Computational aspects of Commutative Algebra and Algebraic Geometry

26.05. – 30.05.1997

organized by

Eberhard Becker, Universität Dortmund, Germany
Wolfram Decker, Universität des Saarlandes, Germany
David Eisenbud, Brandeis University, USA
Hendrik W. Lenstra, Jr., University of California at Berkeley, USA
Barry Trager, IBM Watson Research Center, USA

Modern computer algebra systems allow the computation of complicated examples in Commutative Algebra, Algebraic Geometry and Arithmetic Geometry. During the last couple of years such computations have helped to predict and check many theorems. Vice versa, inspired by complicated examples coming from theory, computer algebra developers have refined their algorithms and implementations. The main goals of this meeting were to

- give developers of computer algebra systems and those who apply computer algebra in their theoretical research the possibility of exchanging ideas,

- to initiate cooperation between developers of different computer algebra systems,

- to present new algorithms and systems and recent theoretical developments as well.

In order to achieve our goals we kept the number of talks to roughly four per day. This allowed plenty of time for discussions at a blackboard or in front of a terminal, software demonstrations and introductionary tutorials, or other activities like a meeting on OpenMath.

1   Gröbner, Buchberger, Faugère in a Nutshell

Dave Bayer, Barnard College, Columbia University

Faugère's talk at this meeting on a new approach to computing Gröbner bases generated much excitement. In response, the organizers requested this survey talk for nonspecialists, a presentation of Gröbner bases and Faugère's method which assumed only "groups, rings, fields". After a review of Gröbner bases for polynomial ideals which included term orders, S-pairs, and their geometric interpretation as the limit of a flat family, we described Faugère's method: In a nutshell, he determines in a combinatorial phase a minimal basis of monomials which support the computation of a Gröbner basis. He then forms a matrix and applies modern, fast methods of linear algebra to the resulting elimination problem. In contrast, Buchberger's algorithm can be understood as combining these phases, with the linear algebra steps determined by the S-pairs.

It was an honor and great fun to describe Buchberger's and Faugère's algorithms to an audience that included Buchberger and Faugère. In the question and answer period, Faugère grinned, and Buchberger made some amplifying remarks.

2   The Hull Resolution

Dave Bayer, Barnard College, Columbia University

This talk describes joint work with Bernd Sturmfels, based on earlier joint work with Bernd Sturmfels and Irena Peeva. We develop a theory of "cellular resolutions" of monomial ideals, which are chains of syzygies modeled after the chain complex which computes the cellular homology of a regular cell complex. We extend this theory to include "monomial modules", which generalize monomial ideals to submodules of the Laurent polynomial ring. We then develop an equivalence of categories between toric ideals and monomial modules, and transfer the theory of cellular resolutions to toric ideals.

Extending a construction of Scarf, we define the "hull resolution" for monomial modules and toric ideals, as a cellular resolution supported on the convex hull of a rescaling of the generating exponents.

3 Composing power series over a finite ring in essentially linear time

D. J. Bernstein, University of Illinois at Chicago

Fix a finite commutative ring R. Let u and v be power series over R, with $v(0) = 0$. I presented an algorithm that computes the first n terms of the composition $u(v)$, given the first n terms of u and v, in $n^{1+o(1)}$ ring operations. The algorithm is very fast in practice when char R is a product of small primes.

4 Functors for Implementing Polynomial Ideal Theory   (The Theorema Project)

Bruno Buchberger, RISC, Austria

The Theorema Project aims at integrating proving support into computer algebra systems. It is motivated by past work in constructive polynomial ideal theory. The emphasis of the project is on proof generation for routine parts of proofs, structured proof presentation in natural language, and smooth interaction with the existing solving and computing facilities of computer algebra systems. Our present system frame is Mathematica 3.0.

We give an overview on the Theorema Project emphasizing the interaction between functors and special provers. A special prover is developed together with each functor. Provers can either be the know "black box" provers relying on algebraic methods or provers that emphasize the imitation of human proof styles. These provers give output in natural language and present proofs in nested cells so that browsing the proofs becomes easy.

The talk is accompanied by demos.

5 Chaos in Commutative Algebra

Ragnar-Olaf Buchweitz, University of Toronto

In this talk we discussed results and problems concerning the Hilbert-Kunz function of a ring in positive characteristic.

We presented earlier results by Kunz, characterizing regular rings through their Hilbert-Kunz functions, Monsky, describing Hilbert-Kunz functions of one dimensional rings and showing that the Hilbert-Kunz multiplicity always

exists.

We then reported on joint work (appeared in J. of Algebra) with Qun Chen calculating the Hilbert-Kunz functions both for elliptic curves in characteristic different from two (the remaining case was settled by Monsky) and for Cayley's cubic surface. As a consequence we obtain that the theoretical lower bound for the Hilbert-Kunz multiplicity of curves or surfaces is always attained.

We then turned our attention to the chaotic features of Hilbert-Kunz functions: Monsky showed that the Hilbert-Kunz function for certain families of quartic plane curves is governed by a "p-adic dynamical system" and determined the Hilbert-Kunz multiplicity in terms of the "escape time" of that system. Another chaotic phenomenon appears when one studies $d(i,j,k) = \dim_K K[x,y]/(F^i, G^j, H^k)$; $\operatorname{char} K = p > 0$; as a function of (i,j,k) for given pairwise coprime homogeneous polynomials F,G,H. When these polynomials are linear, Han showed that d(i,j,k) can be interpreted as the distance from a fractal that is similar to a Sierpinski sponge, or else, a three dimensional version of Pascal's triangle mod p.

In the meantime we have shown that d is a generalized taxicab distance from a fractal if only one of the three polynomial is linear. This result uses Kronecker's description of syzygies in terms of cointinued fraction expansions.

In all the results mentioned, heavy use was made of computer calculations and experiments, mainly using Macaulay and Maple. In fact, most results were predicted on the basis of computer experiments.

6 Yet Another Ideal Decomposition Algorithm

Massimo Caboara, Pasqualina Conti, and Carlo Traverso,
Dipartimento di Matematica, Pisa and Dipartimento di Matematica applicata, Pisa

The problem of decomposing an ideal into pure-dimensional components (resp. reduced pure-dimensional components) is a key step in several basic algorithms of commutative algebra.

Several algorithms have been proposed for this computation, and fall mainly into two classes: the family of projection algorithms, whose prototype is the primary decomposition algorithm of [2], and the direct, syzygy-based algorithms, like [3].

The superiority of one type of algorithms over the other has not been settled; in [3] it is argued that the direct methods are superior since for projection methods "sufficiently generic" projections are needed. This assertion is only marginally true for the current literature — already in [4] "generic linear combinations" are needed only for finding a single univariate polynomial, through linear algebra and a variation of [5], and the algorithms of [6] and [7] compute triangular decompositions through characteristic sets without changes of coordinates.
Moreover projection algorithms do not have the limitation to large characteristics of [3], in particular the example of D. Jaffe in [3] can be easily handled by our algorithm (and indeed by all projection algorithms).

In this paper we describe algorithms for equidimensional decompositions, that can be seen as a marginal modification of an algorithm of [4], but that completely avoid generic or random projections, and does not need lexicographic Gröbner bases or characteristic sets, hence can be a candidate to a best competitor against direct algorithms. Some tests seem to support the belief that our algorithms are much faster than direct algorithms.

The basic computational tools used in this paper are Gröbner bases with respect to suitable orderings, and ideal saturation, i.e. affine variety difference. We stress again that no projection in generic (or random) direction, addition of random linear forms, etc. are used. Computation of the dimension and of the multiplicity are used to guide some steps of the algorithms.

The relation of flatness with variation of staircases, that is our main proof tool, has already been considered in [1]; specialization of Gröbner bases is already a main tool in [2].

References

[1] D. Bayer, A. Galligo, M. Stillman, *Gröbner bases and extensions of scalars*, in: D. Eisenbud, L. Robbiano, *Computational methods in Algebraic Geometry and Commutative Algebra*, Symposia Mathematica 24 (1993)

[2] P. Gianni, B. Trager, G. Zacharias, *Gröbner bases and primary decomposition of polynomial ideals*, J. Symb. Comp. 6, 149–167 (1988)

[3] D. Eisenbud, C. Huneke, W. Vasconcelos, *Direct methods for primary decomposition*, Inventiones Math, 110, (1992), p. 207–235.

[4] M. Alonso, T. Mora, M. Raimondo, *Local decomposition algorithms*, IS-SAC 1990, LNCS (1990)

[5] J.C. Faugère, P. Gianni, D. Lazard, T. Mora, *Efficient computation of zero–dimensional Gröbner bases by change of ordering*, J. Symb. Comp. **16**(4), 329–344 (1993)

[6] D. Lazard, *A new method for solving algebraic systems of positive dimension,* Discr. App. Math, 33:147-160, (1991)

[7] M. Kalkbrener, *A generalized euclidean algorithm for computing triangular representations of algebraic varieties*, J. Symb. Comp., 15:143–167, 1993.

7 "Solving" Problems with `redlog` The Real Enneper Surface

Andreas Dolzmann, University of Passau

We demonstrate how REDLOG can be used to solve a problem in real algebraic geometry: The complex Enneper surface is given explicitly as the image of a polynomial parameterization and implicitly as the complex variety of a polynomial. We show that the corresponding real variety is exactly produced by the restriction of the given parameterization to real parameters. We explain all necessary computation steps, and sketch the algorithms involved.

The REDUCE package REDLOG by A. Dolzmann and T. Sturm provides symbolic algorithms on first-order formulas. Its focus is on simplification of quantifier-free formulas and on real quantifier elimination. Besides the built-in algorithm for quantifier elimination REDLOG provides interfaces to two external implementations of quantifier elimination algorithms: QEPCAD by H. Hong and RQEPRRC by the author.

8 Projective Codes: Construction and Problems

Noam D. Elkies, Harvard University

We recall the construction of Goppa's codes: these are the spaces $\Gamma(L)$ where L is a line bundle on a curve X of genus g with $N > \deg L$ rational points over a finite field F. Here each $c \in \Gamma(L)$ is regarded as an N-tuple of elements

of F by arbitrarily identifying each of the N fibers above $X(F)$ with F. By Riemann-Roch this code consists of at least $|F|^{\deg L+1-g}$ words, any two of which agree on at most $\deg L$ coordinates. If F is fixed and X is "asymptotically optimal" — i.e. varies in a family with $g \to \infty$ and $N/g \to |F|^{1/2} - 1$ (the maximum allowed by Drinfeld-Vlăduţ, which is attained when $|F|^{1/2} \in \mathbf{Z}$ by suitable modular curves X) — the resulting codes have excellent parameters; in particular they have the best parameters known if $|F|$ is a square ≥ 49. We observed recently that one does even better by using instead the set C of all rational functions $f \in F(X)$ whose degree (as maps from X to $\mathbf{P}$) is at most h, considered as N-tuples of elements of $bfP^1(F)$. Any two such can agree on at most $2h$ coordinates, and we can show that for h in the range of interest and X asymptotically optimal the number M of codewords is $((|F| + 1)/|F|)^{N+o(N)}$ times that of the corresponding Goppa codes (with $\deg L = 2h$). We then raise several algorithmic questions suggested by this construction:

1) Given a curve X over some field F, a list $p_1, \ldots, p_N$ of points and elements $c_1, \ldots, c_N \in \mathbf{P}^1(F)$, and an integer $h < N/2$, does there exist a function $f \in F(X)$ of degree $\leq h$ such that $f(c_i) = p_i$ for each i? [The corresponding problem is "easy" for Goppa's codes since it reduces to linear algebra; one can also solve it here by linear algebra if X is rational, or of small genus, but we are interested in large g.]

2) More generally, if $h + e < N/2$ and $f(c_i) = p_i$ holds fo all but e choices of $i \in [1, N]$, recover f. [This is tractable for Goppa if the number e of errors is small enough, but open if e is allowed to be as large as $(N - \deg L)/2$.]

3) Find an easily computable injection $\{1, 2, \ldots, M^{1-\epsilon}\} \hookrightarrow C$, i.e. a labeling of "most" of C, preferably with the inverse map also easily computable. [The corresponding problem for Goppa is again trivial, even with $\epsilon = 0$, once a basis for $\Gamma(L)$ is computed.]

Also, a more conceptual question:

4) The factor $((q + 1)/q)^{N+o(N)}$ (which arises essentially as $L_X(1)/L_X(2)$, as in Schanuel's theorem) means that if X is asymptotically optimal and we choose a random map $\phi : X \to \mathbf{P}^1(F)$ and arbitrarily identify $\mathbf{P}^1(F) - \phi(p)$ with F for each $p \in X(F)$ then the subcode $\{c \in C : \forall p \in X(F), c_p \neq \phi(p)\}$, considered as a subset of F^N, is asymptotically just as good a code as Goppa's. Is there a conceptual reason for this coincidence?

Finally, a question about the construction of asymptotically optimal curves X. All the known examples of simple explicit equations for optimal towers (see Garcia-Stichtenoth) are of the form: X has coordinates $x_1, \ldots, x_r$ and rela-

tions $\Phi(x_j, x_{j+1}) = 0$ ($1 \leq j < r$) for some fixed irreducible polynomial Φ and $r \to \infty$. All such towers turn out to be modular in an appropriate sense (classical $X_0(\cdot)$, Shimura, or Drinfeld).

5) If Φ gives rise to an asymptotically optimal tower of curves, is the tower necessarily modular?

9 Efficient Algorithms and Softwares for Solving Polynomial Equations

Jean-Charles Faugère, Paris VI

This talk presents new algorithms for solving polynomial systems and in particular a new efficient algorithm for computing Groebner bases. To avoid as much as possible intermediate computation, the F4 algorithm computes successive truncated Groebner bases and replaces the classical polynomial reduction found in the Buchberger algorithm by the simultaneous reduction of several polynomials. This powerful reduction mechanism is achieved by means of a symbolic precomputation and by extensive use of sparse linear algebra methods.

Some previously untractable problems (Cyclic 9) are presented as well as an empirical comparison of a first implementation of the algorithms with other well known programs.

10 Computations with Approximate Ideals

P. Gianni and B. Trager, Dipartimento di Matematica, Pisa and IBM Watson Research Center

In this talk we present methods designed for working on zero–dimensional ideals defined by polynomials with "approximate" coefficients. We state bounds sufficient for determining a linear basis for the elements of the ideal in fixed degree.
As an application we find the special adjoints for an approximate plane curve with quadratic singularities. Similar techniques allow one to compute the multiplication matrices for the residue algebra. We show how to use re-ordered Shur factorization to reduce the multivariate problem to a univariate one. This allows us to find the roots of a system of multivariate equations even in the case of multiple roots in a numerically stable way.

11 Overview of Singular

Gert-Martin Greuel, Universität Kaiserslautern

Singular is a special-purpose computer algebra system for commutative algebra, algebraic geometry and singularity theory. The main features of Singular are:

- Computations in very general rings (polynomial rings, localizations of rings at a prime ideal, tensor products of rings) over many ground fields (rational numbers, mod p numbers, Galois fields, transcendental/algebraic extensions) and monomial orderings (all standard monomial orderings, including matrix orderings)

- Very fast standard (resp. Groebner) bases computations

- Polynomial factorization, resultant, and gcd computations

- Large variety of implemented related algorithm: FGLM, Hilbert-driven, Factorizing Buchberger; Minimal resolutions, Primary decomposition; Usual ideal theoretic operations; standard combinatorial algorithms.

- Efficient and flexible communication links based on the MP protocol and library

- Easy-to-use, command-driven user-interface

- Intuitive, C-like programming language

- Extensive libraries of procedures, written in Singular's programming language

- Written in C/C++. Available as binary program for common hard- and software platforms (including most Un*x variants, MS-DOG, MacOS)

12 Computing the Normalization of a Reduced Noetherian Ring $\mathbb{R}$

Theo de Jong, Universität des Saarlandes, Saarbrücken

In this talk we consider the problem of computing the normalization of a reduced Noetherian ring R. Basic is the following normality criterion.

Theorem. Let I be a radical ideal of R. Suppose that for all prime ideals p

of R with $R_{\mathfrak{p}}$ not normal, it follows that $\mathfrak{p} \supset I$. Then $R = \mathrm{Hom}_R(I, I)$ if and only if R is normal.

For I one can take for example the reduced ideal of the singular locus of R, but there might be many more possibilities. It follows from the Cayley-Hamilton theorem that $\mathrm{Hom}_R(I, I)$ is a subring of the normalization. Now suppose the normalization of R is finitely generated over R.

So if we define $R_0 = R$, and $R_{j+1} := \mathrm{Hom}_{R_\mathbf{j}}(I_j, I_j)$ fo some ideal I_i satisfying the conditions of the theorem, we eventually have that R_i is equal to the normalization.

13   FOXBOX

Erich Kaltofen, North Carolina State University

The FOXBOX system puts in practice the black box representation of symbolic objects and provides algorithms for performing the symbolic calculus with such representations. Black box objects are stored as functions.

For instance:a black box polynomial is a procedure that takes values for the variables as input and evaluates the polynomial at that given point. FOXBOX can compute the greatest common divisor and factorize polynomials in black box representation, producing as output new black boxes. It also can compute the standard sparse distributed representation of a black box polynomial, for example, one which was computed for an irreducible factor. We establish that the black box representation of objects can push the size of symbolic expressions far be yond what standard data structures could handle before.

Furthermore, FOXBOX demonstrates the generic program design methodology. The FOXBOX system is written in C++. C++ template arguments provide for abstract domain types. Currently, FOXBOX can be compiled with SA CLIB 1.1, Gnu-MP 1.0, and NTL 2.0 as its underlying field and polynomial arithmetic. Multiple arithmetic plugins can be used in the same computation.

FOXBOX provides an MPI-compliant distribution mechanism that allows for parallel and distributed execution of FOXBOX programs. Finally, FOXBOX plugs into a server/client-style Maple application interface.

14 Solving Systems, Prime Decomposition and Triangular Sets

Daniel Lazard, Université de Poitiers

For solving polynomials systems, Groebner basis have intinsically a double exponential complexity. An alternative approach consists in splitting the problem during the computation and to describe the solutions as a set of triangular systems. There are several methods for such an approach (Kalbrenner, myself, Dongming Wang,...). Recent implementation of these methods by M. Moreno-Maza and P. Aubry have made significant progresses in the practical efficiency of these algorithms. Nevertheless, much work is yet needed to make them competitive with Groebner base approach, and reach the simple exponential complexity with practically efficient algorithms.

15 Linear Algebra with a View towards Polynomial System Solving

B. Mourrain, INRIA, Sophia Antipolis

This talk is an introduction to linear algebra methods for solving a polynomial system $f_1 = \ldots = f_m = 0$. The approach is illustrated by explicit computations in MAPLE. We first describe the quotient algebra A by the ideal $I = (f_1, \ldots, f_m)$ in terms of the multiplication operators. We show how resultant matrices allow to handle this structure, in the generic case. Next, we consider Bezoutian matrices which allow to solve many effective problems for a wider class of polynomial systems. We give a brief description of algebraic residues and some of its numerous applications. The matrices involved in these computations have a structure that we recall. We end with the description of complete methods for solving polynomial systems, exploiting the tools and the structure of the matrices, previously described.

16 Quadratic Algebras – New results.

Jan-Erik Roos, University of Stockholm

Let k be a field, $k[x_1, x_2, \ldots, x_n]$ the commutative polynomial ring in the $x_1, \ldots, x_n$ and let $R = k[x_1, \ldots, x_n]/(f_1, \ldots, f_t)$ where the f_i are quadratic forms in the x_j.
We say that R is a *quadratic algebra*. Let V be the k-vector space gener-

ated by the x_i, and let $T(V)$ be the tensor algebra on V. We can write $R = T(V)/(W)$ where $W \subset V \otimes_k V$ is the subvector space generated by the f_i and the $x_s \otimes x_k - x_k \otimes x_s$. Now define the *dual quadratic algebra* $R^!$ of R by $R^! = T(V^*)/(W^\perp)$, where $V^* = \mathrm{Hom}_k(V, k)$ and $W^\perp = \{f \in V^* \otimes V^*, s.t. f|W = 0\}$ One proves that $R^!$ is a graded Hopf algebra and that furthermore $R^! = U(\eta)$ (= the enveloping algebra of a graded super Lie algebra $\eta = \eta^1 \oplus \eta^2 \oplus \cdots$). The Hilbert series of $R^!$ will be denoted by $R^!(t)$ and according to the Poincaré-Birkhoff-Witt theorem

$$R^!(t) = \frac{(1+t)^{\eta_1}}{(1-t^2)^{\eta_2}} \cdot \frac{(1+t^3)^{\eta_3}}{(1-t^4)^{\eta_4}} \cdots \qquad (*)$$

(in (*) η^i is the rank of η^i). If η is nilpotent of some degree ν, then (*) is a *finite* product and $R^!(t)$ converges for $|t| < 1$. D. Anick and C. Löfwall asked 15 years ago if there existed R such that $\eta = \eta_R$ was not nilpotent, but nevertheless $R^!(t)$ converged for $|t| < 1$ (then $R^!(t)$ is an irrational function). Such examples of R were found by computers studies using MACAULAY and BERGMAN, and the simplest example seems to be

$$R = \frac{k[x, y, z, u, v]}{(y^2, yz + xu, z^2 - yu - xv, zu + yv, u^2)},$$

for which the ranks of the η^i are (when $\mathrm{char} k = 0$)

$$5, 5, 3, 3, 5, 6, 3, 3, 5, 6, 3, 3, \cdots$$

If char $k = p \neq 0$ we have a similar behavior, but the series $R^!(t)$ are different for all p. This has applications in algebraic topology (existence of lots of torsion in integral loop space homology of some finite, simply-connected CW-complexes of dimension ≤ 4).

REFERENCE

Clas Löfwall and Jan-Erik Roos, *A Non Nilpotent 1-2-presented Graded Hopf Algebra whose Hilbert Series Converges in the Unit Circle*, and the literature cited there. Preprint, 1997, available from address above.

17 Riemann Surfaces, Plane Algebraic Curves and their Period Matrices

Robert Silhol, Université Montpellier, and Patricia Gianni, Dipartimento di Matematica, Pisa, Mika Seppälä, University of Helsinki, and Barry Trager, IBM Watson Research Center

The aim of this talk is to present a theoretical basis for computing a representation of a compact Riemann surface as an algebraic plane curve and to compute an numerical approximation for its period matrix. We will describe a program CARSS that can be used to define Riemann surfaces for computations. CARS allows one also to perform the Fenchel-Nielsen twist and other deformations on Riemann surfaces.

Almost all theoretical results presented here are well known in classical complex analysis and algebraic geometry. The contribution of this talk is the design of an algorithm which is based on the classical results and computes first an approximation of a polynomial representing a given compact Riemann surface as a plane algebraic curve and further computes an approximation for a perio d matrix of this curve. This algorithm thus solves an important problem in the general case. (This problem was first solved, in the case of symmetric Riemann surfaces.)

18 Computing Differential Galois Groups

Michael F. Singer, North Carolina State University

At present, we do not know a general algorithm that will compute the Galois group of a linear differential equation with coefficients in a differential field k, even when $k = \overline{Q}(x)$, where $\overline{Q}$ is the algebraic closure of the rational numbers. In this talk we give an introduction to differential Galois theory and give an overview of the techniques used to compute Galois groups in special circumstances. We will focus on two particular techniques:

1. the use of representation theoretic techniques to give algorithms that determine the Galois groups of linear differential equations over $\overline{Q}(x)$ of orders $2, 3$, and 4, and

2. the use of constructive invariant theory to give algorithms that compute the Galois groups of linear differential equations over $\overline{Q}(x)$, assuming that the Galois group is reductive.

Detailed treatements of these subjects (and further references) can be found in the papers *Direct and Inverse Problems in Differential Galois Theory*

and *Computing Galois Groups of Completely Reducible Differential Equations (with E. Compoint)* available at `http://www4.ncsu.edu/~singer`
.

19 Finite Flat Algebras and the Lemma of Diamond

Bart de Smit

In the Springer-volume on the Boston conference on Wiles's proof of Fermat's Last Theorem, one finds Rubin's improvement of the Wiles-Faltings criterion for complete intersections, which avoids the standard limiting process. In recent work of F. Diamond, (Inventiones, 1997) this limiting process is introduced again to give a stronger result.

Diamond raises the question whether one can do this also purely in terms of Artinian rings. This leads to the following fundamental question. Let $A \subset B$ be a finite flat extension of split local artin algebras over a field with the same embedding dimension. Then is it true that every finite B-module which is flat over A is also flat over B? We discuss some partial answers.

20 Higher dimensional partial fractions

Jeremy Teitelbaum, University of Illinois at Chicago

In this talk, which dealt with work in progress, I described a generalization of the decomposition of a univariate rational function into partial fractions to the case of a multivariate rational function with denominator a product of linear forms. In the one-variable case, the coefficients of a partial fraction decomposition may be computed locally by means of residues. In higher dimensions, one must consider a residue which is computed along a complete flag of linear subvarieties of $\mathbf{P}^n$. I defined this residue, described its basic properties, and described the extent to which this type of residue may be used to compute the higher dimensional partial fraction expansion.

The partial fraction decomposition I discussed was originally constructed by Varchenko and Gelfand (see Theorem 21 of Varchenko, A. N. and Gelfand, I.M., Heaviside Functions of a Configuration of Hyperplanes, Functional Analysis and its Applications, Vol. 21, No. 4, 1987, pp. 1-18.) The results on residues grow out of joint work with Peter Schneider of Muenster, Germany, on p-adic symmetric spaces.

21 Normalization

Barry Trager and Patrizia Gianni, IBM Watson Research Center and Dipartimento di Matematica, Pisa

After giving a proposition which reduces the problem of computing the integral closure of a general noetherian ring to the three problems of:

- Compute a universal denominator d (non-zero divisor in the conductor).

- Compute radical of the ideal generated by d.

- Compute ideal quotients

We show that for the common case of affine domains, i.e. domains which are finitely generated over fields of characteristic zero, we can use an effective localization in order to perform most of the computation in one dimensional rings where it can be done with linear algebra, i.e. hermite normal form computations.

22 Computational Geometry Problems in REDLOG

Volker Weispfenning, Universität Passau

REDLOG is a REDUCE-package for first order logic developed by A. Dolzmann and T. Sturm. Its main goal is low-degree real quantifier elimination with answers. We outline the elimination method by test-terms and illustrate the scope of the package by a series of examples in computational geometry. They include automatic theorem proving in geometry, shading and aspects of objects under parallel and central projections, reconstruction of objects from a projection, computation of equidistance surfaces and offsets, and collision problems.

We conclude with some examples in computational solid modeling concerning autoamtic rounding and blending of solids.