Computer-Algebra Rundbrief

Nummer 4 *Fachgruppe 2.2.1* *20. März 1989*

Liebe Kolleginnen und Kollegen,

es stellt sich immer wieder heraus, daß die Kommunikation zwischen verschiedenen Arbeitsgruppen im Bereich der Computer-Algebra verbesserungsbedürftig ist. Oft ist es sogar schwierig, einen Überblick darüber zu gewinnen, wer an welchem Ort in diesem Bereich arbeitet. Wir planen deshalb, in den nächsten Ausgaben dieses Rundbriefes mit kurzen Berichten über Arbeitsgruppen im Bereich der Computer-Algebra zu beginnen. Damit diese Berichte möglichst vollständig werden, bitten wir Sie um eine kurze Beschreibung Ihrer Arbeit in der folgenden Form:

1. *Institution, einige Kontaktpersonen*
2. *Arbeitsgebiet, bisher bearbeitete Probleme*
3. *Pläne für die nächsten ein bis zwei Jahre*

Jeder dieser Punkte sollte nicht mehr als etwa fünf Zeilen umfassen. Diese Beiträge werden dann in den oben erwähnten Bericht übernommen. Auch für Hinweise auf die Arbeit anderer Ihnen bekannter Institutionen wären wir dankbar.

Wie üblich auch hier noch einmal die Bitte um Angabe der Lehrveranstaltungen in Computer-Algebra im WS 89/90 für den nächsten Rundbrief.

Hier noch ein besonderer Hinweis auf zwei Veranstaltungen im Bereich der Computer-Algebra. Auf der GI Jahrestagung in München wird sich unsere Fachgruppe treffen. Die unter Nr. 10 angekündigte Herbstschule über Computer-Algebra wird von unserer Fachgruppe unterstützt. Über beide Veranstaltungen wird Ihnen im Laufe des Sommers noch genauere Information zugehen.

F. Schwarz *J. Neubüser*

Hinweise auf Konferenzen

1. **Computer Aided Proofs in Analysis**

   Cincinnati, USA, 22.3. - 25.3.1989.

   Kontaktadresse: Ken Meyer, Department of Mathematical Sciences, University of Cincinnati, Cincinnati, Ohio 45221-0008.

2. **COCOA II, Computers and Commutative Algebra**

   Genova, Italien, 29.5.-3.6.1989.

   Kontaktadresse: Lorenzo Robbiano, Dipartimento di Mathematica, Università, Via L.B. Alberti 4, 16132 Genova, Italy, Tel. (39) 14-3538732.

3. **Computers & Mathematics**

   Cambridge, Mass., 12.6.-16.6.1989.

   Kontaktadresse: Computers & Mathematics 1989, 62 Eastview, Pleasantville, New York, 10570, U.S.A., Tel. (914) 769-2725.

4. **AAECC 7**

   Toulouse, Frankreich, 26.6.-30.6.1989.

   Kontaktadresse: Professor A. Poli, AAECC/LSI, University P. Sabatier, 118 route de Narbonne, 31062 Toulouse Cédex, France.

[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 St.Augustin. ISSN 0933-5994

5. **IMA Workshop on Computer Algebra and Differential Equations**

   Minneapolis, Minnesota, USA, 26.6.-30.6.1989.

   Kontaktadresse: Prof. W. Miller, Institute for Mathematics and its Applications, University of Monnesota, 524 Vincent Hall, Minneapolis, Minnesota 55455, U.S.A.

6. **ISSAC-89**

   Portland, Oregon, 17.7.-19.7.1989.

   Kontaktadresse: Dennis Arnon, Xerox Palo Alto Research Center, 3333 Coyote Hill Road, Palo Alto, CA 94304, U.S.A., Tel.(415) 494-4425.

7. **First Brazilian School on Computer Algebra**

   Rio de Janeiro, 24.7. - 11.8.1989.

   Kontaktadresse: Dr. Marcelo J.Reboucas, Departemento de Relatividade e Particulas, Centro Brasileiro de Pesquisas Fisicas, Av. Xavier Sgaud, 150, Urca 22.290 Rio de Janeiro (RJ) Brasilien.

8. **AMS Short Course on Kryptology and Computational Number Theory**

   Boulder, Colorado, 6.8. - 7.8.1989.

   Kontaktadresse: M. Foulkes, AMS, P.O.Box 6248, Providence R.I. 02940.

9. **Colloquium on Computational Number Theory**

   Debrecen, Ungarn, 4.9.-8.9.1989.

   Kontaktadresse: Istvan Gaal, Kossuth Lajos University, Mathematical Institute, 4010 Debrecen Pf.12., Hungary.

10. **Herbstschule Computer-Algebra und ihre Anwendungen**

    Bonn, 11.9.-15.9.89

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

11. **Algorithmen für algebraische Zahlen**

    Tübingen, Termin steht noch nicht fest.

    Kontaktadresse: R. Loos, Wilhelm-Schickard-Institut, Universität Tübingen, Auf der Morgenstelle 10, 7400 Tübingen

12. **Meeting on Effective Methods in Algebraic Geometry**

    Pontignano (bei Florenz), Italien 17.4.- 21.4.1990

    Kontaktadresse: C. Traverso, Dipartimento di Matematica, Via Buonarroti 2, I-56100 Pisa. Titel und Abstrakt müssen bis 31.10.89 eingereicht sein.

Berichte von Konferenzen

1. International Course on Computational Real Geometry

   Catania, 12.12.–17.12.1988

   Themen: Einführung in die Reelle Geometrie. Komplexität von Problemen. Anwendung in der Roboter Kinematik. (Probabilistische) Algorithmen in der Geometrie.

   Vorträge (Reihenfolge des jeweils ersten Vortrages):

   J.H. Davenport, Bath, *From Algebraic Numbers to Algebraic Geometrie*; M.F. Coste-Roy, Rennes, *Thom's Lemma and Applications*; J. Heintz, Buenos Aires, *Cylindrical Algebraic Decomposition and Quantifier Elimination*; T. Recio, Santander, *Bounds in Real Algebraic Geometry*; M. Sharir, New York,*Applications of Real Algebraic Geometry to Motion Planning and Computational Geometry*; L. Guibas, DEC, *Arrangements of Algebraic Varieties in High Dimensions.* F. Ulmer

2. Konferenz über Applicable Algebra

   Mathematisches Forschungsinstitut Oberwolfach, 1.1.–6.1.1989

   Die Konferenz konzentrierte sich auf Anwendungen von algebraischen Methoden zur Lösung von Problemen in technischen Anwendungsbereichen wie Nachrichtentechnik und Akustik, Robotik, Vision und Künstliche Intelligenz, sowie VLSI und Schaltungsentwurf, sowie auf Methoden aus den Gebieten Algebraische Geometrie, Algebraische Logik, Arithmetik in reellen komplexen und endlichen Körpern, Darstellungs- und Invariantentheorie, sowie Diskrete Mathematik.

   Zu diesem Treffen wurden neben Algebraikern, die sich mit den genannten Anwendungen beschäftigen und Forschern und Entwicklern aus dem meist ingenieurmäßig orientierten Anwendungsbereich gerade auch Computer-Algebraiker eingeladen, die durch ihre Arbeit eine Verbindung zwischen vielen der oben genannten Gebiete herstellen.

   Vorträge (in chronologischer Reihenfolge):

   M.R. Schroeder, *The Unreasonable Effectiveness of Number Theory in Physics, Music and Communication*; Z.D. Dai, *Functions Defined by de Bruijn Sequences*; L. Budach, *VLSI-Design and Fractals*; U. Rembold, *Autonomous mobile robots*; C. M. Hoffmann, *Trade-Off between symbolic algebraic and floating point computation in solid modeling*; V. Weispfenning, *Comprehensive Gröbner Bases*; J. H. Davenport, *From Gröbner bases to solving equations*; H. J. Stetter, *A computational algorithm for finding all zeros of a multivariate polynomial system*; B. Sturmfels, *Computational versions of the Quillen-Suslin-Theorem*; Ken-ichi Kanatani, *Group theoretical methods in image understanding*; J. Mundy, *An Algebraic Basis for Modeling in Computer Vision*; S.S. Abhyankar, *Invariant Theory*; M. Clausen, *FFT*; D. Jungnickel, *The trace of primitive elements of* $GF(q^m)$; W. Geiselmann, *Selfdual Normal Bases over* $GF(q)$; D. Gollmann, *Multiplication in* $GF(2^n)$; A. Guthmann, *Constructive Arithmetic in* $GF(q)T$; H.H. Nagel, *Algebraic Approaches in Image Sequence Analysis*; B.A. Kutzler, *Algebraic methods for automated geometry theorem proving*; G. Schiffels, *Well Quasi Orders and Gröbner Ideal Bases*; H. Niederreiter, *The linear complexity profile of binary sequences*; D. E. Lazič , *Sphere Packing and Signal Constellations*; B. Haible, *Linear differential equations with polynomial coefficients.*; K. Murota, *LM-matrix and its combinatorial canonical form for systems analysis*; J. Grabmeier, *On sums of characters: zero-testing and interpolation*; A. Shokrollahi, *Fermat Codes*; W. Büttner, *Modelling Complex Applications in Prolog*; J. Cannon, *Knowledge-Based Systems as a Tool for Applied Algebra*; A. Kerber, *The combinatorial use of finite group actions.* W. Geiselmann

3. Computational Group Theory

   Special Session beim Jahrestreffen der AMS, Phoenix, Arizona, 11.1.-14.1.89.

   Auf der Tagung wurden fast alle größeren CA-Systeme demonstriert: DERIVE, MACSYMA, MAPLE, MATHEMATICA, SCRATCHPAD II, SMP; zu der Special Session des weiteren die gruppentheoretischen Systeme: CAYLEY, CAS, GAP, SOGOS, SPAS sowie als stand-alones die Implementationen von TC und NQ aus Canberra.

   Vorträge:

   L. Babai, Budapest, E.M. Luks, U. of Oregon, A. Seress, Ohio State, *Managing permutation groups in* $0(n^4 log^c n) time$; G. Cooperman, L. Finkelstein, Northeastern U., *Short presentations and a strong generating test for permutation groups*; R.H. Gilman, Stevens Inst. of Techn., *Verifying that a group is virtually free*; J. Grover, Lear Astronics, Woodland Hills, Cal., *Modified Todd Coxeter algorithm*; G. Havas, U. Brisbane, *Supercomputer group theory*; J.E. Humphreys, U. of Massachusetts, *Computing decomposition numbers for finite groups of Lie type in the defining characteristic*; S. Magliveras, U. of Nebraska, *Cryptographic applications of computational group theory*; M.F. Newman, Canberra, *A method for proving groups infinite*; E.A. O'Brien, Marquette U., *New methods for generating descriptions of p-groups*; R. Riley, Binghampton, *The system PNCRE for computation with explicit subgroups of* $SL_2(C)$; E.F. Robertson, St. Andrews, Schottland, *On the efficiency of finite simple groups and their direct squares*; M. Schönert, Aachen, *GAP, groups and programming*; C. Sims, Rutgers, *Implementing the Knuth-Bendix procedure and the Baumslag-Cannonito-Miller polycyclic quotient algorithm*; M.C. Slattery, Marquette U., *Proofs of algorithms as implementation tools*; C.R.B. Wright, U. of Oregon, *Algorithms for computing complements to normal subgroups*; H. Zassenhaus, Columbus, Ohio, *Current techniques for computing the group of an equation.* M. Schönert

4. Differential Equations and Computer Algebra

   Université Libre de Bruxelles, 19.1.1989

   Vorträge:

   J. Henrard, *A Survey of Poisson Series Processors*; A. Heck, *Criteria and Formulae for the Inverse of a Polynomial Map*; G. Gielen, *Symbolic Simulation of Analog Integrated Circuits in S- and Z- Domain*; D. Dehin, *Conformal Symmetries and Systems of Partial Differential Equations*; J. Della Dora, *Asymptotic Solutions of Differential and Difference Equations: a Symbolic Computation Approach*; V. Dietrich, *ELISE, an algorithm realized with Maple*; N. Van Den Bergh, *Applications of Maple to Problems in General Relativity*; L. Brenig, J.L. Colot, E. Mund, J. Sengier, *Demonstrations of Maple and SMP on U.L.B. Sun network.*
   F. Schwarz

5. Computer Algebra Nederland

   Centrum voor Wiskunde en Informatica, Amsterdam, 10.3.1989

   Vorträge:

   R.K. Ellis, *Computer algebra in particle physics: The example of heavy flavour production*; M. McCallum, *Ordinary differential equations and computer algebra*; R. Sommerling, *Computing invariants of a differential operator using Dieudonné determinants*; A. Heck, *Criteria and formulae for the inverse of a polynomial map*; J.H.J. Molenkamp, *Automatic error cumulation control*; J.A.M. Vermaseren, *A new formula manipulation program for big expressions.*
   F. Schwarz

Neues über Systeme und Hardware

Derive und Galois — Zwei neue Systeme für PC's

Bernhard Kutzler
Research Institute for Symbolic Computation (RISC-LINZ)
Johannes Kepler Universität, A-4040 Linz

Derive ist das neueste Computer-Algebra System von Soft Warehouse Inc. und die Weiterentwicklung von muMATH. Die wesentlichen Systemmerkmale sind:

- Exakte rationale Arithmetik sowie numerische Approximation auf beliebig viele Stellen.
- Lösen von Gleichungen, Rechnen mit komplexen Zahlen, Trigonometrie, Infinitesimalrechnung, Vektor- und Matrizenrechnung.
- Plotten von 2D und 3D Funktionsgraphen.
- Unterstützung von CGA, EGA, VGA sowie Herkules-Graphik.
- 2D-Ausgabe von Formeln.
- Anwenderfreundliches Benutzerinterface mit On-Line Help.

Derive läuft auf allen IBM PC und dazu kompatiblen Computern unter MS-DOS (Version 2.1 oder höher) mit mindestens 512K Hauptspeicher und einem $5\frac{1}{4}$ Zoll (360K) oder einem $3\frac{1}{2}$ Zoll (760K) Diskettenlaufwerk.

Derive kostet ÖS 2800 + MWSt. (bzw. DM 400) und wird in Europa durch die Firma CIFEG GmbH (Kalkgruberweg 26, A-4040 Linz, Österreich) vertrieben.

Galois ist ein von R. Lidl, R.W. Matthews und R. Wells in Turbo Pascal v3.0 geschriebenes Programmpaket für den Einsatz in Forschung und Lehre. Das System wurde für jene Anwendungen entwickelt, die sich mit modularer Arithmetik sowie Matrizen und Polynomen über endlichen Körpern oder ganzen Zahlen modulo n beschäftigen.

Eine Auswahl der implementierten Routinen ist:

Chinese Remainder Algorithm	Find Primitive Element	Order of Element
Cyclotomic Polynomials	Find Roots	Primality Test
Calculate Determinant	Greatest Common Divisor	Primitivity Test
Calculate Rank	Interpolation	Rank
Evaluate Polynomial	Least Common Multiple	Reduced Echelon Form
Factorization	Minimal Polynomial	Solve Congruences
Find Inverse	Norm	Solve Linear Systems
Find "Next" Prime	Nullspace	Trace

Galois läuft auf allen IBM PC und dazu kompatiblen Computern unter MS-DOS (Version 2.0 oder höher) mit mindestens 640K Hauptspeicher und einem $5\frac{1}{4}$ Zoll (360K) oder einem $3\frac{1}{2}$ Zoll (760K) Diskettenlaufwerk.

Die single use license von Galois kostet ÖS 1650 + MWSt. (bzw. DM 240), die site license kostet ÖS 6200 + MWSt. (bzw. DM 890). Der Vertrieb in Europa erfolgt durch die Firma CIFEG GmbH (Kalkgruberweg 26, A-4040 Linz, Österreich).

Mailbox und elektronisches Bulletin Board für REDUCE

Eberhard Schrüfer
GMD, Institut F1-P
Postfach 1240
5205 St. Augustin
Tel.: 02241 14 2801, EARN: GF1013 at DBNGMD21

Seit kurzem existiert ein elektronisches Bulletin Board für REDUCE Benutzer. Es ist für die Diskussion von Sachfragen gedacht, die für die gesamte REDUCE Gemeinschaft von Interesse sind. In die Verteilerliste für das Bulletin Board kann man sich eintragen lassen, in dem man eine Message an

reduce-forum-request@rand.org (EARN, BITNET)

schickt. Das 'reduce-forum' wird momentan unmoderiert betrieben, d.h. jeder Diskussionsbeitrag wird unmittelbar an *alle* Teilnehmer weitergeleitet. Das Bulletin Board sollte *nicht* für Bug-Reports verwendet werden. Für solche und für Fragen, die nicht von allgemeinem Interesse sind, steht

reduce@rand.org (EARN, BITNET)

zur Verfügung.

Darüberhinaus gibt es jetzt eine *elektronische Library.* Von ihr können Informationen, gewisse Dokumentationen und auch Software abgerufen werden. Der momentane Index (wird weiter ausgebaut) enthält:

```
arith     -  5 Dec 88 - Code for the support of arithmetic in REDUCE
cl        -  8 Feb 89 - Files for Common Lisp front end to REDUCE
examples  - 18 Jan 89 - Various REDUCE examples
groebner  - 17 Jan 89 - Code for Groebner base calculations
info      -  2 Feb 89 - Various information files (e.g., books about REDUCE)
interface - 27 Jan 89 - Code for the GI/S graphical user interface
laplace   - 17 Jan 89 - Direct and Inverse Laplace Transformations
misc      - 27 Jan 89 - Various pieces of code (mostly not documented)
patches   -  8 Feb 89 - Patches correcting various bugs in REDUCE 3.3
series    -  7 Feb 88 - Truncated power series and other series packages
tex       - 28 Jan 89 - Code for producing TeX output from REDUCE
util      - 25 Jan 89 - Various utility packages
vector    - 20 Dec 88 - Vector algebra and calculus packages
```

Nach Eintrag in die Verteilerliste können weitere Informationen zur Library durch Senden einer einzeiligen Message, die aus dem Wort help besteht (entweder im Subject-Feld oder ohne Subject-Feld als Mail-Körper), an reduce-netlibrand.org (EARN, BITNET)

erhalten werden. Bei Schwierigkeiten bitte an den Autor wenden.

SIMATH - ein Computer Algebra System

Prof. Dr. H.G. Zimmer
Fachbereich 9.1 Mathematik
Universität des Saarlandes
6600 Saarbrücken

SIMATH wird im Rahmen einer Kooperation zwischen der Universität des Saarlandes und der Siemens AG am Lehrstuhl Prof. Dr. Zimmer auf dem **Siemens PC MX-2** entwickelt. Bis Mitte des Jahres soll auch eine Auslieferversion für **APOLLO** Workstations (DN3010 und DN4500) auf dem Betriebssystem UNIX fertiggestellt sein.

Aufbau: SIMATH ist streng nach den Konventionen der **Programmiersprache 'C'** geschrieben; die SIMATH-Funktionen lassen sich jedoch vermöge mitgelieferter Konvertierungsroutinen auch in **FORTRAN**-Programme einbinden.

Der **modulare** Aufbau ermöglicht dem Benutzer den **Einbau eigener Programme** an allen Stellen des Systems. SIMATH wird von einer **eigenen Benutzeroberfläche** überlagert, die die System- und Bibliotheksverwaltung auf ein Minimum an Aufwand reduziert. Sämtliche SIMATH-Datentypen werden durch ein **Listensystem** realisiert, das ausgestattet ist mit einem **automatischen garbage collector** und einer **dynamischen Speicherplatzverwaltung**.

SIMATH stellt zur **schnellen, interaktiven Problemlösung** einen **Calculator** zur Verfügung, der die SIMATH-Funktionen im **ONLINE-Betrieb** zugänglich macht.

Alle SIMATH-Programme sowie der SIMATH-**Calculator** sind mit ausführlichen **Dokumentationen und Help-Dateien** ausgestattet, auf die ebenso wie auf ein **Schlüsselwortverzeichnis** interaktiv zuzugreifen ist.

Inhalt: Schwerpunkte von SIMATH liegen im Bereich der **algebraischen Zahlentheorie**. Hier einige Themenbereiche, die z.T. bereits ausführlich behandelt wurden; z.T. sind Algorithmen und Prozeduren zu diesen Themen noch in der Entwicklungsphase.

- Allgemeine Arithmetik, d.h Grundrechenarten, in $\mathcal{Z}, \mathcal{Q}, \mathcal{Z}/\mathrm{m}\mathcal{Z}, \mathcal{F}_q, \mathcal{F}_q(x)$, sowie in algebraischen Zahlkörpern. Sofern es in oben genannten Ringen sinnvoll ist: Chinesischer Restsatz, Primzahltest, Faktorisierung.

- Polynomarithmetik, d.h. Grundrechenarten, Einsetzen, Transformationen, Resultante, Diskriminante, Faktorisierungsroutinen in Polynomringen mit Koeffizienten aus oben beschriebenen Ringen in beliebig vielen Veränderlichen.

- Das Matrizenpaket umfaßt, neben den Grundrechenarten für Matrizen über **allen** oben beschriebenen Ringen, die Berechnung der Hermite-Normal-Form, sofern dies sinnvoll ist, und das Lösen linearer Gleichungssysteme über $\mathcal{Z}$ und $\mathcal{Q}$.

- Arithmetik in algebraischen Zahlkörpern und Funktionenkörpern, Kettenbruchalgorithmus, Berechnung von Ganzheitsbasen, Primdivisorzerlegung, Fundamentaleinheiten, Klassenzahl und Klassengruppen.

- Elliptische Kurven: Birationale Transformationen, Punktarithmetik, global minimales Modell, Höhenberechnung (Néron-Tate-Höhe) und Kongruenzzahlen.

Ansprechpartner: Prof. Dr. H.G. Zimmer, Universität des Saarlandes, D-6600 Saarbrücken
Bau 27.1, Raum 317, Tel.: 0681/302-2206

Publikationen über Computer-Algebra

Stephen Wolfram, *Mathematica* ™ *A System for Doing Mathematics by Computer*, Addison-Wesley Publishing Company, 1988.

Dies ist das Manual zu dem mit großer Publicity angekündigten neuen System von S. Wolfram, das als Nachfolger von SMP anzusehen ist. Von allen Computer-Algebra Systemen stellt Mathematica damit sicher die ausführlichste Beschreibung zur Verfügung. Die wichtigsten Überschriften aus dem Inhaltsverzeichnis sind (in freier Übersetzung): *Eine praktische Einführung in Mathematica. Die Struktur von Mathematica. Fortgeschrittene Mathematik in Mathematica.* Mathematica als eine Computer-Sprache. Der Text ist leicht verständlich geschrieben und mit zahlreichen Beispielen versehen. Für nicht zu umfangreiche Anwendungen, bei denen die vom System zur Verfügung gestellten Funktionen den größten Teil des Codes ausmachen, stellt Mathematica sicher eine echte Alternative dar. Ganz besonderer Wert wurde auf die Verfügbarkeit von Graphik gelegt. Außer einem langen Kapitel darüber, das fast zehn Prozent des gesamten Textes umfaßt, wird das auch durch die äußere Aufmachung unterstrichen - eine dreidimensionale Darstellung in allen Farben des Regenbogens. F. Schwarz.

H. W. Lenstra, R. Tijdeman, *Computational Methods in Number Theory I,II.* Mathematisch Centrum, Amsterdam 1982.

L. Lovász, *An Algorithmic Theory of Numbers, Graphs and Convexity*, Society for Industrial and Applied Mathematics, Philadelphia 1986.

B. F. Caviness, Robert P. Gilbert, Roman Shtokhamer, *An Introduction to Applied Symbolic Computation using Macsyma*, University of Delaware, 1989.

Computer in der Mathematik in den AMS Notices

Die American Mathematical Society (AMS) publiziert seit mehreren Jahren in ihren NOTICES Artikel, die sich mit der Rolle von Computern in der Mathematik auseinandersetzen. Wir geben hier eine Übersicht:

1. „Future Directions in Computational Mathematics, Algorithms, and Scientific Software", *vol. 32, No. 6, Nov. 1985, pp 743 - 757*, ist die Wiedergabe der zentralen Teile eines Berichts, den eine Arbeitsgruppe unter Leitung von W. C. Rheinboldt für die AMS erstellt hat. Der volle Bericht kann von SIAM, 1400 Architects Building, 117 South 17th Street, Philadelphia, Pennsylvania 19103, angefordert werden.

2. In einer von J. P. Buhler herausgegebenen Reihe „Mathematical Software" erschienen folgende zwei Aufsätze:
   N. J. A. Sloane: My Friend MACSYMA.
   vol. 33, No. 1, Jan. 86, pp. 40-43
   A. Ash: A Matrix Laboratory. (Bericht über PC-Matlab)
   vol. 33, No. 3, June 86, pp. 482 - 485

3. Seit Mai 1988 gibt J. Barwise eine bis jetzt regelmäßig erscheinende Spalte „Computers and Mathematics" heraus, in deren sehr lesenswerten „editorials" er sich u. a. kritisch mit Problemen wie der Patentfähigkeit von Algorithmen oder der ungewöhnlich agressiven Markteinführung von MATHEMATICA auseinandersetzt, die aber auch evaluierende Berichte über mathematische Software bringt. Folgende Beiträge sind bisher erschienen:

   - J. Barwise: Editorial.
     vol. 35, No. 5, May/June 88, pp. 693-694
   - J. Barwise: Editorial Notes.
     E. N. Zalta: Are Algorithms Patentable?
     Y. Nievergelt: The HP-28S Brings Computations and Theory Back Together in the Classroom.
     N. Shankar: Observations on the Use of Computers in Proof Checking.
     vol. 35, No. 6, July/August 88, pp. 795-805

- J. Barwise: Editorial Notes.
  B. Simon, R.M. Wilson: Supercalculators on the PC. (Ein Vergleich von: EUREKA, TKSOLVER PLUS, MATHCAD 2.0, POINT FIVE, PC-MATLAB, GAUSS)
  vol. 35, No. 7, Sept. 88, pp. 976-1001
- J. Barwise: Editorial Notes: How to Computerize a Math Department?
  D.F. Holt: The CAYLEY Group Theory System.
  R. J. Palais: Academic Computing and Networking.
  vol. 35, No. 8, Oct. 88, pp. 1134-1148
- J. Barwise: Editorial Notes: Mathematica.
  E. A. Herman: Mathematica, A Review.
  Other comments on Mathematica.
  vol. 35, No. 9, Nov. 88, pp. 1333-1349
- J. Barwise: Editorial: Software and Intellectual Property Rights.
  D. Griffith: Cyclic Random Competition.
  K. Devlin: Mathematics without Theorems. Mathematical Freeware and Shareware: ZG.
  vol. 35, No. 10, Dec. 88, pp. 1469 - 1482
- J. Barwise: Editorial Notes: Why are There so Few Computers in the Classroom? Math. Bulletin Board System.
  J. Barwise, J. Etchemendy: Creating Courseware.
  vol. 36, No. 1, Jan. 89, pp 32 - 40
- J. Barwise: Editorial Notes
  G.-C. Rota: The Barrier of Meaning
  L. A. Lambe: Reviews: Scratchpad II as a Tool for Mathematical Research.
  A. Matchelt: Review: Graphical Aids for Stochastic Processes.
  vol. 36, No. 2, Feb. 89, pp. 141-148.

J. Neubüser

Lehrveranstaltungen über Computer-Algebra im SS 1989

RWTH Aachen
Einführungspraktikum in MAPLE, Neubüser, Klein, Dietrich, Blockpraktikum, 6 Nachmittage.
Universität Essen
Einführung in die Computer-Algebra I, G. Schneider, 2std.
Universität Heidelberg
Algorithmen der Zahlentheorie, B. H. Matzat, 4 Std. mit 2 Std. Praktikum.
Universität Kaiserslautern
Fibonacci's Liber Abbaci - ein frühes Buch zur Computer-Algebra, Lüneburg, 1 Std.
Universität Karlsruhe
Computer Algebra II, Calmet, 3 Std.
Verfahren der schnellen Fourier-Transformation, Clausen, 3 Std.
Theoretische Aspekte der Realisierung von Computer-Algebra-Systemen, Calmet, Tjandra, Ulmer, 2 Std. Seminar.
Abstrakte Datentypen und Spezifikation, Clausen, Gollmann, 2 Std. Seminar.
Computer Algebra, Tjandra, Ulmer, 2 Std. Proseminar.
Universität Linz
Programmiersprachen für Symbolic Computation II (Funktionales Programmieren - LISP), Winkler, 2 Std.
Computer-Algebra II (Symbol-Algorithmen in der Analysis), Rothstein, 2 Std.
Überblick über Symbolic Computation, Buchberger, 2 Std.
Ausgewählte Kapitel aus der algorithmischen algebraischen Geometrie, Sturmfels, 2 Std.
Programmierprojekt Symbolic Computation II, Buchberger, 4 Std.

Vortragsreihe Symbolic Computation, Buchberger, Paule, 1 Std.
Einführung in das wissenschaftliche Arbeiten in Symbolic Computation I, Buchberger, 2 Std.
Projektseminar: Algorithmische algebraische Geometrie, Buchberger, Winkler, 2 Std.

Universität Passau

Seminar über Computer Algebra (gemeinsam mit der Arbeitsgruppe Prof. B. Buchberger, Universität Linz), Weispfennig, Becker, Kredel, 2 Std. n.V.

Universität Saarbrücken

Primzahltests, Buchmann, 2 Std.
Berechnung von Klassengruppen algebraischer Zahlkörper, Buchmann, 2 Std.
Proseminar: Einführung in die Kryptographie, Buchmann, 2 Std.
Fortgeschrittenenpraktikum: Faktorisierung großer Zahlen / lineare Algebra über Ringen / Gitterbasis - Reduktion / Normalformen ganzzahliger Matrizen / Electronic poker, Buchmann, 2 Std.

Universität Tübingen

Computer Algebra, Loos, 4 Std. (mit Rechnerübungen, 2 Std.)

Offene Stellen

An der **Fakultät für Mathematik** ist die Stelle eines/r

Hochschuldozenten/in (C 2)
für Mathematik

die dem neugegründeten Interdisziplinären Zentrum für Wissenschaftliches Rechnen zugeordnet ist, mit der Arbeitsrichtung

Computerunterstützte Gruppen- und Zahlentheorie
(computational group / number theory)

zu besetzen. Es besteht - abgesehen von den Fällen des §61 Abs. 7 UG - keine Möglichkeit, das Beamtenverhältnis als Hochschuldozent auf Zeit über 6 Jahre hinaus zu verlängern. Schwerbehinderte werden bei gleicher Eignung vorrangig eingestellt.
Bewerbungen mit den üblichen Unterlagen (Lebenslauf, Schriftenverzeichnis, Verzeichnis der Lehrveranstaltungen) werden bis zum **31.März 1989** erbeten an den **Dekan der Fakultät für Mathematik, Universität Heidelberg, Im Neuenheimer Feld 288, 6900 Heidelberg.**

Doktoratsstipendien am RISC-LINZ

Research Institute for Symbolic Computation
Johannes Kepler Universität Linz
A-4040 Linz, Austria
Tel. Österreich (732) 2468 / 9219
electronic mail: K313370@AEARN.BITNET

Voraussichtlich ab Wintersemester 1989/1990 werden am RISC-LINZ einige Stipendien für ausländische Doktoratsstudenten zur Verfügung stehen. Das Stipendium selbst ist kostenlos. Das Stipendium beträgt 100.000.- österreichische Schillinge im Jahr. Dieser Betrag sollte die Lebenshaltungskosten abdecken.
Ausgezeichnete Studenten mit Diplom in Mathematik oder Informatik und Interesse an Forschung in Symbolic Computation (Computer Algebra, Computational Logic, Computational Geometry, Automatic Programming etc.) können sich ab sofort um diese Stipendien bewerben. (Lebenslauf, Referenzen, möglichst ausführliche Informationen). Bewerbungen bitte an den Leiter des Instituts, Prof. Dr. Bruno Buchberger, senden (Adresse siehe oben).
RISC-LINZ ist ein selbständiges Institut der Universität Linz mit derzeit 12 Mitarbeitern mit Doktorat und 11 Doktoratsstudenten sowie etlichen Diplomstudenten, die sich alle im Bereich Symbolic Computation betätigen. Das Institut wird in Kürze (Feber 1989) in ein reizvoll renoviertes sehr altes Schloß in sehr schöner Landschaft nahe Linz übersiedeln. Die Computer-Ausstattung ist zufriedenstellend (10 Apollo Workstations, 1 Apollo 10000, 1 Micro-VAX, 4 VAXstations, ein Transputersystem in Anschaffung) und wird noch erweitert. Das Institut arbeitet eng mit den Instituten für Mathematik und Informatik zusammen und wird Impulsgeber und Ausgangspunkt einer neuen Studienrichtung “Mechatronics” werden. Auch gibt es eine Reihe von Kooperationen mit der Industrie.
Hauptziel der Ausbildung am RISC-LINZ ist die Verbindung von Mathematik und Informatik.

Ausschreibung der Stelle
eines ordentlichen Universitätsprofessors für
Symbolisches Rechnen an der Johannes-Kepler-Universität in Linz (Österreich)
(Research Institute for Symbolic Computation)

An der Technisch-Naturwissenschaftlichen Fakultät der Johannes-Kepler-Universität Linz wird eine neue Stelle für einen ordentlichen Universitätsprofessor für Symbolisches Rechnen (Symbolic Computation) eingerichtet. Bewerber/innen sollen ein ausgezeichnetes Profil als Forscher in wenigstens einem der Teilgebiete von Symbolic Computation haben (Computer-Algebra, Computer-Analysis, Computer-Geometrie, Computer-Logic, Formaler Software-Design etc.). Sie sollten außerdem Ambitionen für die Ausbildung von Diplom- und Doktoratsstudenten und, im Rahmen ihres Spezialgebietes, die Eignung und vor allem den Willen haben, industrielle Anwendungen zu moderieren (z. B. Expertensysteme, Geometrisches Modellieren, Roboter-Software, AI-Software, Wissenschaftliche Software). Eine der Verwendung entsprechende abgeschlossene inländische oder gleichwertige ausländische Hochschulbildung und Habilitation bzw. eine gleichzuwertende wissenschaftliche Befähigung ist Voraussetzung. Bewerber/innen aus dem Ausland werden ausdrücklich ermutigt.
Die Technisch-Naturwissenschaftliche Fakultät der Johannes-Kepler-Universität hat für die Arbeitsrichtung Symbolic Computation ein eigenes Institut unter der Leitung von Professor Bruno Buchberger eingerichtet (RISC-LINZ, Research Institute for Symbolic Computation) mit derzeit 8 Mitarbeitern mit Doktorat, 11 Doktoratsstudenten und ca. 25 Diplomstudenten . RISC-LINZ arbeitet in enger Verbindung mit dem Institut für Informatik und dem Institut für Mathematik.
Die Betonung von Symbolic Computation an der Johannes-Kepler-Universiät ist ein Teil und eine Triebfeder der geplanten Erweiterung der Technisch-Naturwissenschaftlichen Fakultät in Richtung “Mechatronics” (intelligente Kontrolle von technischen Vorgängen; 10 ordentliche Professuren geplant) in enger Kooperation mit der Industrie. Der neue Standort von RISC-LINZ, Schloß Hagenberg (11.-16. Jahrhundert), 15 Autominuten von Linz, verbindet die Annehmlichkeiten des städtischen Lebens mit der Abgeschiedenheit in einer der schönsten Landschaften und im Zentrum des kulturellen Angebots Österreichs.
Bewerbungen (Lebenslauf, Kopien einiger wichtiger wissenschaftlicher Publikationen) werden bis zum 31. März 1989 erbeten an: Dekan Prof. Dr. Peter Weiß, Johannes-Kepler-Universität, A4040 Linz (Austria). (Tel: Österreich (732) 2468-312.). Detaillierte Auskünfte erteilt auch der Leiter von RISC-LINZ, Prof. Dr. Bruno Buchberger, Johannes-Kepler-Universität, A4040 Linz. (Tel: Österreich (732) 2468-9219. Electronic mail: K313370@AEARN.bitnet.)

An der von der Baden-Württembergischen Landesregierung neu eingerichteten Forschungsstelle Europäisches Institut für Systemsicherheit (E.I.S.S.) erforschen wir Grundlagen und Verfahren der Datensicherheitstechnik in komplexen Systemen und offenen Netzen. Innerhalb neuer Projekte, die auch im Rahmen europaweiter Kooperationen (Eureka, Esprit, Race) durchgeführt werden, befassen wir uns mit Netzsicherheit und der Entwicklung von Zugangsprotokollen. Die Schwerpunkte liegen dabei vor allem auf den Gebieten Spezifikation, Realisierung und Verifikation sicherer Systeme, logische Grundlagen der Theorie verläßlicher Systeme, mathematische Modellierung und Hardware-Implementierung kryptographischer Algorithmen, insbesondere von Public-Key-Verfahren und Netzmanagement-Protokollen. Zur Mitarbeit in diesen Projekten suchen wir für sofort oder später engagierte

Dipl.-Informatiker/innen
Dipl.-Elektroingenieure/innen
Dipl.-Mathematiker/innen

die sich im Hauptstudium (oder danach) vorzugsweise mit Computer-Algebra, Komplexitätstheorie, Kryptographie oder Datensicherheit und benachbarten Gebieten (z.B Betriebssysteme, Netzwerkarchitekturen, Telematik, Experten- systeme, Logik, VLSI-Design) befaßt haben. Wir erwarten überdurchschnittliche Studienleistungen, interdisziplinäres Interesse, Ideenreichtum und Einsatzbereitschaft sowie Freude zur Teamarbeit. Wir bieten besonders für Absolventen oder Bewerber mit einigen Jahren Berufserfahrung ein personell und apparativ äußerst attraktives Umfeld, in dem Sie die Möglichkeit vorfinden, sich durch Veröffentlichungen und Promotion weiterzuqualifizieren. Sie haben Kontakt zu führenden internationalen Experten, die zur Unterstützung der Wissenserfassung und -dokumentation der aktuellsten Themen von Forschung und Entwicklung im Bereich der Systemsicherheit eingeladen werden. Promovierten Bewerbern bietet sich die Chance, die Verantwortung für ein Projekt zu übernehmen. Unsere vertraglichen Konditionen entsprechen denen der Universität Karlsruhe und sehen einen Zeitvertrag nach BAT vor. Bitte bewerben Sie sich mit aussagekräftigen Unterlagen bei E.I.S.S. Prof. Dr. Thomas Beth, Universität Karlsruhe, Kaiserstr. 8, 7500 Karlsruhe, Tel.: 0721/608-4205.

Kurze Mitteilungen

SAME hat ein elektronisches Network für Computer-Algebra begonnen. Interessenten bitte Mitteilung an dlfrunip11 oder samefrulm11 (beide bitnet) senden. ∗ ∗ ∗ Inzwischen gibt es Fachgruppen für Computer-Algebra in Belgien, Frankreich und Holland. Sprecher und Kontakperson sind H. Caprasse (Liege), D. Lazard (Paris) bzw. H. van Hulzen (Enschede).