Bruno Buchberger, James Davenport,
Fritz Schwarz (editors):

Algorithms of Computeralgebra

Dagstuhl-Seminar-Report; 27
16.-20.12.91 (9151)

ISSN 0940-1121

Tel.: +49-6871 - 2458
Fax: +49-6871 - 5942

Das Internationales Begegnungs- und Forschungszentrum für Informatik (IBFI) ist eine gemeinnützige GmbH. Sie veranstaltet regelmäßig wissenschaftliche Seminare, welche nach Antrag der Tagungsleiter und Begutachtung durch das wissenschaftliche Direktorium mit persönlich eingeladenen Gästen durchgeführt werden.

Bezugsadresse: Geschäftsstelle Schloß Dagstuhl
Informatik, Bau 36
Universität des Saarlandes
W - 6600 Saarbrücken
Germany
Tel.: +49 -681 - 302 - 4396
Fax: +49 -681 - 302 - 4397
e-mail: office@dag.uni-sb.de

Algorithms of Computeralgebra

December 16-20, 1991

Schloß Dagstuhl

Organizers: Bruno Buchberger, James Davenport, Fritz Schwarz

Foreword

Computer algebra has been established as a new field on the borderline between mathematics and computer science for about 20 years now. It has been the goal of this seminar to get together researchers from various subfields in a well balanced mixture. There have been two talks on polynomial factorization (Kaltofen, von zur Gathen), two on number theory (Pethö, Zimmer), five on Gröbner base theory and elimination (Lazard, Möller, Pedersen and Sturmfels, Traverso, Weispfenning), three talks on differential equations (Bronstein, Singer, Schwarz), a talk on Lie algebras (Laßner), on group theory (Michler), on arithmetic (Schönhage), on asymptotic analysis (Gonnet), on algbraic geometry (Giusti and Heintz) and on polynomial zeros (Krandick).

There will be hardly any other field where researchers with such a wide range of interests and different backgrounds have joined to form a new community as it is true for computer algebra. This becomes obvious just by looking at the contents of this brochure. In this situation it is especially important to get together in an informal manner such that new relations between researchers from these various subfields hopefully will be established. With this goal in mind, Schloß Dagstuhl is the ideal place to go. Therefore it will be an important aim to repeat these seminars on a two year schedule.

F. Schwarz

Vorträge

M. Singer: *Bounds and Necessary Conditions for Liouvillian Solutions of (third order) Linear Differential Equations*

This is a report on joint work with F. Ulmer. We show how group theoretic techniques yield the best possible bound for the degree of the minimal polynomial of an algebraic solution of the Riccati equation associated to a linear differential equation $L(y) = 0$. For an irreducible third order equation, this degree belongs to $\{3, 6, 9, 21, 36\}$. We also derive a set of necessary conditions on the coefficients of $L(y) = 0$ for $L(y) = 0$ to have a Liouvillian solution (a solution expressible in terms of integrals, exponentials and algebraic functions). These improve the necessary conditions of the Kovacic algorithms and extend them to third order equations. We also show that if the differential Galois group of $L(y) = 0$ is primitive and unimodular, then there is an algebraic solution such that the number of non-zero coefficients of the minimal polynomial of z does not exceed the smallest degree of an algebraic solution of the Riccati equation. Finally, we derive a bound for the degree of the minimal polynomial of z and show that for third order equations, contrary to the second order case, this degree is always less than the order of the differential Galois group of$L(y) = 0$.

M. Bronstein: *Algorithms for linear ordinary differential equations*

Let K be a field of characteristic 0 with algebraic closure $\bar{K}$, x be an inderminate over K and $L = \sum a_i \partial_x^i \in K[x][\partial_x]$ be an n^{th}-order linear ordinary differential operator with polynomial coefficients. Algorithms that either factor L over $\bar{K}[x]$ or compute the Liouvillian (i. e. closed form) solutions of $Ly = 0$ both reduce to the following question: given an m^{th}-order $\tilde{L} \in K[x][\partial_x]$ (with $m \geq n$), does $\tilde{L}y = 0$ have a solution u such that $du/dx \in \bar{K}[x]$. This question must be answered for several operators of ever-increasing order. While a decision procedure for this subproblem was known in the 19th century, it requires factoring polynomials over $\bar{K}$ and has not been implemented in full generality. We present an efficient algorithm for this question which has been implemented in the AXIOM computer algebra system for operators of arbitrary order over arbitrary fields of characteristic O. The algorithm is "rational" in the sense that algebraic numbers are introduced only if they appear in potential solutions, and not in the singularities of the equation as was previously done. Implementation of the complete Singer algorithm for $n = 2, 3$ based on this building block is in progress.

E. Kaltofen: *Factoring Polynomials over Algebraically Closed Fields*

A polynomial is absolutely irreducible if the polynomial cannot be factored in any extension, algebraic or otherwise, of the coefficient field. When decomposing a multivariate polynomial into its absolutely irreducible factors several questions arise: How are the coefficients of the factors represented? Can the complexity of the algorithm be estimated without regard to the representation of elements in the coefficient-field? How is the problem related to factoring over the coefficient field?
A theorem by Emmy Noether shows that testing for absolute irreducibility can be decided purely by arithmetic in the coefficient field. We show that for coefficients in the usual domains, say the rationals, and with a suitable representation, factorizations over the algebraic closure can be performed within the complexity class $\mathcal{NC}$. More importantly we give new effective versions of certain irreducibility theorems, such as Noether's or Hilbert's. The proofs of these theorems also answer the question on the bit complexity of our algorithm viewed for abstract coefficient fields.

A. Schönhage: *Real and Complex High Precision Squareroot Computations*

Reports on a fast routine SQRT for given $x > 0, \varepsilon = \Delta^{-5} (\Delta = 2^{32})$ to find u such that $|x - u^2| < \varepsilon$. Typical cases ($|logx|$ small) require computation of m words in u, where $m \sim s$.
For moderate m ($m < 676$) a wordwise method WROOT analogous to the school method is used, with $\frac{1}{4}m^2$ inner loops (one *, one +) plus a linear overhead. For large values of N bits precision the FFT-based integer multiplication yields running times for "SROOT" of about $7.5 \cdot N \cdot lgN \cdot lglgN$ time units ($1\ unit \cong 0.2\mu sec$ on a SUN 3/80), like 41 sec for $N = 320000$.
Similar methods are possible for $\sqrt{a + ib}$, with $4 \cdot \frac{1}{4}m^2$ loops wordwise, $15 \cdot N \cdot lgN \cdot lglgN$ units asymptotically.

C. Traverso: *Gröbner bases and integer programming*

The linear programming problem is: given $A = (a_{i,j}) \in \mathbf{Z}^{n,m}$, $c_j \in \mathbf{R}^n$, find $\xi_j \in \mathbf{Z}^n, \xi_j \geq 0$, such that $\sum a_{ij}\xi_j = 0$ and $\sum c_j\xi_j$ minimal.
We give two algorithms for the solution, using Gröbner bases.
Notations If $\eta \in \mathbf{Z}$ let $\eta^+ = \eta$ or 0, $\eta^- = 0$ or η if $\eta \geq 0$ or $\eta < 0$.

First algorithm Consider indeterminates Y_i, X_j, T and

$$f_j = \prod Y^{a_{ij}^+} - X_j \prod Y^{a_{ij}^-}, \quad f_0 = \prod Y_i - 1$$

Consider a term ordering such that $Y_i,\ T > X_j^N$, and $\prod X_j^{\alpha_j} > \prod X_j^{\beta_j}$ implies $\sum c_j\alpha_j \geq \sum c_j\beta_j$; (theorem: it exists iff no descending chains of solutions of $AX = 0$ exist). Consider a Gröbner basis G of (f_j). Let $b_0 = min\ b_i$, and let $g = T^{b_0^-} \prod Y_i^{b_0^- + b_i}$. Let the normal form of g be $T^\phi \prod Y_i^{\eta_i} \prod X_j^{\xi_j}$; then a solution exists iff $\phi, \eta_i = 0$, and the minimal solution is (ξ_j).

Second algorithm Let $\{S_l\}$, $S_l = (s_{lj})$ be a basis of the lattice of integer solution of AX = 0, and $(\bar{\xi}_j)$ a solution in **Z** of AX = B. Assume that the S_l are positive in term-ordering. Let

$$f_l = X_j^{a_{lj}^+} - \prod x_j^{s_{lj}^-}, f_0 = T \prod X_j - 1$$

Consider a Gröbner basis of (f_l) (same term-ordering as above). Let $\bar{\xi}_0 = min\bar{\xi}_i$, $g = T^{\bar{\xi}_0} \prod X_j^{\bar{\xi}_j + \bar{\xi}_0}$; let $T^{\xi_0} \prod X_j^{\xi_j}$ be the normal form of g. Then a solution exists iff $\xi_0 = 0$, and the minimal solution is (ξ_j).

Buchberger algorithm can be modified with some special features that take care of the special form of the ideal basis (difference of monic monomials, all monomials are invertible): common factors can be divided, multiple reductions can be performed easily, special data structures can be used. A dedicated implementation is planned. This is a joint work with P. Conti.

References: P. Conti, C. Traverso, *Buchberger Algorithm and Integer Programming*, Proc. AAECC9, 1991, LNCS, Springer Verlag

F. Ollivier, *Canonical Bases: Relations with Standard Bases, Finiteness Conditions and Application to Tame Automorphisms* in: Mega-90, proceedings, Birkhauser, Progress in Mathematics, 379-400, 1991

L. Pottier, *Minimal solutions of linear diophantine systems: bounds and algorithms*, in: Proceedings RTA '91, Como, LNCS 488, Springer Verlag

Pethö: *Computation of all inequivalent, cubic polynomials up to discriminant 50.000*

My talk is based on a joint work with N. Schulte. The polynomials $P, Q \in Z[x]$ are called equivalent if there exist $\epsilon, \eta \in \{-1, 1\}$, $h \in Z$ with $P(x) = \epsilon R(\eta x + h)$. Let $h(n, D)$ denote the number of classes of polynomials of degree n and discriminant D.

Delone (1928) proved that $h(3, D)$ is finite for any $D \in Z \backslash \{0\}$. In the talk we have given an algorithm for computing representatives of equivalence classes for cubic polynomials with given discriminant. Our method is based on the resolution of cubic index form equations. We applied the method for all $D \leq 50.000$.

Based on the result of the computation we conjecture that

$$lim_{x \to \infty} \frac{1}{x} \sum_{0 < D \leq x} h(3, D)$$

exists.

Lazard: *About Stewart Platforms*

A Stewart platform is a robot with 6 legs, the position of which is commanded by acting on the length of the legs. Computing the position of the platform from the lengths of the legs is a difficult task which appears to be a good test for Gröbner base algorithms. By using various softwares related to Gröbner bases and geometric considerations, it is proved that the number of positions of a planar Stewart platform, if finite, is at most 40. Three open problems are left.

1. Extend the result to non-planar platforms.
2. Explain why in each specific case the number of complex positions is 8, 16, 24 32 or 40.
3. Determine the maximal number of real positions which is between 16 and 40 and guessed to be 16.

. **Möller:** *Gröbner Bases Computation using Syzygies*

Together with C. Traverso (Pisa) and T. Mora (Genova), I developed an algorithm, which based on Buchberger's algorithm computes a Gröbner basis (G. B.) for an ideal and simultaneously a G. B. for its module of syzygies. This simultaneous computation has advantages since it allows to detect many more superfluous S-polynomial reductions than the existing variants of Buchberger's algorithm. Simplified versions of this new algorithm do not compute the syzygies completely - and hence compute only the G. B. for the ideal - but produce still some additional criteria for avoiding superfluous S-polynomial reductions. These simplified versions are also useful for controlling the output of the algorithm when instead of exact arithmetic floating point arithmetic is employed.

. **Giusti and J. Heintz:** *The determination of isolated points and dimension of an algebraic variety can be computed in polynomial time*

We show that the dimension of an algebraic (affine or projective) variety can be computed by a well parallelizable arithmetical network in non-uniform polynomial sequential time in the size of the input. This input is given by a system of polynomial equations written in dense representation. The coordinates of the ambient space can be put in Noether position w. r. t. the variety within the same time bounds.

By the way, we consider as an intermediate problem the determination of the isolated points of the given variety, which is of obvious practical interest. We suppose that the base domain, from where the coefficients of the input polynomials are taken, is infinite and, in the case of an affine variety, that its field of fractions is perfect. If this domain consists of the integers, our algorithms can be realized by boolean networks of the same complexity type (however these networks are not uniform w. r. t. the number of variables occuring in the input polynomial). Our results imply an effective version of the affine Nullstellensatz in terms of degrees and straight line programs.

G. Michler: *Fast Fourier Transforms on Symmetric Groups*

This lecture is a report on a joint paper with S. Linton (University of Cambridge) and J. B. Olsson (University of Copenhagen). According to Diaconis and Rockmore (J. Amer. Math. Soc. 3 (1990)) new efficient algorithms are mandatory for applications in statistics. In particular, they are needed for statistical ranking problems. In my joint article with Linton and Olsson new and practical algorithms are introduced for the computation of the Fourier transforms

$$\hat{f} = \sum_{s \in S_n} f(s)\rho(s) \in GL(m, F)$$

of a function $f : S_n \to F$ from the symmetric group S_n into a field F at all the irreducible representations ρ of S_n are introduced. These algorithms use the model of monomial representations for the irreducible representations ρ of S_n described recently by Inglis, Richardson and Saxl. They are also practical tools for computing inverse Fourier transforms. These algorithms have been implemented and tested for the symmetric groups S_n with $6 \leq n \leq 10$. The CPU times of the computations on an IBM RISC 6000-540 are given in the talk. Our algorithm is easy to implement and requires only small storage place and low start up costs.

J. v. z. Gathen: *Factoring polynomials over finite fields*

A new probabilistic algorithm for factoring univariate polynomials over finite fields is presented. To factor a polynomial of degree n over $\mathtt{F}_q$, the number of arithmetic operations in $\mathtt{F}_q$ - ignoring factors of $\log n$ - is $O(n^2 + n \log q)$. The main technical innovation is a new way to compute Frobenius and trace maps in the ring of polynomials modulo the polynomial to be factored.

V. Weispfenning: *Parametric Gröbner bases - Theory and practice*

Gröbner bases for polynomials with parametric coefficients are well-known to be unstable under specialization of the parameters. We present the construction of comprehensive Gröbner bases that overcome this problem and hence can be used for fast elimination theory. The construction has been implemented in ALDES/SAC-2 and AXIOM by E. Schönfeld and W. Faas at the University of Passau. Let K be an integral domain, $R = [U_1, \ldots, U_m]$, $S = [X_1, \ldots X_n]$. We regard the U_i as parameters and the X_i as the main variables. A specialization is a homomorphism $\sigma \to K'[X_1, \ldots, X_n]$, where K' is an arbitrary field; σ extends canonically to $s : S \to K'[X_1, \ldots, X_n]$.

Theorem. Let $<$ be a term order on the set of terms in $X_1, \ldots, X_n$. There exists an algorithm that from a given finite $F \subseteq S$ computes a finite $G \subseteq S$ with the following property: For every specialization $\sigma : R \to K'$, $\sigma(G)$ is a Gröbner basis of $Id(\sigma(F))$. G is called a *comprehensive* Gröbner basis of $Id(F)$.

For moderate size examples $n \leq 4$, $m \leq 4$, *degree* ≤ 3) the implementation produces a moderate size comprehensive Gröbner basis in running times from a second to about 3 minutes.

B. Sturmfels: *Sparse Elimination Theory*

The $\mathcal{A}$-resultant $\mathcal{R}_{\mathcal{A}}(c_{ij})$ is the unique irreducible polynomial in the generic coefficients of a polynomial system

$$c_{i1}\bar{x}^{a_1} + c_{i2}\bar{x}^{a_2} + \ldots + c_{in}\bar{x}^{a_n} = 0 \qquad (i = 1, \ldots, K+1, \mathcal{A} = \{a_1, \ldots a_n\} \subseteq \mathbf{Z}^K)$$

which vanishes whenever this systemhas a zero in $(\mathbf{C}^*)^K$. In this talk we discuss the $\mathcal{A}$-resultant for the case where $\mathcal{A} = d_1\Delta_{l_1} \times \ldots \times d_r\Delta_{l_r}$ is the vertex set of a product of scaled standard simplices. The corresponding polynomial system consists of $l_1 + \ldots + l_r + 1$ equations which are multihomogeneous of degree $(d_1, \ldots d_r)$ in variables $\bar{x}_i = (x_{i1}, x_{i2}, \ldots, x_{il_i})$, $i = 1, 2, \ldots r$.

We present a joint result with Andrei Zelevinsky, stating that $\mathcal{R}_{\mathcal{A}}$ has at least $r!$ distinct formulas of Sylvester type if ($l_i = 1$ or $d_i = 1$) for $i = 1, 2, \ldots r$. Special cases of particular interest are the hyperdeterminant (all $d_i = 1$) and the Dixon resultant (all $l_i = 1$).

P. Pedersen joint with B. Sturmfels: *Sparse Resultants*

It is possible to generalize the familiar formula $Res(f, g) = a_0^m \prod_{f(\alpha)=0} g(\alpha)$ to the case of $n+1$ mixed, generic Laurent polynomials $f_i = \sum_{q \in \mathcal{A}_i} c_q x^q$, $i = 0, \ldots, n$, where $\mathcal{A}_i \subseteq \mathbf{Z}^n$, $x^q = x_1^{q_1} \ldots x_n^{q_n}$.

Following Bernstein (Fun. Anal.& its applications **9** (1975)) we define:

$S_i = conv(\mathcal{A}_i)$,

$S_{i\nu}$ = minimal supporttree in the direction $\nu \in S^{n-1}$,

$< \nu >^{\perp}$= lattice perpendicular to ν,

L_ν = factor lattice $\mathbf{Z}^n / < \nu >^{\perp}$,

h_ν = height of $S_{0\nu}$ from an arbitrary origin 0 with respect to L_ν.

Then there exists an affine resultant $R(f_0, f_1, \ldots f_n)$ such that

$$\exists \alpha \in (\mathbf{C}^*)^n \quad f_0(\alpha) = f_1(\alpha) = \ldots = f_n(\alpha) = 0 \Leftrightarrow R(f_0, f_1, \ldots f_n) = 0$$

$$(*) \quad R(f_0, f_1, \ldots, f_n) = \prod_{\alpha \in \nu(f_1, \ldots, f_n)} f_0(\alpha) \cdot \Big(\prod_{\nu \in S^{n-1}} R(f_{1\nu}, \ldots, f_{n\nu})^{h^\nu} \Big),$$

(1) All but finitely many factors in the product $\prod_{\nu + S^{n-1}}$ are equal to 1.

(2) $R(f_0, f_1, \ldots f_n)$ is irreducible.

(3) $deg_{f_i}(f_0, f_1, \ldots, f_n) = V(f_0, f_1, \ldots, \hat{f}_i, \ldots, f_n)$ = Minkowski mixed volume.

(4) $R(f_0, f_1, \ldots f_i, f_i', \ldots, f_n) = R(f_0, f_1, \ldots f_i, \ldots, f_n) R(f_0, f_1, \ldots f_i', \ldots, f_n)$.

G. Gonnet: *New algorithms for asymptotic and series computations*

Computing asymptotic series is an important area in computer algebra systems. Whether these are used directly or whether they are used to determine limits, they are needed by various other functions (e.g. definite integration, summation, differential equations).

Most (all?) available computer algebra systems will fail to compute asymptotic expansions for expressions as simple as

$$e^n \left(\sin(\frac{1}{n} + e^{-n}) - \sin(\frac{1}{n}) \right)$$

when $n \to \infty$, or

$$e^{-n^2} \left(e^{an} - e^{bn} + e^{n^2} \right)$$

In this talk we will review some previous algorithms and propose new ones, which by classifying functions in a hierarchy reminiscent of the Risch algorithm, can compute a much wider class of expansions. This new algorithm includes each subexpression in a class. Expressions in a class can be bounded polynomially by any other expression in the same class. Computation of series proceeds by computing a series with respect to the most rapidly varying class first, leaving the others as constants, and recursively so on the leading term. Examples of this algorithm implemented in Maple will be shown.

W. Laßner: *Computer-algebra and Lie-algebras: classification and identification of Lie-algebras*

Symmetry analysis of differential equations by computer algebra systems produces automatically the generators of the symmetry algebra, i. e. their structure constants. If the symmetry is determined as a finite dimensional Lie algebra it remains the identification among Lie algebras from known classification tables. The problem whether two Lie algebras are isomorphic can be decided by the existence of solutions of a system of quadratic equations. The Gröbner bases methods is recommended for an algorithmic treatment. If a complete table of all Lie algebras up to a certain dimension is known then the Gröbner bases method allows in principle an identification for complex Lie algebras. Special techniques are necessary to decide the existence of real solutions in the case of real Lie algebras. Interesting relations exist between the formulation of facts and algorithms in the three theories under consideration, i. e. the symmetry analysis of differential equations, the Lie algebra classification, and the Gröbner bases method. If two Lie algebras are isomorphic and therefore solutions of the quadratic equations exist then there exist always infinitely many solutions due to automorphisms of the Lie algebra. Special algorithms determine independent sets of parameters and the Gröbner bases problem can be reduced. Homogeneity properties of the system under consideration allow an essential speed up of the calculations. Unfortunately, the number of variables depends quadratically on the Lie algebra dimension. The number of equations increases with the third order. At present the method was applied up to seven dimensional Lie algebras. Complete tables of Lie algebras are known up to dimension five. Efficient algorithms and computer aided methods for the representation of mathematical knowledge in the field of Lie algebras classification help

to solve the identification problem for higher dimensional Lie algebras. In addition to the identification problem there was reported an application of the Gröbner bases method to quantum groups.

F. Schwarz: *Reduction and Completion Algorithms for Partial Differential Equations*

Originating from the theory of Riquier and Janet of pde's, an algorithm is described, that takes as input a system of algebraic pde's and returns the corresponding completely involutive systems, i.e. a universal differential Gröbner base. This algorithm is applied to several problems, e. g. determining the size of symmetry groups and finding certain Bäcklund transformations.

H. G. Zimmer: *Algorithms for Elliptic Curves*

By the Mordell-Weil theorem, the group $E(K)$ of rational points of an elliptic curve E over an algebraic number field K is finitely generated, and hence

$$E(K) = E_{tprs}(K)E_{fr}(K)$$

is the direct sum of the group of all rational points of finite order, the finite torsion group $E_{tors}(K)$, and a free group $E_{fr}(K)$ of finite rank r, so that $E_{fr}(K) \cong \mathbf{Z}^r$ $(r \geq 0)$. The algorithms to be discussed concern:

1. The determination of elliptic curves E over number fields K of small degree having largetorsion groups $E_{tors}(K)$.
2. The determination of all possible torsion groups $E_{tors}(K)$ of elliptic curves E with integral j-invariants over number fields K of small degree.
3. The construction of elliptic curves E over $K = \mathbf{Q}$ with large rank r.
4. The determination of the rank r and the computation of a basis of the free group $E_{fr}(K)$ for certain classes of elliptic curves E over $K = \mathbf{Q}$ ("Manin-Algorithm").

The algorithms concerning 1), 2) are of interest, e. g., with respect to the boundedness conjecture for the order of the torsion group $E_{tors}(K)$; the algorithms concerning 3), 4) are relevant, e. g., in view of the conjecture that the rank r of E over $K(= \mathbf{Q})$ is unbounded and in view of the famous conjectures of Birch and Swinnerton-Dyer.

W. Krandick: *Isolation of polynomial complex roots*

Applying the "principle of the argument" from complex analysis to rectangles provides an efficient algorithm for polynomial complex root isolation. The algorithm reduces complex root isolation to real root isolation, and uses the coefficient-sign variation method to accomplish the latter. Computing time experiments suggest that the presented algorithm can be recommended as an efficient first step in a complex root calculation scheme, namely to provide starting points for a rapidly converging root approximation method. The average computing time of the algorithm seems to be approximately cubic in the degree

of A and linear in the length of its coefficients. The algorithm uses the method described in G. E. Collins, "Infallible calculation of polynomial zeros to specified precision", *Mathematical Software, Academic Press, New York*, pages 35–68, 1977. However, some flaws are corrected and various non-trivial improvements are made. The corrected algorithm accounts for the possibility that certain polynomials which arise in the computation either have multiple roots or vanish identically. A bisection strategy can be chosen so as to minimize the memory requirements of the algorithm. One of the basic computational steps can be avoided for almost all input polynomials without compromising infallibility. In case the input polynomial is real, degrees of certain polynomials which arise in the computation can be reduced to obtain a speed-up. The computing time might be further reduced by using interval arithmetic.

Dagstuhl-Seminar 9151:

List of Participants (update: 10.06.92)

Manuel **Bronstein**
ETH Zürich
Institut für Wissenschaftliches Rechnen
Abteilung Informatik
ETH-Zentrum
CH-8092 Zürich
Switzerland
bronstein@inf.ethz.ch
tel.: +41 (1) 254-7474

Bruno **Buchberger**
Johannes Kepler Universität
Institut für Mathematik
A-4040 Linz
Austria

Bob F. **Caviness**
University of Delaware
Dept. of Computer &
Information Sciences
Newark DE 19716
USA
caviness@ee.udel.edu

George E. **Collins**
RISC Research Institute
Johannes Kepler University
4040 Linz
Austria
gcollins@risc.uni-linz.ac.at
tel.: +43-7236-3231-44

James **Davenport**
School of Mathematical Science
University of Bath
75 Gt - Pulteney St.
Bath BA2 7AY
England

Jean **Della Dora**
Laboratoire LMC - IMAG
46 Avenue Felix Viallet
38031 Grenoble Cedex
France

Benno **Fuchssteiner**
Fachbereich Mathematik-Informatik
Universität Paderborn
Postfach 16 21
4790 Paderborn
Germany

Joachim **von zur Gathen**
Dept. of Computer Science
University of Toronto
Toronto Ontario M5S 1A4
Canada
gathen@theory.toronto.edu

Marc **Giusti**
Centre de Mathématiques
91128 Palaiseau Cedex
France
giusti@orphee.polytechnique.fr
tel.: +33-1-69-33-45-85

Gaston H. **Gonnet**
Dept. of Computer Science
University of Waterloo
Waterloo N2L 3G1
Canada

Johannes **Grabmeier**
Wissenschaftliches Zentrum
IBM Deutschland GmbH
Tiergartenstraße 15
6900 Heidelberg
Germany
grabm@gysvmhdi
tel.: +49-6221-404-329

Hubert **Grassmann**
FB Mathematik
Humboldt-Universität Berlin
Postfach 12 97
1086 Berlin
Germany
hgrass@hubinf.uucp

Erich **Kaltofen**
Dept. of Computer Science
Rensselaer Polytechnic Inst.
Troy NY 12181
USA
kaltofen@cs.rpi.edu

Werner **Krandick**
Mathematical Sciences
Universität Linz
RISC
4040 Linz
Austria
krandick@risc.uni-linz.ac.at

Wolfgang **Laßner**
Sektion Informatik
Universität Leipzig
Augustusplatz 10-11
7010 Leipzig
Germany
lassner@informatik.uni-leipzig.dbp.de
tel.: +37-41-719-2398

Daniel **Lazard**
LITP (tour 45-55)
Université Paris VI
4 Place Jussieu

75252 Paris Cédex 05
France
dl@posso.ibp.fr

Rüdiger **Loos**
Wilhelm Schickard Inst.
Universität Tübingen
7400 Tübingen
Germany

B.H. **Matzat**
Interdisziplinäres Zentrum für
Wissenschaftliches Rechnen (IWR)
Universität Heidelberg
Im Neuenheimer Feld 368
6900 Heidelberg
Germany

Gerhard **Michler**
Institut für Experimentelle Mathematik
Universität GHS Essen
Ellernstraße 29
4300 Essen 12
Germany
mat4bb@deohrz1a.binet
tel.: +49-201-320 6440 / 6439 (secr)

Teo **Mora**
Dept. di Math.
Univ. Degli Studi Genova
Via L.B. Alberti 4
16132 Genova
Italy
THEOMORA@IGECUNIV.bitnet

Michael H. **Möller**
FB Mathematik
Fernuniversität Hagen
Lützowstraße 125
5800 Hagen 1
Germany
MA105@DHAFEU11.bitnet
tel.: +49-2331/9872286

Klaus-Peter **Neuendorf**
Fachbereich Informatik
Humboldt-Universität Berlin
Unter den Linden
1080 Berlin
Germany
neuendor@hubinf.uucp

Paul **Pedersen**
Computer Science Dept.
Cornell University
Ithaca NY 14852
USA
paul@cs.cornell.edu
tel.: +1-607-255-9730

Attila **Pethö**
Department of Computer Science
Kossuth Lajos University
P.O. Box 12
4010 Debrecen
Hungary
h2988pet@ella.hu
tel.: +36-52-16666

Michael **Pohst**
Mathematisches Institut
Heinrich-Heine-Universität Düsseldorf
Universitätsstr. 1
4000 Düsseldorf 1
Germany
POHST@DD0RUD81.bitnet

Arnold **Schönhage**
Institut für Informatik II
Universität Bonn
Römerstraße 164
5300 Bonn 1
Germany
tel.: +49-228/550201

Fritz **Schwarz**
Institut F1
Schloß Birlinghoven
GMD mbH
Postfach 1240
5205 St. Augustin1
Germany
GF1002@DBNGMD21.bitnet
tel.: +49-2241-14-2782

Michael **Singer**
Dept. of Mathematics
North Carolina State University
Box 8205
Raleigh NC 27695-8205
USA
singer@matmfs.ncsu.edu

Laurent **Stolovitch**
Laboratoire TIM 3
Institut IMAG
B.P. 68
38402 St. Martin d'Heres cédex
France

Bernd **Sturmfels**
Dept. of Mathematics
Cornell University
Ithaca NY 14853
USA
bernd@mssun7.msi.cornell.edu

Carlo ***Traverso***
Dipartimento di Matematica
Universita di Pisa
Via F. Buonarroti 2

56100 Pisa
Italy
traverso@dm.unipi.it
tel.: +39-50-599513

Annick **Valibouze**
Maitre de Conférences
Université Paris 6
LITP
4 Place Jussieu
75252 Paris cedex 05
France
avb@litp.ibp.fr / avb@sysal.ibp.fr
tel.: +33-1-44-27-62-43

Volker **Weispfenning**
Fakultät für Mathematik und Informatik
Universität Passau
Innstraße 33
8390 Passau
Germany
weispfen@unipas.fmi.uni-passau.de
tel.: +49-851-509-317

Waldemar **Wiwianka**
Fachbereich Mathematik-Informatik
Universität Paderborn
Postfach 16 21
4790 Paderborn
Germany
waldemar@uni-paderborn.de

Horst Günter **Zimmer**
Fachbereich 9 - Mathematik
Universität des Saarlandes
Im Stadtwald 15
6600 Saarbrücken 11
Germany
zimmer@math.uni-sb.de
tel.: +49-681-302-22 06

Zuletzt erschienene und geplante Titel:

H. Alt , B. Chazelle, E. Welzl (editors):
Computational Geometry, Dagstuhl-Seminar-Report; 22, 07.10.-11.10.91 (9141)

F.J. Brandenburg , J. Berstel, D. Wotschke (editors):
Trends and Applications in Formal Language Theory, Dagstuhl-Seminar-Report; 23, 14.10.-18.10.91 (9142)

H. Comon , H. Ganzinger, C. Kirchner, H. Kirchner, J.-L. Lassez , G. Smolka (editors):
Theorem Proving and Logic Programming with Constraints, Dagstuhl-Seminar-Report; 24, 21.10.-25.10.91 (9143)

H. Noltemeier, T. Ottmann, D. Wood (editors):
Data Structures, Dagstuhl-Seminar-Report; 25, 4.11.-8.11.91 (9145)

A. Dress, M. Karpinski, M. Singer(editors):
Efficient Interpolation Algorithms, Dagstuhl-Seminar-Report; 26, 2.-6.12.91 (9149)

B. Buchberger, J. Davenport, F. Schwarz (editors):
Algorithms of Computeralgebra, Dagstuhl-Seminar-Report; 27, 16.-20.12.91 (9151)

K. Compton, J.E. Pin , W. Thomas (editors):
Automata Theory: Infinite Computations, Dagstuhl-Seminar-Report; 28, 6.-10.1.92 (9202)

H. Langmaack, E. Neuhold, M. Paul (editors):
Software Construction - Foundation and Application, Dagstuhl-Seminar-Report; 29, 13..-17.1.92 (9203)

K. Ambos-Spies, S. Homer, U. Schöning (editors):
Structure and Complexity Theory, Dagstuhl-Seminar-Report; 30, 3.-7.02.92 (9206)

B. Booß, W. Coy, J.-M. Pflüger (editors):
Limits of Modelling with Programmed Machines, Dagstuhl-Seminar-Report; 31, 10.-14.2.92 (9207)

K. Compton, J.E. Pin , W. Thomas (editors):
Automata Theory: Infinite Computations, Dagstuhl-Seminar-Report; 28, 6.-10.1.92 (9202)

H. Langmaack, E. Neuhold, M. Paul (editors):
Software Construction - Foundation and Application, Dagstuhl-Seminar-Report; 29, 13.-17.1.92 (9203)

K. Ambos-Spies, S. Homer, U. Schöning (editors):
Structure and Complexity Theory, Dagstuhl-Seminar-Report; 30, 3.-7.2.92 (9206)

B. Booß, W. Coy, J.-M. Pflüger (editors):
Limits of Information-technological Models, Dagstuhl-Seminar-Report; 31, 10.-14.2.92 (9207)

N. Habermann, W.F. Tichy (editors):
Future Directions in Software Engineering, Dagstuhl-Seminar-Report; 32; 17.2.-21.2.92 (9208)

R. Cole, E.W. Mayr, F. Meyer auf der Heide (editors):
Parallel and Distributed Algorithms; Dagstuhl-Seminar-Report; 33; 2.3.-6.3.92 (9210)

P. Klint, T. Reps (Madison, Wisconsin), G. Snelting (editors):
Programming Environments; Dagstuhl-Seminar-Report; 34; 9.3.-13.3.92 (9211)

H.-D. Ehrich, J.A. Goguen, A. Sernadas (editors):
Foundations of Information Systems Specification and Design; Dagstuhl-Seminar-Report; 35; 16.3.-19.3.9 (9212)

W. Damm, Ch. Hankin, J. Hughes (editors):
Functional Languages:
Compiler Technology and Parallelism; Dagstuhl-Seminar-Report; 36; 23.3.-27.3.92 (9213)

Th. Beth, W. Diffie, G.J. Simmons (editors):
System Security; Dagstuhl-Seminar-Report; 37; 30.3.-3.4.92 (9214)

C.A. Ellis, M. Jarke (editors):
Distributed Cooperation in Integrated Information Systems; Dagstuhl-Seminar-Report; 38; 5.4.-9.4.92 (9215)