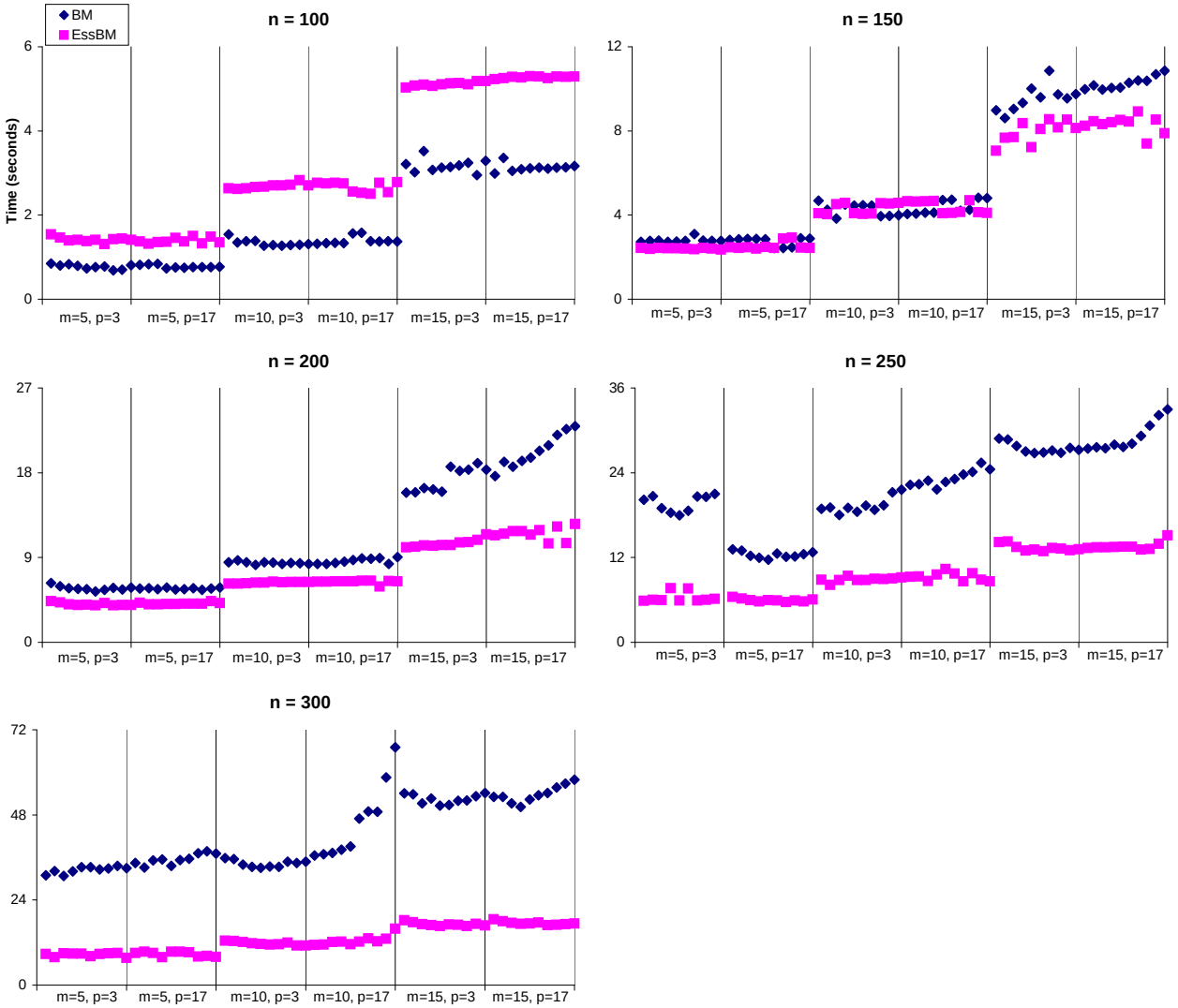


Figure 4: Run-times for 10 randomly generated varieties and *grevlex*.



"Approximate Commutative Algebra" – an ill-chosen name for an important discipline

Hans J. Stetter, Vienna
stetter@aurora.anum.tuwien.ac.at

Classical algebra has always considered itself as a discipline in *Discrete Mathematics*, even when it dealt with objects over the real or complex numbers ($\mathcal{R}$ or $\mathcal{C}$), where the inherent topology of the number fields would have invited the use of analytic tools. A first change occurred only when the models of applied mathematics required the treatment of larger and larger systems of linear equations and the emerging electronic computers permitted the implementation of algorithms with huge data sets. In the rapidly growing "Numerical Linear Algebra", norms and distances, contractive iterations etc. were used as standard tools: Classical linear algebra over $\mathcal{R}$ and $\mathcal{C}$ became embedded into Analysis. (As a consequence, in the 2000 Mathematics Subject Classification of the AMS, "Numerical Linear Algebra" is not listed as a subdiscipline of Algebra but of Numerical Analysis.)

In the 1980's, software systems for algebra began to develop at a large scale: Mathematica and Maple have become widely used general-purpose systems while other systems deal with more specialized areas. But to the distress of application scientists using polynomials and other algebraic relations in their models, none of these systems admitted the use of *floating-point data* within algebraic computations. Finally, the resulting pressure began to erode the resistance of algebraists against numerical operations in algebraic algorithms: Slowly, the conceptual background for the use of data with limited accuracy is now considered in polynomial algebra and algorithms with such data are implemented.

Obviously, this is no longer a mere subdiscipline of Commutative Algebra; so what should it be called. The natural analog to Numerical Linear Algebra, viz. "Numerical Commutative Algebra" has, perhaps, sounded too anti-algebraic for an algebraically trained mind. In any case, a recent workshop exclusively devoted to this new area[1] was named "Approximate Commutative Algebra"! And it appears that the word "approximate" is becoming popular amongst computational algebraists in the context of data with limited accuracy. In my opinion, this is *unfortunate* and *should not be continued*; in the remainder of this article, I will explain my reasons.

First of all, the connection of the word "approximate" with a mathematical discipline is antithetic; there can be approximate solutions of some mathematical problem but an approximate mathematical theory is a contradiction in itself! Let us again consult the 2000 MSC: There appears **no "approximate" mathematical discipline** in that voluminous overview of all of mathematics. Also, to my knowledge, the term "approximate linear algebra" has never been seriously proposed or used. So why should the analogous embedding into analysis of commutative algebra over numerical fields be ear-marked in this way, which may lead to serious misinterpretations by outsiders.

In order to support the natural alternate name "Numerical Commutative Algebra" and to discourage the use of "approximate" in connection with algebraic objects, I will shortly display the character of Numerical

[1] Workshop B1 of the Special Semester on Gröbner bases and related methods, Univ. Linz, Feb. 2006

Linear Algebra; then I will show that the new nonlinear algebraic discipline is an immediate analog. So what is Numerical Linear Algebra (NLA):

NLA is Linear Algebra (LA) over the real or complex numbers, with a *transfer of their natural topology.* This topology is associated with the *data* of the discipline, *not with its objects*! All technical terms from LA retain their their full meaning in NLA: Linear space, basis, linear (in)dependence, linear transformation, etc. etc. However, since an n-dimensional linear space L over $\mathcal{R}$ is isomorphic with some $\mathcal{R}^n$, there is now a topology *within* L: Elements (points) have neighborhoods, two elements have a distance, an element can be a good approximation of another one, etc. And an approximation to a requested element can be *successively improved*, iterative algorithms become a natural tool.

The constructive problems to be solved are the same as in LA; but through their data, these problems are conceived as embedded into a *continuous* metric setting. This widens the scope for their treatment immensely. And, as an important consequence, the analytic embedding permits the consideration of the problems for *data with a finite accuracy* (approximate *data*). Due to the underlying linear structure, most of these extensions are straightforward and have become standard by now. While textbooks on LA and on NLA appear very different at a first glance, their contents can really be related readily by the described analytic embedding.

I claim that the transition from Commutative Algebra (CA) to "Numerical Commutative Algebra" (NCA) (rather than "Approximate Commutative Algebra") is fully analogous to that from LA to NLA: We consider areas of commutative algebra not over arbitrary fields or rings but over the analytically structured fields of the real or complex numbers, and we transfer their metric into our considerations.

The numerical computation of zeros of univariate polynomials or of systems of multivariate polynomials has followed this approach for a long time: With current software and hardware, approximate zeros of huge polynomial systems are generated on the spot. But Newton's method and its variants have always been considered as analytic not as algebraic procedures. Commutative algebra, on the other hand, considers the *complete zero set* of the *polynomial ideal* defined by a polynomial system.

The translation and extension of this intrinsically algebraic approach into NCA requires – in the end – the design of an algorithm which analyzes the structure of the ideal and computes approximations for *all* zeros of the polynomial ideal to a requested accuracy, or to the meaningful accuracy permitted by approximate data. Note that this goal goes far beyond the potential of CA where generally the algorithmic generation of a Groebner basis is as far as one can proceed, even for integer coefficients.

When we strive to use and extend classical CA for real or complex coefficients in this way, we must be very careful with our concepts and terminology. What should be the meaning of an "approximate polynomial"? As a mathematical object, we must represent a polynomial with (some) coefficients of specified limited accuracy by the *set* of all polynomials which round to our given polynomial. Obviously, at the specified level of accuracy, the polynomials in this set are *indistinguishable*; but each member of the set is an ordinary polynomial in the classical sense and obeys the classical rules. Because it does not carry a connotation, a term like "empirical polynomial" is much preferable to describe such an object.

An algebraic assertion about an empirical polynomial is true if it is true *in the classical sense* for some polynomial in the set: A number is a zero of an empirical polynomial if it is an *exact* zero of one of its indistinguishable polynomials, and a given empirical polynomial is a member of a specified polynomial ideal if there is some polynomial within the set which is *strictly* in the ideal, etc. Thus the indetermination remains exclusively in the data and does not affect the mathematical structure. This corresponds directly to analogous notions in NLA where, e.g., a vector x with components of limited accuracy lies in a specified linear space if some vector which rounds to x is strictly in this space.

A good example of the misleading potential of "approximate" mathematical objects is displayed by the term "approximate vanishing ideal" which I have recently seen used. While some polynomial may "nearly vanish" on a set of empirical points in some $\mathcal{R}^n$, the ideal of several such polynomials will mostly contain polynomials *without* that property.

In my book[2] , there are many examples which show that the mathematically consistent extension of concepts in CA to NCA requires the same considerations and steps as the extension from LA to NLA. Because this extension is less straightforward in the nonlinear case, it appears particularly important to retain the meaning of the classical algebraic concepts and not to blur the situation by attaching the word "approximate" to them. In particular, the principal analogy with NLA should be emphasized by calling the new emerging discipline "*Numerical* Commutative Algebra".

[2]Numerical Polynomial Algebra, XVI + 472 pp., SIAM Publ., Philadelphia, 2004

ISSAC 2006 Poster Abstracts

Communicated by
Zhendong Wan

Dimension vector and the size of the formal solution space of system of PDEs

Mei Jianqin and Zhang Hongqing
Department of Applied Mathematics
Dalian University of Technology
Dalian 116024 P.R.China

meiqin-303@sohu.com
zhanghq@dlut.edu.cn

In a sense, knowing what is big and what is small is more important than being able to solve partial differential equations. Combining the standard form in the Riquier-Janet theory and Cartan character in Cartan-Kähler theory, a new definition about the dimension of solution space has been put forward. The size of formal solution space measured by a dimension vector, which can be uniquely determined independence of ordering and compatible with physical problem.

Small, Browser-Based Computer Algebra Systems

Markus A. Hitz
North Georgia College & State University
Dahlonega, GA 30597, USA

mahitz@ngcsu.edu

Recent versions of web browsers, such as Mozilla Firefox, natively support major parts of the Scalable Vector Graphics (SVG), and the Mathematical Markup Language (MathML) standards. Both languages are defined in XML, as is the latest version of HTML (XHTML). Objects that are created in one of these languages reside in separate XML namespaces within the tree defined by the Document Object Model (DOM). They can be accessed and manipulated through JavaScript programs that can modify, create, or delete entries in the DOM tree. The combination of scripts and XML data structures enables us to build small computer algebra systems that include graphics (2D and 3D plots), basic symbolic capabilities, and formatted output of mathematical objects. Small systems can be used, either embedded in web pages, or as special purpose applications. They can be tailored to individual needs in presentations, or for on-line instruction.

We investigate the special challenges that implementors of such systems have to face. JavaScript is an interpreted language with limited support of object-oriented programming. Therefore, we cannot expect to see the kind of performance we would get from optimized C++ computer algebra libraries. However, general purpose computer algebra systems also use command-interpretation as the main interaction with users. Unlike Java or C++, JavaScript bases its object-oriented constructs on "prototypes" (as opposed to classes). Furthermore, inheritance and typing are severely limited. On the other hand, its simple interface to DOM elements makes it extremely powerful, and provides intuitive tie-ins for developers.

We began to port a small computer algebra system, JSCL-Meditor, from Java to JavaScript. It was originally designed to be a MathML-editor. In the meantime, it evolved into a system with limited symbolic capabilities that can run on small platforms, such as PDAs. We intend to keep most of the modules, while improving support of content-MathML and adding SVG-based graphics components. We consider our implementation to be a first proof-of-concept for a client-side system. We will continue to add modules and user interfaces that allow for improved interaction with graphical, and geometrical objects.

References

[1] `http://www.w3.org/TR/SVG11/`, Scalable Vector Graphics.

[2] `http://www.w3.org/TR/MathML2/`, MathML version 2.0.

[3] `http://jscl-meditor.sourceforge.net/`, the JSCL-Meditor project.

Abstracts of Special Session on Differential Algebra American Mathematical Society, Eastern Section Spring Meeting

Stevens Institute of Technology
April 14–15, 2007

Communicated by
William Sit
Dept. of Math., The City College of The City University of New York (wyscc@sci.ccny.cuny.edu)

The Special Session on Differential Algebra of the American Mathematical Society (AMS) Eastern Section Spring Meeting, will be held on April 14–15, 2007 at Stevens Institute of Technology, New Jersey, USA. The following abstracts of invited speakers at this Special Session have been edited for reproduction by kind permission of AMS. With some exceptions, they are listed in alphabetical order by presenters. For all abstracts, only the email contact information of the presenter is given. The Special Session is jointly organized by the Kolchin Seminar in Differential Algebra of the City University of New York and the Department of Mathematics and Computer Science at Newark Campus of Rutgers, the State University of New Jersey. For further information, please visit site below.

`http://www.sci.ccny.cuny.edu/~ksda/ams.html`

Galois Theory and Spectral Theory

A Preliminary Report

Primitivo B. Acosta-Humanez
Dept. of Appl. Math., Technical University of Catalonia, Barcelona, Spain (primitivo.acosta@upc.edu)

The aim of this talk is to show an application of Differential Galois Theory in Spectral Theory. In a particular case, we analyze the integrability and the Galois groups of the stationary Schroedinger equation. For example, if the potential is a polynomial, then the Galois group of the Schroedinger equation is a connected non abelian group. On the other hand, if the potential is not a rational function, but there exists a hamiltonian change of variable, then we can algebrize the differential equation preserving the identity component of the Galois group in the original Schroedinger equation: this is the case of Lame equation and Mathieu equation. Finally, we can generate families of Schroedinger equations using the Darboux transformation, Kovacic algorithm and operators theory, where the principal fact is that the Darboux transformation is covariant, isogaloissian and isospectral transformation. This fact plays an important role in quantum mechanics.

Symplectic Properties of the Space of Differential Equations in the Space of Logarithmic Systems

Jonathan Alexander Aïdan
175, rue Chevaleret, Bureau 7C08, 75013 Paris, France (aidan@math.jussieu.fr)

Let $n \geqslant 1$, let S be a finite set of points of the Riemann sphere, and let $\mathcal{M}$ be the moduli space of irreducible fuchsian systems of rank n with logarithmic singularities lying in S and given "generic" local monodromies. This space is

naturally endowed with a symplectic structure ω. Let further $\mathcal{E}$ be the space of irreducible Fuchsian differential equations of order n, with singularities lying in S and same local monodromies. Following a construction of van der Put and Singer, we can locally embed $\mathcal{E}$ as a subspace $\mathcal{N}$ of $\mathcal{M}$. As remarked by N. Katz, the dimension of $\mathcal{N}$ is half the dimension of $\mathcal{M}$. We elaborate on this remark by proving that $\mathcal{N}$ is a Lagrangian subspace of $\mathcal{M}$ relatively to the symplectic structure ω.

Arithmetic Partial Differential Equations

[†]Alexandru Buium and Santiago Simanca

Dept. of Math. and Stat., University of New Mexico, Albuquerque, NM 87131 ([†]buium@math.unm.edu)

We develop an arithmetic analogue of linear partial differential equations in two independent "space-time" variables. The spatial derivative is a Fermat quotient operator, while the time derivative is a usual derivation. This allows us to "flow" integers or, more generally, points on algebraic groups with coordinates in rings with arithmetic flavor. In particular, we show that elliptic curves have certain canonical "arithmetic flows" on them that are arithmetic analogues of the convection, heat, and wave equations. The same is true for the additive and the multiplicative group.

Borel-Laplace Summation of q-Series and Confluence

A Preliminary Report

Lucia Di Vizio

IMJ, Topologie et geometrie algebrique, 175 rue du Chevaleret, 75013 Paris, France (divizio@math.jussieu.fr)

We will explain the issues of confluence for Borel-Laplace summation through some examples. Then we will give a partial answer to the general problem. This is a joint work in progress with Changgui Zhang.

Canonical Representation of Radical Differential Ideals

Oleg Golubitsky

Ontario Research Centre for Computer Algebra and Dept. of C. Sc.,
University of Western Ontario, London, Ontario N6A5B7, Canada (oleg.golubitsky@gmail.com)

For every radical differential ideal, one can compute a decomposition into prime (or characterizable) components, which allows to test ideal membership. This representation of the radical differential ideal is not unique in three respects:

- The components are not unique.
- The representation of each component by a characteristic set is not unique.
- The decomposition and representation of each component depend on the choice of ranking on derivatives.

We will discuss how to make the representation unique, namely:

- A prime decomposition uniquely determined by the radical differential ideal can be computed by extending the algorithm for testing inclusion of quasi-algebraic sets proposed by W. Sit.

- The canonical characteristic set of a prime differential ideal can be obtained by imposing restrictions proposed by F. Boulier et al. We list some of its properties.
- In particular, the canonical characteristic set defines a differential analogue of the Gröbner cone. This will lead us to an algorithm that computes a ranking-independent universal characteristic decomposition of a radical differential ideal.

Local Differential Galois Group and Adjoint Representation

Elie Compoint and †Anne Duval

Cité Scientifique, UFR de mathématiques, 59655 Villeneuve d'Ascq, France (†duval@math.univ-lille1.fr)

We construct a (generally) maximal torus containing the exponential torus and develop an algorithm to reduce the weight subspaces of dimension higher than 1 to root subspaces. We also study the regularity of the exponential torus in the local differential Galois group.

Iterative q-Difference Galois Theory

A Preliminary Report

Charlotte Hardouin

IWR, University of Heidelberg, Im Neuenheimer Feld 368, D-69120 Heidelberg, Germany (charlotte.hardouin@gmail.com)

From the beginning, the Galois theory of q-difference equations has been built for q not equal to a root of unity. This choice was made in order not to increase the field of constants to a transcendental field. However Peter Hendricks has studied this problem for $q^m = 1$ in his Ph. D. work under the supervision of Marius van der Put. He built a fiber functor from the category of q-difference modules over $\mathbb{C}(z)$ with value in the category $\mathrm{Vect}_{\mathbb{C}(z^m)}$ of vector spaces of finite dimension over $\mathbb{C}(z^m)$. But this construction is not totally satisfying and to stay in the spirit of Kolchin, we do not want to have such transcendental base fields for Galois groups.

For q-difference theory, the problem is not the characteristic but the roots of unity. Inspired by the work of B. H. Matzat and Marius van der Put for differential Galois theory in positive characteristic, we consider also a family of *iterative difference operators* instead of considering just one difference operator, and by this way we avoid increasing the constant field, succeed to set up a Picard-Vessiot Theory for q-difference equations where q is a root of unity, and relate it to a Tannakian approach.

Patching and Differential Galois Groups

A Preliminary Report

‡David Harbater and †Julia Hartmann

‡Dept. of Math., University of Pennsylvania, 209 S. 33rd Street, Philadelphia, PA 19104-6395

†IWR, University of Heidelberg, Im Neuenheimer Feld 368, D-69120 Heidelberg, Germany (†julia.hartmann@iwr.uni-heidelberg.de)

Patching methods (building a global object by building it locally) are an important tool for solving inverse problems in classical Galois theory. In this talk, we describe a new formulation of patching over fields, which can be used to patch differential modules. We explain applications to the realization of differential Galois groups.

Differential Central Simple Algebras and Non-Commutative Picard-Vessiot Cocycles

[†]Lourdes Juan and [‡]Andy R. Magid

[†]Dept. of Math., Texas Tech University, Box 1042, Lubbock, TX 79410

[‡]Dept. of Math., University of Oklahoma, Norman, OK 73019 ([†]lourdes.juan@ttu.edu)

Let K be a differential field of characteristic zero with algebraically closed subfield of constants C. A differential central simple algebra, and in particular a differential matrix algebra, over K is trivialized by a Picard-Vessiot extension E of K. This yields a bijection between isomorphism classes of differential algebras and Picard-Vessiot cocycles $Z^1(G(E/K), PGL_n(C))$ which cobound in $Z^1(G(E/K), PGL_n(E))$. We will prove these results and illustrate how the differential Brauer group of an algebraically closed field can be non trivial.

$\mathbf{PGL_3}$ as a Differential Galois Group

Arne Ledet

Dept. of Math. and Stat., Texas Tech University, Lubbock, TX (arne.ledet@ttu.edu)

A Picard-Vessiot extension M/K with differential Galois group G is the function field of a G-torsor. The G-torsors are classified by the non-Abelian cohomology $H^1(K, G)$. In cases where this cohomology can be suitably 'parametrised', this allows us to describe the structure of the Picard-Vessiot extensions. This approach will be illustrated in the case of the projective linear group PGL_3.

Jacobi's Work on Normal Forms of Differential Systems

A Preliminary Report

François Ollivier

LIX, Ecole polytechnique, 91128 Palaiseau CEDEX, France (francois.ollivier@lix.polytechnique.fr)

In 1866 was first published Jacobi's posthumous paper *The reduction to normal form of a non-normal system of differential equations* (in Latin). A method is given there to compute a normal form of a system $P_i = 0$, using a minimal number ℓ_i of derivatives of P_i. The given bound is generically true and sharp. The ℓ_i may be computed using the algorithm Jacobi gave to compute "Jacobi's bound" on the system order, a forgotten ancestor of Kuhn's Hungarian method for the assignment problem (1955).

He also provides a generic method to eliminate all variables except one, using again as few derivatives as possible, a very interesting result for improving the algorithmic complexity of a resolvent computation.

These are described using the formalism of differential algebra in order to give precise proofs following Jacobi's ideas. The content of some unpublished part of manuscript II/13b (Jacobis Nachlaß, Archiv der Berlin-Brandenburgischen Akademie der Wissenschaften) will also be presented. Jacobi considers there the more general problem of finding all possible normal forms for a given system, giving precise conditions for a system of order n in two variables to have less than $n + 1$ possible normal forms (or characteristic sets) for all orderings.

Dimension of Difference Field Extensions

Alexander B. Levin
Dept. of Math., The Catholic University of America
620 Michigan Ave, NE, Washington, DC 20064 (levin@cua.edu)

In this talk we consider properties of main dimensional characteristics of a finitely generated difference field extension: difference dimension polynomials and the limit degree of the extension. In particular, we show that if the difference transcendental degree of a finitely generated difference field extension G/F is zero, then G contains a subfield H such that the extension G/H is algebraic and H is a finitely generated difference field extension of F with respect to a smaller set of basic translations. We also discuss the relation of the limit degree to the problem of compatibility of difference field extensions.

Subfields of the Complete Picard-Vessiot Closure of a Differential Field

A Preliminary Report

Andy R. Magid
Dept. of Math., University of Oklahoma, 601 Elm Room 423, Norman, OK 73019 (amagid@ou.edu)

The Picard–Vessiot closure $(E)_1$ of a differential field E (differential fields always assumed to have algebraically closed characteristic zero field of constants) is the compositum of all its Picard–Vessiot extensions. If F is a differential field, its complete Picard–Vessiot closure F_∞ is $\cup_{i\geqslant 0}F_i$ where $F_0 = F$ and $F_{i+1} = (F_i)_1$. There is a semi–Galois correspondence between all differential subfields of F_∞ over F and subgroups of the group G of all differential automorphisms of F_∞ over F. We characterize the (differentially) finitely generated subfields of F_∞ (containing F).

Standard Bases in Differential Algebra

Eugueny V. Pankratiev
Dept. of Mechanics and Math., Moscow State University, Leninskie Gory, 1, Moscow, 119992, Russia (epankrat@gmail.com)

Constructive methods in rings of differential polynomials are connected, first of all, with characteristic sets of differential ideals whose theory was developed by Ritt and Kolchin for prime differential ideals. Later it had been extended to a larger class of perfect differential ideals.

In the case of linear partial differential polynomials, this theory may be treated as the theory of Gröbner bases of differential modules, to which all methods and approaches of commutative Gröbner bases are applicable, in particular, the theory of staggered bases by Gebauer and Möller. Specifying some parameters in their algorithm, we obtain Janet's bases, a particular case of involutive bases.

Ollivier and Carra-Ferro proposed a definition of standard bases of differential ideals based on admissible orderings of differential monomials. Unfortunately, this basis is infinite for most of differential ideals (e.g., the ideal $[y^2]$). Investigations in this area had been suspended for a long time.

Zobnin discovered that these bases become finite if, instead of the lexicographic ordering, we consider other orderings of differential monomials. This fact revived the interest in this subject and initiated the study of orderings of differential monomials.

Differential Equations and Frobenius Structures

B. Heinrich Matzat
IWR, University of Heidelberg, Im Neuenheimer Feld 368, D-69120 Heidelberg, Germany (matzat@iwr.uni-heidelberg.de)

The (strong) Frobenius structure for differential equations was introduced by B. Dwork for p-adic differential equations. In the case of positive characteristic the existence of a (strong) Frobenius structure is equivalent to the finiteness of the differential Galois group. This fact can be used, for example, to construct additive polynomials with given Galois group and to develop algebraicity criteria in characteristic zero.

A Generalization of the Riemann-Hilbert Problem

Claude Mitschi
Institut de Recherche, Mathématique Avancée, 67000 Strasbourg, France (mitschi@math.u-strasbg.fr)

We discuss the existence of systems of linear ordinary differential equations with coefficients in $\mathbb{C}(z)$ that satisfy generalized monodromy data at prescribed, possibly irregular, singularities. This inverse problem reduces to the classical Riemann-Hilbert problem if all the singularities are required to be Fuchsian, and to the Birkhoff standard form problem if there are exactly two, one of which Fuchsian, prescribed singularities. This generalized Riemann-Hilbert problem is naturally related to the inverse problem in differential Galois theory over $\mathbb{C}(z)$ as far as one is concerned with the Poincaré rank of the singularities. The talk presents joint work with Stéphane Malekthe and the late Andrey A. Bolibrukh.

O-Minimality and Quantifier Elimination in Some Non Quasi-Analytic Classes

A Preliminary Report

Alexandre Rambaud
Equipe de Logique Mathématique, UFR de Mathématiques, Université Paris 7, France and
Institut de Mathématiques, Avenue du champ de Mars, 6, 7000 Mons, Belgium (alexandre.rambaud@umh.ac.be)

I extend the results of [$R1$] which deal with classes of restricted real quasi-analytic functions, to classes of non quasi-analytic functions.

More precisely, in [$R1$] only classes of functions, C^∞ on a whole compact box of $\mathbb{R}^n$ and quasi-analytic on this box, were considered. Now, we study some well-closed classes of functions, C^∞ on an open bounded box, continuous on the closure of this box and which satisfy a condition of non-degeneration (equivalent to quasi-analycity in the former case), expressed via model theory. For example, certain of these classes come from solutions of differential equations.

I obtain, like in [$R1$], results of o-minimality (which generalize for example those of [$vdDS$]) and of quantifier elimination, which imply in particular, preparation theorems in the considered classes.

[$vdDS$]: L. van den Dries and P. Speissegger, "The real field with convergent generalized power series", Trans. Amer. Math. Soc., 350 (1998), 4377-4421.
[$R1$]: A. Rambaud, "Quasi-analycité, o-minimalité et élimination des quantificateurs", Ph.D. thesis, Université Paris 7, 2005.

Tannakian Formalism for Linear Differential Algebraic Groups

Alexey Ovchinnikov
Dept. of Math., North Carolina State University, Box 8205, Raleigh, NC 27695-8205 (aiovchin@ncsu.edu)

Tannaka's Theorem states that a linear algebraic group G is determined by the category of finite dimensional G-modules and the forgetful functor. We extend this result to linear differential algebraic groups by introducing a category corresponding to their representations and discuss how this category determines such a group.

We also provide conditions for a category with a fiber functor to be equivalent to the category of representations of a linear differential algebraic group. This generalizes the notion of a neutral Tannakian category used to characterize the category of representations of a linear algebraic group.

A Theorem of Sit

[†]Wai Yan Pong and [‡]Matthias Aschenbrenner
[‡]Dept. of Math., Stat., and C. Sc., University of Illinois at Chicago, 851 S. Morgan St. (M/C 249) Chicago, IL 60607-7045
[†]Dept. of Math., California State University Dominguez Hills, 1000 E. Victoria Street, Carson, CA 90747 ([†]wpong@csudh.edu)

In 1975, Sit showed that the set of Kolchin (dimension) polynomials is well ordered by eventual dominance. We will give an order-theoretic proof of this theorem and consider its applications in the model theory of differential fields.

Factorization in Skew Polynomial Rings

Yang Zhang
Department of Mathematical Science, DePaul University, Chicago, IL 60614 (yzhang24@depaul.edu)

Efficient algorithms are presented for factoring polynomials in the skew polynomials over complex number field and quantum planes.

Spectra of Rings Differentially Finitely Generated over a Subring

Dmitry Trushin
Dept. of Mechanics and Math., Moscow State University, Leninskie Gory, 1, Moscow, 119992, Russia (trushindima@yandex.ru)

We consider differential rings that are algebras over the field of rational numbers. We present some ideas that are useful for investigation of such rings.

One of them uses the relation between the spectrum of an arbitrary differential ring and its differential spectrum. We consider pairs of properties. One of them characterizes the spectrum and the other one does it for the differential spectrum. If the first property holds, the other one is satisfied as well. The described pairs of properties allow us to reduce the study of a differential ring to the study of this ring considered as an ordinary ring.

To prove a theorem describing the structure of differential integral domains differentially finitely generated over a subring, we apply results about characteristic sets of differential ideals of the ring of differential polynomials over an integral domain.

The main proved theorems enable us to reduce the proof of propositions in differential algebra to the proof of some propositions of commutative algebra. We distinguish a very dense subset of spectrum with good properties and discuss analogues of differential algebraic varieties. Also, as an illustration of the presented method, some analogues of geometric theorems are proved without using the universal field.

Analytic q-Difference Equations, Universal Rings, and Universal Galois Groups

Marius van der Put

Dept. of Math., University of Groningen, P.O.Box 800, 9700 AV Groningen, Netherlands (mvdput@math.rug.nl)

Let q be a complex number satisfying $0 < |q| < 1$ and let $K = \mathbf{C}(\{z\})$ be the field of the convergent Laurent series. The automorphism ϕ of K given by $\phi(z) = qz$ makes K into a difference field. A difference module is a finite dimensional vector space over K, provided with a bijective map Φ satisfying $\Phi(f \cdot m) = \phi(f) \cdot \Phi(m)$. A difference module has a Picard-Vessiot ring and a (difference) Galois group.

One also considers difference modules over the difference field of the formal Laurent series $\widehat{K} = \mathbf{C}((z))$. For the latter category of modules we will give an explicit description of the universal difference ring and its universal Galois group. For the category of the difference modules over K we present a tentative description of the universal difference ring and its corresponding universal Galois group.

Symbolic-Numeric Computation of Implicit Riquier Bases for PDE

[†]Wenyuan Wu and Greg Reid

Dept. of Appl. Math., University of Western Ontario, London, Ontario N6A5B7, Canada ([†]wwu25@uwo.ca)

Riquier Bases for systems of analytic PDE are, loosely speaking, a differential analogue of Grobner Bases for polynomial equations. They are determined in the exact case by applying a sequence of prolongations and eliminations to an input system of PDE.

We present a symbolic-numeric method to determine Riquier Bases in implicit form for systems which are dominated by pure derivatives in one of the independent variables and have the same number of PDE and unknowns.

The method is successful provided the prolongations with respect to the dominant independent variable have a block structure which is uncovered by Linear Programming and certain Jacobians are non-singular when evaluated at points on the zero sets defined by the functions of the PDE. For polynomially nonlinear PDE, homotopy continuation methods from Numerical Algebraic Geometry can be used to compute approximations of the points.

We give a differential algebraic interpretation of Pryce's method for ODE, which generalizes to the PDE case. A major aspect of the method's efficiency is that only prolongations with respect to a single (dominant) independent variable are made, possibly after a random change of coordinates.

Gröbner Bases in Difference-Differential Modules and Their Applications

Franz Winkler

RISC, J. Kepler Universität, A-4040 Linz, Austria (Franz.Winkler@jku.at)

Recently we have introduced a construction of Gröbner bases for difference-differential (d-d) modules, based on a new concept of generalized term ordering for exponent vectors over the integers. We further investigate the key concept of S-polynomial for such difference-differential bases. We also apply the method to compute the difference-differential dimension polynomial of a d-d module and of a system of linear partial difference-differential equations. This is joint work with M. Zhou of Beihang University in Beijing.

Abstracts of the Second International Workshop on Differential Algebra and Related Topics

Rutgers University at Newark
April 12–13, 2007

Communicated by
William Sit

Dept. of Math., The City College of The City University of New York (wyscc@sci.ccny.cuny.edu)

The Second International Workshop on Differential Algebra and Related Topics will be held on April 12–13, 2007 at the Newark Campus of Rutgers, the State University of New Jersey, USA. It is jointly organized by the Department of Mathematics and Computer Science at Rutgers University at Newark, and the Kolchin Seminar in Differential Algebra of the City University of New York. The abstracts of the tutorial talks to be presented at the Workshop are given below, in alphabetical order by speaker. Interested (especially women, minority, or junior) researchers are encouraged to participate and funding is available. For further information, please visit the site below.

`http://newark.rutgers.edu/~liguo/DARTII/diffalg.html`

Overview of Baxter Algebras

Marcelo Aguiar
Dept. of Math., Texas A & M University, College Station, Texas 77843 (maguiar@math.tamu.edu)

We discuss old and recent results on Baxter algebras, from work of Cartier and Rota in the 60's to current work of Guo and others. We will touch on topics such as Spitzer's identity, Loday's dendriform algebras, and the Yang-Baxter equation, among others.

The Painlevé Equations—Nonlinear Special Functions

Peter A. Clarkson
Institute of Mathematics, Statistics and Actuarial Science, University of Kent, Canterbury, Kent, CT2 7NF, United Kingdom
(P.A.Clarkson@kent.ac.uk)

The six Painlevé equations (P_I–P_{VI}) were first discovered around the beginning of the twentieth century by Painlevé, Gambier and their colleagues in an investigation of nonlinear second-order ordinary differential equations. Recently there has been considerable interest in the Painlevé equations primarily due to the fact that they arise as reductions of the soliton equations which are solvable by inverse scattering. Although first discovered from strictly mathematical considerations, the Painlevé equations have arisen in a variety of important physical applications including statistical mechanics, random matrices, plasma physics, nonlinear waves, quantum gravity, quantum field theory, general relativity, nonlinear optics and fibre optics. Further the Painlevé equations may be thought of a nonlinear analogues of the classical special functions.

In this lecture I will give an introduction to the Painlevé equations. In particular I shall discuss many of the remarkable properties which the Painlevé equations possess including connection formulae, Bäcklund transformations associated discrete equations, and hierarchies of exact solutions.

Hopf Algebras of Labeled Trees and Some Associated Differential Algebra Structures

Robert Grossman

Dept. of Math., Stat., and C. Sc., University of Illinois at Chicago, 851 S. Morgan St. (M/C 249) Chicago, IL 60607-7045 (grossman@uic.edu)

It is well known that the vector space spanned by rooted trees forms a Hopf algebra. We survey several such Hopf algebras and describe some of the their duals. In particular, we consider Hopf algebras H of trees that are labeled by derivations in $\mathrm{Der}(R)$. Here k is a field, R is a commutative k-algebra, and $\mathrm{Der}(R)$ is the Lie algebra of derivations of R.

We describe a construction that gives R an H-module algebra structure and show this induces a differential algebra structure of H acting on R. The construction extends the notion of a R/k-bialgebra introduced by Nichols and Weisfeiler.

This is joint work with Richard Larson.

The Complete Picard-Vessiot Closure of the Constants

Andy R. Magid

Dept. of Math., University of Oklahoma, 601 Elm Room 423, Norman, OK 73019 (amagid@ou.edu)

The compositum of all the Picard-Vessiot extensions of a given base differential field, unlike the algebraic closure of the field, may itself have proper Picard-Vessiot extensions. Iterating this, in general countably many times, produces a differential field that has no proper Picard-Vessiot extensions, and is minimal over the base with this property. This field is called the complete Picard-Vessiot closure. Its group of differential automorphisms over the base controls the differential subfield structure, even though the group is not (pro)algebraic and the correspondence is not a full Galois connection. We will focus on the natural special case when the base field is the (algebraically closed, characteristic zero) field of constants.

Model Theory and Differential Algebra

David Marker

Dept. of Math., Stat., and C. Sc., University of Illinois at Chicago, 851 S. Morgan St. (M/C 249) Chicago, IL 60607-7045 (marker@math.uic.edu)

Many model theoretic phenomena arise naturally in differntial fields. We will describe some model theoretic questions that lead to interesting questions in differential algebraic geometry.

Differential Galois Theory in Positive Characteristic

An Introduction

B. Heinrich Matzat

IWR, University of Heidelberg, Im Neuenheimer Feld 368, D-69120 Heidelberg, Germany (matzat@iwr.uni-heidelberg.de)

We will give an introduction to differential Galois theory in positive characteristic and explain interrelations between Picard-Vessiot extensions in positive characteristic and in characteristic zero. The lecture summarizes work of M. van der Put and the speaker.

Computable Model Theory and Differential Algebra

Russell G. Miller

Dept. of Math., Queens College (CUNY), 65–30 Kissena Blvd., Flushing, New York 11367 (Russell.Miller@qc.cuny.edu)

Model theory is the study of mathematical structures and the extent to which they can be described by statements and formulas. Computable model theory considers the effectiveness of results in model theory: whether they can actually be given or realized by algorithms. For example, a computable field is a field F in which the basic operations of addition and multiplication can be computed algorithmically, and one can then ask whether there exists a *splitting algorithm* for deciding whether a given polynomial in $F[X_1, \ldots, X_n]$ is reducible there.

We will give a tutorial in computable model theory, oriented towards results on fields and towards an audience with no serious background in either computability or model theory. Differential algebra is a natural subject for study by computable model theorists, yet there are precious few results for computable differential fields. (It should be understood that this is not the same thing as *computational* differential algebra, although there certainly should be some relation between the two.) As an example, we will describe Rabin's well-known result that every computable field F has a computable algebraic closure, but that F itself can be a computable subfield of the algebraic closure if and only if there is a splitting algorithm for $F[X]$. One would expect some sort of analogous result for computable differential fields and their differential closures, yet to the speaker's knowledge, no such work has been done.

Computable model theory has always restricted itself to countable structures, since the natural domain for computability is the natural numbers. However, we will present work by the speaker which also considers certain uncountable structures $\mathcal{S}$, called *locally computable* structures, by effectively describing the finitely generated substructures of $\mathcal{S}$, rather than giving a global description of $\mathcal{S}$. This concept was only recently developed and has not as yet been widely applied, but fields and differential fields are natural choices for its use.

Introduction to Symbolic-Numeric Completion Methods for PDE

Greg Reid

Dept. of Appl. Math., University of Western Ontario, London, Ontario N6A5B7, Canada (reid@uwo.ca)

Differential elimination methods apply a finite sequence of differentiations and eliminations to general systems of PDE to extract potent information about their solutions. Much recent progress has been made in the design and implementation of exact algorithms, applying to exact input sytems, by researchers such as Boulier, Hubert, Mansfied, Seiler, Wittkopf and others. Though powerful, such methods cannot be applied to approximate systems, since the strong underlying use of rankings of partial derivatives often induces instability, by forcing such methods to pivot on small quantities.

The talk will be an introduction to the new area of symbolic-numeric methods for completion of PDE. Main features include the focus on geometric methods and the use of Homotopy continuation methods for the detection of new constraints by slicing varieties in jet space with random hyperplanes. Our most recent work on this topic will be presented by Wenyuan Wu at the related AMS Special Session on Differential Algebra.

Differential Dependence and Differential Groups

Michael F. Singer
Dept. of Math., North Carolina State University, Box 8205, Raleigh, NC 27695-8205 (singer@math.ncsu.edu)

I will develop a Galois theory of linear difference equations where the Galois groups are linear differential groups. These groups measure the differential dependence among solutions of linear difference equations. We will show how this theory can be used to prove anew Hölder's Theorem that the Gamma function satisfies no differential polynomial equation, Hardouin's recent results concerning differential dependence of solutions of first order difference equations and new results concerning differential dependence of solutions of higher order difference equations.

Solving Linear Differential Equations

Marius van der Put
Dept. of Math., University of Groningen, P.O.Box 800, 9700 AV Groningen, Netherlands (mvdput@math.rug.nl)

We concentrate on linear differential equations (or differential modules) over the differential field $\mathbb{C}(z)$. The theme, probably introduced by L. Fuchs, is to solve a differential equation in terms of equations of lower order. This problem has led to the highly interesting paper of G. Fano (1900). The work of M. F. Singer opened a new perspective on this theme. We continue this direction and apply the powerful theory of representations of semi-simple Lie algebras in order to obtain a systematic way for solving the problem. This involves differential Galois theory, Tannaka theory, simple algebraic groups and it leads to algorithms.

Solving Second and Third Order Linear ODE's in Terms of Special Functions

Mark van Hoeij
Dept. of Math., Florida State University, Tallahassee, FL 32306 (hoeij@math.fsu.edu)

In this talk an algorithm will be presented for solving any second or third order linear ordinary differential equation with rational function coefficients that is solvable in terms of Bessel, Kummer, or Whittaker functions.

Acknowledgement. The organizers of this Second International Workshop on Differential Algebra and Related Topics (DART-II) gratefully acknowledge partial funding from the National Security Agency, the National Science Foundation, and various offices at the Newark Campus of Rutgers, The State University of New Jersey. Additional funding sources, when confirmed, will be acknowledged in the Workshop program.

AMS Special Session: Computational Algebraic and Analytic Geometry for Low-dimensional Varieties

Communicated by
Mika Seppälä, Tony Shaska, Emil Volcheck

We are pleased to present abstracts from the AMS special session titled "Computational Algebraic and Analytic Geometry for Low-dimensional Varieties" held on January 8, 2007 at the AMS/MAA Joint Mathematics Meetings in New Orleans. We wish to thank the authors and the AMS for their permission to communicate these abstracts here. For more information on this series of special sessions, visit `http://www.AlgebraicCurves.net/` .

The 100th Anniversary of the Uniformization Theorem

Peter Buser (EPFL Lausanne) and Mika Seppälä (Florida State University)

The Uniformization theorem states that every Riemann surface is universally covered by the unit disc, the complex plane or the sphere. This classical theorem has an extremely interesting history. It begins with Riemann's remarkable thesis in 1851 in which not only the concept of a Riemann surface is created but in which we also find the famous Riemann mapping theorem, stating that every bounded simply connected domain in the complex plane is conformally equivalent to the unit disc. For a proof Riemann used the so-called Dirichlet principle which at that time was motivated by physical evidence and which soon afterwards was criticized by Weierstrass as standing on insecure mathematical grounds. Finding a correct proof challenged many a famous mathematician like Schwarz, Klein, Poincaré and Hilbert. At the same time the concept of a Riemann surface evolved and the (yet to prove) Riemann mapping theorem gradually became the Uniformization theorem. In 1906 the Finnish mathematician Severin Johannson used Harnack's inequality to prove the Uniformization theorem under a certain technical hypothesis. Koebe and Poincaré immediately recognized Harnack's inequality as being the number one missing tool in all that preceded and published, independently of each other, a complete proof in 1907. Today we connect the Uniformization theorem with many other famous mathematicians like Ahlfors, Bers or Lehto. And there is still a challenge: Prove an explicit version! This seems to be possible only with numerical and symbolic computational tools and there is much ongoing research in this direction.

The Rees Algebra and the Moving Curve Ideal

David A. Cox (Amherst College)

The method of moving curves was introduced by Sederberg and Chen in 1995 and has been used to solve the implicitization problem. When one considers all moving curves that follow a given curve parametrization, one gets the "moving curve ideal." This ideal is of great interest in commutative algebra, when it is called the "ideal of relations defining the Rees algebra". This talk explored two aspects of this ideal:

First, for most degree four parametrizations, it is possible to construct explicit minimal generators for the moving curve ideal. There are two moving lines of degree two in the parameters, two moving conics of degree one in the parameters, and the implicit equation. Furthermore, these generators are easily computed from the two moving lines using determinants Jouanolou calls "Sylvester forms." The proofs involve local cohomology and local duality.

Second, suppose we have a parametrized curve C of degree n. The classical method to uniformize C uses adjoint curves of degrees $n-1$ or $n-2$. Sendra observed that these curves lie in the moving curve ideal of the parametrization. The conjecture is that *all* linear systems (meaning degree one in the parameters) of moving curves of $n-1$ or $n-2$ consist of adjoint curves. Since adjoint curves are defined in terms of the singularities of C, this indicates an interesting relation between the singularities of C and the moving curve ideal.

Endomorphism Algebras of Abelian Varieties

Arsen Elkin (Colorado State University) and Yuri Zarhin (Pennsylvania State University)

We discuss determination of the absolute endomorphism algebras of abelian varieties by examining the interaction of the action of these algebras and the Galois action on various modules associated with abelian varieties, such as prime-order torsion, Tate modules. In particular, we consider abelian varieties X of dimension $(q-1)/2$ in which the image of the Galois representation on the 2-torsion module X_2 is isomorphic to $\mathrm{PSL}(2,q)$, where $q \equiv \pm 3 \pmod 8$, and the algebra of $\mathbb{F}_2$-endomorphism of X_2 that are Galois invariant is isomorphic to $\mathbb{F}_4$. This implies that the Galois action on the 2-torsion is simple, but not absolutely so, over $\mathbb{F}_2$. The subalgebras of $\mathrm{End}_{\mathbb{F}_2}(X_2)$ that are Galois stable and contain the identity automorphism can then be categorized, and, as a result, so can be the images of the action of the ring of absolute endomorphism on X_2.

Examples are drawn from Jacobian varieties $J(C)$ of hyperelliptic curves $C : y^2 = f(x)$ in characteristic different from 2 with $\deg(f) = q+1$ and the Galois group of the splitting field of $f(x)$ is isomorphic to $\mathrm{PSL}(2,q)$. For example, if such a jacobian has genus 2 and admits multiplication by an order of discriminant congruent to 5 modulo 8 of a quadratic field D over the base field, then the absolute endomorphism algebra of $J(C)$ is either D itself, or the characteristic p of the base field is positive and $X = J(C)$ is supersingular. The latter outcome can be ruled out if p splits in D by lifting the representation of $\mathrm{PSL}(2,q)$ on X_2 given by the Galois action to a representation on the 2-adic Tate module.

Suppose we restrict ourselves to characteristic 0, but allow the dimension to vary. There exists the surjective homomorphism (the restriction) from the Galois group of the 4-division field to the Galois group of the 2-division field over the base field. Consideration of a lifting of this homomorphism allows us to show that X is either absolutely simple, in which case its algebra of absolute endomorphisms is isomorphic to $\mathbf{Q}$ or a quadratic field, or $q \equiv 3 \pmod 8$ and X is absolutely isogenous to a self-product of an elliptic curve with complex multiplication by $\mathbf{Q}(\sqrt{-q})$.

Linear precision for parametric patches

Luis D. Garcia-Puente (Texas A&M University) and Frank Sottile (Texas A&M University)

In this paper, we discuss a specific topic on geometric modelling, which is the science of modeling curves, surfaces, and higher-dimensional objects by small patches (e.g., Bézier patches). We present a characterization of one important property, linear precision, for multi-sided parametric patches of any dimension.

We show that every parametric patch has a unique reparametrization which has linear precision and we give a geometric criterion for when this reparametrization is rational. We apply this criterion to show that the classical Bézier simploids are the only toric patches based on products of simplices which have linear precision. We also present a simple numerical algorithm to compute the parametrization of a toric patch having linear precision, and apply our analysis to barycentric coordinates for polytopes.

The p-torsion of hyperelliptic curves with extra automorphisms

Darren B. Glass (Gettysburg College)

We examine the relationship between the automorphism group of a hyperelliptic curve defined over an algebraically closed field of characteristic p and the p-rank of the curve, which measures the number of p-torsion points in the Jacobian of the curve. In the case where $p = 2$, we use results of Deuring and Shafarevich to exploit the wild ramification found when dealing with hyperelliptic curves and use this data to show how 'extra' automorphisms impose restrictions on the genera and 2-ranks of such curves. In particular, for given numbers g and f we are able to describe all possible automorphism groups of hyperelliptic curves with genus g and 2-rank f. In the case where our base field is of characteristic $p > 2$ these methods are not as robust, but we are able to show some restrictions on the extra automorphisms that may occur for hyperelliptic curves given genera and p-ranks.

Simultaneous Surface Resolution in Cyclic Galois Extensions

Nan Gu (Purdue University)

(joint work with Shreeram S. Abhyankar)

The problem of Simultaneous Resolution asks the following: given a finite algebraic field extension L of an n-dimensional algebraic function field K/k, can we find non-singular projective varieties X and Y with function fields respectively K and L, such that Y is the normalization of X in L? We showed that this is not always possible when $n = 2$ and L/K has Galois group Z_q where q is divisible by a prime square. Using a theorem of Harbater and Pop, the result can be extended to the cases when the Galois group of L/K is $H \oplus Z_q$, where H is any finite group. The key part of the construction is a lemma to compute the integral closure explicitly of a local domain R in a finite cyclic field extension of its quotient field. It is also noted in the talk that a refinement of this computational lemma actually extends the result to $H \oplus Z_q$ where q is any integer greater than 3.

Syzygies of toric varieties

Milena S. Hering (IMA), Henry Schenck (Texas A&M University) and Gregory Smith (Queen's)

We study the equations defining a projective variety and the higher syzygies between them using multi-graded regularity as introduced by Maclagan and Smith. As an application, we obtain a sufficient condition for the power of an ample line bundle on a toric variety guaranteeing that the corresponding embedded variety is projectively normal and generated by quadratic equations, and that the first p syzygies are linear. This technique also yields new results for the syzygies of Veronese-Segre embeddings.

For more information see `http://front.math.ucdavis.edu/math.AG/0502240`
and my thesis `http://www.ima.umn.edu/~hering/thesis.pdf`

Theta Constant Identities for Jacobians of Cyclic 3-Sheeted Covers of the Sphere and Representations of the Symmetric Group

Yaacov Kopeliovich

We find identities between cubic powers of theta constants with rational characteristics evaluated at the period matrix of τ_R, for R a cyclic 3-sheeted cover of the sphere with $3k$ branch points $\lambda_1, \ldots, \lambda_{3k}$. These identities follow from the Thomae formula. This formula expresses sixth powers of theta constants as polynomials in $\lambda_1, \ldots, \lambda_{3k}$. We apply the representation of the symmetric group to find relations between the polynomials and hence relations between cubic powers of the associated theta constants.

Curves generated on surfaces by the Gilman-Maskit algorithm

Vidur Malik

The Gilman-Maskit algorithm determines whether or not two elements of $\mathrm{PSL}(2,\mathbb{R})$ generate a non-elementary discrete group. Gilman-Keen reinterpreted the algorithm as an unwinding and winding of curves about each other when the group was discrete, but did not contain any elliptic or parabolic elements. Here we examine the behavior of the winding and unwinding of the curves in the general case, including the orbifold case. We show that elliptic generators create curves that are self-wound and modify the Gilman-Keen formula to account for these self-windings. In doing so we distinguish between an algebraically primitive elliptic element, say A, which may not be geometrically primitive and its self-wound counterpart A^β which is both algebraically and geometrically primitive.

Equations for the space of rational curves on the Lagrangian Grassmannian

James Ruffo (Texas A&M University)

Spaces of curves in algebraic varieties are important objects of interest in algebraic geometry. They are typically non-compact, and compactifications are introduced to facilitate their study. Drinfel'd defined a compactification when the curves are rational and the ambient variety is a homogeneous space, called the space of quasi-maps. This variety has applications to geometric representation theory, quantum cohomology, and for Grassmannians, linear systems theory. We study the space of quasi-maps for the Lagrangian Grassmannian, describing the generators of its ideal in a natural projective embedding. The form of this generating set yields interesting geometric consequences, which we describe.

Efficient Divisor Arithmetic on Hyperelliptic Curves: Cantor Versus NUCOMP

Renate Scheidler (University of Calgary) and Andreas Stein (University of Wyoming)

Many problems arising in computational number theory, arithmetic geometry, and cryptography require fast arithmetic on degree zero divisor of a hyperelliptic curve C over a finite field $\mathbb{F}_q$. If $C : y^2+h(x)y = f(x)$ (with $h, f \in \mathbb{F}_q[x]$) is a standard nonsingular model of C, then it is easy to determine whether the place at infinity of $\mathbb{F}_q(x)$ is ramified, inert, or split in the function field of C. Then C is said to be *imaginary*, *unusual*, and *real*, respectively.

In almost all situations, every equivalence class of degree zero divisors on C defined over $\mathbb{F}_q$ contains a unique *reduced* divisor, allowing for efficient arithmetic in the degree zero divisor class group via reduced representatives. The only exceptional scenario is when C is unusual of genus, in which case a given class

may not contain any reduced divisors, but instead contain $q+1$ "almost reduced" divisors. Moreover, in the real scenario, the exact same divisor class arithmetic techniques can be employed for efficient arithmetic in the (principal) *infrastructure* of C. This structure does not form a group, but it is possible to define a distance that imposes an order on this set and behaves "almost" additively under addition and subsequent reduction of infrastructure divisors. As a result, the infrastructure can be used to significantly speed up computational solutions to a variety of number theoretic problems, such as computing the divisor class number, and can also be employed as the basis for fast cryptographic protocols.

A unified description of the arithmetic on degree zero divisors for all three hyperelliptic curve models can be given via continued fraction expansions in a suitable field of Puiseux series. Divisor class and infrastructure arithmetic is traditionally conducted by first adding two reduced degree zero divisors and subsequently reducing the result; this is Cantor's algorithm or derivations thereof. A lesser known, but significantly faster method is the NUCOMP procedure developed by Shanks in the 1980's. Shanks introduced NUCOMP (short for "new composition") in connection with arithmetic of binary quadratic forms. The algorithm can easily be generalized to ideal arithmetic in quadratic number fields and divisor arithmetic on hyperelliptic curves. Our approach was to formulate an optimized version and analyze this method in the unified setting for all three hyperelliptic curve models.

Cantor's algorithm has the disadvantage that the addition of two reduced divisors produces a semi-reduced divisor that is in general not reduced. In fact, with very high likelihood, this semi-reduced divisor has basis polynomials whose degrees are twice as large as the degrees of the basis polynomials of the original two input divisors. Therefore, the subsequent reduction step operates on polynomials of doubly large degree. The idea behind NUCOMP is to eliminate those expensive reduction operations on larger-sized polynomials. NUCOMP stops the addition process before completion and applies an intermediate recursion which is equivalent to reduction with the substantial advantage that the occurring quantities are of much smaller degree. Instead of evaluating the continued fraction expansion of a quadratic irrationality, a rational approximation of this quadratic irrationality is computed via the extended Euclidean Algorithm. The smaller operands in NUCOMP then correspond to quantities in the extended Euclidean Algorithm.

Instead of using the rather expensive continued fraction algorithm that produces the aforementioned intermediate operands of double size, the reduction is performed again using the much less costly extended Euclidean Algorithm. The basis polynomials are only computed once the divisor is reduced or almost reduced. As a result, the sizes of the intermediate operands are significantly smaller, and the divisor produced by NUCOMP is very close to being reduced.

The conclusion is that our improved formulation of NUCOMP offers performance improvements over Cantor's algorithm for even very small genera. Numerical computations provide evidence for the excellent performance of NUCOMP. These results will have important applications to cryptographic protocols such as the Diffie-Hellman key exchange protocol or signature schemes based on hyperelliptic curve arithmetic. In fact, the complexity analysis will show that NUCOMP is a faster way of computing the group operation or the infrastructure operation in any situation where hyperelliptic curve arithmetic is needed. It remains to be seen how explicit formulas based on NUCOMP for low genus curves compare to the currently known best such formulas.

Toric surface codes and Minkowski sums

John Little (Holy Cross) and Henry Schenck (Texas A&M University)

Toric codes are evaluation codes obtained from an integral convex polytope $P \subset \mathbb{R}^n$ and finite field $\mathbb{F}_q$. They are, in a sense, a natural extension of Reed-Solomon codes, and have been studied recently by

J. Hansen, D. Joyner, D. Ruano, and others.

We obtain upper and lower bounds on the minimum distance of a toric code constructed from a polygon $P \subset \mathbb{R}^2$ by examining *Minkowski sum* decompositions of subpolygons of P. Our results give a simple and unifying explanation of bounds of Hansen and empirical results in Joyner; they also apply to previously unknown cases. Let $d(C_P(\mathbb{F}_q))$ be the minimum distance of the toric code determined by the polygon P. Our main result is the following:

Theorem: Let $\mathbb{F}_q$ be a finite field and let $P \subset \mathbb{R}^2$ be an integral convex polygon strictly contained in $\square_{q-1}$. If $q \geq (4i+3)^2$ (where i is the number of interior lattice points of P), and ℓ is the largest positive integer such that there is some $P' \subseteq P$ that decomposes as a Minkowski sum $P' = P_1 + P_2 + \cdots + P_\ell$ with nontrivial P_i, then there exists some $P' \subseteq P$ of this form such that

$$d(C_P(\mathbb{F}_q)) \geq \sum_{i=1}^{\ell} d(C_{P_i}(\mathbb{F}_q)) - (\ell - 1)(q-1)^2.$$

In many cases, this bound is tight.

Genus calculations for towers of function fields arising from equations of C_{ab} curves

Caleb M. Shor (Bates College)

The introduction of geometric Goppa codes in the late 1970s has led to an interest in the genera of function fields over finite fields. We present a large class of function fields arising from the defining equations of C_{ab} curves and calculate the genera. Instead of using the Hurwitz genus formula, for which one needs to know about ramification, we instead use the Riemann-Roch theorem to calculate the genus by counting the number of Weierstrass gap numbers associated to a particular divisor. These function fields are of interest because the Riemann-Roch spaces of functions associated to certain divisors in these function fields are easy to calculate, so one can create the associated Goppa codes.

Bernstein–Sato polynomial in low dimension

Darren Salven Tapp (Purdue University)

Let f be a polynomial function on $\mathbb{C}^n$. In such a case there is a polynomial $b_f(s) \in \mathbb{C}[s]$ such that

$$P(s) \bullet f^{s+1} = b_f(s) f^s,$$

where $P(s) \in \mathbb{C}\langle x_1, \ldots, x_n, \partial_1, \ldots, \partial_n \rangle[s] = D_n[s]$ is an operator. Such a $b_f(s)$ which is of minimal degree and monic is called the Bernstein–Sato polynomial of f.

For example we have,

$$\partial_x^2 \bullet x^{2s+2} = (2s+2)(2s+1)x^s,$$

and in fact $b_{x^2}(s) = (s+1)(s+\frac{1}{2})$.

It is known $b_f(s)$ has negative rational roots greater than $-n$. The Bernstein–Sato polynomial encodes certain information about the singularities of f. For example it relates to: an embedded resolution of f,

Hodge spectrum, Milnor fiber monodromy, Igusa ζ-functions, multiplier ideals and jumping coefficients including the log canonical threshold that can be defined as

$$\sup\left\{c \mid \int_B \frac{1}{|f|^{2c}} < \infty\right\},$$

where B varies over small balls. We may take these small balls to be centered at $0 \in \mathbb{C}^n$ when f is homogeneous.

An algorithm to compute the Bernstein–Sato polynomial of a polynomial was discovered by Oaku [3]. This algorithm uses Gröbner basis computations in the Weyl algebra D_{n+2}. This is a non-commutative ring with $2n+4$ variables, and thus the computational complexity is extremely bad. Thus there is a need for new methods. An example of what is possible is a theorem of U. Walther [2, 4].

Theorem 0.1 (Walther) *Let $\mathcal{A}$ be a set of k linear forms in n-variables such that any n of them are independent. Let*

$$f = \prod_{L\in\mathcal{A}} L \qquad \textit{Then}$$

$$b_f(s) = (s+1)^{n-1} \prod_{i=1}^{2k-n-2} \left(s + \frac{i+n}{k}\right).$$

This theorem leads us naturally to the question.

Question 0.2 *What if we remove the assumption of linear independence?*

When $n = 2$ we consider

$$f = L_1^{m_1} \cdots L_k^{m_k} \tag{0.1}$$

where the L_j are pairwise linearly independent linear forms. Theoretically computing of $b_f(s)$ can be broken into two parts. First find a polynomial $b(s)$ with $b_f(s)|b(s)$. Then verify roots of $b(s)$ are roots of $b_f(s)$. For $q(s) \in \mathbb{Q}[s]$ one may define an ideal $\mathfrak{a}_{q(s)} \subseteq R$ with: $\mathfrak{a}_1 = (f)$, $Jac(f) \subseteq \mathfrak{a}_{(s+1)}$, if $q(s)|r(s)$ then $\mathfrak{a}_{q(s)} \subseteq \mathfrak{a}_{r(s)}$, and $\mathfrak{a}_{q(s)} = R$ if and only if $b_f(s)|q(s)$

Thus we may use computations of this ideal to bound $b_f(s)$. We were able to show:

Theorem 0.3 *Let f be as in 0.1, $\psi(s)$ be the least common multiple of the polynomials*

$$\prod_{\ell=1}^{m_j} \left(s + \frac{\ell}{m_j}\right).$$

Then

$$b_f(s)|\psi(s) \prod_{\ell=0}^{d+k-4} \left(s + \frac{\ell+2}{d}\right) := b(s), \tag{0.2}$$

where $d = \deg(f) = m_1 + m_2 + \cdots + m_k$.

The result is obtained by using an algorithm to add a factor to $q(s)$ as to make $\mathfrak{a}_{q(s)}$ bigger. We use two methods to verify that all the roots of the bound are indeed roots: investigating the cohomology of the Milnor fiber, and computing the jumping coefficients of f.

Suppose f homogeneous, $\deg(f) = d$, and let $F = V(f-1)$ be the Milnor fiber of f, then by [4] there exists a $\mathbb{Z}$-grading on $H_{dR}^{n-1}(F) = \bigoplus_{r\in\mathbb{Z}} U_r$ such that

$$[U_r \neq 0] \Longrightarrow \left[b_f\left(-\frac{r+n}{d}\right) = 0\right].$$

We use a resolution of singularities of the projective closure of F to obtain:

Theorem 0.4 *Let f be as in (0.1). Then $U_r \neq 0$ for $k-3 \leq r < d+k-4$.*

This theorem verifies some of the roots of $b_f(s)$. In our low dimensional case it is not hard to calculate the jumping coefficients of f, and this will verify others [1]. Putting these results together we obtain.

Theorem 0.5 *Let $b(s)$ be as in (0.2) and assume that*

$$\sum_{m_j \leq \frac{d}{k-2}} m_j \geq \frac{d}{2} \quad \textit{then}$$

$$[b_f(\alpha) = 0] \Longleftrightarrow [b(\alpha) = 0]$$

It is expected that the condition on the m's is not needed for the truth of the conclusion.

References

[1] Lawrence Ein, Robert Lazarsfeld, Karen E. Smith, and Dror Varolin. Jumping coefficients of multiplier ideals. *Duke Math. J.*, 123(3):469–506, 2004.

[2] Saito. Morihiko. Bernstein-Sato polynomials of hyperplane arrangements.

[3] Toshinori Oaku. Algorithms for b-functions, induced systems, and algebraic local cohomology of D-modules. *Proc. Japan Acad. Ser. A Math. Sci.*, 72(8):173–178, 1996.

[4] Uli Walther. Bernstein-Sato polynomial versus cohomology of the Milnor fiber for generic hyperplane arrangements. *Comp. Math.*, 141(1):121–145, 2005.

Myrberg Numerical Uniformization of Elliptic and Hyperelliptic Curves

Robert S. Todd (Florida State University)

The numerical uniformization problem for algebraic curves is to find a discontinuous Möbius group uniformizing a given Riemann surface or algebraic curve. Myrberg's algorithm allows for a numerical approximation of Schottky uniformization of elliptic and some hyperelliptic curves. This method also provides the possibility of generalization to a larger class of hyperelliptic curves than traditional elliptic curve uniformization.

The next special session in this series is tentatively scheduled to take place during the 2009 AMS/MAA Joint Mathematics Meetings in Washington, DC (January 7–10, 2009).

OSCAS – Maxima

David Joyner*

11-19-2006

At the kind invitation of ACM SIGSAM Chair Emil Volcheck, this will start a series of regular columns on open source[1] computer algebra systems. I will consider this series a success if it encourages one of you to contribute in even a small way (submit a bug report or just an encouraging email to the developers!) to one of the systems listed below.

A *computer algebra system* (CAS) is a mathematical software package capable of symbolic manipulation. The commercial CAS industry is big business. Few people know more about the CAS industry than Darren McIntyre, VP of Worldwide Sales at Maplesoft. He estimates the worldwide yearly expenditures on computer algebra (buying licenses, employee salaries, and so on) is at least $ 600 million [Mc]. Clients include not just students and universities, but diverse industries who often find that a CAS is a convenient programming environment to model industrial problems.

1 The terrain

Axiom	open source	http://wiki.axiom-developer.org
CADABRA	GPL	http://www.aei.mpg.de/~peekas/cadabra/
DoCon	open source	http://www.haskell.org/docon
GAP	GPL	http://www.gap-system.org
GIAC	GPL	http://www-fourier.ujf-grenoble.fr/~parisse/giac.html
GINAC	GPL	http://www.ginac.de
GTYBALT	GPL	http://wwwthep.physik.uni-mainz.de/~stefanw/gtybalt/
JScience	BSD	http://www.jscience.org/
LiDIA	"open source"	http://www.cdc.informatik.tu-darmstadt.de/TI/LiDIA/
Macaulay2	GPL	http://www.math.uiuc.edu/Macaulay2/
Magnus	GPL	http://sourceforge.net/projects/magnus/
MAS	"open source"	http://alice.fmi.uni-passau.de/mas.html
Mathomatic	LGPL	http://mathomatic.orgserve.de/math/
Maxima	GPL	http://maxima.sourceforge.net
NTL	GPL	http://www.shoup.net/ntl/
Pari	GPL	http://pari.math.u-bordeaux.fr
SAGE	GPL	http://sage.scipy.org
Scilab	'open source"	http://www.scilab.org
Singular	GPL	http://www.singular.uni-kl.de
Symmetrica	public domain	http://www.mathe2.uni-bayreuth.de/axel/symneu_engl.html
Yacas	GPL	http://yacas.sourceforge.net

I have left out CAFE (Computer Algebra and Functional Equations), a group writing a collection of CAS libraries (see http://www-sop.inria.fr/cafe/main-e.html). They appear to be written in Aldor and Maple by (the late) Manuel Bronstein. I cannot determine the license (if any) they are released under.

*Address: Mathematics Department US Naval Academy, Annapolis, MD 21402, USA, wdjoyner@gmail.com

[1]The open source definition is here: http://www.opensource.org/docs/definition.php.

I am also unsure if the "open source" licenses of LiDIA, MAS, and Scilab are compatible with the above-mentioned open source definition. Several of these are under very active development and some of these are essentially dead. Two other sources of information are the Computer algebra handbook [GKW] and the internet sites [CA].

In any case, we see from this table that there are a lot of open source computer algebra systems out there. Some of these are special purpose (such as Symmetrica) and others are general purpose (such as Axiom). We shall start this series by surveying Maxima, a general purpose CAS.

2 Maxima

Maxima is perhaps the most popular general purpose open source CAS. Its latest release (as of November 2006) is 5.10. The next release (Maxima 5.11) is tentatively planned for the beginning of 2007.

2.1 History

The Maxima homepage and the Maxima FAQ (this information is basically due to Stavros Macrakis) explains some history.

Maxima is a descendant of Macsyma, the legendary computer algebra system developed in the late 1960s at the Massachusetts Institute of Technology. Symbolics licensed Macsyma from M.I.T. and registered "Macsyma" as a trademark at some point (presumably with M.I.T.'s permission). When Macsyma source ceased to be freely available, pressure was put on M.I.T. (mostly by Richard Fateman) to transfer the code which had been developed largely with Department of Energy (DOE) funding to the DOE, which then released it to others under certain conditions. That codebase was called DOE Macsyma. DOE-Macsyma, still available from US Dept of Energy, can be licensed under terms more generous than GPL upon request.

The Maxima branch of Macsyma was maintained by William Schelter from 1982 until he passed away in 2001. In 1998 he obtained permission to release the source code under the GNU General Public License (GPL). Since his passing a group of users and developers has formed to bring Maxima to a wider audience.

Pages 8-9 of the Maxima book [Max] has a more detailed history. More Macsyma history can be found in [GKW].

Figure 1: William Schelter.

2.2 Basics

- *website*: `http://maxima.sourceforge.net/`
  wiki: `http://maxima.sourceforge.net/wiki/`

- *Documentation*:
  Online reference manual:

`http://maxima.sourceforge.net/docs/manual/en/maxima.html`
(also available in pdf). This has been translated into Spanish and Portuguese.
Maxima tutorials are available in English, Spanish, Portuguese, German, and Italian from the website.
There are also slightly older Maxima documents in French.
There is also an excellent Calculus textbook which uses Macsyma extensively [BI-G].

- *Interfaces*:
  - Command line.
  - *front-end GUIs*: xmaxima, wxmaxima (cross platform), TeXmacs (cross platform), Imaxima, Kayali, Symaxx.
  - *web interfaces*: There are several lists on the page:
    `http://maxima.sourceforge.net/relatedprojects.shtml`
- *Availability*:
  Source code: Maxima is written in Common Lisp and can be made to compile using either Clisp, GCL, CMUCL, SBCL, or OpenMCL. It has been compiled on Linux, Windows, Mac OSX, and FreeBSD machines.
  `http://maxima.sourceforge.net/wiki/index.php/Maxima%20ports`
  Binary: It is available as a binary for linux and windows (cygwin not required).
- *Support*:
  There is an active email list:
  `http://maxima.sourceforge.net/maximalist.html`
  This list is also used by developers as well.
- *License*:
  GPL. However, Maxima's graphics uses openmath (which is GPL'd) and gnuplot (which is not GPL'd).

2.3 Active developers

Maxima has a very talented group of active developers. At the present day the major contributors seem to be Robert Dodier, Barton Willis, Raymond Toy, Stavros Macrakis (especially generating bug reports and bug fixes), Mario Rodriguez Riotorto (docs and share packages, especially), Vadim Zhytnikov (especially packaging the Windows build), and David Billinghurst (differential equations). There are also people working on various projects closely or not-so-closely related – e.g., Andrej Vodopivec (WxMaxima), Camm Maguire (GCL). Unfortunately, it is not possible in this short column to name everyone involved in Maxima. However, I hope that this list of active developers provides solid evidence that this CAS continues to grow and improve.

2.4 Capabilities

Using Maxima, one can manipulate symbolic and numerical expressions, including differentiation, integration (symbolic and numerical), Taylor series, Laplace transforms, ordinary differential equations, systems of linear equations, special functions, elliptic functions, polynomials, orthogonal polynomials, sets, lists, vectors, matrices, and tensors. There are also some probability and statistics functions. Maxima yields high precision numeric results by using exact fractions, arbitrary precision integers, and arbitrarily precision floating point numbers. Maxima can plot functions and data in two and three dimensions. Maxima also has several special-purpose packages, such as for tensor calculus, solving recursive equations, and summation identities.

The main page to the reference manual describes the topics in more details (`http://maxima.sourceforge.net/docs/manual/en/maxima.html`).

Here is a cool example using Maxima's `plotdf` package and `openmath` (both written by W. Schelter): To show the direction field of the differential equation $y' = x + y$ and the solution that goes through $(2, -0.1)$, use the commands:

```
(%i1) load("plotdf");
(%i2) plotdf(x+y,[trajectory_at,2,-0.1]);

(%o2)                                0
```

This produces the following pretty plot:

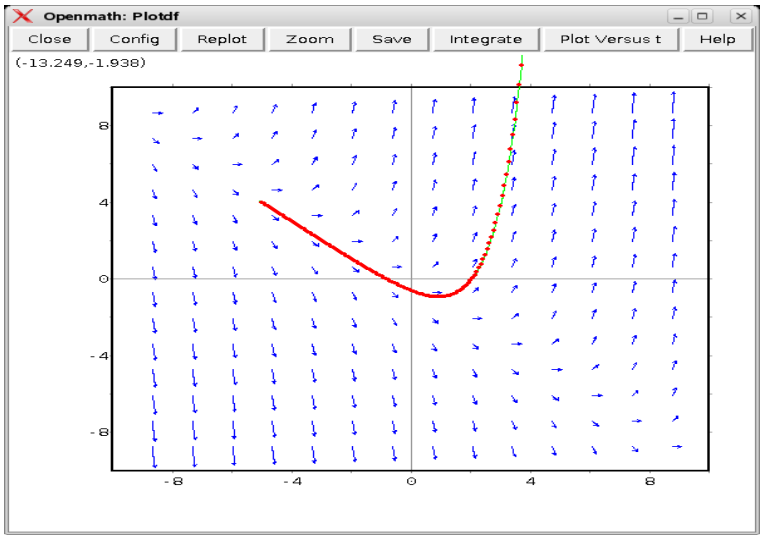


Figure 2: A direction field plot.

2.5 Thanks

I have benefited greatly from emails with Robert Dodier, whom I thank for his generous help. Of course, only I am responsible for any mistakes. If you have corrections or comments, please email me.

In the next column, we'll look into Axiom and Aldor. Until then, have fun computing!

References

[CA] `http://en.wikipedia.org/wiki/List_of_computer_algebra_systems`
`http://en.wikipedia.org/wiki/Comparison_of_computer_algebra_systems`
`http://wiki.axiom-developer.org/RosettaStone`

[GKW] J. Grabmeier, E. Kaltofen, V. Weispfenning, *Computer Algebra Handbook*, Springer, 2003.

[Mc] D. McIntyre, private communication, 11-2006.

[Max] P. Ney de Souza, R. J. Fateman, J. Moses, C. Yapp, **The Maxima Book**, 19th September 2004. Available online at:
`http://maxima.sourceforge.net/docs/maximabook/maximabook-19-Sept-2004.pdf`

[BI-G] A. Ben-Israel, R. Gilbert, **Computer-supported calculus**, Springer-Verlag, 2002.

International Symposium on Symbolic and Algebraic Computation ISSAC 2007

http://www.cs.uwaterloo.ca/issac2007/

University of Waterloo, Waterloo, Ontario, Canada

March 29, 2007

The International Symposium on Symbolic and Algebraic Computation (ISSAC) is the premier annual conference to present and discuss new developments and original research in all areas of symbolic computation and computer algebra. This year ISSAC will be held July 29 – Aug 1, 2007 at the University of Waterloo in Canada. Planned conference activities include invited talks, presentation of original research papers, poster sessions, tutorial courses and software demonstrations. Proceedings, as well as abstracts of posters, will be distributed at the conference. The satellite workshops Symbolic-Numeric Computing (SNC) and Parallel Symbolic Computation (PASCO) will be held at the nearby University of Western Ontario in the preceding week.

Topics of the ISSAC meeting include (but are not limited to):

- **Algorithmic mathematics.**
  Algebraic, symbolic and symbolic-numeric algorithms. Simplification, function manipulation, equations, summation, integration, ODE/PDE, symbolic and exact linear and multi-linear algebra, computational number theory and group theory, and geometric computing.
- **Computer Science.**
  Theoretical and practical problems in symbolic computation and algebraic computation. Systems, problem solving environments, user interfaces, software, libraries, parallel/distributed computing and programming languages for symbolic computation, concrete analysis, benchmarking, theoretical and practical complexity of computer algebra algorithms, automatic differentiation, code generation, mathematical data structures and exchange protocols.
- **Applications.**
  Using algebraic, symbolic or symbolic-numeric computation in an essential or novel way in treating problems in application areas such as engineering, computer assisted modelling and design, economics and finance, physical and biological sciences, computer science, logic, mathematics, statistics, education.

Conference Organization

- *General Chair:* Dongming Wang (France, China)
- *Program Chair:* Bernard Mourrain (France)
- *Tutorials Chair:* J. Rafael Sendra (Spain)
- *Local Arrangements:* Keith Geddes, Mark Giesbrecht, George Labahn, Arne Storjohann (Waterloo)

Sponsors: The ACM, The Fields Institute, Maplesoft, MITACS and the University of Waterloo.

SAGE DAYS 3

Communicated by David Joyner

SAGE Days 3 will be held at IPAM (Institute for Pure and Applied Mathematics) at UCLA. Come to SAGE Days 3 and learn about and help create free open source software for research and teaching in algebra, geometry, number theory, cryptography, and numerical computation.

Talks that everyone cares about will be in the mornings, and in the afternoons, we'll have more specialized talks by the same speakers. In the afternoons, we may also try to organize various tutorials for those not interested in the specialized talks. Also, the goal is to try to give something of a theme to each of the two days. We'll have slightly fewer talks than the last SAGE Days.

The first day will be targeted to people who are not experts on SAGE, which for our purposes, might mean anyone who isn't a SAGE Developer, but might like to be. An example of this might be a "State of the Union" talk by William in the morning, and a talk on what an undergraduate can do to get involved with SAGE in the afternoon. If anyone has ideas for good coding projects that undergraduates can get involved with, let us know.

The second day will be targeted at SAGE Developers. The morning will be talks about things that everyone needs to hear about, and the afternoon talks will be talks about more specified topics that people might be interested in. So, using SD2 for examples again, we'd have David Harvey's talk on SAGE Architecture, and in the afternoon, Martin Albrecht's talk on F4.

Organizing committee: Craig Citro, David Joyner, Kristin Lauter, Nathan Ryan, William Stein (chair)

See `http://sage.math.washington.edu/sage/days3` for more details.

COMPSAC 2007, Call for Papers

Communicated by Atilla Elci

COMPSAC 2007 – 31st Annual International Computer Software and Applications Conference

Beijing, July 24-27, 2007

COMPSAC is a major international forum for researchers, practitioners, managers, and policy makers interested in computer software and applications. Starting with 2006, COMPSAC is designated as the IEEE Computer Society Signature Conference on Software Technology and Applications. Based on this designation COMPSAC organizers are able to work with other key functions of the Computer Society to create more values for the conference volunteers and participants.

Proposals for workshops are solicited for consideration of affiliation with COMPSAC 2007. Affiliated workshops will be held in conjunction and co-located with the conference and other affiliated workshops. The purpose of these workshops is to provide a platform for presenting novel ideas in a less formal and possibly more focused way than the conference itself. As such, they also offer a good opportunity for young researchers to present their work and to obtain feedback from an interested community. Workshop organizers are responsible for establishing a program committee, collecting and evaluating submissions, notifying authors of acceptance or rejection in due time, and ensuring a transparent and fair selection process, organizing selected papers into sessions, and assigning session chairs.

Researchers and practitioners are invited to submit a one-page concept paper proposing a workshop to the 31st COMPSAC Workshop Chair, Atilla Elci `atilla.elci@emu.edu.tr`, by Dec. 8, 2006. Submission may be made by e-mail with "COMPSAC Preliminary Workshop Proposal" in the subject header and supplying data on the Preliminary Workshop Proposal Format. Feedback will be provided to the workshop proposers by Dec. 15, 2006. An accepted proposal will then be detailed using the Final Workshop Proposal Format by its organizers. Other important due dates are mentioned below.

The selection of the workshops to be included in the final COMPSAC program will be based upon several factors, including the scientific / technical interest of the topics, the quality of the proposal, balance and distinctness of workshop topics, and the capacity of the conference workshop program.

Workshops use the same paper submission system with COMPSAC 2007. Proceedings of the COMPSAC Workshops will be printed as a separate volume by IEEE Computer Society Press to be made available to all conference registrants on site. All workshop papers will as well be electronically available through IEEE Xplore Digital Database. Any further information needed for preparing a workshop proposal can be obtained by contacting the COMPSAC Workshop Chair.

For more information please visit the web site `http://www.compsac.org/`

Issue Date: Oct. 16, 2006.

Calculemus 2007, Call for Papers

June 27–30, 2007 · RISC Institute · Castle of Hagenberg, Austria

Communicated by Manuel Kauers and Wolfgang Windsteiger

Calculemus is a series of conferences dedicated to the integration of computer algebra systems (CAS) and automated deduction systems (ADS) towards the development of universal mathematical assistant systems (MAS).

Currently, symbolic computation is divided into several (more or less) independent branches, traditional ones (e.g. computer algebra and theorem proving) as well as newly emerging ones (on user interfaces, knowledge management, theory exploration, etc.). The main concern of the Calculemus community is to bring these developments together in order to facilitate the theory, design, and implementation of integrated MAS that will routinely be used by mathematicians, computer scientists, and engineers in their every-day business.

For the upcoming Calculemus meeting, which will be held jointly with MKM2007 in Hagenberg, Austria, we seek original research papers in this context.

The scope of Calculemus covers all aspects of developing mathematical assistant systems, in particular, the interplay of automated reasoning and computer algebra. Potential areas of interest are:

- Automated reasoning in computer algebra
- Computer algebra in automated reasoning
- Interdisciplinary systems
- Infrastructure for mathematical services
- Theory exploration techniques
- Theory, design, and implementation of MAS
- Case studies and applications of MAS

Important Dates:
February 12, 2007: Submission deadline
March 12, 2007: Notification of acceptance
March 26, 2007: Camera ready copies due
June 27–30, 2007: Conference

Keynote Speakers:
Thomas Hales, University of Pittsburgh
John Harrison, Intel Inc.
Peter Paule, RISC-Linz

Submission: Please submit your full paper of at most 12 pages prepared with the standard LNCS class style as .pdf or .ps file electronically on or before February 12, 2007. Detailed formating instructions can be found on the Calculemus website.

Proceedings: Accepted papers will be published in the LNAI series of Springer.

Program Committee: Alessandro Armando (DIST, Italy), Christoph Benzmüller (University of Cambridge, UK), Olga Caprotti (University of Helsinki, Finland), Jacques Carette (McMaster, Canada), Timothy Daly (Carnegie Mellon, USA), William M. Farmer (McMaster, Canada), Keith O. Geddes (Waterloo, Canada), Tom Hales (Pittsburgh, USA), Hoon Hong (North Carolina State University, USA), Deepak Kapur (New Mexico, USA), Manuel Kauers (RISC-Linz, Austria, Chair), Laura Kovacs (RISC-Linz, Austria), Petr Lisonek (Simon Fraser University, Canada), Roy McCasland (University of Edinburgh, UK), Renauld Rioboo (Universtite Pierre et Marie Curie, France), Volker Sorge (University of Birmingham, UK), Klaus Sutner (Carnegie Mellon, USA), Thomas Sturm (University of Passau, Germany), Wolfgang Windsteiger (RISC-Linz, Austria, Chair).

Further Information: `http://www.risc.uni-linz.ac.at/about/conferences/Calculemus2007/`

ISSAC 2005 Awards

Austin Lobo, Chair, ISSAC 2005 Poster Committee
Peter Paule, Chair, ISSAC 2005 Program Committee
Emil Volcheck, Chair, ACM SIGSAM

ACM SIGSAM established the ISSAC Distinguished Paper and Distinguished Student Author Awards in 2002 to recognize excellent work presented at ISSAC and encourage submissions of high quality. At ISSAC 2005 in Beijing, awards were presented in the categories of Distinguished Paper, Distinguished Student Author, and Distinguished Poster.

Each Distinguished Paper Award is accompanied by a citation that describes the achievements of the authors in a way that we hope can be understood by non-specialists. For this we have two goals in mind: first, to explain to a department chair or supervisor why the work of the author(s) deserved recognition, and second, to communicate progress and excitement in the field of computer algebra to the greater scientific community.

We would like to thank the Program Committee and the Poster Committee for their careful deliberations in selecting the award winners. We would also like to thank the members of the Program Committee who assisted in preparing the award citations.

The Distinguished Paper and Distinguished Student Author awards are funded by an ACM SIGSAM endowment. Funds for the Distinguished Poster awards are provided by ISSAC.

We thank Maplesoft for their generosity in providing eleven complimentary copies of Maple™ 10 to the award winners.

To read more about the ISSAC awards and guidelines, visit `http://sigsam.org/ISSAC_Awards/` .

Distinguished Paper Awards

Two Distinguished Paper Awards were presented at ISSAC 2005. Each carried a prize of USD 400, shared among the authors.

The first award goes to Erich Kaltofen and Pascal Koiran for their paper "On the Complexity of Factoring Bivariate Supersparse (Lacunary) Polynomials." The citation reads as follows:

> A primary goal of the field of computer algebra and symbolic computation is to find new and better ways of computing with mathematical objects. Polynomials are one of the most fundamental objects in computer algebra, and yet a natural sparse representation can present seemingly intractable complexity. More specifically supersparse polynomials are polynomials defined over the rational numbers with relatively few terms whose exponents can be very large integers. While such polynomials have a compact representation as a sum of non-zero terms, some fundamental operations that we take for granted as being easy for ordinary polynomials, such as evaluating at integers, are generally infeasible.

> Kaltofen and Koiran extend results of Hendrik Lenstra, Jr. for supersparse polynomials from the univariate to the bivariate case: they exhibit algorithms that can find all linear and quadratic factors of supersparse polynomials in polynomial time. They succeed by fusing classical computer algebra techniques of interpolation and modular reduction with modern randomized methods and deep bounds from algebraic number theory and Diophantine equations.
>
> This work also contributes significantly to our theoretical understanding of algorithms for supersparse polynomials by analyzing the general complexity of factoring and testing irreducibility. They show that a number of such problems are co-NP-hard, implying for example that a fast algorithm for such a problem would give a fast algorithm for integer factorization.
>
> For these contributions, ACM SIGSAM awards Erich Kaltofen and Pascal Koiran the ISSAC 2005 Distinguished Paper Award.

The second award goes to Bernard Mourrain and Philippe Trébuchet for their paper "Generalized Normal Forms and Polynomial System Solving". The citation reads as follows:

> Solving systems of polynomial equations stands as one of the great challenges of computer algebra. Rewriting a polynomial in a simpler form using a set of polynomial equations is an important and closely related problem. This paper addresses the challenge of solving a system by developing a better way to simplify a polynomial with respect to that system.
>
> The authors generalize the standard technique of simplification with respect to a monomial term ordering to create a framework of reducing families, reduction operators, and choice functions that leads to a generalized normal form for polynomials. Their generalization of term ordering builds on the Macaulay resultant and holds the potential for better numerical stability properties. They apply this framework to systems of polynomial equations with finitely many solutions where they use conventional numerical linear algebra techniques to compute the solution. The greater freedom in simplification afforded by this framework holds significant promise for improving our ability to solve systems of polynomial equations.
>
> For this contribution, ACM SIGSAM awards Bernard Mourrain and Philippe Trébuchet the ISSAC 2005 Distinguished Paper Award.

Distinguished Student Author Awards

Christiaan van de Woestijne received an award for his paper "Deterministic equation solving over finite fields" and a prize of USD 400.

Xavier Dahan, Wenyuan Wu, and Yuzhen Xie received awards for their paper "Lifting techniques for triangular decompositions" coauthored with Éric Schost and Marc Moreno Maza. Each student received a prize of USD 200.

Distinguished Poster Awards

The ISSAC Poster Committee selected two winners this year.

Evelyne Hubert and Irina Kogan received an award for their poster "Rational and Replacement Invariants of a Group Action". Each received a prize of USD 100.

Xavier Dahan, Marc Moreno Maza, Éric Schost, Wenyuan Wu, and Yuzhen Xie received an award for their poster "On the Complexity of the D5 Principle". Each received a prize of USD 40.

Algebraic Biology 2007

July 2–4, 2007, Johannes Kepler University, Linz,

Research Institute for Symbolic Computation, Castle of Hagenberg, Austria

Communicated by Temur Kutsia

Aims and Scope: The Second International Conference on Algebraic Biology, AB'07, is an international forum to promote discussion and interaction between researchers who intend to apply symbolic computation—computer algebra and computational logic—to various issues in biology. The conference covers all aspects of applications of algebraic and logic methods in biology, addressing

- molecular sequence analysis
- molecular structure analysis
- molecular evolution
- genomics
- proteomics
- gene regulation
- gene expression
- gene ontology
- network inference
- mathematical modeling
- model identification
- system analysis and design
- system verification
- synthetic biological systems

and other problems in biology with symbolic methods including, but not restricted to:

- polynomial methods
- group theoretical methods
- rewriting methods
- automated reasoning methods
- automata methods
- formal language methods
- combinatoric methods
- gene ontology
- symbolic-numeric algorithms (sequential, parallel, distributed, grid processing).

In addition to the sessions with contributed papers, tutorial sessions will be organized. Tutorials will be given by leading experts in life sciences and symbolic computation. **Submission:** Authors are invited to submit original papers that have not been submitted for publication elsewhere. Submissions should be at most 15 pages including references, prepared in LaTeX and formatted according to the Springer llncs style. Submitted papers will be peer-reviewed, and the accepted papers will be published by Springer Verlag.

Important Dates:
December 11, 2006: Registration of abstracts.
December 18, 2006: Submission of full papers.
March 5, 2007: Notification.
April 2, 2007: Camera-ready paper submission.
July 2–4, 2007: Conference.

Keynote Speakers:
Reinhard Laubenbacher,
Virginia Bioinformatics Institute (USA)
Bud Mishra, New York University (USA)
Gheorghe Paun,
Romanian Academy of Sciences

Program Committee: Tatsuya Akutsu (Japan), Hirokazu Anai (Japan, Conference and PC Co-Chair), Armin Biere (Austria), Bruno Buchberger (Austria, Conference Co-Chair), Vincenzo Capasso (Italy), Luca Cardelli (UK), Gautam Dasgupta (USA), Francois Fages (France), Shinji Hara (Japan), Sepp Hochreiter (Austria), Hoon Hong (USA, Conference Co-Chair), Katsuhisa Horimoto (Japan, PC and Conference Co-Chair), Hans Irschik (Austria), Erich Kaltofen (USA), Veikko Keränen (Finland), Temur Kutsia (Austria, PC Co-Chair), James F. Lynch (USA), Manfred Minimair (USA), Enno Ohlebusch (Germany), Stanly Steinberg (USA), Bernd Sturmfels (USA), Carolyn L. Talcott (USA), Ashish Tiwari (USA), Jens Volkert (Austria), Dongming Wang (China/France), Kazuhiro Yokoyama (Japan), Ruriko Yoshida (USA).

Further Information: http://www.risc.uni-linz.ac.at/about/conferences/ab2007/

Differential Algebra and Related Topics
April 12–15, 2007
Workshop II and AMS Special Session

Communicated by William Sit

The Kolchin Seminar in Differential Algebra of The City University of New York and the Department of Mathematics at Rutgers University at Newark are pleased to announce the second joint International Workshop and AMS Special Session on Differential Algebra and Related Topics. The joint conferences will bring together experts from different areas related to differential algebra. The purpose is to disseminate the methods and results of differential algebra to other areas, to encourage potential collaborations, and to attract graduate students and new researchers. During the workshop, invited speakers will give expository or survey talks on their fields. The Special Session at the AMS Eastern Section Meeting for Spring 2007 will bring the participants further up to date on the most current research through invited research reports.
Topics: Including but not limited to: Differential and difference algebra, differential Galois theory, differential algebraic geometry, differential algebraic groups, model theory, computational differential algebra, Rota-Baxter type algebras, and applications to combinatorics, arithmetic geometry, control theory, dynamical systems, and integrability theories.

	Workshop	AMS Special Session
Date:	April 12–13, 2007	April 14–15, 2007
Location:	Rutgers University at Newark	Stevens Institute of Technology
URL:	newark.rutgers.edu/~liguo/DARTII/diffalg.html	www.sci.ccny.cuny.edu/~ksda/ams.html
Contact:	Li Guo (liguo@newark.rutgers.edu)	Jerry Kovacic (jkovacic@verizon.net)

Confirmed Speakers (alphabetical order):
Workshop: Marcelo Aguiar, Peter Clarkson, Robert Grossman, Andy Magid, David Marker, B. Heinrich Matzat, Greg Reid, Brahim Sadik, Michael Singer, Marius van der Put, Mark van Hoeij.
AMS Special Session: Primitivo Acosta-Humanez, B. Heinrich Matzat, Alexandru Buium (Santiago Simanca), Claude Mitschi, Lucia Di Vizio, Alexey Ovchinnikov, Anne Duval (Élie Compoint), Eugueny Pankratiev, Oleg Golubitsky, Sylvie Paycha, Charlotte Hardouin, Wai Yan Pong, Julia Hartmann, Brahim Sadik, Lourdes Juan, Michael Singer, Arne Ledet, Franz Winkler, Aleksandr B. Levin, Yang Zhang, Andy Magid.

Organizers:

Phyllis Cassidy (CCNY and Smith College, emerita)
Richard Churchill (Hunter College and Graduate Center of CUNY)
Li Guo (Chair for Workshop, Rutgers University at Newark)
William Keigher (Rutgers University at Newark)
Jerry Kovacic (Chair for AMS Special Session, City College of CUNY)
William Sit (City College of CUNY, emeritus)

Funding: Limited funding for the Workshop for participants with US citizenship or permanent residence status is expected from the National Security Agency. Applications for support should be sent to Li Guo. All AMS participants must bear their own expenses, including AMS registration fee.

2007 Federated Computing Research Conference

June 8–16, 2007, San Diego, California, USA

http://www.acm.org/fcrc/

Communicated by Julie Goetz, ACM, SIG Publications

The Federated Computer Research Conference (FCRC) assembles a spectrum of affiliated research conferences and workshops into a week long coordinated meeting held at a common time in a common place. This model retains the advantages of the smaller conferences, while at the same time, facilitates communication among researchers in different fields in computer science and engineering. Mornings of FCRC week will begin with joint plenary talks on topics of broad appeal to the computing research community.

The ACM 2007 Federated Computing Research Conference will be held June 8-16 in San Diego, CA. Affiliated conferences include:

- COLT 2007: 20th Annual Conference on Learning Theory
  http://www.learningtheory.org/colt2007/
- CRA-W 2007: CRA-W Mentoring Workshop
  http://www.cra.org/main/cra.events.upcoming.html
- EC 2007: The Eighth ACM Conference on Electronic Commerce
  http://stiet.si.umich.edu/ec07/
- EXPERIMENTAL CS 2007: Workshop on Experimental Computer Science
  http://www.cs.huji.ac.il/~feit/exp/
- HOPL-III: The Third ACM SIGPLAN History of Programming Languages Conference
  http://research.ihost.com/hopl/
- IEEE Complexity 2007: IEEE Conference on Computational Complexity
  http://www.computationalcomplexity.org
- ISCA 2007: International Symposium on Computer Architecture
  http://www.cse.ucsd.edu/isca2007/
- LCTES 2007: ACM SIGPLAN/SIGBED Conference on Languages, Compilers, and Tools for Embedded Systems
  http://www.cs.purdue.edu/lctes07
- PADS 2007: Principles of Advanced and Distributed Simulation Workshop
  http://www.pads-workshop.org
- PASTE 2007: ACM SIGPLAN-SIGSOFT Workshop on Program Analysis for Software Tools and Engineering
  http://paste07.cs.washington.edu

- PLAS 2007: Programming Languages and Analysis for Security Workshop
  `http://www.cs.umd.edu/~mwh/PLAS07/`
- PLDI 2007: ACM SIGPLAN Conference on Programming Language Design and Implementation
  `http://ties.ucsd.edu/PLDI`
- SIGMETRICS 2007: International Conference on Measurement and Modeling of Computer Systems
  `http://www.cs.cmu.edu/~sigm07/`
- SPAA 2007: ACM Annual Symposium on Parallelism in Algorithms and Architectures
  `http://www.cs.jhu.edu/~spaa/2007/`
- STOC 2007: Annual ACM Symposium on the Theory of Computing
  `http://www.research.att.com/~dsj/stoc07.html`
- VEE 2007: International Conference on Virtual Execution Environments
  `http://vee07.cs.ucsb.edu/`

2007 Federated Computing Research Conference Keynote Speakers

- Dr. Frances Allen, 2007 ACM Turing Award Winner
- Chuck Moore, AMD
- David Culler, Berkeley and Deborah Estrin, UCLA
- Avi Wigderson, Princeton
- Guy Steele, SUN
- Ed Lazowska, Washington

Programming Languages for Mechanized Mathematics Workshop

web page: http://www.cas.mcmaster.ca/plmms07/, e-mail: carette@mcmaster.ca

Calculemus 2007 Workshop, Hagenberg, Austria

June 29-30, 2007

The intent of this workshop is to examine more closely the intersection between programming languages and mechanized mathematics systems (MMS). By MMS, we understand computer algebra systems (CAS), [automated] theorem provers (TP/ATP), all heading towards the development of fully unified systems. There are various ways in which *programming languages* and *systems for mathematics* meet:

- Many systems for mathematics contain a dedicated programming language (and are frequently built in that same language); some proof assistants (like the Ltac language for Coq) also have an embedded programming language. Often this language captures only algorithmic content, and *declarative* or *representational* issues are avoided.
- The *mathematical languages* of many systems for mathematics are very close to a functional programming language (ex: the language of HOL can be used as a functional PL that is very close to ML and Haskell). On the other hand, these languages also contain very rich specification capabilities rarely available in most computation-oriented programming languages. Even then, many specification languages (B, Z, Maude, OBJ3, CASL, etc) still have more representational power.
- Conversely, functional programming languages have been getting "more mathematical" all the time (eg: dependent types). But they are still not quite ready to 'host' mathematics. There are some promising languages on the horizon (Epigram, Omega) as well as some hybrid systems (Agda, Focal), although it is unclear if they are capable of expressing the concepts present in mathematics.
- Systems for mathematics are used to prove programs correct (eg: via Hoare logic). An interesting question is what improvements are needed for this both on the side of the mathematical systems and on the side of the programming languages.

This workshop will accept two kinds of submissions: full research papers as well as position papers. Research papers should be no more than 15 pages in length, and positions papers no more than 3 pages. Submission will be through EasyChair. An informal version of the proceedings will be available at the workshop, with a more formal version to appear later. We are looking into having the best papers completed into full papers and published as a special issue of a Journal (details to follow).

Important Dates: April 25, 2007: Submission Deadline; June 29-30, 2007: Workshop.

Program Committee Lennart Augustsson [Credit Suisse], Wieb Bosma [Radboud University Nijmegen, Netherlands], Jacques Carette (co-Chair) [McMaster University, Canada], David Delahaye [CNAM, France], Jean-Christophe Filliâtre [CNRS and Universit de Paris-Sud, France], John Harrison [Intel Corporation, USA], Josef Urban [Charles University, Czech Republic], Markus (Makarius) Wenzel [Technische Universitt Mnchen, Germany], Freek Wiedijk (co-Chair) [Radboud University Nijmegen, Netherlands], Wolfgang Windsteiger [University of Linz, Austria]

Location and Registration Location and registration information can be found on the Calculemus web site. http://www.risc.uni-linz.ac.at/about/conferences/Calculemus2007/

A Series of International Scientific Events
RISC Summer 2007

June/July 2007 · Research Institute for Symbolic Computation · Johannes Kepler University Linz · Austria

Communicated by Temur Kutsia

Research Institute for Symbolic Computation, RISC-Linz, in June/July 2007 organizes a series of international scientific events *RISC Summer 2007*, consisting of the following conferences and schools:

- CoCoA's International School in Computer Algebra.
  June 18–22, 2007. RISC, Castle of Hagenberg, Austria.
- 9th International Conference on Effective Methods in Algebraic Geometry, MEGA'07.
  June 24–30, 2007. Strobl am Wolfgangsee, Austria.
- 2nd RISC/SCIEnce Training School in Symbolic Computation.
  June 25–July 8, 2007. RISC, Castle of Hagenberg, Austria.
- 2nd International Conference on Algorithmic Information Theory, AIT'07.
  June 25–26, 2007. RISC, Castle of Hagenberg, Austria.
- 14th International Symposium on the Integration of Symbolic Computation and Mechanized Reasoning, Calculemus'07.
  June 27–30, 2007. RISC, Castle of Hagenberg, Austria.
- 6th International Conference on Mathematical Knowledge Management, MKM'07.
  June 27–30, 2007. RISC, Castle of Hagenberg, Austria.
- 2nd International Conference on Algebraic Biology, AB'07.
  July 2–4, 2007. RISC, Castle of Hagenberg, Austria.
- 6th International Symposium for Parallel and Distributed Computing, ISPDC'07.
  July 5–8, 2007. RISC, Castle of Hagenberg, Austria.

Further Information: `http://www.risc.uni-linz.ac.at/about/conferences/summer2007/`

NumAn 2007, Conference in Numerical Analysis

Recent Approaches To Numerical Analysis: Theory, Methods and Applications
http://www.math.upatras.gr/numan2007/

September 3-7, 2007, Kalamata, Greece

Communicated by Ilias S. Kotsireas

NumAn provides an opportunity to learn of new developments and to present original research results in all areas of Numerical Analysis such as Theory, Methods and Applications.

The aims of the conference are:

1. to promote scientific activities, directions and pursuits on subjects that pertain to the conference,
2. to foster an exchange of views and ideas,
3. to study the theoretical background required for methods, algorithms and techniques used in applications,
4. to establish directions of theoretical results towards applications,
5. to highlight open problems and future directions of numerical analysis.

The program of NumAn 2007 will include invited presentations, contributed research papers and posters, covering theory, methods and applications of Numerical Analysis.

Conference Topics: Specific topics include, but are not limited to: Numerical ODEs, Numerical PDEs, Scientific Computing and Algorithms, Stochastic Differential Equations, Approximation, Numerical Linear Algebra, Numerical Integral Equations, Error Analysis and Interval Analysis, Difference Equations and Recurrence Relations, Interpolation and Extrapolation, Numerical problems in Dynamical Systems, Optimization and Nonlinear Equations Applications to the Sciences (Computational Physics, Computational Statistics, Computational Engineering etc.), Differential Algebraic Equations, Numerical methods in Fourier analysis, High Performance Scientific Computing, Applied and Industrial Mathematics.

Proceedings: Papers presented at the conference may be submitted for publication in a Special Issue of the *Journal of Computational and Applied Mathematics* http://www.elsevier.com/locate/cam published by Elsevier. Details for paper submission to this special issue will be announced at the conference.

Financial Support: Some financial support will be available from the conference, to cover expenses of graduate students and post-doctoral fellows.

Invited Speakers: N. Apostolatos, N. Artemiadis, D. Bertsekas, C. Dafermos, A. Fokas, A. Hadjidimos, E. Houstis, P. Ligomenides, G. Nicolis, C. Tsallis.

Organizing Committee: E. Gallopoulos, University of Patras, Elias N. Houstis, University of Thessaly, Ilias S. Kotsireas, Wilfrid Laurier University, Dimitrios Noutsos, University of Ioannina, Michael N. Vrahatis, University of Patras.

Applications of Computer Algebra 2007

http://www2.oakland.edu/aca/index.cfm

July 19-22, 2007, Oakland University, USA

Communicated by Tanush Shaska

Organization:

- Chair: Tanush Shaska
- Local Organizers:
  J. Nachman
  T. Shaska

Conference Theme: The ACA series of conferences is devoted to promoting the applications and development of Computer Algebra and Symbolic Computation. Topics include computer algebra and symbolic computation in engineering, the sciences, medicine, pure and applied mathematics, education, communication and computer science.

Special sessions: We are still accepting proposals to organize sessions at the conference. Sessions are expected to have 4 or more speakers and to be relevant with one of the conference themes. Proposals for organizing a session should be sent to shaska@oakland.edu

Approved sessions:

1. Applications of computer algebra in enumerative and algebraic combinatorics, A. Tefera, M. Apagodu and M. Zeleke.
2. Non-Standard Applications of Computer Algebra, E. Roanes-Lozano, M. Wester
3. Coding theory, D. Joyner, T. Shaska, C. Shor.
4. Computer algebra in education, M. Beaudin, M. Wester, A. Akritas, B. Pletsch
5. Computational algebraic geometry, T. Shaska, A. Elezi
6. Symbolic Symmetry Analysis and Its Applications. N. Bila, I. Kogan
7. Algebraic and Numerical Computation for Engineering and Optimization Problems, D. Chibisov, V. Ganzha, E. W. Mayr
8. Numerical Algebraic Geometry, C. Wampler, A. Sommese
9. Approximate Algebraic Computation Session, R. Corless, H. Kai, T. Sasaki, K. Shirayanagi.

Proceedings: There will be a volume proceedings for the conference.

East Coast Computer Algebra Day
ECCAD 2007

web page: eccad07.washcoll.edu, e-mail: alobo2@washcoll.edu

Washington College, Chestertown, Maryland, USA

April 21 2007

ECCAD 2007 at Washington College in Chestertown, Md., is the 14th annual meeting of students, researchers, and practitioners of Computer Algebra and Symbolic Computation. It is a venue for sharing new results and work in progress and for meeting in informal settings in a relaxed atmosphere.

- When: Saturday, April 21, 2007.
- Registration is requested.
- Proposals for poster presentations are solicited and will be entertained until April 14^{th}
- Events
  - Three talks by invited specialists.
  - Poster Presentations and Software Demonstrations
  - A Moderated Panel Discussion on "Computer Algebra: The Road Ahead."
- Wired and Wireless network access will be available.

The meeting is sponsored by Washington College and the National Science Foundation. Subject to approval of a pending NSF proposal, there will be travel funds for US-based students and recent PhDs.

- Organizer: Austin Lobo, Washington College.
- Poster Chair: Markus Hitz, NGCSU.
- Panel Moderator: Emil Volcheck, ACM-SIGSAM.
- Local Arrangements: John May, University of Delaware; Michael McLendon, Washington College; Jennifer Whitehead, Washington College.
- Advisory Council: Bruce Char, Drexel University; Erich Kaltofen, North Carolina State University; B. David Saunders, University of Delaware; William Sit, City College of the City University of New York; Stephen Watt,University of Western Ontario, Canada.

Symbolic-Numeric Computation 2007

www.orcca.on.ca/conferences/snc2007

July 25-27, 2007

Invited Speakers

André Galligo, U Nice
Erich Kaltofen, NCSU
Nick Trefethen, U Oxford
Charles Wampler, GM Research
Lihong Zhi, MMRC CAS

Topics

- Hybrid symbolic-numeric algorithms
- Approximate polynomial GCD and factorization
- Symbolic-numeric methods for polynomial systems
- Structured matrices in symbolic-numeric computation
- Differential equations for symbolic-numeric computation
- Symbolic-numeric algorithms for algebraic geometry, geometric computation and optimization
- Implementation of symbolic-numeric algorithms
- Model construction with approximate algebraic algorithms
- Applications of symbolic-numeric computation
- Numerical algebraic geometry

Important Dates

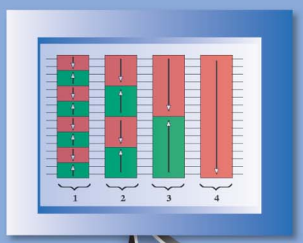
Submission deadline:	April 9, 2007
Notification:	May 28, 2007
Camera ready version due:	June 15, 2007

Program Committee

Dario Bini, Italy
Robert Corless, Canada
James Demmel, USA
Ioannis Emiris, Greece
Marc Moreno Maza, Canada
Bernard Mourrain, France
Victor Pan, USA
Greg Reid, Canada
Tateaki Sasaki, Japan
Andrew Sommese, USA
Jan Verschelde (Chair), USA
Dongming Wang, France
Zhonggang Zeng, USA

Joint Speakers

AD Kennedy, U Edinburgh
KO Geddes, U Waterloo (after dinner)



Parallel Symbolic Computation 2007

www.orcca.on.ca/conferences/pasco2007

July 27-28, 2007

Invited Speakers

Mike Bauer, UWO
Matteo Frigo, Cilk Arts
Thierry Gautier, INRIA
Katherine Yelick, UC Berkeley

Topics

- Parallel computer algebra
- High performance for exact and approximate procedures
- Analysis of parallel algorithms for algebraic computations
- Parallel computing for number theory, combinatorial and discrete methods
- Distributed data-structures for algebraic computation
- Implementations of solvers on multi-cores, SMPs, clusters, supercomputers and grids
- Interactive parallel symbolic computation
- Volunteer computing for symbolic problems
- Applications of parallel symbolic computation

Important Dates

Submission deadline:	April 16, 2007
Notification:	May 28, 2007
Camera ready version due:	June 15, 2007

Program Committee

Gene Cooperman, USA
Jean-Guillaume Dumas, France
Jean-Charles Faugère, France
Mark Giesbrecht, Canada
Erich Kaltofen, USA
Anton Leykin, USA
Marc Moreno Maza (Chair), Canada
Jean-Louis Roch, France
David Saunders, USA
William Stein, USA
Carlo Traverso, Italy
Gilles Villard, France

General Chairs:	Stephen M. Watt (SNC)	watt@orcca.on.ca	Local Arrangements:	Oleg Golubitsky	oleg@orcca.on.ca
	Marc Moreno Maza (PASCO)	moreno@orcca.on.ca		Éric Schost	schost@orcca.on.ca
Administration:	Meg Borthwick	meg@csd.uwo.ca	Publicity:	François Lemaire	lemaire@lifl.fr

MITACS NSERC CRSNG ORCCA FIELDS Western acm In Cooperation Maplesoft SHARCNET

University of Western Ontario, London Canada