Computeralgebra–Rundbrief

Nummer 10 *Fachgruppe 2.2.1* *28. 2. 1992*

Liebe Kolleginnen und Kollegen,

am Ende dieses Jahres stehen bereits wieder Neuwahlen der Computeralgebra-Fachgruppenleitung an. Je ein Mitglied der Fachgruppenleitung wird von DMV, GAMM und GI bestimmt. Sie, die Mitglieder der Fachgruppe, wählen 9 weitere Mitglieder der Fachgruppenleitung. Sie werden gebeten, für diese Wahl bis zum 1.7.92 Vorschläge an Prof. Dr. V. Weispfenning, Universität Passau - Lehrstuhl für Mathematik, Postfach 2540, W-8390 Passau, zu senden.

Alle Vorgeschlagenen werden danach gefragt werden, ob sie sich zur Wahl stellen. Mit der Nr. 11 des Rundbriefs werden Sie dann im September/Oktober 1992eine Liste der Kandidaten und Wahlunterlagen erhalten. Sie können dann bis zu 9 Kandidaten aus der Kandidatenliste anstreichen (Kumulierung ist nicht zulässig). Für die Rücksendung der Wahlumschläge wird eine Frist von ca. 4 Wochen gesetzt werden. Diejenigen 9 Kandidaten, die die meisten Stimmen auf sich vereinen, bilden zusammen mit den 3 von DMV, GAMM und GI benannten Delegierten die neue Fachgruppenleitung, die ihre Arbeit am 01.03.93 aufnehmen soll.

Da sich der zweijährige Wahlmodus doch als sehr kurz herausgestellt hat, haben wir die Satzung diesbezüglich geändert. Die Amtszeit der Fachgruppenleitung wird deshalb ab dieser Wahl 3 Jahre betragen.

Bitte machen Sie von Ihrem Recht auf Mitbestimmung der Fachgruppenleitung Gebrauch, zunächst durch Benennung von Kandidaten, von denen Sie erwarten, daß sie die Sache der Computeralgebra tatkräftig unterstützen werden.

Aus gegebenem Anlaß haben wir eine Rubrik Leserbriefe *eingefügt und hoffen auf viele Beiträge Ihrerseits. Über die aktive Computeralgebra-Gruppe CAMASA in Italien finden Sie einen Bericht in dieser Ausgabe.*

V. Weispfenning *J. Grabmeier*

Hinweise auf Konferenzen

1. **Partial Differential Equations and Group Theory**

   Advanced 5-day course by INRIA and GMD, Bonn, 06–10.04.1992.

   Kontaktadresse: GMD, M. Dresen, Institut für methodische Grundlagen (F1 P), Postfach 1316, W. 5205 Sankt Augustin 1

Schwarz

2. **MEGA-92 – Effective Methods in Algebraic Geometry**

   Nizza, Frankreich, 20.-24.04.1992.

   Kontaktadresse: Teo Mora, Dipartimento di Matematica, Via L.B. Alberti 2, I-16100 Genova, theomora@igecuniv.bitnet.

3. **DISCO 92, Design and Implementation of Symbolic Computation Systems**

   Bath, England, 23.–24.04.1992.

   Organisation: J.H. Davenport (Bath), J.P. Fitch (Bath), jhd=disco@maths.bath.ac.uk, +44-225-826181, jpff@maths.bath.ac.uk, +44-225-826820, School of Mathematical Sciences, U Bath, GB-Bath BA2 7AY.

4. **Computational Group Theory**

   Mathematisches Forschungsinstitut Oberwolfach, 07.–13.06.1992.

   Tagungsleitung: J. Neubüser (Aachen), C. Sims (New Brunswick). Teilnahme nur auf Einladung.

[0]**Impressum** *Computeralgebra–Rundbrief* Herausgegeben von der Fachgruppe 2.2.1 *Computeralgebra* der GI, DMV und GAMM, Redaktionsschluß 28.02 und 31.08. Anschrift: Dr. J. Grabmeier, IBM Wissenschaftliches Zentrum Heidelberg, Tiergartenstraße 15, Postfach 103068, 6900 Heidelberg. Elektronische Adresse: grabm@dhdibm1.earn. Telefax: 06221-404-296. ISSN 0933-5994

5. **Deutsch-Französische Tagung Computeralgebra und Anwendung**

   Saint-Louis(Ober-Elsaß), Frankreich, 15.-17.06.1992

   Achtung, diese Konferenz wurde verschoben, bitte beachten Sie den neuen Termin.

   Kontaktadresse: L.R.Oudin, A.Carriere, Deutsch-Französisches Forschungsinstitut Saint-Lous, Postfach 1260. D-7858 Weil am Rhein 1

6. **Formal power series and algebraic combinatorics**

   University of Quebec at Montreal, 15.–19.06.1992.

   Kontaktadresse: P. Leroux, LACIM, Univ. du Quebec, Case Postale 8888, Succursale A, Montreal, Canada H3C 3P8, elektr. Adr.: lacim@lacim.uqam.ca.

7. **RISC-LINZ Summer School in Computer Algebra**

   Universität Linz, Austria, 06.–11.07.1992. Winkler ?

   Kontaktadresse: F. Winkler, RISC-LINZ, Universität Linz, A-4040 Linz, Austria, elektr. Adr.: winkler@risc.uni-linz.ac.at

8. **RISC-LINZ Summer Course on Quantifier Elimination**

   Universität Linz, Austria, 13.–17.07.1992. Collins ?

   Kontaktadresse: G.E. Collins, RISC-LINZ, Universität Linz, A-4040 Linz, Austria, elektr. Adr.: gcollins@risc.uni-linz.ac.at

9. **International Workshop on Mathematics Mechanization: Theories and Applications of Algebraic Equation Solving.**

   Academia Sinica, Peking, China, 16.–18.07.1992.

   Kontaktadresse: Wu Wen-tsü, Mathematics Mechanization Research Center, Institute of Systems Science, Peking, 100080, Volksrepublik China, elektr. Adr.: bmadis@ica.beijing.canet.cn.

10. **ISSAC'92**

    Berkeley, Kalifornien, USA, 27.–29.07.1992.

    Kontaktadresse: R. Fateman, EECS Dept., Comput. Sci. Div., 571 Evans Hall, U of California, USA-Berkeley, CA 94720, elektr. Adr.: fateman@cs.berkeley.edu, +1-510-642-1879 or E. Kaltofen, Dept. Comput. Sci., Rensselaer Polytechnic Institute, USA-Troy, NY 12180-3590, elektr. Adr.: kaltofen@cs.rpi.edu, +1-528-276-6907.

11. **Computational Mathematics and Artificial Intelligence**

    Karlsruhe, 03.–06.08.1992. Calmet

    Kontaktadresse: J. Calmet, Universität Karlsruhe, elektr. Adr.: KG05@DKAUNI2.BITNET.

12. **Symbolic, algebraic and validated numerical computation**

    Dagstuhl Seminar, 03.–07.08.1992. Rump

    Organisatoren: James H. Davenport, F. Krückeberg, R. E. Moore, S. M. .Rump. Teilnahme nur auf Einladung.

    Kontaktadresse: Prof. Dr. S. M. Rump, Technische Informatik III, TU Hamburg–Harburg, Eißendorfer Straße 38, D–2100 Hamburg 90.

13. **Workshop on "Algebraic Approaches to Geometric Reasoning"**

    Universität Linz, Austria, 17.–19.08.1992. Hong ?

    Kontaktadresse: H. Hong, RISC-LINZ, Universität Linz, A-4040 Linz, Austria, elektr. Adr.: hhong@risc.uni-linz.ac.at

14. **DMV-Jahrestagung: Sektion Wissenschaftliches Rechnen**

    Humboldt-Universität Berlin, 14.–18.09.1992.

    Sektionsleitung: P. Deuflhard, Berlin, V. Weispfenning, Passau

Berichte von Konferenzen

1. **CAMASA '91, Convegno Nazionale di Calcolo Algebrico e Simbolico**
Cagliari, Italy, 21.03.–23.03.1991.

Die Liste der Vorträge dieser Konferenz (siehe auch den Beitrag in der Rubrik *Berichte von den Arbeitsgruppen*:

A. Miola: *TASSO, A system for mathematical problem solving*; G. Attardi, C. Traverso: *A network implementation of Buchberger algorithm*; M.E. Alonso, T. Mora, M. Raimondo: *Local decomposition algorithms*; M. Grieco, B.Zucchetti: *The tangent cone algorithm for modules and resolutions over local rings*; E. Strickland: *An algorithm related to the structure of the center of a quantized enveloping algebra at a root of 1*; G.M. Piace: *Computation of co-characters and codimensions of relatively free algebras*; Rene Schoof: *Algorithms for integer factorization (invited)*; I. Del Corso, R. Dvornicich: *A converse of Artin's density theorem: the case of cubic fields*; G. Niesi: *CoCoA updates to version 1.4 and goes on*; M. Caboara: *Dynamic evaluation of Groebner bases*; Dominique Duval: *Applications of dynamic evaluation to geometry (invited)*; S. Audoly, A.Buttu, G. Bellu, L. D'Angio': *Procedures to investigate injectivity of polynomial maps and to compute the inverse*; P. Cellini: *Real solutions of zero-dimensional systems*; F. P. Pierantonio: *An algebraic viex of inheritance and subtyping in Object Oriented Programming*; M. Regio, M. Temperini: *Object oriented methodology for the specification and treatment of mathematical objects*; G. Forcellese, M. Temperini: *The use of a deductive method into an oramework*; T. Krick, A. Logar: *An algoritm for the computation of the radical of an ideal in the ring of polynomials*; L. De Floriani, E. Puppo: *An on-line algorithm for constrained Delaunay triangulation*; L. Cerlienco, F. Piras: *On the cofinite ideals of a polynomial algebra*; G. Carra' Ferror: *Minimal Hilbert polynomials in algebraic geometry and differential algebra*; A.M. Bigatti, M. Caboara, L. Robbiano: *On the computation of Hilbert Poincare series*; A. Bertoni, P. Massazza: *Algorithms for the Hadamard product of holonomic formal series*; M. Torelli: *Combinatorial manipulation of symmetric functions*; Claude Kirchner: *Constrained deduction (invited)*; G. Gallo: *Some remarks about the membership problem for differential ideals*; S. Anelli, E. Damiani, O. D'Antona, D. Loeb: *Tiling bricks with... Mathematica*; E. Sernesi, C.Traverso: *Absolute factorization and absolute irreducibility tests, a review*; F. Rossi, W. Spangher: *Some computation of the openness of loci for modules*; V. Cutello: *A note on the decidability problem for a topological syllogistic involving the notion of topological product*; R. Ru: *A sorted logic with union and partition of sorts*; H. Michael Moeller : *Linear bases and Groebner bases (invited)*; P. Conti: *Groebner bases and diphantine linear systems*; C. Limongelli, A. Miola: *Abstract specification of numeric and algebraic computation methods*; S. Bonamico, G. Cioni, A. Colagrossi: *A Gentzen based deduction method for mathematical problem solving*; L. Cerlienco, M. Mureddu: *Algebraic interpolation in higher dimension: a combinatorial approach*; L. Robbiano: *Bounds for degrees and number of elements in Groebner bases*; M.G. Marinari, H.M. Moeller, T. Mora: *Groebner bases of ideals defined by functionals with an application to ideals of projective points.*

Teo Mora, Genua

2. **Programming Enviroments for High Level Scientific Problem Solving**
Karlsruhe, 23.–27.9.1991

Dies war die sechste "Working Conference" der WG (working group) 2.5 der IFIP, die sich mit Scientific Computing beschäftigte. Sie wurde von dem Institut für angewandte Mathematik der Universität Karlsruhe mit organisiert. Den Vorsitz des Programmkommitees teilten sich B. Einarsson und L.D. Fosdick. Die Proceedings werden bei North-Holland erscheinen und von P. Gaffney und E. Houstis herausgegeben werden. U. Kulisch und A. Schreiner waren die lokalen Organisatoren. Wie üblich bei den Arbeitskonferenzen der IFIP war die Teilnahme nur auf Einladung möglich. Das Gleiche galt für die Vortragenden, die ausgewählt wurden, um folgende Gebiete abzudecken: Intelligent Assistants, Mathematical Methods, Systems and Tools, Interaction and Visualization and System Engineering (2 Sitzungen). Die Teilnehmerzahl wurde gering gehalten (unter 100), um eine Arbeitsatmosphäre herzustellen. Aus demselben Grund gab es nach jedem Vortrag genügend Zeit für ausgedehnte Diskussionen. Zusätzlich schloß sich an jede Sitzung eine fünfzehnminütige Diskussion an. Die Konferenz war interdisziplinär angelegt und von einem Programmkommitee vorbereitet, das seine Arbeit bereits 1988 aufnahm (Treffen in Stanford 1988, Beijing 1989, Jerusalem 1990). Die Vorträge im einzelnen in zeitlicher Reihenfolge:

S. S. Tong: *Integration of Symbolic and Numerical Methods for Optimizing Complex Engineering Systems*, W.M. Gentleman: *Symbiotic Computation: Opportunities and Complications*, P.C. Abbott: *Problem Solving Using Mathematica*, S. Rump: *Accuracy Control and Estimation, Self-Validating Systems and Software Environments for Scientific Computation*, W. Schoenauer: *Polyalgorithms with Automatic Method Selection for the Iterative Solution of Linear Equations and Eigenproblems*, J.A. Nelder: *The Computer as Statistical Assistant* , R.F. Boisvert: *Toward an Intelligent System for Mathematical Software Selection*, M. Shimasaki: *Fractals in Quaternions and their Application to Computer Graphics*, V.P. Gerdt: *Computer Algebra Tools for Higher Symmetry Analysis of Nonlinear Evolution Equations*,

B. Buchberger: *Groebner Bases in Mathematica: Enthusiasm and Frustration*, D. Duval: *Examples of Problem Solving using Computer Algebra*, S. Feldman: *Environments for Large-Scale Scientific Computation*, H. Zima: *Software Tools for Parallel Program Development*, W.R. Dyksen: *Fortran Interface Blocks as an Interface Description Language for Remote Procedure Call*, N. Hurley: *An Integrated Problem Solving Environment for Numerical Simulation of Engineering Problems*, M. Clarkson: *Expert System as an Intelligent User Interface for Symbolic Algebra*, A. Miola: Design and Implementation of Symbolic Computation Systems, E. Houstis: *Parallel Ellpack*, J. Purtilo: *Dynamic Software Reconfiguration Supports Scientific Problem Solving Activities*, Y. Umetani: *Visual DEQSOL: A Visual and Interactive Environment for Numerical Simulation*, E. Grosse: *Display of Functions of Three Space Variables and Time Using Shaded Polygons and Sound*, H.J.W. Spoelder: *Distributed Visual Programming Environment: an Attempt to Integrate Third Generation Languages with Advanced User Environments*, P.M. Dew: *Visualization and its Use in Scientific Computation*, J.A. van Hulzen: *Automated Generation of Optimized Numerical Code for Jacobians and Hessians*, N. Holsti: *Transcript Editing, A Simple User Interface Tool*, A. Bonadio: *Mathematical User Interfaces for Graphical Workstations*, D. Gay: *Toward an Environment for Mathematical Programming*, J. Reid: *The Fortran 90 Standard*, K. Broughan: *SENAC: Lisp as a Platform for Constructing a Problem Solving Environment*, J. Rice: *Future Research Directions in Scientific Problem Solving Environments*, C.W. Cryer: *The ESPRIT Project FOCUS*, S.J. Hague: *Use of Knowledge Bases for Problem Solving – The FOCUS Approach*

J. Calmet, Karslsruhe

3. **Parallel Computation, Special Session: Parallel Symbolic Computation**
Salzburg, Austria, Europe, 30.09.–02.10.1991.

Im Rahmen der "*Ersten internationalen Konferenz des ACPC (Austrian Center for Parallel Computation)*" gab es auch eine gut besetzte Sitzung über 'Parallel Symbolic Computation'. Der Schwerpunkt lag bei dieser Sitzung auf Computer Algebra. Als eingeladener Vortragender sprach Dr. P. Wang (Kent State University) über seine Erfahrungen mit der Parallelisierung von Computeralgebra-Algorithmen. Der Themenbereich der weiteren Vorträge reichte von paralleler Multiplikation, über Probleme aus der Graphentheorie bis zu einem Ansatz der Parallelisierung des 'Buchberger Algorithmus' und zur Verwendung einer Bibliothek von parallelen C-Routinen zur Berechnung und Manipulation von Polynomen. Die große thematische Bandbreite dieser Vorträge unterstreicht die Bedeutung von 'Symbolic Computation' innerhalb des stark wachsenden Gebietes der 'Parallel Computation'.

Die Vorträge im einzelnen in zeitlicher Reihenfolge mit kurzen Inhaltsangaben:

P. Wang: *Symbolic Computation and Parallel Software*, in diesem eingeladenen Vortrag befaßte sich Dr. Wang mit der Parallelisierung von zwei grundlegenden Computeralgebra-Algorithmen, nämlich mit einem Algorithmus zur Parallelisierung der Faktorisierung univariater Polynome, sowie mit einer parallelen Version des Berlekamp-Algorithmus. Außerdem zeigte der Vortragende die Möglichkeit der automatischen Erzeugung von parallelem Code auf; D. Wang: *On the Parallelization of Characteristic-Set-Based Algorithms*, dieser Vortrag zeigte die Verwendung eines Ansatzes grobkörniger Parallelität zur Parallelisierung von Algorithmen, die auf dem Prinzip der charakteristischen Mengen basieren. Zur Realisierung der Parallelität wurde hier das Computeralgebra-System Maple verwendet; P. Lippitsch: *Multiplication as Parallel as Possible*, dieser Vortrag zeigte die Möglichkeit, Methoden aus dem Bereich der Computeralgebra auch für Problem im Bereich des Hardwaredesigns anzuwenden. Konkret wurde die Möglichkeit einer VLSI-Implementierung eines bekannten, parallelen Multiplikationsalgorithmus betont; J. Zerovnik: *On the Existence of an Efficient Parallel Algorithm for a Graph Theoretic Problem*, in diesem Vortrag diskutierte der Vortragende einen parallelen Algorithmus, mit dessen Hilfe man eine Reihe interessanter und wichtiger Fragestellungen der Graphentheorie an konkreten Graphen beantworten kann; D. Hawley: *A Buchberger Algorithm for Distributed Memory Multi-Processors*, dieser Vortrag beschäftigte sich, startend vom Bereich des 'Constraint Logic Programming', mit einer Möglichkeit der Parallelisierung des Buchberger-Algorithmus. Die Bedeutung dieses Ansatzes liegt darin, daß beim 'Constraint Logic Programming' der Buchberger-Algorithmus zur Lösung sehr rechenintensiver Subprobleme herangezogen werden kann; W. Küchlin: *On the Multi-Threaded Computation of Modular Polynomial Greatest Common Divisors*, das Hauptgewicht in diesem Vortrag lag in der Vorstellung einer Bibliothek von parallelen C-Routinen (basierend auf dem parallelen Betriebssystem Mach), mit deren Hilfe eine sehr effiziente Parallelisierung von Computeralgebra-Algorithmen möglich wird. Außerdem ist durch die Verwendung des Betriebssystems Mach eine große Portabilität gegeben. Ferner wurde die Verwendung dieser Bibliothek am Beispiel eines Algorithmus zur Berechnung des grösten gemeinsamen Teilers von Polynomen benutzt.

Hans Wolfgang Loidl, Linz

4. **AAECC-9, Ninth International Symposium on Applied Algebra, Algebraic Algorithms, and Error Correcting Codes**

New Orleans, 07.–10.10.1991

Diese neunte Konferenz wurde von T.R.N. Rao, T. Mora und Skip Mattson organisiert. Sie sind auch die Herausgeber der Proceedings, die als Band 359 der Lecture Notes in Computer Sciences beim Springer-Verlag erschienen. Die Hauptthemen der Konferenz gibt bereits der Name an mit Ausnahme der Kryptographie, die ebenfalls gut vertreten war. Die Teilnehmerzahl war ungewöhnlich gering (ca. 90–100). Der Hauptgrund lag darin, daß die Konferenz in einem teuren Hotel (das Monteleone) in der Innenstadt von New Orleans stattfand. In Zukunft wird sie alle zwei Jahre organisiert werden, um einen hohen Standard der akzeptierten Arbeiten zu sichern. Die nächste Konferenz wird im März 93 in Puerto Rico mit Unterstützung des Mathematischen Institut der University of Cornell abgehalten werden. Die endgültigen Daten werden gegen Ende des Jahres feststehen. Als letztes sei angemerkt, daß es in Zukunft keine informellen Vorträge (d.h. solche, die nicht in den Proceedings erscheinen) mehr geben wird. Die Vorträge in zeitlicher Reihenfolge: P. Cellini, P. Gianni, C. Traverso: *Algorithms for the Shape of Semialgebraic Sets. A New Approach*, H. Janwa: *On the Parameters of Algebraic Geometric Codes*, E. Kaltofen, B.D. Saunders: *On Wiedemann's Method of Solving Sparse Linear Systems*, S.N. Litsyn: *Fast Algorithms for Decoding Orthogonal and Related Codes*, W.V. Vasconcelos: *Jacobian Matrices and Constructions in Algebra*, T. Becker: *Homogenity, Pseudo-Homogenity, and Gröbner Basis Computations*, T. Beth, F. Schaefer: *Arithmetic on Non-Supersingular Elliptic Curves*, G. Butler: *Implementing Some Algorithms of Kantor*, J.F. Canny: *Computing Roadmaps of General Semi-Algebraic Sets*, J.F. Canny: *An Improved Sign Determination Algorithm*, H. Chung: *The 2-nd Generalized Hamming Weight of Double-Error Correcting Binary BCH Codes and Their Dual Codes*, P. Conti, C. Traverso: *Buchberger Algorithm and Integer Programming*, M. Diab: *New Systolic Architectures for Cyclic Code Encoding*, M.J. Dinneen, M.R. Fellows, V. Faber: *Algebraic Constructions of Efficient Broadcast Networks*, C. van Eijl, G. Cohen, G. Zémor: *Error-Correction for WIMs and WUMs*, G. Gallo, B. Mishra, F. Ollivier: *Some Constructions in Rings of Differential Polynomials*, L.P. Holmquist, L.L. Kinney: *Concurrent Error Detection in Sequential Circuits Using Convolutional Codes*, T. Krick, A. Logar: *An Algorithm for the Computation of the Radical of an Ideal in the Ring of Polynomials*, W. Kuechlin, D. Lutz, N. Nevin: *Integer Multiplication in PARSAC-2 on Stock Microprocessors*, G. Lachaud, J. Stern: *Polynomial-Time Construction of Spherical Codes*, L. Langemyr: *Algorithms for a Multiple Algebraic Extension II*, P. Langevin: *On the Orphans and Covering Radius of the Reed-Muller Codes*, Y. Li, X. Wang: *A Joint Authentication and Encryption Scheme Based on Algebraic Coding Theory*, A.C. Lobstein, P. Solé: *Arithmetic Codes — Survey, Recent and New Results*, R. Morelos-Zaragoza, S. Lin: *Some Results on Linear Unequal-Error-Protection Codes Specified by their Generator Matrix*, G. Moreno Socias: *An Ackermannian Polynomial Ideal*, T. Mostowski, E. Rannou: *Complexity of the Computation of the Canonical Whitney Stratification of an Algebraic Set in Cn*, F. Otto: *Some Undecidability Results for Weakly Confluent Monadic String-Rewriting Systems*, P. Pedersen: *Calculating Multidimensional Symmetric Functions Using Jacobi's Formula*, P. Pedersen: *Multivariate Sturm Theory*, M. Perret: *Binary Spherical Geometric Codes*, A. Poli, M. Belkasmi: *An Algebraic Construction of Generalized Beenker's Codes*, J. Rifà, J. Borrell: *Improving the Time Complexity of the Computation of Irreducible and Primitive Polynomials in Finite Fields*, J. Rifà, J. Pujol: *Completely Transitive Codes and Distance Transitive Graphs*, J.-J. Risler : *Placement of Curved Polygons*, F. Rodier: *On the Weights of the Elements of the Duals of Binary BCH Codes*, F. Rossi, W. Spangher: *Computation of the Openness of Some Loci of Modules*, Y. Saitoh, H. Imai: *Random and Byte Error Correcting Codes for Asymmetric or Unidirectional Error Control*, S. Sakata: *Finding a Minimal Polynomial Vector Set of a Vector of nD Arrays*, P. Solé: *Covering Codes and Combinatorial Optimization*, O.N. Ua̧n, Ü. Aygölü, E. Panayirci: *Decoding of Quadrature Partial Response-Trellis Coded Signals (QPR-TCM) in the Presence of Intersymbol Interference and Noise*, F. Ulmer: *On Algebraic Solutions of Linear Differential Equations with Primitive Unimodular Galois Group*, F.S. Vainstein: *Error Detection and Correction in Numerical Computations by Algebraic Methods*, K. Zeng, D.-Y. Wei, T.R.N. Rao: *d-Functions in Vk(F2) and Self-Decimation of m-Sequences*, L. Zhang, B. Vuketic: *Multilevel Modulation Codes for Rayleigh Fading Channels*

J. Calmet, Karlsruhe

5. **DIMACS Workshop on Computation in Groups**

Rutgers, NJ, USA, 07.-10.10.1991.

Daß dies bereits die zweite in diesem Jahr von DIMACS organisierte Konferenz zum Thema Computeralgebra war (vgl. Bericht Nr. 2 in Nr. 9 des Rundbriefs), unterstreicht die Bedeutung, die man dort unserem Arbeitsgebiet beimißt.

In der Computational group theory gibt es seit ca. 10 Jahren neben schon länger bestehenden Arbeitsgruppen, die Algorithmen mit dem direkten Zweck der Anwendung auf gruppentheoretische Probleme entwickeln und implementieren, eine wachsende Zahl von Mathematikern, die die Komplexität von gruppentheoretischen Algorithmen insbesondere für Permutationsgruppen untersuchen, sehr oft ohne jeden Bezug zu konkreten Implementationen oder sogar Implementationsmöglichkeiten. Diese Entwicklung wurde vor allem durch die Entdeckung von G. Luks (Oregon) ausgelöst, daß Algorithmen von Ch. Sims (Schreier-Sims Methode) zur Konstruktion von Permutationsgruppen zugleich den Beweis der polynomialen Lösbarkeit gewisser Isomorphieprobleme von Graphen dienen können. (Siehe Ch.M. Hoffmann, *Group-Theoretic Algorithms and Graph Isomorphism.* Lecture

Notes in Computer Science 136, Springer, 1982.)

In der Folgezeit haben eine Reihe von Gruppentheoretikern (L. Babai, W. Kantor, P. Neumann, u.a.) erkannt, daß die Klassifikation der endlichen einfachen Gruppen und die O'Nan-Scott Klassifikation der primitiven Permutationsgruppen Verbesserungen von worst-case Komplexitätsabschätzungen für Permutationsgruppenalgorithmen liefern.

Ein offensichtliches Ziel der Tagung war es, diese sehr theoretischen Untersuchungen und konkrete Implementationen und Systementwicklungen wieder in engeren, gegenseitig nützlichen Kontakt zu bringen. Man kann sagen, daß in vielen Vorträgen und einer Panel-Diskussion erfreuliche Ansätze zur Erreichung dieses Ziels sichtbar wurden; wir hoffen insbesondere - und haben dazu bereits einige Verabredungen getroffen - daß das Aachener Gruppentheoriesystem GAP bei solchen Bemühungen eine Rolle spielen wird, auch wenn man sicher hinzufügen muß, daß hier noch eine Menge Arbeit zu tun ist.

Die Vorträge im einzelnen in zeitlicher Reihenfolge:

L. Babai: *Combinatorial Methods for Algorithms in Finite Groups*, J. Dixon: *Computing Ordinary representations of finite groups*, J. Neubüser: *Coxeter Group, some GAP, some remarks*, P. Neumann, C. Praeger: *Algorithms for Computing Matrix Groups*, A. Rosenberg: *Almost all Cayley Graphs are almost direct product graphs and why we care*, D. Holt: *Computing Quotients of finitely presented groups*, K. Blaha: *Minimum Bases for Permutation Groups. The Greedy Algorithm*, C. Sims: *Complexity Issues in Infinite Group Theory*, E. Luks: *Polynomial time Computation and Permutation Groups*, L. Soicher: *Computing with Graphs and Groups*, A.A. Ivanov: *Package for computing with Coherent Configurations*, L. Pyber: *Generation and Enumeration of Permutation Groups*, G. Cooperman: *New tools for Computational Group Theory*, L. Finkelstein: *New tools for Computational Group Theory*, I. Weisz: *PERM-A program for computing Strong Generating Sets*, B. York: *Implications of Parallel Architectures for Group Computations*, C. Lam: *Application of Group Theory to Combinatorial Searches*, G. Schneider: *Computing Loewy Series of* $Sz(8)$, D. Rockmore: *Computing of Isotypic Projections for Data on Homogeneous Spaces*, M. Clausen: *FFT on non-abelian groups*, L. Ronyai: *Computations in Associative Algebras*, N. Sarawagi: *Group Membership for Primitive Groups*, A. Goodman: *Subdirectly reducible groups and edge minimal graphs with a given automorphism group*, W. Kantor: *Orders of elements*, A. Seress: *Composition factors in Primitive Groups*, R. Beals: *Structure forest in nearly linear time for small base groups*, P. Mark: *Parallel Algorithms for Sylow's Theorem*, J.H. Conway: *Infinite reflection groups as a tool for computing.*

An einem Abend fand eine Demonstration von gruppentheoretischen Programmen statt. Hierbei wurden vorgestellt:

D. Holt and S. Rees: *Computing with quotients of finitely presented groups*, J. Leon: *Partition backtrack algorithms for permutation groups*, J. Neubüser and F. Celler: *GAP*, L. Soicher: *Computing with graphs and groups*, G. Havas: *Algorithms for computing with finitely presented groups*, C. Lam: *ISOM*, A. Seress and I. Weiss: *PERM: Computing strong generating sets for permutation groups*, A.A. Ivanov: *Computing with coherent configurations*, A. Cohen: *LIE: A system for computing with Lie groups.*

J. Neubüser, Aachen

6. **Algorithmen der Computeralgebra**

Dagstuhl Seminar, 16.–20.12.1991.

Vom 16. bis zum 20. Dezember 1991 fand das erste Seminar über Computer Algebra in Dagstuhl statt. Die Oberwolfach ähnliche Atmosphäre war für die etwa 25 Teilnehmer eine ideale Umgebung für Diskussionen am Rande des Tagungsprogramms. Ein ähnliches Seminar soll in etwa zwei Jahren wiederholt werden. Es folgt eine Aufstellung der Vortragenden und ihrer Vortragsthemen:

M. Singer: *Bounds and necessary conditions for Liouvillian solutions of linear differential equations*, M. Bronstein: *Algorithms for symbolic solution of differential equations*, E. Kaltofen: *Factoring polynomials over the algebraic closure*, A. Schönhage: *Real and complex high precision squareroot computations*, C. Traverso: *Gröbner bases and integer programming*, A. Pethö: *Computation of all non-equivalent, irreducible cubic polynomials up to discriminant 50.000*, D. Lazard: *Steward Platform*, M. Möller: *Gröbner bases computation using syzygies*, M. Giusti: *The dimension of an algebraic variety can be computed in polynomial time*, G. Michler: *Fast fourier transformations on groups and* *statistical ranking pro- blems*, J. v. z. Gathen: *Factoring polynomials over finite fields*, H. Grassmann: *Identities of 2 x 2 matrices*, V. Weispfenning: *Parametric Gröbner bases - Theory and practice*, B. Sturmfels: *Sparse resultants II*, G. Gonnet: *New algorithms for asymptotic and series computations*, W. Laßsner: *Computer algebra and lie algebras: classification and identification of lie algebras*, F. Schwarz: *Reduction and completion algorithms for partial differential equations*, H. G. Zimmer: *Algorithms for elliptical curves*, W. Krandick: *Isolation of polynomial complex roots.*

F. Schwarz, St.Augustin

Neues über Systeme und Hardware

Maple V

Ab sofort ist Scientific Computers alleiniger autorisierter Distributor für das Softwarepaket MAPLE V.

MAPLE V ist ein interaktives Werkzeug für Computeralgebra, ausgelegt für Wissenschaftler, Ingenieure, Forscher, Professoren und Studenten, um numerische und symbolische mathematische Probleme zu verstehen und zu lösen.

MAPLE V beinhaltet mehr als 2.000 Funktionen, u.a. aus den Bereichen Allgemeine Mathematik, Objektmanipulation, Kombinatorik, Differentiation, Geometrie, Gruppentheorie, lineare Algebra, lineare Optimierung, Zahlentheorie, Polynome, Statistik.

Weitgehende Grafikmöglichkeiten, wie eine Vielzahl von 2D und 3D Plotfunktionen, erlauben ausgeklügelte Darstellungen der Rechnerergebnisse.

Gegenüber der im Computeralgebra-Rundbrief Nr. 3 vom 25.10.1988 vorgestellten MAPLE 4.2 Version beinhaltet MAPLE V erheblich mehr Funktionen und graphische Darstellungsmöglichkeiten.

MAPLE V wird für alle gängigen Computerplattformen angeboten; als User-Interface stehen je nach Rechner MS-DOS, X-Windows-MacIntosh- UNIX-, VMS-, CMS-Versionen zur Verfügung.

Für Hochschulen kann MAPLE V in Form von attraktiven Multi-User-, Site- und Campus-Lizenzen angeboten werden.

Auf Anforderung übersendet Scientific Computers GmbH eine Demodiskette und bietet MAPLE V fr die beim Kunden vorhandene Plattform an.

Unterlagen, Demodiskette und Angebote sind erhältlich bei:

Scientific Computers GmbH
Franzstrae 107, Postfach 18 65
5100 Aachen
Tel.: 0241-26041, Fax.: 0241-44983

Scientific Computers GmbH, Aachen

GP/Pari Calculator Version 1.35.01

Der GP/Pari-Calculator (kurz: GP) der Autoren C.Batut, D.Bernardi, H.Cohen und M.Olivier stellt ein interaktives Computeralgebra-System dar, wie man es von Maple, Mathematica udgl. kennt. Der Umfang der verfügbaren Routinen ist zwar bei weitem nicht so groß wie der der Standardsoftware, enthält aber insbesondere für Algebraiker und Zahlentheoretiker interessante Routinen (Klassenzahl und Grundeinheiten quadratischer Zahlkörper,LLL-Algorithmus, Prozeduren zu elliptischen Kurven) sowie eine recht komfortable Grundaussstattung an Routinen aus der linearen Algebra (Matrizen- und Polynomkalkül). Neben den sehr effizient programmierten Arithmetikroutinen für ganze, rationale und reelle Zahlen verfügt GP auch über die Möglichkeit, p-adische Zahlen (mit vorgegebener Präzision) zu verarbeiten. GP enthält zusätzlich die Möglichkeit, eigene Funktionen zu definieren, und besitzt mit 4 (vier!) for-Schleifen-Konstrukten (for, fordiv, forprime, forstep) sowie den weiteren Kontrollstrukturen if, until und while sehr komfortable Features.

Sämtliche Routinen sind in C programmiert (für einige Rechner - insbesondere für Sun-Workstations - wurden zusätzlich sehr schnelle Assembler-Routinen für einige rechenintensive Prozeduren angefertigt), und zwar so, daß sie ohne Schwierigkeiten in eigene C-Programme eingebunden werden können. Allerdings ist die von diesen Routinen geforderte Verwaltung des internen Rechnerspeichers gewöhnungsbedürftig, speziell trifft dies auf die die Funktion gerepile zu, die für die garbage collection verantwortlich ist. Die Funktionsweise dieser und anderer Routinen ist in einem über 70 Seiten starken Users Guide (englisch) gut erläutert und mit einem Programmbeispiel eingehend erläutert.

Das wichtigste Faktum zum Schluß: GP/Pari ist frei erhältlich per anonymous ftp aus Frankreich (Internet-Addresse: 192.33.148.32) oder aus den USA (Internet-Addresse: 128.97.64.16, in /pub/pari als komprimierter tar-Archiv-File pari-1.35a.tar.Z).

D. Berntzen, Münster

CAIS: das Computeralgebra-Informationssystem

Wie schon im letzten Rundbrief Nr. 9 angekündigt wurde, ist am Konrad-Zuse-Institut in Berlin das Computeralgebra-Informationssystem in Betrieb genommen worden. Damit soll allen an der Computeralgebra-Interessierten die Möglichkeit gegeben werden, sich über neuere Entwicklungen — sowohl in der Computeralgebra-Fachgruppe als auch bei der Software — zu informieren.

Insbesondere sind die folgenden Rubriken eingerichtet:

1 : Mitteilungen der Fachgruppenleitung

2 : Computeralgebra-Rundbriefe

3 : Computeralgebra-Systeme — Beschreibungen

4 : Anfragen/Antworten/Diskussionen

Beim Punkt 4 handelt es sich - im Gegensatz zu anderen Diskussionsgruppen - um eine moderierte Diskussionsliste. Schicken Sie daher Nachrichten, die ins CAIS unter 4. abgelegt werden sollen, bitte an mich. Meine elektronische Adresse ist `mat420@de0hrz1a.bitnet`.

Zur Benutzung des Systems sind schon verschiedene allgemeine Einführungen veröffentlicht worden. Ich möchte daher lieber eine kurze Beispielsitzung wiedergeben, um den Einstieg zu erleichtern.

Der Zugang ist sowohl offline (über electronic mail) als auch interaktiv möglich, und dabei gibt es auch wieder zwei Wahlmöglichkeiten: entweder per `X.29` oder via `telnet`. Da die meisten Nutzer selbst keinen `X.29`-Anschluß haben und deshalb über ein gateway am Rechenzentrum gehen müssen, will ich mich auf die zweite Möglichkeit des Zugangs beschränken, den `telnet`-Zugriff. Dieser ist von jeder am Internet angeschlossenen Workstation möglich und es müssen keine Parameter eingestellt werden. Daher ist die Benutzung denkbar einfach.

Zum Zugriff auf die elib geben Sie bitte von Ihrem Terminal das Kommando

```
telnet elib.zib-berlin.de
```

Dann wird Ihr Rechner versuchen, eine Verbindung nach Berlin aufzubauen. Es kommt ziemlich schnell (manchmal aber auch nicht) die Meldung `connected` und dann der Login-prompt. Geben Sie als Userid `elib` ein; ein Paßwort ist nicht erforderlich. Nun erscheint ein Menu, in dem die verschiedenen Dienste der elib aufgeführt sind - neben der Computeralgebragibt es noch eine Reihe weiterer interessanter Punkte! Um zur Computeralgebra-Unterabteilung zu kommen, geben Sie bitte die Zahl `10` ein und drücken `<return>`.

Wenn Sie sich nun die alten Ausgaben des Computeralgebra-Rundbriefes ansehen wollen, so geben Sie jetzt die Zahl `2` ein und im nächsten Menupunkt die Nummer des gewünschten Rundbriefes - dann wird dieser auf dem Bildschirm ausgegeben.

Um zum nächsthöheren Menupunkt zurückzukehren, genügt das Kommando `up`, und mit `quit` können Sie die elib an jeder Stelle verlassen. Das Kommando `top` bringt Sie sofort zurück zum Einstiegsmenu.

Wenn Sie jedoch eine Information nicht nur ansehen wollen, sondern auch in `hardcopy` auf Ihrem Rechner haben wollen, ist **einmalig** etwas mehr Vorarbeit erforderlich. Da die elib keine Benutzer-Zugangs-Kontrolle hat, kann man auch nicht feststellen, wer sich gerade eingeloggt hat. Es ist daher sinnvoll, sich selbst erst einmal zu registieren. Dann kann man sich Daten auch per `email` zuschicken lassen, um sie anschließend auf dem eigenen Rechner weiterverarbeiten zu können.

Zuerst teilen Sie der elib Ihren Bildschirmtyp mit, dann ist die Steuerung etwas komfortabler. Falls Sie an einem `VT100`-Terminal sitzen (oder einem anderen, das `vt100` emuliert, z.B. eine `X-Windows`-Sitzung), geben Sie bitte das Kommando

```
term vt100
```

- analog für andere Bildschirmtypen. Wenn die elib Ihr Terminal nicht kennt, so werden Sie entsprechend infomiert.

Anschließend wählen Sie im Hauptmenu den Punkt 2 an: `check-in menu`. Nun erhalten Sie detaillierte Ausführungen und schließlich die Aufforderung, sich zu registieren. Wählen Sie irgendeine Userid (vielleicht Ihre eigene auf Ihrem eigenen Rechner - die ist einfacher zu merken) und ändern Sie das Standard-Paßwort in ein Paßwort, an das Sie sich erinnern können. Als nächstes sollten Sie die Anweisungen befolgen und eine Testmail an `elib@sc.zib-berlin.de` schicken, die genauso aussieht wie im Text beschrieben. Der Grund: die elib ist dann in der Lage, festzustellen, wie Sie elektronisch erreichbar sind. Die Userid, die Ihnen die elib zugewiesen hat, wird intern mit Ihrer email-Anschrift verknüpft und Sie erhalten automatisch eine Bestätigung. Damit ist eigentlich alles getan, Sie können jedoch die weiteren Menupunkte ausfüllen für die interne Datenbank.

Geben Sie nun - und bei allen weiteren Sitzungen - das Kommando

```
password <userid>
```

und beantworten Sie die Frage nach dem Paßwort, dann sind Sie der elib als individueller Nutzer bekannt. Wenn Sie sich nun aus einem Menu Dateien zuschicken lassen wollen, genügt das Kommando

```
send <nummer>
```

und die Datei wird Ihnen elektronisch zugesandt.

Da die elib sehr gut dokumentiert ist - Sie können an jeder Stelle das Kommando 'help' geben - können Sie weitere Möglichkeiten, die Ihnen das System bietet (und das sind sehr viele) selbst erforschen.

Ich wünsche Ihnen viel Spaß bei der Benutzung des CAIS und bin für Anregungen jederzeit dankbar.

Gerhard Schneider, Essen

REDUCE Version 3.4

Zum 15. Juli 1991 während ISSAC91 hat Tony Hearn die Version 3.4 des Computeralgebra-Systems REDUCE freigegeben. Die vorausgegangene Entwicklungsphase war erstmalig dadurch gekennzeichnet, daß in der seit Anfang 1989 über electronic Mail zugänglichen REDUCE Library schon frühzeitig neue oder fortgeschriebene Moduln öffentlich zugreifbar waren, was sich für Entwickler und Anwender als gleichermaßen förderlich erwiesen hat. Die REDUCE Library hat auch zu einer verstärkten Bereitstellung von Anwenderpaketen geführt. Die meisten der bis Mitte 1991 in der Library versammelten Moduln sind nun Bestandteil von REDUCE 3.4, allerdings meist in integrierter Form. Das Paket Gröbner z.B. entspricht leistungsmäßig seinem letzten Stand in der Library, jedoch bedient sich nun der SOLVE Modul von REDUCE intern dieses Paketes, wenn die • Lösung nichtlinearer Gleichungssysteme - eine neue Leistung - verlangt wird.

Zwei weitere neue Aspekte sind: • Ein neuer Modus *rounded* gestattet einheitlich die numerische Auswertung von Ausdrücken (reell und komplex) in Gleitkommaarithmetik mit einer frei wählbaren Genauigkeit, die auch dynamisch (adaptiv) variiert werden kann und auch für die Berechnung elementarer Funktionen gilt. • Für die schon lange in REDUCE unterstützten LET-Regeln ist mit dem **Ruleset** eine neue syntaktische Basis angelegt worden. Ein Ruleset ist eine als Liste zusammengefasste Folge von Regeln, die insgesamt aktiviert oder deaktiviert werden kann, und zwar sowohl global als auch lokal (d.h. auf eine einzelne Auswertung bezogen). Rulesets sind ein geeignetes Hilfsmittel zur Codierung von Kalkülsystemen, da sie Pattern-Matching, Fallunterscheidung und Kontrolle der Auswertungsabfolge vereinen.

Für die übrigen Leistungsmerkmale sei auf einschlägige Schriften verwiesen, insbesondere auf die Library selbst: man schicke an *redlib@elib.zib−berlin.de* je einen Brief mit dem Subject *send info−package* bzw. *send intro.tex from documents* (Antwort in LaTeX). Diese Informationen können zusammen mit Angaben zum Bezug von REDUCE auch in gedruckter Form direkt vom ZIB angefordert werden (Tel: 030-89604-205, Email: *melenk@sc.zib − berlin.de*). Ein Wermutstropfen bleibt die Graphik: zwar schon während ISSAC 91 vorab zu besichtigen, ist sie immer noch nicht fertiggestellt. Als Übergangslösung gibt es derweil ein Interface zu dem sehr hübschen GNUPLOT Paket.

Mit REDUCE 3.4 bleibt die Entwicklung nicht stehen: die mit der Freigabe zunächst obsolet gewordene Library enthält schon wieder neue und erweiterte Moduln.

Zum Abschluß noch ein Blick auf die technische Front: REDUCE ist für (fast) alle im Wissenschaftsbetrieb eingesetzten Rechner erhältlich, vom kompatiblen AT386 (bald auch unter Windows 3.0) bis hinauf zur Cray Y. Novitäten: • Auf dem Urgestein IBM /370 Nachf. läuft REDUCE jetzt im XA-Mode, d.h. mit erheblich erweitertem Speichervolumen • Auch VAX REDUCE wurde mit einem dynamischen Arbeitsspeicher aufgerüstet • Unter den REDUCE Workstations nehmen derzeit die RISC-Schlangen HP9000-7x0 leistungsmäßig die Spitzenposition ein: sie schaffen den Standardtest in 1.7 Sekunden bzw. darunter (IBM ES/9000: 2.1 sec, IBM RS/6000-550: 2.4 sec, SPARC2: 2.7 sec, IRIS310: 2.84 sec, AT486: 7.7 sec) und werden nur von den Cray's signifikant übertroffen; • unsere Kollegen in England arbeiten an einer Implementierung für MACs; • füer die Kleinrechner (z.b. 386/DOS) wird es demnächst ein *personal* REDUCE zu einem deutlich reduzierten Preis geben.

Herbert Melenk, Berlin

Berichte über Arbeitsgruppen

The CAMASA group in Italy

CAMASA (the acronym stands for **C**alcolo **A**lgebrico: **M**etodi, **A**lgoritmi, **S**istemi, **A**pplicazioni) is the Italian Research Group in Symbolic Computation. It is funded by MURST (Board for the University and Scientific-Technological Research) at a national level and coordinates other projects or contracts funded by research agencies in Italy. Its aim is the coordination of the research activity in Symbolic Computation and the diffusion of this discipline through the organization of schools and meetings, also at an international level.

The most recent Project (October 90) collects 76 researchers and 10 units (Cagliari, Catania, Genova, L'Aquila, Milano, Pavia, Pisa, Roma La Sapienza, Roma Tor Vergata, Trieste). Moreover other researchers are involved in Symbolic Computation which are not part of CAMASA.

The italian activity in Symbolic Computation covers a wide spectrum of research areas: commutative algebra, polynomial equation solving, differential algebra and differential equations, real algebraic geometry, invariant theory, theory of algebraic group representations, combinatorics, automatic deduction, rewriting techniques, languages and systems for Symbolic Computation, applications to mechanics and robotics, applications to system theory, applications to didactics, production of systems for Symbolic Computation , parallelization, numerical - symbolical integration.

Since its birth in 1985, CAMASA has organized several international meetings and workshops (COCOA I, Genova, 1986; Computing Tools for Research and Develoment in Science and Engineerings, Capri, 1987; ISSAC 88 and AAECC 6, Roma, 1988; COCOA II, Genova, 1989; DISCO '90, Capri, 1990; MEGA '90, Castiglioncello, 1990) and two international schools (International course on automated reasoning in geometry, Catania 1987; International course on computational real geometry, Catania, 1988). There has been also a continuous activity of formation through the organization of schools for a national audience.

CAMASA organizes periodical meetings; the first one was held in Pavia in December 1986 and its abstracts are published in the SIGSAM Bulletin; a second one was held in Trieste in April 1989. The third one was held in Cagliari, March 21-23, 1991. The program of this meeting, whose abstracts are available too in the SIGSAM Bulletin, can be find in the section *Berichte von Konferenzen*.

Teo Mora, Genua

Publikationen über Computeralgebra

- T. Mora, C. Traverso (ed.) *Effective Methods in Algebraic Geometry* 1991, ISBN 0-8176-3546-7, Birkhäuser.
- K. R. Meyer, D. S. Schmidt *Computer Aided Proofs in Analysis* 1990, ISBN 3-540-97426-1, Springer.
- L. Bachmair *Canonical Equational Proofs* 1991, ISBN 0-8176-3555-6, Birkhäuser.
- A. Griewank, G. F. Corliss (ed.) *Automatic Differentiation of Algorithms: Theory, Implementation, and Application, Proceedings in Applied Mathematics 53* 1991, ISBN 0-89871-284-X, SIAM List Price 48.50/$SIAMMemberPrice$38.80 Order Code PR53 1992, Proceedings in Applied Mathematics 53

  An introduction and reference on techniques for evaluating derivatives of functions given by computer programs. By applying variants of the chain rule, first and higher derivatives are obtained efficiently and accurately. A survey of 28 software implementations and an extensive bibliography are included.

This volume is appropriate for developers and users of numerical packages for nonlinear computational problems, e.g. optimization, nonlinear equations, ODE's, implicit ODE's, PDE's, computer manufacturing, and system development. A knowledge of differential calculus and some programming experience will assist appreciation of the material.

SIAM

- M. Mignotte *Matematics for Computer Algebra* 1992, ISBN 0-387-97675-2, Springer.
- Besprechung von mathPAD sollte hier rein

Lehrveranstaltungen über Computeralgebra im WS 1991/92

- **RWTH Aachen**
  Einführungspraktikum in MAPLE, Neubüser, Klein, Dietrich, Blockpraktikum.
- **Universität Augsburg**
- **Universität Bayreuth**
- **Universität Basel**
- **Universität Bonn**
- **Universität Bonn**
  Effiziente Numerische Algorithmen, A. Schönhage, V4.
  Seminar Computeralgebra, A. Schönhage, O. Geupel, S2.
- **Universität Clausthal-Zellerfeld**
  Projektgruppe Computeralgebra, Lex, Söding, P2.
- **Universität Düsseldorf**
- **Universität Erlangen-Nürnberg**
  Computeralgebra: Polynomarithmetik, H. Meyn , K. Kalb , V2+P2.
- **Universität-Gesamthochschule Essen, Institut für Experimentelle Mathematik**
  Effektive Algorithmen, T.V. Tran, V2.
  Paralleles Rechnen, W. Happle, P2.
- **Universität Heidelberg**
  Computeralgebra, G. Malle. V2+P2.
- **Universität Karlsruhe**
  Applications of Algebra in Cryptology, Beth, Nyberg. V3.
  Algorithmische Zahlentheorie, Beth, Geiselmann, Schaefer-Lorinser. S2.
  Computeralgebra: Algorithmische Zahlentheorie, Beth, Geiselmann, Schaefer-Lorinser. P4.

  Computeralgebra: Algebraische Algorithmen, Calmet. V3.
  KI und mathematisches Wissen, Calmet, Homann, Tjandra. S2.
  Entwurf von Computeralgebra-Systemen, Calmet, Homann, Seiler, Tjandra. P4. **Universität Karlsruhe**
  Computeralgebra, Th. Beth, W. Geiselmann, F. Schaefer-Lorinser, P2. *Angewandte Kombinatorik*, Th. Beth, V2.
- **Universität Leipzig**
  Einführung in die Computeralgebra, W. Laßner, V2.
  Grundlagen der Computeralgebra, W. Laßner, V2.
  Fachpraktikum: Symbolisches Rechnen II, W. Laßner, St. Forner, P 2.
  Forschungsseminar Computeralgebra, W. Laßner, H.-G. Gräbe, S 2.

- **RISC Linz**

  Logik fUr Mathematiker und Informatiker II, J. Pfalzgraf, V2
  Überblick über Symbolic Computation, B. Buchberger, V2
  Computer Algebra für Fortgeschrittene, F. Winkler, V2
  Analytische Kombinatorik, P. Paule, V2
  Funktionales Programmieren (LISP), F. Winkler, V2
  Formale Spezifikation und Verifikation, H. Rolletschek, V2
  Algorithmische Algebraische Geometrie, S. Stifter, V2
  Geometrische Grundlagen für Symbolic Computation, S. Stifter, V2
  Algorithmische Kombinatorik, P. Paule, V2
  Automatisches Beweisen B, D. Wang, V2
  Rewriting in Mathematik und Logik, H. Hong, V2
  Theoretical Foundations of Parallel Computation, T. Jebelean, V2
  Parallel Algorithms for Symbolic Computation, H. Hong, V2
  Konnektionistische Systeme/ Neuronale Netze, J. Pfalzgraf, V2
  Selected Topics in Computer Algebra II, G. Collins, V2
  Privatissimum Quantifier Elimination, G. Collins, PV2
  Diplomanden- und Dissertantenstunde II, G. Collins, S3
  Praktikum Paralleles Rechnen, W. Schreiner, P2
  Softautomation: Simulation und Programmierung, M. Mayr, J. Heinzelreiter, V2
  Projektseminar: Algorithmen für CAD und Roboterprogrammierung, B. Buchberger, S. Stifter, S2
  Projektseminar: Software und Hardware für paralleles Rechnen, B. Buchberger, S2
  Projektseminar: Algorithmische und algebraische Geometrie, B. Buchberger, F. Winkler, S2
  Projektseminar: Software-Technik im Bereich Symbolic Computation, B. Buchberger, F. Lichtenberger, S2
  Projektseminar: Algorithmische Kombinatorik, B. Buchberger, P. Paule, S2
  Programmierprojekt parallele Software II (Transputersystem, Workstationnetz), B. Buchberger, W. Schreiner, P4
  Literaturseminar Symbolic Computation II, B. Buchberger + Assistenten, S2
  Programmierprojekt Symbolic Computation II, B. Buchberger + Assistenten, P4
  Vortragsreihe Symbolic Computation, B. Buchberger, F. Winkler, V1
  Praktische Beweistechnik und wissenschaftliches Arbeiten in Symbolic Computation, B. Buchberger, V2
  Diplomanden- und Dissertantenstunde II, B. Buchberger + Assistenten, S3

- **Technische Universität München**

- **Universität Passau**
  Oberseminar Computeralgebra, V.Weispfenning, Th. Becker, H. Kredel, S3.

- **Universität-Gesamthochschule Paderborn**

- **Universität des Saarlandes, Saarbrücken**

-

- **Eidgenössische Technische Hochschule Zürich**
  Aufbau symbolischer Rechensysteme, R. Mäder, V2+P1.
  Problemlösen mit Mathematica, R. Mäder, S3.
  Symbolic Integration, M. Bronstein, V2+P1.

Leserbriefe

- Im Bericht über die DMV-Jahrestagung im Rundbrief Nr. 9 erwähnt Herr Hering, daß wir zwei HP 700 aus Aachen mitgebracht haben. Das stimmt so nicht ganz, denn leider haben auch wir keine zwei HP 700. Die beiden Maschinen waren vielmehr eine freundliche Leihgabe der Firma Hewlett Packard, für die ich mich hier noch einmal sehr herzlich bedanken möchte. Richtig ist allerdings, daß wir die beiden Maschinen *auftreiben* mußten, weil die Bielefelder Tagungsleitung dazu nicht in der Lage war. Eine haben wir von Aachen aus in Bielefeld *gefunden*, wo sie gerade zu einer Demonstration in chemischen Institut eingesetzt war, die andere haben wir in der Tat im Privat-PKW aus Aachen mitgebracht, wo sie im hiesigen Institut für Mechanik im Probebetrieb war. Wir hoffen allerdings, zum Jahresende unsere erste HP 730 für die Mathematik in Aachen anschaffen zu können.

Kurze Mitteilungen

- Die elektronischen Adressen folgender Mitglieder der Fachgruppenleitung haben sich geändert: Prof. Dr. H.G. Zimmer: zimmer@math.uni-sb.de. Prof. Dr. M. Pohst: ?????.
- Die Institute ICM (Institute de Calcul Mathematique, Paris, Frankreich) und Kent State Univ, Ohio, USA bieten Promotionsstipendien für Studenten aus der Europäischen Gemeinschaft und den USA auf dem Gebiet *Quantitative estimates for polynomials in one or several variables* mit Anwendungen u.a. in Computeralgebra an. Das Programm wird von der National Science Foundation (USA), der C.N.R.S. (Frankreich), dem französischen Verteidungsministerium und der DIGITAL Eq. Corp. unterstützt.

  Kontaktadressen: Prof. B. Beauzamy, ICM, Universite de Paris 7, 2 Place Jussieu 75251 Paris CEDEX 05, Frankreich und Prof. Per Enflo, Prof. Paul Wang, Dept. of Math, Sciences, Kent State Univ., Kent, Ohio 44242, USA.
- Das Release 3.1 von GAP aus Aachen soll demnächst fertiggestellt sein. Die genaue Ankündigung werden Sie im sci.math und sci.math.symbolic sowie natürlich im CAIS finden. Die Entwickler bitten von Vorabanfragen abzusehen.
- Großes Interesse fanden die beiden von IBM und NAG gemeinsam durchgeführten AXIOM-Informationsveranstaltungen in München und Heidelberg. Zwei weitere solche Informationstage sind für den 06.05.1992 in Düsseldorf und für den 08.05.1992 in Berlin geplant. Auskunft und Anmeldung bei U. Harris, NAG GmbH, Schleissheimerstr. 5, 8046 Garching bei München, Tel.: 089-3207395, Telefax: 089-3207396.