Computer-Algebra Rundbrief

Nummer 5 *Fachgruppe 2.2.1* *15. November 1989*

Liebe Kolleginnen und Kollegen,

unsere Fachgruppe besteht nun seit zwei Jahren und wir möchten dies zum Anlaß nehmen, wieder einmal zu fragen: Was haben wir in dieser Zeit erreicht, um unser Gebiet voranzubringen? Unser erstes Ziel, die Kenntnis über unser Gebiet zu verbreiten, haben wir durch verschiedene Veranstaltungen verfolgt. So findet auf den Jahrestagungen der DMV nun schon fast regelmäßig eine Veranstaltung zur Computer-Algebra statt – teilweise trifft dies auch auf die entsprechenden Jahrestagungen der GI und der GAMM zu – und in Zusammenarbeit mit der DIA wurde im vergangenen September in Bonn eine Herbstschule abgehalten, die sich wohl zu einer Dauereinrichtung entwickeln wird und deren Schwerpunkt auf Anwendungen liegt (siehe auch die Ankündigung an anderer Stelle dieses Rundbriefes). Des weiteren wird das jährlich stattfindende International Symposium on Symbolic and Algebraic Computation im Jahr 1991 von der GMD in Bonn veranstaltet werden – wir möchten Sie schon jetzt bitten, dies in Ihrer Planung zu berücksichtigen, da dies sicher ein gute Chance ist, ohne große Reisekosten an dieser auf dem Gebiet der Computer-Algebra führenden Tagung teilzunehmen. Im gleichen Jahr soll in der neu zu gründenden Fortbildungsstätte Dagstuhl der GI eine Veranstaltung über Computer-Algebra stattfinden. Für weitere Anregungen und konstruktive Kritik sind wir natürlich jederzeit dankbar.

Die Berichte über Computer–Algebra Gruppen in Deutschland haben wir aus Platzgründen vollständig auf den nächsten Rundbrief verschoben.

Immer wieder werden Fragen betreffend der Verfügbarkeit von Computer-Algebra Systemen gestellt. Wir haben deswegen aus früheren Rundbriefen eine Übersicht zusammengestellt, die Ihnen zusammen mit diesem Rundbrief zugesandt wird. Sie wird in unregelmäßigen Abständen auf den neuesten Stand gebracht werden und ist auf Anforderung erhältlich.

Zusammen mit diesem Rundbrief erhalten Sie ein Exemplar der Ordnung der Fachgruppe Computer–Algebra, die von den Gründungsmitgliedern beschlossen und von DMV, GAMM und GI akzeptiert worden ist. Nach dieser findet im Jahr 1990 erstmals eine Wahl der Fachgruppenleitung statt. 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 1.3.90 Vorschläge an Dr. F. Schwarz (Anschrift wie im Impressum) zu senden.

Alle Vorgeschlagenen werden danach gefragt werden, ob sie sich zur Wahl stellen. Mit der Nr. 6 des Rundbriefs werden Sie dann im April/Mai 1990 eine 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 1.10.90 aufnehmen soll.

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 Computer-Algebra tatkräftig unterstützen werden.

F. Schwarz, J. Neubüser

Hinweise auf Konferenzen

1. **Scratchpad II und experimentelle Mathematik**

   Essen, 30.11.-1.12.1989.

   Kontaktadresse: Dr. H. Gollan, Institut für Experimentelle Mathematik, Ellernstr. 29, 4300 Essen 2, E-mail MAT422 at DE0HRZ1A.BITNET.

[0]**Impressum** *Computer-Algebra Rundbrief* Herausgegeben von der Fachgruppe 2.2.1 *Computer-Algebra* der GI. Anschrift: Dr. F. Schwarz, GMD, Institut F1, Postfach 1240, 5205 Sankt Augustin 1. ISSN 0933-5994

2. **Computeralgebra und Differentialgleichungen**

   Leipzig, DDR, 5.2.–16.2.1990.

   Kontaktadresse: Interdisziplinäres Seminar für wissenschaftlichen Nachwuchs an der Karl–Marx–Universität, Goethestraße 6 PSF 920, DDR–7010 Leipzig.

3. **Symposium on Symbolic Computation**

   Zürich, Schweiz, 5.3.–7.3.1990.

   Kontaktadresse: Prof. Dr. H. Laeuchli, Mathematik, HG G 62.3, ETH-Zentrum, CH-8092 Zürich, Schweiz.

4. **Workshop on Number Theory and Algorithms**

   Berkeley, Kalifornien, 26.3.–29.3.1990.

   Kontaktadresse: Prof. H.W. Lenstra jr., Departement of Mathematics, UC Berkeley

5. **Minisymposium: Symbolverarbeitung in der Mechanik** auf der GAMM-Tagung 1990

   Hannover, 9.4.–12.4.1990.

   Ansprechpartner: Dr. E. Kreuzer, Meerestechnik II, Technische Universität Hamburg–Harburg, Eißendorfer Str. 42, 2100 Hamburg 90.

6. **International Symposium on Design and Implementation of Symbolic Computation Systems**

   Capri, Italy, 10.4.-12.4.1990.

   Kontaktadresse: Prof. Alfonso Miola, Dip. Informatica e Sistemistica, Via Buonarroti 12, 00185 Roma, Italy. Phone: (+39)–6–7312367/7312328/733412, Fax number:(+39)–6–734616

7. **Effective Methods in Algebraic Geometry (M E G A 90)**

   Pontignano, Siena, Italy, 17.4.–21.4.1990.

   Kontaktadresse: Carlo Traverso, Dipartimento di Mathematica, Via Buonarroti 2, 56100 Pisa, Italy. E-Mail: Traverso@icnucevm.bitnet

8. **DMV-Seminar Konstruktive Zahlentheorie**

   Schloß Mickeln bei Düsseldorf, 5.8.–12.8.1990.

   Kontaktadresse: M. Pohst, Mathematisches Institut, Universität Düsseldorf, Universitätsstr. 1, 4000 Düsseldorf, Tel.: 0211/3112188.

9. **Second International Joint Conference of ISSAC–90 and AAECC–8**

   Tokyo, Japan, 20.8.–24.8.1990.

   Deadline für eingereichte Beiträge (Eingang): **31.3.1990**

   Beiträge ISSAC–90 an:Dr. Tateaki Sasaki, ISSAC Program Committee Co–Chairman, The Institute of Physical and Chemical Research, Wako–shi, Saitama 351–01, JAPAN
   Beiträge AAECC–8 an: Prof. Hideki Imai, AAECC Program Committee Co-Chairman, Faculty of Engineering, Yokohama National University, Tokiwadai, Hodogaya-ku, Yokohama 240, JAPAN.

   Kontaktadresse: Conference Secretariat IJC-2, c/o Scientist, Inc., Yamazaki Bldg., 3–2 Kanda Suruga–dai, Chiyoda-ku, Tokyo 101, JAPAN, Phone (03)253–8992, Fax (03)255–6847.

10. **Advances in Robot Kinematics**

    Linz, Austria, 10.9.–12.9.1990.

    Kontaktadresse: Bernhard Kutzler, RISC-Linz, Johannes Kepler University, A-4040 Linz, Austria, ph. +7236/3231-45, fax + 7236/3331-30, e-mail Bitnet: K311940 AEARN
    bzw. *Jožef Stefan* Institute, University of Edvard Kardelj, Ljubljana, Yugoslavia.

11. **Greco Calcul Formel**

    Luminy, France, 10.9.–15.9.1990.

    Kontaktadresse: D. Lazard, Université Paris VI, 4 pl. Jussieu, 75252, Paris Cedex 85, France; Tel.:(33)1-43267660; UUCP: Lazard at litp.ibp.fr

12. **2. Herbstschule Computer-Algebra und ihre Anwendungen**

    Bonn, 24.9.–28.9.1990.

    Kontaktadresse: Frau Offermanns, Deutsche Informatik Akademie, Wissenschaftszentrum, Ahrstraße 45, 5300 Bonn 2, Tel.: 0228-302164.

13. **International Symposium on Symbolic and Algebraic Computation ISSAC '91**

    Bonn, 15.7.–17.7.1991.

    Kontaktadresse: Frau Harms, GMD Schloß Birlinghoven, Postfach 1240, 5205 Sankt Augustin 1, Tel. 02241-142473.

Berichte von Konferenzen

1. Third CAYLEY Users Conference

   Essen, 17.11.–19.11.1988.

   Auf dieser Tagung wurden in einer Reihe von Vorträgen verschiedene Algorithmen aus der Gruppen- und Darstellungstheorie vorgestellt und ihre Implementation in das CAYLEY-System diskutiert. Ferner wurde die Bedienung dieses Systems sowie seine Benutzeroberfläche online demonstriert. Für die ca. 50 Teilnehmer aus ganz Europa standen 17 Bildschirmarbeitsplätze an drei verschiedenen Systemen (IBM 4381 mit CMS, IBM 6150 mit AIX, Siemens WS30 mit Unix) zum eigenständigen Arbeiten mit CAYLEY zur Verfügung.

   Vorträge (in chronologischer Reihenfolge):

   G. Michler, *Introduction*; J. Cannon, *CAYLEY: past, present and future*; D. Holt, *Permutation groups in CAYLEY*; G. Schneider, *Representation Theory in CAYLEY: Tools and Algorithms*; Ch. Leedham-Green, *An introduction to computing with p-groups*; J. Cannon, *The new soluble group module in CAYLEY*; R. Curtis, *Natural generators for the Mathieu groups*; G. Schneider, *Library management in CAYLEY*; B. Sandling, *Group rings*; J. Cannon, *Basic strategies for computing with fp-groups*; N. Klingen, *Algebraic number theory with the help of CAYLEY*; M. Pohst, *A computational number theory package: KANT*; H. Gollan, *A representation theory case study: J_1 in char 2.*

   Proceedings sollen als SIGSAM-Bulletin erscheinen. G. Schneider

2. Meeting on Computer and Commutative Algebra, COCOA II

   Universität Genua, Italien, 29.5.–3.6.1989.

   Die Konferenz beschäftigte sich mit algorithmischen Techniken in der kommutativen Algebra und der (reellen und komplexen) algebraischen Geometrie; darüberhinaus wurden Anwendungen solcher Techniken in der Differentialalgebra und in Noetherschen, nichtkommutativen Algebren behandelt. Ein zentrales Thema bildete die Frage der asymptotischen und praktischen Komplexität der dargestellten Verfahren aus den Bereichen Eliminationstheorie, Gröbner- und Standardbasen Techniken, Quantorenelimination und spezieller Probleme. Dabei spielten Anwendungen tiefliegender Methoden der algebraischen Geometrie (lokale Kohomologie, effektive Nullstellensätze) eine wichtige Rolle.

   Bei der Demonstration von Computer Algebra Systemen wurde insbesondere das neue Macintosh-System CoCoA (Universität Genua) vorgestellt, das eine benutzerfreundliche Oberfläche für Fragen der algebraischen Geometrie bietet; ferner das DOS-System ALPI (Universität Pisa), das neue Strategien zur Gröbner- und Standardbasenberechnung benutzt.

   Vorträge (in chronologischer Reihenfolge):

   C. Traverso, Pisa, *A new critical pair completion algorithm for standard and Gröbner bases*; V. Weispfenning, Passau, *Comprehensive Gröbner bases*; T. Recio, Santander, *Towards a catalogue of shapes for plane* *real algebraic closed connected curves with double points*; M. Giusti, Palaiseau, *On the Castelnuovo regularity for curves*; W. Vasconcelos, Rutgers, *The equations of commuting pairs of matrices*; B. Sturmfels, Linz, *Gröbner bases of determinantal ideals*; B. Buchberger, Linz, *Gröbner bases and determinant polynomials*; L.J. Billera, Rutgers, *Gröbner bases methods for multivariate splines*; A. Giovini - G. Niesi, Genova, *CoCoA System Presentation*; D. Lazard, Paris, *Solving algebraic systems*; J. Heintz, Buenos Aires, *The complexity of the membership problem for polynomial ideals*; A. Galligo, Nice, *What property of local cohomology is used in the proof of the sharp effective Nullstellensatz?*; B. Trager, IBM Yorktown Heights, *Good reduction of curves and applications*; F. Winkler, Linz, *A p-adic approach to the computation of Gröbner bases*; M. Sweedler, Cornell, *Bases for subalgebras*; H.M. Möller, Hagen, *On solving systems of algebraic equations by decomposition*; T. Gateva, Sofia, *On the noetherianity of some finitely presented associative algebras*; Brownawell, Penn State Univ, *New results on the effective Nullstellensatz*; M.F. Roy, Rennes, *Effective real algebra and geometric applications*; J.J. Risler, Paris, *Connected components of real algebraic and semialgebraic sets*; W. Lassner, Leipzig, *Ordering problems and symbol representation in envelopping algebras*; G. Carra'Ferro, Catania, *Minimal Hilbert polynomial in algebraic geometry and differential algebra*; P. Gianni, Pisa, *Efficient computation of zero-dimensional Gröbner bases by change of ordering*; M. Stillman, Cornell, *Finding the image of a polynomial map corresponding to a line bundle*; D. Bayer, Harvard, *Two new algorithms for computing Hilbert polynomials*; K.J. Nishimura, Nagoya, *On Nagata rings*; R. Fröberg, Stockholm, *A faster way to count the solutions of an inhomogeneous system of equations with applications to cyclic n-roots*, J. Elias, Barcelona, *The reduction number of one-dimensional local rings*; W. Vasconcelos, Rutgers, *On the equations of Rees algebras*; A. Simis, Salvador de Bahia, *Rees algebras of some special ideals*; Ngo Viet Trung, Hanoi, *The Hilbert function of integral closures of powers of parameter ideals.* V. Weispfennig

3. Computers & Mathematics

Konferenz am MIT, Cambridge, Massachusetts, 13.6.–17.6.1989.

Die Konferenz war die dritte einer Reihe von Konferenzen, welche sich im weiteren Sinne mit der Anwendung des Computers als Mittel in der mathematischen Forschung befaßte. Die Konferenz bestand aus 21 Hauptvorträgen, 36 Vorträgen, 8 3-stündigen Minikursen, 10 Tutorials von Computer Algebra Programmen, sowie Demonstration der CA Programme Mathematica, Maple, Macsyma, $f(z)$, Scratchpad und einiger Computer Hersteller.

Hauptvorträge (in chronologischer Reihenfolge):

M.F. Barnsley, Georgia Tech., *Mathematics and Graphics of Fractals*; R.J. Baxter, ANU, *Arithmetic Series, Expansions, and Exact Results in Statistical Mechanics*; P. Borwein, Dalhousie, *Ramanujan and Maple: Classical Analysis and Symbolic Computation*; A. Chorin, Berkeley U., *Random Computation and Differential Equations*; D.V. and G.V. Chudnovsky, Columbia U., *How We Use Computer Algebra for Supercalculations*; J.H. Conway, Princeton U., *Computers and Frivolity*; D. Cox, U. of Illinois, *Supercomputing Graphics: Convergence of Art and Mathematics*; M.J. Creutz, Brookhaven, *Roulette Wheels and Quantum Field Theory*; M.M. Denneau, IBM Research, *Supercomputing in the Early 1990's: Teraflops and Beyond*; G.K. Francis, U. of Illinois, *Novel Ways to Paint and Animate Surfaces Extended in Four or More Dimensions*; J.W. Goodman, Stanford U., *Computing in the Photonic Age*; R.W. Gosper, Symbolics, Inc., *How I Find Funny Looking Formulas*; A.H. Guth, MIT, *The Birth of the Cosmos*; R.H. Miller, Chicago, *Playing God: Building Galaxies in a Computer*; A. Odlyzko, AT&T Bell Labs, *Computational Insights into Problems of Combinatorics and Number Theory*; J. Schwartz, MIT/Harvard, *Software for Students to Make Mathematics: Lessons from Secondary Geometry and Algebra*; N.J.A. Sloane, AT&T Bell Labs, *Computers and the Search for Error-Correcting Codes*; A.R. Smith, PIXAR, *How To Make Pictures With A Computer*; D. Stanton, Minnesota, *Undergraduate Exploration into Combinatorics Using Computers*; H.S. Wilf, U. of Pennsylvania, *How to Prove Billions of Combinatorial Identities at Once.*

Vorträge (in chronologischer Reihenfolge):

T.A. Ager and R.A. Ravaglia, Stanford U., S. Dooley, Berkeley, *Representation of Inference in Computer Algebra Systems with Applications to Intelligent Tutoring*; A.G. Akritas, U of Kansas, *Exact Algorithms for the Matrix-Triangularization Subresultant PRS Method*; J. Baddoura, MIT, *Integration in Finite Terms and Simplification with Dilogarithms*; F. Bergeron, U. du Quebec a Montreal, *A Story About Computing with Roots of Unity*; M.J. Beeson, San Jose State, *Logic and Computation in MATHPERT: An Expert System for Learning Mathematics*; G. Copperman and L. Finkelstein, Northeastern, P.W. Purdom Jr., Indiana, *Fast Group Membership Using a Strong Generating Test for Permutation Groups*; P.J. Costa and R.H. Westlake, Raytheon, Wayland, MA, *Example of Computer Enhanced Analysis*; D. Duval, U de Grenoble, *Simultaneous Computations of Different Characteristics*; M.R. Fellows, Idaho, N.G. Kinnersley and M.A. Langston, Washington State U., *Finite-Basis Theorems and a Computation-Integrated Approach to Obstruction Set*

Isolation; W. Feurzeig, P. Horwitz, A. Boulanger, BBN Labs, *Advanced Mathematics from an Elementary Viewpoint: Chaos, Fractal Geometry, and Nonlinear Systems*; E. Freire, E. Gamero, E. Ponce, U Sevilla, Spain, *An Algorithm for Symbolic Computation of Hopf Bifurcation*; A. Galligo, Nice and INRIA/Sophia Antipolis, C. Traverso, Pisa, *Practical Determination of the Dimension of an Algebraic Variety*; V. Ganzha, Novosibirsk & TU München, R. Liska, TU of Prague, *Application of the Reduce Computer Algebra System to Stability Analysis of Difference Schemes*; K.O. Geddes and T.C. Scott, Waterloo, *Recipes for Classes of Definite Integrals Involving Exponentials and Logarithms*; V.P. Gerdt and N.A. Kostov, Inst Nuclear Research, Dubna, *Computer Algebra in the Theory of Ordinary Differential Equations of Halphen Type*; C. Graci, J.Y. Narayan, R. Odendahl, SUNY, Oswego, *Bunny Numerics: A Number Theory Microworld*; M.V. Hildebrand, Harvard, J. Weeks, Ithaca, NY, *A Computer Generated Census of Cusped Hyperbolic 3-Manifolds*; H.J. Hoover, Alberta, *Why Integration is Hard*; J.K. Johnstone, Johns Hopkins, *Working with Ruled Surfaces in Solid Modeling*; D. Kapur, SUNY, Albany, K. Madlener, U. Kaiserslautern, *A Completion Procedure for Computing a Canonical Basis for a k-Subalgebra*; D. Leites, Stockholm, G. Post, Twente, The Netherlands, *Cohomology to Compute*; H.S. Mills and M.H. Vernon, Lewis & Clark State College, *Using Macsyma to Calculate the Extrinsic Geometry of Tubes in Riemannian Manifolds*; D.L. Rector, U of California at Irvine, *Semantics in Algebraic Computation*; N.W. Rickert, Northern Illinois U., *Efficient Reduction of Quadratic Forms*; D. Rockmore, Harvard, *Computation of Fourier Transforms on the Symmetric Group*; T. Sakkalis, New Mexico State U., *Signs of Algebraic Numbers*; D.Y. Savio and E.A. Lamagna, Rhode Island, S.-M. Liu, Northwestern, *Summation of Harmonic Numbers*; M.F. Singer, North Carolina State, *Liouvillian Solutions of Linear Differential Equations with Liouvillian Coefficients*; N. Strauss, Pontificia U. Catolica, Rio, *Algorithm and Implementation for Computation of Jordan Form*; H.-Q. Tan, U of Akron, *Symbolic Derivation of Equations for Mixed Formulation in Finite Element Analysis*; A. Thorup, Copenhagen, A. Hefez, U Fed do Esperito Santo, Vitoria, Brazil, *Symmetric Matrices with Alternating Blocks*; H.F. Trotter, Princeton, *Use of Symbolic Methods in Analysing an Integral Operator*; A. Valibouze, LITP, Paris, *Symbolic Computation with Symmetric Polynomials: An Extension to Macsyma*; P. Viana, MIT and Pontificia U. Catolica, Rio, *Classicality of Trigonal Curves of Genus Five*; E.R. Vrscay, Waterloo, *Iterated Function Systems and the Inverse Problem of Fractal Construction Using Moments*; D. Wang, Academia Sinica, Beijing, *Computer Algebraic Methods for Investigating Plane Differential Systems of Center and Focus Type.*

Minikurse:

T. Banchoff, Brown, *Interactive Computer Graphics and Differential Geometry*; M. Bronstein and B.M. Trager, IBM Research, J.H. Davenport, U of Bath, *Symbolic Integration is Algorithmic*; G. Butler, Sydney, *An Introduction to Computational Group Theory*; J.S. Devitt, Saskatchewan, M. Henle, Oberlin, *Computers in Undergraduate Mathematics: Making it Happen*; W.H. Kahan, Berkeley, *The Regrettable Failure of Automated Error Analysis*; Y. Nievergelt, E. Washington, *The HP-28S as a Bridge Between Theory and Applications*; H.-O. Peitgen, U Bremen and U of California, Santa Cruz, R.F. Voss, IBM Research, *The Science of Fractal Images*; L. Robbiano, Genua, *Gröbner Bases: A Foundation for Commutative Algebra.*

Tutorials:

A.V. Bocharov, Acad. of Science, Pereslavl, USSR, *SCOLAR*; G. Butler, Sydney, *CAYLEY*; K.O. Geddes, Waterloo, *MAPLE*; A.C. Hearn, RAND Corporation, *REDUCE*; R.D. Jenks, IBM Research, *SCRATCHPAD*; R. Petti, Symbolics, Inc, *MACSYMA*; M. Schönert, Aachen, *GAP*; M. Stillman, Cornell, D. Bayer, Columbia, *MACAULAY*; D. Stoutemeyer, Soft Warehouse, *DERIVE*; S. Wolfram, Wolfram Research, *MATHEMATICA*.

Proceedings sind im Springer-Verlag erschienen, E. Kaltofen, S.M. Watt, *Computers and Mathematics*, 1989.

Martin Schönert

4. Workshop on Symbolic Computation Methods in Differential Equations

   University of Minnesota, USA, 26.6.–30.6.1989.

   Dieser Workshop wurde vom IMA für Interessenten an Computer-Algebra Systemen veranstaltet, die vorher selbst nicht zu den Anwendern gehörten. Von den etwa 70 Teilnehmern dürfte ein signifikanter Anteil auch in Zukunft Computer-Algebra in ihrem jeweiligen Arbeitsgebiet anwenden. Der Schwerpunkt der Anwendungen für Differentialgleichungen lag bei den Systemen REDUCE und Scratchpad. Die etwa 20 Stunden Vorträge wurden im wesentlichen von A. C. Hearn (Rand Corpoaration), S. M. Watt (IBM Yorktown Heights) und F. Schwarz (GMD, Sankt Augustin) gehalten.

F. Schwarz

5. AAECC–7 Konferenz

   Toulouse, Frankreich, 26.6.–30.6.1989.

   Hauptthema war die Theorie der fehlerkorrigierenden Codes. Aus dem Bereich der Computer–Algebra gab es nur wenige Beiträge, die sich in zwei Gruppen gliedern lassen:

   Auf der einen Seite die „Italienische Schule“ der nicht kommutativen Algebra und der Gröbner Basen mit dem System AIPI um die Professoren Mora, Robiano und Traverso – der eingeladene Vortrag von Theo Mora verdient besondere Erwähnung –, auf der anderen Seite die Gruppe aus Paris, die sich mehr mit geometrischen Fragestellungen (Giusti) und Resolventen (Valibouze) befaßte.

   Die Proceedings werden in “Applied Discrete Mathematics” erscheinen. J. Calmet

6. ISSAC-89

   Portland, Oregon, 17.7.–19.7.1989.

   Die Computer-Algebra Tagung, die jährlich gemeinsam von ACM-SIGSAM und SAME veranstaltet wird, fand dieses Jahr in Portland/Oregon statt. Diese Veranstaltungen sind sicher eine gute Möglichkeit, schnell einen Überblick über aktuelle Arbeit zu erhalten. Die Kürze der Veranstaltung, nur drei Tage, und damit notwendig verbunden die Komprimierung der Beiträge auf 20 min wird dadurch ermöglicht, daß der fertige Tagungsband zu Beginn vorlag. Der genaue Titel ist: *Proceedings of the ACM-SIGSAM 1989 International Symposium on Symbolic and Algebraic Computation, ISSAC'89*, ACM Press, 1989, Gaston Gonnet, Editor.

   Eingeladene Vorträge (in chronologischer Reihenfolge):

   Michael Singer, *A Survey of Formal Solutions of Differential Equations*; Andrew M. Odlyzko, *Symbolic Algebra in Mathematics: Dreams and Reality*; John Cannon, *Designing a Software Environment for Studying Algebraic Structures*; Dominique Duval, *Computing with Algebraic Numbers–An Example of Dynamic Evaluation*; Richard Rand, *Computer Algebra–the Method of Averaging and Elliptic Functions*; Herbert Melenk, *Decomposition of Polynomial Equation Systems by Gröbner Type Methods.*

   Vorträge (in chronologischer Reihenfolge):

   M.A. Barkatou, *On the Reduction of Linear Systems of Difference Equations*; John Shackell, *A Differential-Equations Approach to Functional Equivalence*; Richard J. Fateman, *Series Solutions of Algebraic and Differential Equations: A Comparison of Linear and Quadratic Algebraic Convergence*; Fritz Schwarz, *A Factorization Algorithm for Linear Ordinary Differential Equations*; Erich Kaltofen, Thomas Valente, Noriko Yui, *An Improved Las Vegas Primality Test*; Victor Pan, *On Some Computations with Dense Structured Matrices*; François Ollivier, *Inversibility of Rational Mappings and Structural Identifiability in Automatics*; Franz Winkler, *Knuth-Bendix Procedure and Buchberger Algorithm–A Synthesis*; Richard J. Fateman, *Lookup Tables, Recurrences and Complexity*; Robert Grossman, Richard G. Larson, *Labeled Trees and the Efficient Computation of Derivations*; Chanderjit Bajaj, John Canny, Thomas Garrity, Joe Warren, *Factoring Rational Polynomials Over the Complexes*; Trevor J. Smedley, *A New Modular Algorithm for Computation of Algebraic Number Polynomial Gcds*; Stan Cabay, George Labahn, *A Fast, Reliable Algorithm for Calculating Padé–Hermite Forms*; Maria E. Alonso, Teo Mora, Mario Raimondo, *Computing With Algebraic Series*; John Abbott, *Recovery of Algebraic Numbers from their p-adic Approximations*; John F. Canny, Erich Kaltofen, Lakshman Yagati, *Solving Systems of Non-Linear Polynomial Equations Faster*; Russell Bradford, *Some Results on the Defect*; Laureano Gonzàlez, Henri Lombardi, Tomàs Recio, Marie-Françoise Roy, *Sturm–Habicht Sequence*; James M. Purtilo, *MINION: An Environment to Organize Mathematical Problem Solving*; John Fitch, *Can REDUCE be Run in Parallel?*; J.A. van Hulzen, B.J.A. Hulshof, B.L. Gates, M.C. van Heerwaarden, *A Code Optimization Package for REDUCE*; Michael C. Dewar, *IRENA–An Integrated Symbolic and Numerical Computation Environment*; Theodore H. Einwohner, Richard J. Fateman, *A MACSYMA Package for the Generation and Manipulation of Chebyshev Series*; Sanjiva Weerawarana,Paul S. Wang, *GENCRAY: A Portable Code Generator for Cray Fortran*; Carlo Traverso, Leombattista Donati, *Experimenting the Gröbner Basis Algorithm With the AlPI System*; Bruce R. Miller, *A Program Generator for Efficient Evaluation of Fourier Series*; Manuel Bronstein, *Simplification of Real Elementary Functions*; Keith O. Geddes, L. Yohanes Stefanus, *On the Risch–Norman Integration Method and Its Implementation in MAPLE*; J.S. Devitt, *Unleashing Computer Algebra on the Mathematics Curriculum*; Robert A. Ravenscroft, Jr. & Edmund A. Lamagna, *Symbolic Summation with Generating Functions*; Bruce W. Char, *Automatic Reasoning About Numerical Stability of Rational Expressions*; Guoting Chen, *Computing the Normal Forms of Matrices Depending on Parameters*; Marc Giusti, *On the Castelnuovo Regularity for Curves*; Bernhard Kutzler, *Careful*

Algebraic Translations of Geometry Theorems; G.E. Collins, J.R. Johnson, *Quantifier Elimination and the Sign Variation Method for Real Root Isolation*; Stanley Rabinowitz, *On the Computer Solution of Symmetric Homogeneous Triangle Inequalities*; Sidney C. Porter, *Dense Representation of Affine Coordinate Rings of Curves With one Point at Infinity*; B. David Saunders, Hong R. Lee, S. Kamal Abdali, *A Parallel Implementation of the Cylindrical Algebraic Decomposition Algorithm*; André Deprit, Etienne Deprit, *Massively Parallel Symbolic Computation*; Françoise Siebert-Koch, *Parallel Algorithm for Hermite Normal Form of an Integer Matrix*; Jürgen Avenhaus, Dieter Wißmann, *Using Rewriting Techniques to Solve the Generalized Word Problem in Polycyclic Groups*; N. Kuhn, K. Madlener, *A Method for Enumerating Cosets of a Group Presented by a Canonical System*; Gene Cooperman, Larry Finkelstein, Eugene Luks, *Reduction of Group Constructions to Point Stabilizers*; Mitsuhiro Okada, *Strong Normalizability for the Combined System of the Typed Lambda Calculus and an Arbitrary Convergent Term Rewrite System*; Peter O'Hearn, Zbigniew Stachniak, *Note on Theorem Proving Strategies for Resolution Counterparts of Non–Classical Logics*; Neil V. Murray, Erik Rosenthal, *Employing Path Dissolution To Shorten Tableaux Proofs*; Claude Kirchner, Hélène Kirchner, *Constrained Equational Reasoning*; Annick Valibouze, *Résolvantes et Fonctions Symétriques.* F. Schwarz

7. AMS Short Course Cryptology and Computational Number Theory

   Boulder, Colorado, 6.8.–10.8.1989.

   Über zwei wichtige Ereignisse auf dieser Tagung soll kurz berichtet werden:

   Über den "Short Course in Cryptology and Computational Number Theory" und über die "Special Session on Computational Number Theory".

   Der "Short Course" war gedacht als eine breite Einführung in das Gebiet. Vorträge wurden gehalten über "The Search for Provably Secure Systems" (Shafi Goldwasser), "Primality Testing" (Arjen Lenstra), "Factoring" (Carl Pomerance), "The Discrete Logarithm Problem" (Kevin S. McCurley), "The Rise and Fall of Knapsack Cryptosystems" (Andrew M. Odlyzko), "Pseudorandom Number Generators in Cryptography and Number Theory" (Jeffrey C. Lagarias).

   In der "Special Session on Computational Number Theory" gab es Vorträge über neue Entwicklungen, z.B. bei diskreten Logarithmen in Klassengruppen, bei der Faktorisierung von Polynomen über endlichen Körpern und insbesondere bei der Faktorisierung ganzer Zahlen mit Hilfe des Number Theory Sieve von Pollard. Es wird erwartet, daß letzterer Algorithmus die erwartete Laufzeit bei der Faktorisierung von n von $\exp(\sqrt{\log n \log\log n})$ auf $\exp(\sqrt[3]{\log n}\sqrt[2]{\log\log n})^c$ herabsetzt. J. Buchmann

8. Colloquium on Computational Number Theory

   Debrecen, Ungarn, 4.9.–8.9.1989.

   Organisationskomittee:

   A. Pethoe, Debrecen, (Chairman); K. Gyoery, Debrecen; M. Pohst, Düsseldorf; H.C. Williams, Winnipeg; H.G. Zimmer, Saarbrücken; I. Gaal, Debrecen, (Sekretär).

   Im Mittelpunkt der Konferenz standen die Präsentation und Diskussion von Algorithmen in der Zahlentheorie. Die behandelten Themen erstreckten sich auf die elementare, die analytische und die algebraische Zahlentheorie sowie auf die algebraische Geometrie. Dabei wurde die enge Verzahnung von Theorie und Computer-Anwendungen deutlich.

   Insbesondere hatten die Teilnehmer während der Tagung Gelegenheit, theoretische Fragestellungen oder Vermutungen auf den dort vorhandenen PC's (IBM- kompatiblen Rechnern und Siemens MX-2) numerisch zu untersuchen bzw. zu testen. In Ergänzung zu den Vorträgen fanden Präsentationen der zahlentheoretisch ausgerichteten Computer-Algebra Systeme KANT (Düsseldorf) und SIMATH (Saarbrücken) statt.

   Vorträge (in zeitlicher Reihenfolge):

   J. Buchmann, *Subexponential class group computation*; S. Düllmann, *Implementation of a subexponential class group algorithm*; K. Nakamula, *Class number computation by elliptic units and cyclotomic units*; D. Ford, *Totally complex quartic fields of small discriminants*; M. Pohst, *Remarks on index divisors*; J. von Schmettow, *KANT - a tool for computations in algebraic number fields*; N. Schulte, *Index form equations in cubic number fields*; B. Arenz, *Computing fundamental units from independent units*; U. Schröter, *Computation of fundamental units in algebraic number fields*; T. Gulyas, *Modification of the Fincke-Pohst method for solving* *norm equations*; F. Halter-Koch, *Regulators and class numbers of real quadratic fields*; E. Bayer, *Semi-dual normal bases*; H.G. Zimmer, *The rank of elliptic curves upon quadratic extension*; P. Serf, *Congruent and non- congruent numbers*; J. Brillhart, *Parity theorems for partition functions and modulo 2 reciprocation of infinite modularpart functions*; G. Turnwald, *On a conjecture of Graham*; H. Cohn, *Computation of singular moduli by multivalued modular equations*; C. Hollinger, *SIMATH - A computer algebra system I*; A. Stein,*SIMATH - A computer algebra system II*; I. Gaal, *On the computer resolution of some diophantine equations*; J.H. Evertse, *Effective results on the solutions of Thue equations*; R.J. Ströker, *On Thue equations associated with certain quartic and sextic number fields*; N. Tzanakis, *On the practical solution of the Thue-Mahler equation*; S.A. Stepanov, *On structure complexity of primitive normal basis of a finite field*; H.C. Williams,*An introduction to the CUFFQI algorithm of Shanks*; V. Fleckinger, *Power basis of ring of integers in ray class fields of imaginary quadratic fields*; R. Mollin, *Gauss' class number one problem for real quadratic fields*; M. Tasche, *Number theoretic transforms and a theorem of Sylvester-Kronecker*; G. Steidl, *On a symmetric radix representation of Gaussian integers*; Ju.V. Melnicuk, *Algorithms for representation of real numbers by fast convergent series*; B. Kovacs, *Number systems*; G. Niklasch, *A "fastest" Euclidean algorithm*; B. Tropak, *A numerical method for the determination of the cyclotomic polynomial coefficients*; B.J. Birch, *A letter from Elkies to Sloane*; J. Chahal, *On a theorem of Bass, Milnor and Serre*; I. Nemes, *On the solution of the diophantine equation* $\{Gn\} = P(x)$ *with sieve algorithm*; Nguyen Quoc Thang, *On the Hasse principle*; A. Pethoe, *Application of a polynomial transformation to the construction of a public key cryptosystem.* Prof. Dr. H.G. Zimmer

9. Herbstschule Computer-Algebra und ihre Anwendungen

   Bonn, 11.9.–15.9.1989.

   Dies war die erste Herbstschule in Computer-Algebra einer Serie, die gemeinsam von der DIA und der GMD veranstaltet wird. Der Schwerpunkt bei diesen Veranstaltungen liegt auf Anwendungen, wobei eine wichtige Zielgruppe Anwender von Mathematik in Industrie und Forschung sind. Dies wird schon durch den umfangreichen praktischen Teil unterstrichen. Die Veranstaltung wird in erweiterter Form im nächsten Jahr wiederholt. F. Schwarz

Neues über Systeme und Hardware

Neue Version von Derive

Vom Computer-Algebrasystem **Derive** gibt es die neue Version 1.4, die noch leistungsfähiger und damit attraktiver geworden ist. Zu den Neuigkeiten gehören u.a.:

- Neue Vektor- und Matrixfunktionen:
  - VECTOR(u,n,k,m,s) vereinfacht zu einem $\frac{(m-k+1)}{s}$ dimensionalen Vektor, der in der i-ten Zeile die Auswertung der Funktion u(n) an der Stelle $k + (i-1)s$ enthält.
  - ELEMENT(v,n) vereinfacht zum n-ten Element des Vektors v.
  - ELEMENT(m,n,k) vereinfacht zum k-ten Element der n-ten Zeile der Matrix m.
  - TRACE(m) berechnet die Spur der Matrix m.
  - ROW_REDUCE(A,B) augmentiert die Matrix A mit der Matrix B und führt anschließend das Gaus'sche Eliminationsverfahren durch. Dieser Befehl eignet sich besonders zur Lösung inhomogener linearer Gleichungssysteme.
  - CROSS(v,w) berechnet das Kreuzprodukt der beiden Vektoren v und w.
- Neue Vektoranalysis-Funktionen:
  - GRAD(u) vereinfacht zu dem Gradienten von u bzgl. der Koordinatenvariablen x, y und z.
  - DIF(v) vereinfacht zur Divergenz von v.
  - LAPLACIAN(u) ist der Laplace-Operator.
  - CURL(v) berechnet die Rotation des 2- oder 3-dimensionalen Vektors v.
  - POTENTIAL(v,w) berechnet das Potential des Vektorfeldes v.

◇ VECTOR_POTENTIAL(v,w) berechnet das Vektor–Potential des Vektorfeldes v.

Anbieter: Institut für Angewandte Informatik GmbH, Thienhausenerstr. 57, 5657 Haan 1, Tel.:(02129) 59985, Fax.:(02129) 59924.
Preis: 410.-DM + MWST.

ZIB Berlin erweitert REDUCE Angebot

Das Konrad-Zuse-Zentrum Berlin (ZIB) bietet schon seit mehreren Jahren REDUCE für die Cray-Rechnerserien an. Seit September 1989 sind nun auch Workstation-Versionen hinzugekommen, und zwar für

SUN-3 (Prozessor 68020),
SUN-4 (Prozessor SPARC) und
SUN-386i (Prozessor 80386).

Versionen für

DEC DI3100 (Prozessor MIPS) und
Silicon Graphics IRIS (Prozessor MIPS)

sind in Vorbereitung.
In allen Fällen basiert REDUCE auf Implementierungen auf Portable Standard LISP (PSL), die hoch optimierten Maschinencode für das jeweilige Rechnersystem produzieren. Die Implementierungen für SPARC, 80386 und MIPS sind Entwicklungen des ZIB, die 68020 Version wurde in wesentlichen Punkten verbessert. Besonders leistungsfähig ist die SPARC-Version, da die RISC-Architektur bei der LISP-Ausführung voll zur Geltung kommt: hier wird der Bereich größter Mainframes erreicht. Einige CPU-Zeiten für den REDUCE-Standardtest:

SUN 3/50 (16MHz) 32.5 sec
SUN 3/60 (20MHz) 20.2 sec
SUN 386i (20MHz) 15.5 sec
SUN 3/260 (25MHz) 16.2 sec
SUN 4/260 (16MHz) 5.4 sec
CRAY 2 1.9 sec
CRAY Y-MP 0.8 sec

Weitere Information durch: H. Melenk, Konrad-Zuse-Zentrum für Informationstechnik, Heilbronner Str. 10, 1000 Berlin 31, email: zb6260@db0zib21 (EARN bis Ende 1989), Melenk@sc.zib-berlin.dbp.de (X400).

Symbol-Mathematik-Paket MACSYMA jetzt auf PC verfügbar

Ab sofort kann die volle Performance, Funktionalität und Produktivität von **MACSYMA** auch auf 386er PC's unter DOS zum Einsatz kommen.

Hardware- und Software-Anforderungen für die PC-Version

	Minimal-Konfiguration	Empfohlene Konfiguration
Hauptspeicher	4 MB	6 MB
Swap Space	8 MB	10 MB
Hard Disk	30 MB	40 MB
Graphik-Adapter	EGA, CGA oder VGA	
Windows	MS-Windows ist teilweise enthalten	MS-Windows, MS-Paint

Anbieter: Symbolics GmbH, Mergenthalerallee 77–81, D-6236 Eschborn/Ts.
Preis: 7620.-DM + MWST. (für Universitäten gelten gesonderte Bedingungen)

Publikationen über Computer-Algebra

D.Stauffer, F.W.Hehl, V.Winkelmann, J.G.Zabolitzky, *Computer Simulation and Computer Algebra - Lectures for Beginners*, Springer-Verlag, 1988.

Das Kapitel *Reduce for Beginners* enthält eine elementare Einführung in die algebraische Version von REDUCE, die durch einige Aufgaben angereichert ist. F. Schwarz

A.G. Akritas, *Elements of Computer Algebra with Applications*, John Wiley & Sons,1989.

Die wichtigsten Kapitel aus dem Inhalt sind *Greatest Common Divisors of Polynomials over the Integers and Polynomial Remainder Sequences*, *Factorization of Polynomials over the Integers* und *Isolation and Approximation of the Real Roots of Polynomial Equations.* In diesen Gebieten hat der Autor selbst in den letzten Jahren eigene neue Ergebnisse veröffentlicht. Sie geben für das jeweilige Gebiet eine gute Einführung, die bis zum neuesten Stand der Forschung reicht. Insbesondere dürfte auch das Literaturverzeichnis von Interesse sein. Als Begleitmaterial für Vorlesungen ist es ebenfalls sicher gut geeignet, allein schon wegen seiner zahlreichen Übungsbeispiele. Die *Implementierung* von Algorithmen wird so gut wie nicht behandelt, der Autor empfiehlt das System MAPLE für diesen Zweck. F. Schwarz

Lehrveranstaltungen über Computer-Algebra im WS 1989/90

RWTH Aachen

Computational Group Theory, Neubüser, Vorlesung 4-stündig, Übung 2-stündig.
Einführungspraktikum MAPLE, Neubüser, Klein, Dietrich, Blockpraktikum, 6 Nachmittage.

Universität Bonn

Software-Entwicklung in der symbolischen Version von REDUCE, F. Schwarz, 2-stündig mit Übungen.

Universität Karlsruhe

Computer–Algebra Praktikum, Calmet, Ulmer, 2-stündig.
Seminar Algebraische Algorithmen–Entwicklung, Beth, Geiselmann, Maisel, 2-stündig.

Universität Linz

Softwaresysteme für Computer-Algebra, S. Stifter, 2-stündig
Logisches Programmieren - PROLOG, B. Kutzler, 2-stündig
Einführung in die Computer-Algebra, F. Winkler, 2-stündig
Algebraische Geometrie und Kommutative Algebra, F. Winkler, 2-stündig
Symbolische und numerische Methoden in der Dynamik, W. Hirschberg, 2-stündig
Literaturseminar aus Symbolic Computation I, B. Buchberger, 2-stündig
Programmierprojekt Symbolic Computation I, B. Buchberger, 4-stündig
Projektseminar - Algorithmische algebraische Geometrie, B. Buchberger, F. Winkler, 2-stündig
Projektseminar - Symbolic Computation in Education, n, B. Buchberger, B. Kutzler, 2-stündig

Universität Passau

Computer-Algebra, Thomas Becker, 4-stündig
Praktikum zur Computer-Algebra, H. Kredel, V. Weispfennig, 4-stündig

Kurze Mitteilungen

Ankündigung einer neuen Zeitschrift *Applicable Algebra in Engineering, Communication and Computer Science*, Beiträge bitte senden an: Prof. Dr. Jacques Calmet, Inst. of Algorithms and Cognitive Sciences, Haid–und–Neu–Str. 7, 7500 Karlsruhe 1, West Germany. $***$ Im Rahmen eines gemeinsamen Studienprojektes des Mathematischen Forschungsinstitutes Oberwolfach und der IBM Deutschland ist das Computer-Algebrasystem Scratchpad dort auf einer IBM RT 6150 Workstation verfügbar. $***$ In den Niederlanden wurde im März diesen Jahres innerhalb des Zentrums für Wissenschaft und Informatik (CWI) der Forschungsbereich *Computer Algebra Nederland* (CAN, Kontaktadresse: Arjeh Cohen, +31 20 592 8020, email: marc@cwi.nl) eingerichtet. Der Wissenschaftsbetrieb beginnt im Dezember. $***$