Nummer 25 **Oktober 1999**

Mitteilungen der Sprecher 3

Hinweise auf Konferenzen 3

Berichte von Konferenzen 8

Der Nobelpreis in Physik 1999 13
Computeralgebra-Programm Schoonschip – ein Meilenstein bei der Renormierung nicht-abelscher Eichtheorien 13

Themen und Anwendungen der Computeralgebra 14
K. Hantzschmann, Appr. Lösungen von Differentialgleichungen . . . 14

Computeralgebra in Lehre, Ausbildung und Weiterbildung 17
M. Ermert, Laptop zum Spicken – Computer beim Abitur 17
H. Knechtel, Computeralgebra-Systeme in der Schule 18
P. Drijvers, The Dutch Perspective 22

Publikationen über Computeralgebra 25

Besprechungen zu Büchern der Computeralgebra 26
Wolff, Gloor, Richard, Analysis Alive 26
Jungnickel, Networks and Algorithms 27
Mignotte, Ştefănescu, Polynomials: An Algorithmic Approach . . . 27
Kamerich, A Guide to Maple 28
Koblitz, Algebraic Aspects of Cryptography 28

Lehrveranstaltungen zu Computeralgebra im WS 1999/2000 31

Kurze Mitteilungen 32

Fachgruppenleitung Computeralgebra 1999-2002, Impressum 35

Werbeseite der Fa. Texas Instruments

Mitteilungen der Sprecher

Liebe Mitglieder der Fachgruppe Computeralgebra,

am 4. Oktober kam die Fachgruppenleitung in Heidelberg zusammen, um über aktuelle Themen zur Förderung der Computeralgebra in Deutschland zu diskutieren. Eines der wichtigsten Themen, das uns schon lange in der Fachgruppenleitung beschäftigt, war dabei die Entwicklung der Computeralgebra an den Schulen. Aus diesem Grund hatte die Fachgruppenleitung einen Vertreter aus dem Schulbereich, Herrn Knechtel, als Fachexperten in dieser Wahlperiode gewonnen. Wir verweisen auf seinen Artikel über den Einsatz von Computeralgebra in Schulen der BRD in diesem Heft. Wie es bei unseren Nachbarn in den Niederlanden dazu aussieht, zeigt ein zweiter Artikel. Nachdem die Fachgruppenleitung - federführend waren die Kollegen Kerber und Koepf - im letzten Jahr in Schloss Thurnau eine Tagung zum Thema Computeralgebra in Lehre, Ausbildung und Weiterbildung *organisiert hat, wird sie auch im nächsten Jahr eine Tagung mit der gleichen Zielsetzung in Thurnau durchführen. Die Entwicklung der Computeralgebra an Schulen wird auch weiterhin von uns als Fachgruppenleitung verfolgt und mit Aktivitäten unterstützt werden.*

Das Benchmarking ist ebenfalls ein Thema, das uns schon lange beschäftigt. Wir haben inzwischen in unserem Kreis einen Vertreter, Prof. Dr. Greuel, gefunden, der sich als Referent dafür einsetzt. Neben den Aktivitäten von Herrn Dr. Kredel zum Thema Benchmarking, über die an dieser Stelle in vorangegangenen Heften schon berichtet wurde, ist jetzt ein Projekt mit dem Schwerpunkt "polynomiale Systeme" entstanden. Das Zusammenführen der vorhandenen Aktivitäten und das Einbringen von Knowhow aus anderen Gebieten wird eine unserer Aufgaben in der nächsten Zeit sein.

In der Physik wurden schon früh Computeralgebra-Systeme entwickelt und eingesetzt. Eines führte zu dem diesjährigen Nobelpreis in Physik, vgl. den Beitrag in diesem Heft. In der Fachgruppenleitung wurden wir von Prof. Dr. Hehl auf aktuelle Entwicklungen in der Physik informiert. Er hat uns als Fachexperte in den vergangenen Wahlperioden beraten. Jetzt ist er zurückgetreten. Anlaß dazu ist ein bevorstehender längerer Auslandsaufenthalt. An dieser Stelle möchten wir ihm im Namen der ganzen Fachgruppe herzlich für sein Engagement und seinen Rat danken.

Zur Regel geworden ist die Sektion Computeralgebra auf der Jahrestagung der DMV. In diesem Jahr fand sie in Mainz statt. Die Computeralgebra war durch einen Hauptvortrag von Bernd Sturmfels und eine eigene Sektion vertreten. Diese wurde von den Kollegen Pfister und Plesken geleitet und hatte einen relativ guten Zuspruch. Auch für die DMV 2000 in Dresden ist eine Sektion Computeralgebra geplant. Auch bei der nächsten Jahrestagung der GAMM wird die Computeralgebra eine eigene Sektion haben. Sie wird geleitet von Prof. Dr. Greuel. Hinweise auf weitere Tagungen finden Sie auf den folgenden Seiten. Besonders möchten wir dabei auf das Computeralgebra-Symposium an der FH Konstanz hinweisen, das von der Fachgruppenleitung durch das Entsenden von Referenten gefördert wird.

H. Michael Möller *M. Pohst*

Hinweise auf Konferenzen

1. **RWCA'00 – Seventh Rhine Workshop on Computer Algebra**

   Bregenz, Austria, 22.3. – 24.3.2000

   Topics: The topics of the workshop include all aspects of Computer Algebra, from theory to applications and systems.

   Purposes: This is the seventh edition of a workshop initiated in Strasbourg in 1988 and held every second year. To avoid competition with well-established conferences in the field, the workshop is kept as informal as possible. Its two main purposes are to offer an opportunity to young researchers and newcomers to present their work and to be a regional forum for researchers in the field. Despite this latter goal, the workshop is open worldwide to submissions and attendance.

   Program Committee: Moulay Barkatou (Grenoble), Leon Brenig (Brussels), Manuel Bronstein (Sophia Antipolis), Jacques Calmet (Karlsruhe), Arjeh Cohen (Eindhoven), Gaston Gonnet (Zurich, program committee chair), Tudor Jebelean (Linz), Werner Krandick (Paderborn), Daniel Lazard (Paris), Ton Levelt (Nijmegen), Malcolm MacCallum (London), Elizabeth Mansfield (Canterbury), Thom Mulders (Zurich, workshop chair), Peter Paule (Linz), Fritz Schwarz (Sankt Augustin), Joachim von zur Gathen (Paderborn), Carlo Traverso (Pisa), Gilles Villard (Grenoble), Franz Winkler (Linz),

Submissions: Submit either a full paper or an extended abstract to the workshop chair. Submissions are not formally refereed and can thus be submitted later elsewhere. Accepted submissions will appear in locally printed proceedings, intended for attendees only. Please state the author's name, address and E–mail (if available).

Submission by regular mail: Send two copies. Submission by E–mail (preferable): Send a LaTeX-file and a postscript-file (for comparison only).

Important Dates:
- October 31, 1999: Submitted papers must be received
- December 17, 1999: Notification of acceptance

Organization: *Workshop Chair:* Thom Mulders, Inst. of Scientific Computing, ETH-Zentrum, CH-8092 Zurich, Tel: +41-1-6327473, Fax: +41-1-6321374, `mulders@inf.ethz.ch`

Program Committee Chair: Gaston Gonnet, Inst. of Scientific Computing, ETH-Zentrum, CH-8092 Zurich, Tel: +41-1-6327470, Fax: +41-1-6321374, `gonnet@inf.ethz.ch`

Information: Updated information will be available on the WWW at `http://www.inf.ethz.ch/rwca00/` . For more information, please contact the workshop chair.

2. **T^3 – teachers teaching teachers**

   Dallas, USA, 16.3. – 19.3.2000

   `http://www.t3ww.org/docs/t3wwnat00.htm`

3. **Computeralgebra-Symposium Konstanz (CASK)**

   Konstanz, 9.3. – 10.3.2000

   Örtliche Tagungsleitung: Prof. Dr. Elkedagmar Heinrich, Dr. Hans-Dieter Janetzko

   Nähere Informationen ab Ende März über die Homepage der FH: `http://www.fh-konstanz.de`

   Adresse: Fachhochschule Konstanz, Brauneggerstr. 55, 78462 Konstanz, Email: `heinrich@fh-konstanz.de` .

4. **GAMM – Jahrestagung**

   Göttingen, 3. – 7.4.2000

   Leitung der Sektion Computeralgebra und -analysis: Prof. Dr. Gert-Martin Greuel.

5. **Computeralgebra in Lehre, Ausbildung und Weiterbildung**

   Thurnau, 26. – 28.4.2000

   Aufgrund des großen Erfolgs der ersten Tagung dieser Art, welche vom 22.-25. April 1998 in Thurnau stattfand, veranstaltet die Fachgruppe Computeralgebra (FG CA) im Frühjahr 2000 eine zweite Tagung zum Thema *Computeralgebra in Lehre, Ausbildung und Weiterbildung* über den Einsatz von Computeralgebrasystemen im Unterricht.

   Ziel ist es, den im ersten Treffen initiierten Austausch zwischen den Kultusministerien, den für die Fortentwicklung der curricularen Lehrpläne zuständigen Instituten und den Experten aus Wissenschaft, Lehre und Schule weiterzuführen. Wir erhoffen uns insbesondere wieder Berichte über die in den einzelnen Bundesländern stattfindenden Lehrversuche und über geplante Lehrplanreformen.

   Verantwortlich ist das Organisations- und Programmkomitee in Zusammenarbeit mit der Fachgruppe Computeralgebra. Es besteht aus

   - Prof. Dr. A. Kerber, Bayreuth (FG CA, Leitung und lokale Organisation),
   - Prof. Dr. Wolfram Koepf, Leipzig (FG CA, Referent für Lehre und Didaktik),
   - Heiko Knechtel, Bückeburg (FG CA, Fachexperte Schule),
   - Dr. Günter Schmidt, Mainz (MNU),
   - Prof. Dr. Günter Törner, Duisburg (Fachgruppe Didaktik der Mathematik der DMV) und
   - Prof. Dr. Hans-Georg Weigand, Gießen (Gesellschaft für Didaktik der Mathematik).

   Bitte senden Sie Ihre Anmeldung an Prof. Kerber (`kerber@btm2xh.mat.uni-bayreuth.de`) oder Prof. Koepf (`koepf@imn.htwk-leipzig.de`) (s. Adressen Fachgruppenleitung).

6. **IMACS-ACA – Applications of Computer Algebra**

   Saint Petersburg, Russia, 25.6. – 29.6.2000

   General Chair: Nikolay Vassiliev

   Program Chairs: Victor Edneral, Richard Liska, Michael Wester

   Organizing Committee: Stanly Steinberg, Michael Wester, Yuri Matiyasevich, Anatoly Vershik

   Local Arrangements: Elena Novikova, Nikolay Mnev, Vyacheslav Nesterov, Sergei Slavyanov,

Scientific Committee: Bruno Buchberger RISC-Linz, Jacques Calmet Univ. of Karlsruhe, Arieh Cohen Eindhoven Univ.Tech, Rob Corless Univ. of Western Ontario, Andre Deprit Ntl. Bureau of Standards, Sam Dooley IBM Yorktown Heights, Keith Geddes Univ. of Waterloo, Vladimir Gerdt Institute of Nuclear Res., Gaston Gonnet Zurich, Richard Jenks IBM Yorktown Heights, Erich Kaltofen N. Carolina State Univ., Deepak Kapur Univ. of New Mexico, Wolfgang Kuechlin Univ. of Tuebingen, Bernard Kutzler BK Techware, Luis Laita Univ. Politecnica Madrid, Richard Liska Tech. Univ. Prague, Yuri Matiyasevich Steklov Inst. of Math. St. Petersburg, Alexander Michalev Moscow State Univ., Michael Monagan Simon Fraser Univ., Matu-Tarow Noda Ehime Univ., Mohamed O. Rayes Texas Instruments Dallas, Tomas Recio Univ. de Cantabria, Eugenio Roanes-Lozano Univ. Complutense de Madrid, Tateaki Sasaki Univ. of Tsukuba, Stanly Steinberg Univ. New Mexico, David Stoutemeyer Soft. Warehouse, Nikolay Vassiliev Steklov Inst. of Math. St. Petersburg, Anatoli Vershik Steklov Inst. of Math. St. Petersburg, Emil Volcheck National Security Agency, Volker Volker Weispfenning, Univ. of Passau, Franz Winkler J.Kepler Univ. Linz.

Session on Education: Education has become one of the fastest growing application areas for computers in general and computer algebra in particular. Computer algebra tools such as TI-92/89, DERIVE, MATHEMATICA, MAPLE, AXIOM, REDUCE, MACSYMA, or MUPAD make powerful teaching tools in mathematics, physics, chemistry, biology, economy, etc..

The goal of this session is to exchange ideas and experiences, to hear about classroom experiments, and to discuss all issues related with the use of computer algebra tools in classroom (such as assessment, change of curricula, new support material, ...)

If you have anything of the above which you would like to share with colleagues in the inspiring atmosphere of an IMACS-ACA conference, then please make a submission comprising title, author(s), abstract (10 lines min, 20 lines max).

Format of submission: Plain ASCII text in English sent to email b.kutzler@eunet.at.

Deadline for submission: March/April 2000

More info about the conference can be obtained from:
e-mail: `wester@math.unm.edu`
web: `http://www.pdmi.ras.ru/EIMI/2000/imacs/index.html`.

7. FPSAC'00 – Formal Power Series and Algebraic Combinatorics

Moscow, Russia, 26.6. – 30.6.2000

Topics Algebraic and bijective combinatorics and their relations with other parts of mathematics, combinatorial and computer algebra, computer science and physics.

Conference program Invited lectures, contributed presentations, poster session, problem session and software demonstrations.

Official languages The official languages of the conference are English, French and Russian.

Invited Speakers Not all invited speakers are known at this time. The following scientists have already accepted to give an invited talk at FPSAC'00: G.P. Egorychev (Russia), M. Hazewinkel (The Netherlands), O. Kharlampovitch (Canada), J. Propp (USA), M. Shimonoso (USA), S. Zvonkin (France).

Call for papers and posters Authors are invited to submit extended abstracts of at most twelve pages by *November 15, 1999*.
To submit your papers, preferably use the submission server of the conference, which is available through the Internet at the http address `http://www.liafa.jussieu.fr/~fpsac00!`. If you are unable to use the submission server, please either send *one* single postcript file at the address `fpsac00@liafa.jussieu.fr` or send *four* copies of the extended abstract to the following address: LIAFA - Universite Paris 7 - Attention: Daniel KROB - SFCA/FPSAC'00 - 2, place Jussieu - 75251 Paris Cedex 05 - France.

Authors from former Soviet Union can also submit their paper by sending by e-mail *one* single postcript file at the address `fpsac00@cnit.msu.ru` or by sending four copies of their extended abstract at the following address: Moscow State University - Department of Mechanics and Mathematics - Attention: Prof. A.V. Mikhalev - FPSAC'00 - Moscow 119899 - Russia.

The submitted papers should begin with a summary written in English and in another official language of the conference (translation assistance will be provided if necessary). Authors should indicate the mode of presentation which they consider appropriate for their paper, i.e. lecture or poster session. The notifications of acceptance or rejection are scheduled for January 15, 2000.

Open problem session Contributions to the problem session are invited in advance of the conference dates. People interested in submitting a problem should submit it as described above, before *June 1, 2000*.

Software demonstrations Demonstrations of software relevant to the topics of the conference are encouraged. People interested in giving a software demonstration should submit before *January 15, 2000* a paper including the hardware requirements, as described above.

Program committee S.A. Abramov (Russia), S. Ariki (Japan), N. Bergeron (Canada), C. Bessenroth (Germany), L.A. Bokut' (Russia), M. Bousquet Melou (France), C. Greene (USA), T. Guttmann (Australia), D. Krob (France, *co-chair*), G. Labelle (Canada), A.A. Mikhalev (Hong Kong – Russia, *co-chair*), A.V. Mikhalev (Russia), A. Odlyzko (USA), M. Petkovsek (Slovenia), R. Pinzani (Italy), D. Rawlings (USA), B. Sagan (USA), V. Strehl (Germany), S. Sundaram (USA), M. Wachs (USA), H.F. Yamada (Japan), J. Zeng (France).

Participant support Limited funds are available for partial support of participants, in particular for students and scientists from Eastern Europe countries.

Location The conference will take place in the *Main Building of M.V. Lomonosov Moscow State University*. The first talk is scheduled on June 26, 2000 at 9:00 a.m.

Further information All important informations concerning FPSAC'00 can be found on the conference web site available through the Internet at the http address `http://www.liafa.jussieu.fr/~fpsac00`. A mirror site is also available at the http address `http://www.cnit.msu.ru/~fpsac00`. More details will be given in future announcements. For any further question, just write to `fpsac00@cnit.msu.ru`.

Organizing committee V.A. Artamonov (Russia), J. Delagnes (Paris), M. Delest (France), G. Duchamp (France), S.T. Glavatsky (Russia), D. Krob (France), V.N. Latyshev (Russia), P. Leroux (Canada), R. Mantaci (France), V.T. Markov (Russia), A.A. Mikhalev (Hong Kong and Russia), A.V. Mikhalev (Russia, *Chairman*), J.C. Novelli (France), C. Precetti (France), G.B. Shabat (Russia), M.V. Zaicev (Russia), A.A. Zolotykh (Russia), K.A. Zubrilin (Russia).

8. The 4th Int. DERIVE/TI-92/TI-89 Conference

Liverpool, UK, 12.7. – 15.7.2000

The conference has four main strands:
1. Applications of computer algebra in mathematics teaching.
2. Reflections on the experiences in the learning, teaching and assessment of mathematics using computer algebra, - what worked and what didn't.
3. Research concerning the use of computer algebra in mathematics education.
4. The use of programming and scripting capabilities of computer algebra systems to do mathematics.

An important part of the conference will be the keynote addresses given by noted authorities in the use of computer algebra in mathematics education and assessment. The following individuals have agreed to be keynote speakers:
Josef Böhm, The Derive User Group, Austria
Richard Browne, Qualifications and Curriculum Authority, UK
David Sjöstrand, Elof Lindaelvs Gymnasium, Sweden
David Stoutemyer, Soft Warehouse/ Texas Instruments, USA

Further information: `http://www.cms.livjm.ac.uk/derive2k/`

9. WGA11 – The Use of Technology in Mathematics Education at ICME9

Makuhari, Japan, 31.7. – 6.8.2000

The International Commission on Mathematical Instruction (ICMI) organises an ICME every four years. The next one is in Makuhari, Japan from July 31 to August 6, 2000. (Makuhari is in Tokyo, about half way between the downtown area and Narita International Airport - about 40 km from central Tokyo.)

Aims Here are some early thoughts on what we expect people to gain from participating in Working Group for Action No. 11 (WGA11): The Use of Technology in Mathematics Education (Computers, Calculators, IT Media).

Find out about international issues and trends in this area: Educational issues (e.g. curriculum developments incorporating the Internet), Political issues (e.g. banning of calculators in schools), Technical issues (e.g. principles of instructional design for software). Share experiences related to these kinds of issues: Practical experiences (e.g. effective forms of professional development), Research observations and conclusions (e.g. evaluating student use of software), Advice offered to others (e.g. inclusion of dynamic geometry software in curricula).

Be informed about recent developments: Emerging trends in practice (e.g. use of graphics calculators in public examinations), Demonstrations of new kinds of significant technologies (e.g. affordable computer algebra), Emerging consensus (e.g. the Internet will continue to be important).

The Call for contributions contains an outline of elements of the possible structure of the group. Here is a slightly more elaborated version, to take advantage of having more space:

Level of education: Primary school (elementary school), Secondary school (high school), Post-secondary school (technical education, undergraduate education, graduate education), Teacher education (pre-service and in-service).

Technology in use: Calculators (basic calculators, scientific calculators and graphics calculators), Computers (computer algebra systems (CAS), spreadsheets, data analysis programs, CAS-capable graphics calculators), Tools designed for educational use (such as function graphers, probability simulators, dynamic geometry software), Learning environments, simulations and microworlds designed for educational use Integrated multimedia and tool software (such as hypertext tools, microworlds), Internet and telecommunications (WorldWideWeb, List servers, Email, Java).

Type and focus of contribution: Presentations and project reports: Reflective software presentations, presentation of classroom materials (including assessment), report on teaching experiments, courses or broader innovative projects. Survey reports on facts, trends and intentions: regional, national or international developments concerning syllabi, assessment regulations, availability of hardware and software in schools and homes, factual computer use in schools, teacher education programs and teachers' qualifications and acceptance Visions: What do we expect, what do we wish for technology-supported mathematics teaching in 2015? Software reflections and evaluations of existing programs and programs to be developed: What are the merits of various types of software? What software do we need in the future? What do we expect? Principles for designing software and multimedia. Curriculum development issues associated with technology: reflections on goals and appropriate mathematical content in technology-rich settings, new curricular emphases, new societal demands, cultural aspects. Contributions might focus on specific domains, such as new goals, contents, materials and teaching methods for algebra, statistics or geometry. Principles of instructional design (including didactical engineering, teacher development and assessment) specific for the integrated use of computers, calculators and telecommunications in mathematics education Empirical research studies with theoretical components: studies of cognitive and communicative aspects of software-supported learning and using mathematics of individuals and groups of students, classroom studies, experimental studies, etc; the methodology of research studies in this domain.

Meetings: The WGA will meet at least four times over the duration of the Congress. At least two sessions will be devoted to work in subgroups. This will ensure that there are opportunities for significant personal involvement of participants in areas of their interest, and a chance to get to know colleagues from around the world. We expect that some of the time of participants will be spent in groups that are small enough for personal contacts to be made. It is expected by the IPC that people will attend all of the meetings of their chosen WGA, to allow significant and extended activities to be undertaken. We expect that contributors to the WGA will be available to contribute to all sessions scheduled.

Presentations: All formal offers to present at the WGA will be finally made by the IPC on the basis of suggestions from us. The IPC are responsible for controlling the participation of individuals in the ICME. However, anyone interested in making a presentation should contact us (the Co-Chief Organizers) in the first instance. We will expect a written version of papers before the Congress. Depending on the number of contributions, the time for oral presentations during the WGA sessions will vary. The Organizing Team will decide on the allocation of time that will be available for each presentation; we plan to combine very short presentations with longer ones (plenaries, overviews, introductory papers, papers as basic stimuli for discussions). Some subgroups may decide to mainly focus on discussion, assuming that all the participants may have already read the paper. We plan to make papers available on the WWW before the Congress so that all participants can prepare for the discussions and presentations at the Congress.

Publication: We expect that there will be a good case for preparing a publication of some of the proceedings of the WGA, both to provide a more permanent and reflective record of the events to participants and also to provide information to the wider international audience of those not able to attend. Details of the scope and size, refereeing, editing, publishing and financial matters associated with this publication are still to be determined. Any advice on this would of course be welcome, whether from potential contributors, readers or publishers.

Organizers: Rolf Biehler, Institut fuer Didaktik der Mathematik (IDM,) Universitaet Bielefeld, Postfach 100131, 33501 Bielefeld, Germany, Tel: +49-521-106-5058, Fax: +49-521-106-2991, Email: `rolf.biehler@uni-bielefeld.de`, Internet: `http://www.uni-bielefeld.de/idm/personen/rbiehler/rbiehler.htm`.

Barry Kissane, The Australian Institute of Education, Murdoch University, Murdoch WA Australia 6150, Tel: +61-8-9360-2677, Fax: +61-8-9360-6296, Email: `kissane@central.murdoch.edu.au`,
Internet: `http://wwwstaff.murdoch.edu.au/~kissane`.

10. ISSAC 2000 – International Symposium on Symbolic and Algebraic Computation

St. Andrews, Scotland , 7.8. – 9.8.2000

The International Symposium on Symbolic and ALgebraic Computation 2000 (ISSAC 2000) will take place at the University of St. Andrews, Scotland from 7th-9th August 2000 (Mon. to Wed.), preceded by a day of workshops on Sunday August 6th.

ISSAC is a yearly international symposium that provides an opportunity to learn of new developments and to present original research results in all areas of symbolic mathematical computation.

Topics of the meeting include, but are not limited to:
Algorithmic mathematics: Algebraic, symbolic, and symbolic-numeric algorithms including: simplification, polynomial and rational function manipulations, algebraic equations, summation, integration, linear algebra and matrix computations, number theory, ODE/PDE, complex computation, group computations, and geometric computing;
Computer science: Theoretical and practical problems in symbolic mathematical computation including: computer algebra systems, problem solving environments, programming languages and libraries for symbolic computation, user interfaces, data structures, software architectures, parallel/distributed computing, mapping algorithms to architectures, concrete analysis and benchmarking, complexity of computer algebra algorithms, artifical intelligence techniques, automatic differentiation and code generation, mathematical data exchange protocols;
Applications: Problem treatments incorporating algebraic, symbolic or symbolic-numeric computation in an essential or novel way, including engineering, economics and finance, physical and biological sciences, computer science, logic, mathematics, statistics, and use in education.

The **Overall Chair** of ISSAC 2000 is Prof. Tomas Recio, Universidad de Cantabria. The **Local Arrangements Chair** is Dr. Steve Linton, University of St Andrews.

Further information:`http://www-history.mcs.st-and.ac.uk/issac2000/`

11. T^3 – teachers teaching teachers

Columbus, USA, 16.3. – 18.3.2001

`http://www.t3ww.org/docs/t3wwnat01.htm`

Berichte von Konferenzen

1. **CASC-99 The Second Workshop on Computeralgebra in Scientific Computing**

   München, 31.5. – 4.6.1999

   Dies ist der 2. Workshop der CASC-Serie. Weitere Informationen dazu auf der URL:
   `http://www14.informatik.tu-muenchen.de/konferenzen/CASC99/`

   Richard Liska: *Where Numerics can Benefit from Computer Algebra in Finite Difference Modelling of Fluid Flows*, Anders Eriksson, Yunhua Luo, Costin Pacoste: *Computer Algebra Investigation of Equivalence in 4-node Plane Stress/Strain Finite Elements*, Michel Fournié: *Symbolic derivation of Different Class of High Order Compact Schemes for Partial Differential Equations*, V.G. Ganzha, E.V. Vorozhtsov: *Implementation of Aerodynamic Computations with Mathematica*, Vladimir P. Gerdt, Vladimir V. Kornyak, Matthias Berth, Günter Czichowski: *Construction of Involutive Monomial Sets for Different Involutive Divisions*, Vladimir P. Gerdt: *Completion of Linear Differential Systems to Involution*, Gerd Baumann: *Solution of Ordinary Differential Equations with MathLie*, Yves A. Papegay: *From Modeling to Simulation with Symbolic Computation: An Application to Design and Performance Analysis of Complex Optical Device*, Tim Wichmann, Ralf Popp, Walter Hartong, Lars Hedrich: *On the Simplification of Nonlinear DAE Systems in Analog Circuit Design*, Vladimir F. Kovalev: *Computer Algebra Tools in Construction of Renormgroup Symmetries*, Gerrit Handrich: *Quantization by Presentation: The Nambu-Goto String in* $1+3$ *Dimensions*,

   Brian J. Dupée, James H. Davenport: *An Automatic Symbolic-Numeric Taylor Series ODE Solver*, Radu Zapotinschi: *Symbolic Analysus of Computational Algorithms with SYDNA*, W. Govaerts, Yu. A. Juznetsov, B. Sijnave: *Bifurcations of Maps in the Software Package CONTENT*, A.N. Prokopenya, N.I. Chochits, R. Kragler (short talk): *Simulation of Forces in Classical Mechanics*, Hans J. Stetter: *Posynomials with Coefficients of Limited Accuracy*, Joachim von zur Gathen, Jaime Gutierrez, Rosario Rubio: *On Multivariate Polynomial Decompositon*, Alexii Yu. Uteshev: *Localization of Roots of a Polynomial Not Represented in Canonical Form*, Rainer Steinwandt: *Decomposing Systems of Polynomial Equations*, Nikolay Vasiliev: *Complexity of Momomial Evaluations and Duality*, M. Cafaro, B. Paternoster: *Analysis of Stability of Rational Approximations Through Computer Algebra*, Sergey Gutnik: *Symbolic-numeric Investigations for Stability Analysis of Satellite Systems*, Vladimir V. Kornyak: *Cohomology of Lie Suberalgebras of Hamiltonian Vector Fields: Computer Analysis*, R. González-Díaz, P. Real: *Computing Cocycles on Simplicial Complexes*, Werner M. Seiler (Invited lecture): *Indices and Solvability for General Systems of Differential Equations*, V. Y. Pan, A. Zheng, M. Abu Tabanjeh, Z. Chen, S. Providence: *Superfast Computations with Singular Structured Matrices over Abstract Fields*, fA.N. Prokopenya, N.I. Chochits, R. Kragler (short talk): *Simulation of Forces in Classical Mechanics*, Gaston H. Gonnet, Allan Bonadio (Invited lecture): *Partial Inverse Heuristic for the Approximate Solution of Non-linear Equations*, Vladimir P. Gerdt, Soso A. Gogilidze: *Constrained Hamiltonian Systems and Gröbner Bases*, Victor F. Edneral: *About Normal Form Method*, Eugenio Roanes-Lozano, E. Roanes-Macínas, L.M. Laita: *Geometric Interpretation of Strong Inconsistency in Knowledge Based Systems*, Christoph Richard, Andreas Weber: *A Symbolic Numeric Environment for Analyzing Measurement data in Multi-Model Settings*, Manfred Göber, Wolfgang Küchin, Stefan Müller, Andreas Weber: *Extending a Java Based Framework for Scientific Software-Components*, Yoshio Uwano, Nikolai Chekanov, Vitaly Rostovtsev, Sergue Vinitsky: *On Normalization of a Class of Polynomial Hamiltonians: From Ordinary and Inverse Points of View.*

   Volker Weispfenning (Passau)

2. **1999 IMACS – Conference on Applications of Computer Algebra**

   El Escorial (near Madrid), Spain, 24.6. – 27.6.1999

   Näheres zu der Tagung und der IMACS-ACA-Serie, sowie Electronic Proceedings auf der URL: `http://math.unm.edu/aca.html`
   Session: Computer Algebra Meets Education I / Bernhard Kutzler
   Bernhard Kutzler: *Setting the Tone: CAS as pedagogical tools*, Josef Boehm: *Basic Skills versus Technology .. not a Contradiction but a Completion*, Gary A. Harris: *The Use of Mathematics Specific Technology in Capstone Mathematics Teacher Preparation Courses*, Justo Cabezas, Eugenio Roanes-Lozano: *Some Reflections About the Impact of Computer Algebra Systems in the Ordering of the Curricula of Mathematics*, Bill Pletsch: *A Computer Classroom Lecture: Asymptotic Convergence of Rational Functions*, Vlasta Kokol-Voljc: *Exam questions when using CAS for school mathematics teaching*, Michel Beaudin: *Using the TI-92Plus: Examples*, Bengt Ahlander: *Why use CAS with TI89 in mathematical education? Classrooms experiments* Garry Clark, Edward Redden: *Using Logo as a Scaffolding ot Develop Algebraic Thinking in a Virtual Classroom*, Miguel de Guzman: *Discovery Experiences in Synthetic Geometry with DERIVE*, E. Roanes-Macias, E. Roanes-Lozano: *About how to implement Geometric Transformations on a CAS*, Tenoch E. Cedillo A.: *A number-based approach to introductory algebra: A study with 11-12 year olds using graphic calculators*, Badr Defouad: *Instrumentation processes underlying the use of TI92 at high school level*, A. Cavallone, C. D'Apice, M. Marsella, S. Salerno: *A didactical laboratory: image filtering*

   Session: Approximate Algebraic Computation : towards Symbolic-Numeric Algorithms / Tateaki Sasaki, Matu-Tarow Noda, Bernard Mourrain, Robert Corless
   Jean-Michel Muller, Vincent Lefevre: *New results on the Table Maker's Dilemma*, Hans Stetter: *Polynomial Algebra with Coefficients of Limited Accuracy*, Hiroshi Sekigawa: *A System of Automatic Algorithm Stabilization*, Hiroshi Kai: *To Be Announced*, Victor Y. Pan: *To be announced*, Tateaki Sasaki: *Mechanism of Cancellation Errors in Multivariate Hensel Construction with Floating-point Numbers*, A. Fronville: *Exacts predicates for arrangement of arcs of circle*,

d. Rupprecht: *Approximate p-adic CGD computation*, B. Mourrain: *Towards numerical stability in normal form algorithms*, Matu T. Noda: *Hybrid Rational Function Approximation and its Applications*, M. Giesbrecht: *Approximate polynomial decomposition*, B. Trager, P. Gianni: *On approximate ideals*

hjkhjklhlh **Session: Combinational and Computational Methods in Algebraic Geometry/ Jie-Tai Yu, Vladimir Shpilrain**

Josef Schicho: *The Parameterization Problem for Algebraic Surfaces*, Jaime Gutierrez, Rosario Rubio: *Computing subfields in pure trascendental extensions*, Lenny Makar-Limanov: *Again* $x + x^2y + z^2 + t^3 = 0$, Vladimir Shpilrain: *Invariants of algebraic varieties*

Session: Toric Ideals and Integer Programming/ Lorenzo Robbiano

Lorenzo Robbiano: *Computing Toric Ideals*, Anna Bigatti: *New algorithms for Computing Toric Ideals*, Raymond Hemmecke: *Decomposing Graver Test Sets in Stochastic Programming*, Serkan Hosten: *Initial Ideals of Toric Ideals and Group Relaxations in Integer Programming*

Session: Computer Algebra for Dynamical Systems and Mechanics I/ Victor Edneral, Ilias Kotsireas, Nikolay Vasiliev

Victor Edneral: *Computer Algebraic Approximations–Creation of Approximated Solutions of Scientific and Engineering Problems in Symbolic Form*, A.V. Banshchikov, L.A. Bourlakova, V.D. Irtegov: *solving the problem of stabilization of a gyroscopic system with the help of Computer Algebra*, L.A. Bourlakova, V.D. Irtegov: *About investigation of systems with first integrals* J. Palacián, P. Yanguas: *Analytical Approach for Simplifying Dynamical Systems of Polynomial Type*, A. Abad, A. Gavin, J.F. San-Juan: *Communications of the Poisson Series Processors PSPC with General Scientific Software*, Raya Khanin, Matthew Cartmell: *Parallelisation of Perturbation Analysis: the method of Multiple Scales applied to vibration problems*, Jean-Charles Faugere: *Some computational experiment in Celestial Mechanics*, G. Carra Ferro: *Some remarks on differential Hilbert polynomials in two variables*, G. Carra Ferro, Vladimir Gerdt: *Extended Characteristic Sets of Finitely Generated Differential Ideals*, Alexander Aranson: *Enumeration of intersections of Newton's polyhedrons*, G. Eichenmueller: *symbolic Computation of Formal Solutions for 2 and 3 Dimensional Dynamical Systems*, Driss Boularas: *A new classification of planar homogeneous quadratic systems*, J. Mikram, F. Zinoun: *Computation of Normal Forms of Hamiltonian systms in the Presence of Poisson Commuting integrals (Liouville-Integrability and Birkhoff Normal Forms)*

Session : Applications of Computer Algebra to Signal Processing/ Jeremy Jonson, Markus Pueschel

Hyungju Park: *Minimal Syzygies and Multidimensional Filter Design*, Markus Pueschel: *Group Representations and Automatic Derivation of Fast Signal Transforms*, Dan Rockmore: *A Wreath Product Approach to Signal and Image Processing*, Ivan Selesnick: *Groebner Bases and Wavelet Design*, Jean-Charles Faugere, Fabrice Rouillier: *To be announced*, Jeremy Johnson: *To be announced*

Session: Computer Algebra Meets Education II / Bernhard Kutzler

Frank Postel, Ralf Hillebrand: *A Tutorial Mathematical System for Elementary Schools*, Jim Schultz: *High-Powered Technology in a Low-Level Mathematics Course*, Rein Prank: *A Scheme for Conservative Use of Computer Algebra*, G Albano, A. Cavallone, C. D'Apice, G. Gargiulo: *Mathematica and didactical innovation: a quadric use case*, A. Kehagias, P.N. Vlachos: *Computer Aided Instruction for Business Calculus in an International Liberal Arts College*, Ralf Hillebrand, Frank Postel: *Flexible Mathematical GUI Controls for Mathematical Electronical Documents*, May C. Abboud: *Mathematica in Undergraduate Mathematics Courses– A Teaching or Learning Aid?*, Marilo Lopez Gonzalez, Javier Rodrigo Hitos: *Searching roots for three degree polynomials with the help of Mathematica*, Joseph D. Myers, Kelley B. Mohrmann, Terry T. Crow: *Derivations and Visualizations for the Hydrogen Atom*, Alain Moussiaux: *CONVODE: A Reduce package for solving differential equations*, Paolo Boieri: *Exploring sequences with DERIVE*

Session: Teaching of Efficient Mathematics/ A. Akritas, Gennadi Malaschonok

Rafael J. Villanueva Mico, A. Hervas: *A project of Computer Aided Learning: A course of Computer*, Juan A. Aledom, Juan C. Cortes, Fernando L. Pelayo: *A study of particular methods for the approximate construction of some regular polygons by using Mathematica 3.0*

Session: Computer Aided Geometric Design and Computer Algebra/ L. Gonzalez-Vega, J.R. Sendra

Tomas Recio: *Missing points and branches of real parametric curves*, Andres Iglesias, Akemi Galvez: *Applying general-purpose symbolic and numerical computation programs for Computer Graphics and CAGD. Some applications to industry*, Josef Schicho: *Proper Parametrization of Real Algebraic Surfaces*, Jesus Espinola, Laureano Gonzalez-Vega, Ioana Necula: *An algorithm for approximate conversion of rational B-spline curves/surfaces and its implementation*, Lorenzo Robbiano: *Groebner Bases and Statistics*

Session: Demos of Computer Algebra Systems/ Michael Wester, Winfried Neun

Michael Wester: *Some Perspectives on the Usability of Computer Algebra Systems*, Michel Beaudin: *Solving a RLC Circuit Convolution with DERIVE for Windows*, Lorenzo Robbiano: *The Computer Algebra System CoCoA*, Volker Weispfenning: *The REDLOG Package–Tools and Applications*, Ralf Hillebrand, Frank Postel: *MuPAD–An Open Computer Algebra System and its Approach of Software Integration*, Carlos Enriguez Turiño: *Computer Algebra Applied to Mathematical Cartography*

Session: Applications of Computer Algebra To Robotics/ Peter Kovacs

Jean-Pierre Merlet: *Forward kinematics of parallel robots*, Jean-Charles Faugere, Luc Rolland, Fabrice Rouillier: *Using Computer algebra tools for off-line studies of parallel manipulators*, Manfred Husty, Adolf Karger: *Self-Motions of Griffis-Duffy Type Parallel Manipulators*, Peter Kovacs: *Functional Ideal Decomposition–a Tool for Kinematics*

Session: Symbolic-Numeric Interface and Problem Solving Environments I/ Richard Liska, Stanly Steinberg, Robert van Engelen

Richard Liska: *Finite Difference Numerical Modelling Supported by Computer Algebra*, Robert van Engelen: *Ctadel: A Computer Algebra System for the Generation of Efficient Numerical Codes for PDEs*, Ravi Venkatesan: *Invariant Variational Principles and Associated Numerical Schemes for Regularization of III-Posed Problems*

Session: Symbolic-Numeric Interface and Problem Solving Environments II/ Richard Liska, Stanly Steinberg, Robert van Engelen
Ravi C. Venkatesan: *Group Invariant Finite-Difference Schemes for Advection Equation*, Michel Fournie: *Usefulness of computer algebra methods in numerical simulations*, Brian J. Dupee, James H. Davenport: *Prototyping Symbolic-Numeric Algorithms using Naglink*, Massimo Cafaro, Beatrice Paternoster: *A symbolic-numerical package for linear stability analysis of numerical methods for ODEs*, Christoph Richard, Andreas Weber: *A Symbolic Numeric Environment for Analyzing Measurement Data in Multi-Model Settings*, Terence Etchells: *Extraction of Low Order Boolean Rules from Trained Neural Networks using a Computer Algebra System*

Session: Computer Algebra for Dynamical Systems and Mechanics II/ Victor Edneral, Ilias Kotsireas, Nikolay Vasiliev
Ilias Kotsireas: *Computational aspects of the N-body problem*, B. Elmabsout, M. Barbosu: *The study by symbolic of the sign of the riemannian curvature in the configuration space of the 3-body problem and applications*, Antonio Elipe, André Deprit: *Oscillators in Resonance*, Nikolay Vasiliev: *Construction of Invariants of Simplectic Mapping*, Rodney Coleman: *Some properties of the symplectic Lie algebra*

Session: Interaction on Physics, Number Theory and Computer Science I/ Hoang Ngoc Minh
M. Bigotte: *Colored multiple zeta values relations table*, D. Bradley: *Nested Sums and Iterated Integrals*

Session: Computer Algebra in the Spanish Educational System
Justo Cabezas Corchero: *Aparicion de nuevos contenidos curriculares en matematicas mediante la aplicacion de nuevas tecnologias*, Tomas Recio: *Las herramientas euclideas y el ordenador*, Agustin Carrillo: *Diferentes opciones para la resolucion de problemas con calculadoras graficas*, Lola Rodriguez Soalleiro: *Cambios curriculares en la enseñanza del Algebra*, Eugnio Roanes Macias, Eugenio Roanes Lozano: *Busqueda automatica de lugares geometricos*, Rafael Perez Gomez, Miguel Posadas: *Matematicas en Pantalla*

Session: Computations in Pure Mathematics (Algebra, Analysis, Geometry, .../ Maria-Emilia Alonso, Francisco Castro, Laureano Gonzalez-Vega
V. Alvarez, J.A. Armario, P. Real: *Homology of semidirect product of groups*, M.J. Jimenez, P. Real, B. Silva: *Analyzing the transference of the coalgebra structure on the homology of CDGAs*, Rocio Gonzalez-Diaz, Pedro Real: *Steenrod reduced powers and computability*, L.M. Camacho, J.R. Gomez, R.M. Navarro: *The use of Mathematica for the classification of some nilpotent Lie algebras*, J.C. Benjumea, F.J. Echarte, D. Fernandez, M.C. Marquez, J. Nuñez, F. Ramirez: *New ways of defining filiform Lie algebras*, Maribel Hartillo: *About an algorithm of T. Oaku*, Jose Maria Ucha: *Slopes in submodules of a free module*, P. Pison-Casares, A. Vigneron-Tenorio: *Computing Toric first Syzygies*, F. Orecchia: *The ideal generation conjecture for s general rational curves*, A. Montes: *Basic Algorithms for Specialization in Groebner Bases*, Bill Pletsch: *The Generation of Polya Polynomials using Macsyma, with Applications*, Bernard Mourrain: *Duality in Effective Algebraic Geometry*, F. Gaeta: *A Fast Computation of Hook Schur Functions*

Session: Teaching of Efficient Mathematics
Juan A. Aledo, Juan C. Cortes, Fernando L. Pelayo: *A comparative study between two general methods for the approximate construction of regular polygons by using Mathematica 3.0*, Alkiviadis Akritas, Stelios Kapranidis, Athina Katalifou: *Possibilities for Alternative Uses of the "Calculus and Mathematica" Approach*, Alkiviadis Akritas, Zamir Bavel: *Classical Mathematics with Mathematica*, Alkiviadis Akritas, Zamir Bavel: *Calculus and the Race Track Principle*, David J. Jeffrey: *Some elementary mathematics revisite and revised*, Igor Gachkov, Kenneth Hulth: *Teaching Error-Correcting Codes, Discrete Mathematics and Modern Algebra with Computer Algebra*, Gennadi Malaschonok, Natalia Malaschonok: *Teaching of efficient mathematics*, Gennadi Malaschonok: *Efficient methods of mathematical analysis*

Session: Mathematics on the Internet/ Angel Diaz, Erich Kaltofen
Olgea Caprotti: *Interfacing Proof Checkers With OpenMath*, Mike Dewar: *Plug and Play Mathematical Components*, Angel L. Diaz: *To be announced*, Dave Raggett: *Mathematics on the Web–Past, Present and Future*, Murray Sargent: *Unicode Encoding of Mathematics*, Stephen Watt: *Stylesheets for Mathematical Web Pages*, Andreas Weber: *Accessing Quantifier Elimination Packages Over the Internet Out of General Purpose Systems*, Erich Kaltofen: *Concluding Discussion of the Issues Addressed in the Talks (Moderator with Audience Participation)*

Session: Applications of Quantifier Elimination/ Volker Weispfenning, Hoon Hong
Hirokazu Anai, Shinji Hara: *A Robust Control system Design by a Special Quantifier Elimination Method using a Sturm-Habicht Sequence*, Laureano Gonzalez-Vega, Neila Gonzalez-Campos: *A Special Quantifier Elimination Algorithm for Pham Systems*, David J. Jeffrey: *A new solution of the quartic problem: with application ot integration*, Gerardo Lafferriere, George J. Pappas, Sergio Yovine: *Reach Set Computation for Linear Vector Fields using quantifier Elimination*, Petru Pau, Josef Schicho: *Quantifier Elimination for Trigonometric Polynomials by Cylindrical Trigonometric Decomposition*, Stanly Steinberg: *The Study of Stability using Computer Algebra*, Volker Weispfenning: *Semilinear motion planning in REDLOG*

Session: Interaction on Physics, Number Theory and Computer Science II/ Hoang Ngoc Minh
Hoang Ngoc Minh: *Functional Equations on Polylogarithms with Axiom*, Mike Hoffman: *Algebraic Structures on the Set of Multiple Zeta Values*, N. Imafuji: *Computer aided Knot Theory using Mathematica and MathLink*, G. Jacob: *Combinatorics on Algebraic Identification*, M. Ochiai: *Computational Construction of representation matrices for parallel version polynomial invariants*, Y. Sakata: *Computational Decomposition of homeomorphisms into canonical Dehn's twists*, Z. Wojtkowiak: *On l-adic iterated integral*

Volker Weispfenning (Passau)

3. ISSAC'99 – International Symposium on Symbolic and Algebraic Computation

Vancouver, British Columbia, Canada, 28.7. – 31.7.1999

Näheres zu der Tagung und der ISSAC-Serie auf der URL:
`http://www.cecm.sfu.ca/ISSAC99/`.
Vor der eigentlichen Tagung fanden wie üblich am 28.07.99 Tutorials statt.
Tutorial 1, Robert M. Corless and Lawrence F. Shampine, *Numerical Solution of Differential Equations in a Computer Algebra Environment*

Tutorial 2, Frédéric Chyzak, *Symbolic Manipulation, Summation and Integration of Special Functions and Combinatorial Sequences – The Holonomic Approach*

Ferner ein Workshop zu "Internet Accessible Mathematical Computation" organisiert von P. Wang und N. Kajler. Vorträge des Workshops:

Contributed Papers I: Theme: "Mathematics on the Internet" Steve Linton, Andrew Solomon: *GAP, OpenMath, and MCP*, Richard Fateman: *Analysis of a Web Interface for Mathematics: Experiences with Integral Queries for TILU*, Xiao Gang: *WIMS: A Server for Interactive Mathematics on the Internet*, Marc Giusti: *About MEDICIS*, Olga Caprotti: *Interactive mathematics with Strong OpenMath*

Contributed Papers II: Theme: "IAMC Support"
Andreas Weber, Wolfgang Küchlin: *A Framework for Internet Accessible Software Components for Scientific Computing*, Richard Zippel: *The MathBus*, Arthur Norman: *Synchronization of Distributed Development Software*, Ralf Hillebrand: *Flexible Mathematical GUI Controls for Mathematical Electronical Documents*

Vorträge der Haupttagung

Session 1: Polynomial Systems
M. Giusti, E. Schost: *Solving overdetermined polynomial systems*, M. Elkadi, B. Mourrain: *A new algorithm for the geometric decomposition of a variety*, C. Andradas, T. Recio, J.R. Sendra: *Base field restriction techniques for parametric curves*, S. Moritsugu, K. Kuriyama: *On Multiple Zeros of Systems of Algebraic Equation.*

Session 2: Non-commutativity Problems
J.J. Wavrik: *Commutativity Theorems. Examples in Search of Algorithms*, W.A. de Graaf, J. Wisliceny: *Construction bases of finitely presented Lie algebras using Gröbner bases in free algebras*, G.P. Brunick, L.S. Heath, C.A. Struble, E.L. Green: *Efficient Construction of Drinfel'd Doubles*

Invited Talk 1
Jonathan M. Borwein: *Experimental Mathematics and Exact Computation*

Session 3: Polynomials
V. Shoup: *Efficient Computation of Minimal Polynomials in Algebraic Extensions of Finete Fields*, E. Kaltofen, M.B. Monogan: *On the Genericity of the Modular Polynomial GCD Algorithm*, Z. Zilic, K. Radecka: *On Feasible Multivariate Polynomial Interpolations over Arbitrary Fields*

Session 4: Seminumerical Algorithms
V. Kislenkov, M. Mitrofanov, E. Zima: *How fast can we compute products?*, J. von zur Gathen, M. Nöcker: *Computing Special Powers in Finite Fields*, S. Bratus, I. Pak: *On sampling generating sets of finite groups and product replacement algorithm*

Session 5: Asymptotics and Series Expansions
J. Shackell: *Star Product and the Representation of Asymptotic Growth*, C.J. Rust, G.J. Reid, A.D. Wittkopf: *Existence and Uniqueness Theorems for Formal Solutions of Analytic Differential Systems*, Y.O. Macutan: *formal Solutions of Scalar Singularly Perturbed Linear Differential Equations*, C.-P. Jeannerod, E. Pflügel: *A Reduction Algorithm for Matrices Depending on a Parameter*

Session 6: Quantifier Elimination
V. Weispfenning: *Mixed Real-Integer Linear Quantifier Elimination*, C.W. Brown: *Guaranteed Solution Formula Construction*, S. McCallum: *A Note about Projection in the Presence of an Equational Constraint*, A. Dolzmann, T. Sturm: *P-adic Constraint Solving*

Invited Talk 2 Michael F. Singer: *Galois Theory of Difference Equations*

Session 7: Linear Algebra
S.P. Tsarev: *On factorization of nonlinear ordinary differential equations*, G.Chen, J. Della Dora: *Rational Normal Form of Dynamical Systems by Carleman Linearization*, M. Bronstein, A. Fredet: *Solving linear differential equations over* $C(x, xp(int(f(x)dx)))$

Session 8: Linear Algebra
T. Mulders, A. Storjohann: *Diophantine Linear System Solving*, B. Beckermann, G. Labahn, G. Villard: *Shifted Normal Forms of Polynomial Matrices*, J. Abbot, M. Bronstein, T. Mulders: *Fast Deterministic Computation of Determinants of Dense Matrices*

Session 9: Symbolic-Numerics
M.A. Hitz, E. Kaltofen, Y.N. Lakshman: *Efficient Algorithms for Computing the Nearest Polynomial with a Real Root and Related Problems*, R.M. Corless, M.W. Giesbrecht, D.J. Jeffrey, S.M. Watt: *Approximate Polynomial Decomposition*, D. Villard, M.B. Monagan: *ADrien: an implementation of Automatic Differentiation in Maple*

Session 10: System Issues
N.J. Doye: *Automated Coercion for Axiom*, L. Bernardin, B. Char, E. Kaltofen: *Symbolic Computation in Java: An Appraisement*, L. Lamben, V. Pascual, J. Rubio: *Specifying Implementations*, A.A. Adams, H. Gottliebsen, S.A.

Linton, U. Martin: *Automated theorem proving in support of computer algebra: symbolic definite integration as a case study*

Invited Talk 3
Bernd Sturmfels: *Gröbner Deformations of Hypergeometric Differential Equations*

Session 11: Differential and Difference Equations II
D. Boucher: *About the polynomial solutions of homogeneous linear differential equations depending on parameters*, S.A. Abramow, M. van Hoeij: *Desingularization of linear difference operators with polynomial coefficients*, M.A. Barkatou: *Rational Solutions of Matrix Difference Equations. Problem of Equivalence and Factorization*

Session 12: Interface and Communication
O. Arsac, S. Dalmas, M. Gaëtano: *The Design of a Customizable Component to Display and Edit Formulas*, P.S. Wang: *Design and Protocol for Internet Accessible Mathematical Computation*, H. Le, C. Howlett: *Client-Server Communication Standards for Mathematical Computation*

Volker Weispfenning (Passau)

4. EQUADIFF 99

Berlin, 1.8.–7.8.1999

Die Konferenz *International Conference on Differential Equations* (EQUADIFF 99) mit über 600 Teilnehmern fand vom 1.-7. 8. 1999 in Berlin statt. Eine von vielen Minisymposia war *Computer Algebra Tools*, die von Jan Sanders (Vrije Universiteit Amsterdam) organisiert wurde. Die eingeladenen Vorträge waren:
– Algorithms from representation theory (J. Sanders),
– Algorithmic invariant theory and dynamics (K. Gatermann),
– Using symbolic method to classify evolution equations (Jing Ping Wang/J. Sanders),
– A method for computing center manifold and normal forms (Pei Yu).

Karin Gatermann (Berlin)

Computeralgebra-Programm Schoonschip
Ein Meilenstein bei der Renormierung nicht-abelscher Eichtheorien

Die Königlich Schwedische Akademie der Wissenschaften hat den Nobelpreis in Physik für das Jahr 1999 gemeinsam verliehen an:

Professor Gerardus 't Hooft, Utrecht Universität, Utrecht, Niederlande, und
Professor emeritus Martinus J.G. Veltman, Bilthoven, Niederlande.

Entscheidung der Akademie der Wissenschaften:
"für ihre entscheidenden, die Quantenstruktur betreffenden Beiträge zur Theorie der elektroschwachen Wechselwirkung in der Physik".

Einer, der nicht die Hoffnung aufgegeben hatte, nicht-abelsche Eichtheorien renormieren zu können, war Martinus J.G. Veltman. Er war zu Ende der 60er Jahre neu ernannter Professor an der Universität in Utrecht. Veltman hatte ein Computerprogramm **Schoonship** entwickelt, welches symbolisch algebraische Vereinfachungen der komplizierten Ausdrücke durchführte, die sich in allen Quantenfeldtheorien bei quantitativen Berechnungen ergeben. 20 Jahre früher hatte zwar Feynman das Berechnungsproblem systematisiert und die sogenannten Feynmandiagramme, die schnell in der Welt der Forschung angenommen wurden, eingeführt; aber damals gab es keine Computer. Veltman glaubte felsenfest an die Möglichkeit, einen Weg zu finden, um die Renormierung auszuführen, und sein Computerprogramm war ein Meilenstein in der umfangreichen Arbeit, verschiedene Ideen auszutesten.

Im Frühjahr 1969 bekam Veltman einen jungen, 22 Jahre alten Schüler, Gerardus 't Hooft, der seinen Wunsch ausgedrückt hatte, Hochenergiephysik studieren zu dürfen. Nachdem er eine erste kleine Abhandlung geschrieben hatte wurde 't Hooft im Herbst des gleichen Jahres als Doktorand angenommen. Die Aufgabe war, bei der Suche nach einer Methode zur Renormierung nicht-abelscher Eichtheorien mitzuarbeiten. Er war überaus erfolgreich und veröffentlichte schon 1971 zwei Arbeiten, die einen wichtigen Durchbruch im Forschungsprogramm darstellten.

Mit Hilfe von Veltmans Computerprogramm wurde nun 't Hoofts Teilergebnis bestätigt und gemeinsam arbeiteten sie eine funktionierende Berechnungsmethode im Detail aus. Somit war die nicht-abelsche Eichtheorie der elektroschwachen Wechselwirkung eine funktionierende theoretische Maschinerie geworden und man konnte, genau wie vor 20 Jahren, mit genauen Berechnungen beginnen.

Die Aussagen der Theorie werden bestätigt. Wie schon oben dargestellt, sagte die elektroschwache Theorie schon von Anfang an die Existenz der neuen Teilchen W und Z voraus. Aber erst durch 't Hoofts und Veltmans Arbeiten konnte man beginnen, physikalische Größen, bei denen die Eigenschaften von W und Z eine Rolle spielen, genauer zu berechnen. In dem Beschleuniger LEP bei CERN ist es in letzter Zeit gelungen, große Mengen von W und Z unter kontrollierbaren Verhältnissen zu erzeugen. Vergleiche zwischen Messungen und Rechnungen haben immer große Übereinstimmung gezeigt und sie stärken dadurch die Aussagen der Theorie.

Eine spezielle Größe, die ausgehend von den Ergebnissen am LEP mit 't Hoofts und Veltmans Berechnungsmethode erhalten werden konnte, ist die Masse des sogenannten top-Quarks, des schwersten der beiden Quarks, die zu der dritten Familie des Standardmodells gehören. Dieses Quark wurde zum ersten Mal direkt 1995 an dem Fermilabor in den USA beobachtet, aber seine Masse war schon einige Jahre früher vorhergesagt worden. Die Übereinstimmung zwischen Experiment und Theorie war auch hier zufriedenstellend.

Die offizielle Pressmitteilung der Königlich Schwedischen Akademie der Wissenschaften vom 12 Oktober 1999 ist zu finden unter: `http://www.nobel.se/announcement-99/phyty99.html`

Approximative Lösungen von Differentialgleichungen mit Algorithmen der Computeralgebra

Karl Hantzschmann
Universität Rostock

Algorithmen der Computeralgebra beruhen durchgängig auf algebraischen Konzepten und haben das Bestimmen geschlossener (symbolischer) Lösungen zum Ziel. Die Computeranalytik hingegen versteht sich in einem gewissen Sinn als Pendant zur Numerischen Mathematik. Ihr Anliegen besteht vorrangig in der Nutzung von Computeralgebra-Systemen für kontrollierte analytische Näherungslösungen bei nicht geschlossen lösbaren oder nur mit nicht vertretbarem Aufwand lösbaren Aufgaben. Die Zielstellung der Computeranalytik läßt sich wie folgt zusammenfassen:

- Bestimmung analytischer (symbolischer) Näherungslösungen, die die inhärenten Eigenschaften des gegebenen Problems und den möglichen Einfluß von Parametern möglichst gut widerspiegeln
- Formelausdrucke einfach und transparent gestalten bei Gewährleistung realer Genauigkeitsansprüche
- Beurteilung der Genauigkeit der Näherungslösungen durch Fehlerabschätzungen, die ohne manuelle Aufbereitung vollständig vom Computer geliefert werden.

Hierbei kommen klassische und neue Approximationsverfahren der Mathematischen Analysis in Kombination mit Methoden der Computeralgebra zur Anwendung. Symbolische Arbeitstechniken werden mit der bewährten numerischen Nutzung des Computers sinnvoll verbunden. Daraus resultieren für die zum Einsatz kommenden Computeralgebra-Systeme hohe Anforderungen an die Schnittstelle zwischen symbolischen und numerischen Operationen. Die Entwicklung nahm ihren Anfang vor ca. zwei Jahrzehnten in Dresden. Von N. J. Lehmann, von dem entscheidende Impulse dazu ausgingen und der international als Mitbegründer der Computeranalytik gilt, und seinen Schülern wurde eine Reihe von Algorithmen entwickelt und rechentechnisch aufbereitet [3, 4, 9, 10].
Eines der Hauptfelder der Computeranalytik ist das Bestimmen formelmäßiger Näherungslösungen für Differentialgleichungen. Aus den Zielen der Computeranalytik leitet sich ab, dass vor allem solche mathematischen Approximationsverfahren interessieren, die sich einem vorgegebenen Problem automatisch anpassen und mit vertretbarem Aufwand übersichtliche einfache Formelausdrucke liefern.
Gute Resultate in diesem Sinne konnten mit einem Zweistufenkonzept für gewöhnliche Differentialgleichungen erzielt werden. In einem ersten Schritt wird das gegebene Problem durch ein geeignet gewähltes "Nachbarproblem" adaptiert, das mit Algorithmen der Computeralgebra geschlossen lösbar ist. Die Fundamentallösungen fungieren dann in einem zweiten Schritt als Basis für einen angepaßten Näherungsansatz. Wenn also das Problem in der Form $L(y) = 0$ (L gewöhnlicher Differentialoperator der Ordnung n) mit n linear unabhängigen Nebenbedingungen $U(y) = r$ gegeben ist, ersetzt der Adaptionsschritt $L(y)$ durch einen "benachbarten" Differentialoperator hinreichend hoher Ordnung $\tilde{L}(y; a_0, ..., a_m)$. Wenn vertretbar wird der linearen Abhängigkeit von den freien Parametern in der Form $\tilde{L}(y) = \sum_{i=0}^{m} a_i L_i^{n_i}(y)$ der Vorzug gegeben. Die a_i ($i = 0, ..., m$) werden dann mit Hilfe geeignet gewählter "Adaptionskriterien" bestimmt. Mit den über algebraische Methoden ermittelten Fundamentallösungen von $\tilde{L}(y) = 0$ wird im nachfolgenden eigentlichen Approximationsschritt ein Ansatz $\tilde{y} = \sum_{i=1}^{k} c_i \varphi_i$ gemacht. Die Parameter c_i ($i = 1, ..., k$) lassen sich über geeignet wählbare "Approximationskriterien" mit Bezug auf die gegebene Aufgabe unter Berücksichtigung der Nebenbedingungen ermitteln.
Dieses Zweistufenkonzept bietet neben dem Vorteil, eine enge Problemanpassung zu ermöglichen, einen breiten Spielraum zur Entwicklung verschiedener Algorithmen je nach Wahl der verwendeten Approximationskriterien in beiden Schritten und Festlegung der Klasse der Nachbarprobleme. Hinzu kommt, dass dieses Konzept eine zweifache Möglichkeit zur Steuerung der Genauigkeit bietet und den symbolischen und numerischen Berechnungsaufwand entscheidend reduziert.

Ausgehend von diesem einfachen Grundkonzept konnten für verschiedene Aufgabenklassen problemangepaßte Algorithmen entwickelt werden (z. B. [7]). Mit $\tilde{L}$ hat man die Möglichkeit, das System der Ansatzfunktionen dem qualitativen Verhalten der Lösung anzupassen (z. B. Polynome, rationale Funktionen, Exponentialfunktionen, ...). Es gelingt, die große Vielfalt an Projektionsmethoden in dieses Grundkonzept zu integrieren [6]. Noch ungelöst ist die Frage, inwieweit es gelingt, die beiden Approximationskriterien problemangepaßt und genauigkeitsorientiert auszuwählen und damit eine effiziente Steuerung der Genauigkeitsansprüche zu erreichen.
Eine Modifikation dieser Strategie stellt die Entwicklung eines Algorithmus zur näherungsweisen Bestimmung der nichtexponentiellen Lösungen für eine Klasse linearer gewöhnlicher Differentialgleichungen beliebiger Ordnung mit polynomialen Koeffizienten $L(y) = \sum_{i=0}^{n} q_i(x)y^{(i)}(x) = 0$ ($q_i \in K[x], i = 0, ..., n, K$ Konstantenkörper der Charakteristik 0) dar [2]. Der Funktionenraum, in dem sich die Näherungslösung befinden soll, wird durch Differentialoperatoren $\tilde{L}$ festgelegt, die ausschließlich "elementare" Lösungen im Sinne der Differentialalgebra (elementare Erweiterungen von $K(x)$) besitzen und sich dabei in Faktoren der Ordnung 1 mit Koeffizienten aus $\bar{K}(x)$ ($\bar{K}$ algebraischer Abschluß von K) zerlegen lassen. Mit Hilfe von Aussagen zur Struktur der Lösungsfunktionen aus der Computeralgebra lassen sich effiziente Algorithmen aufbereiten, die exakte Lösungen aus der Menge der exponentiellen Funktionen über K, d. h. Funktionen der Form $y(x) = exp(\int u(x)dx)(u \in \bar{K}(x))$, ermitteln, falls solche existieren [1]. Die benötigten Differentialoperatoren 1. Ordnung werden in einer rekursiven Prozedur vom gegebenen Differentialoperator als rechte Linearfaktoren abgespalten.
Näherungslösungen ohne realistische Fehleraussagen sind praktisch wertlos. Das Bereitstellen implementierbarer Fehlerabschätzungen ist deshalb ein zentrales Anliegen der Computeranalytik. Aufbauend auf einem in [8] vorgeschlagenen Konzept hat sich eine Vorgehensweise bewährt, die bei Zugrundelegen einer sinnvoll abgegrenzten Funtionenklasse für die in den Aufgaben auftretenden Koeffizientenfunktionen mit den heute verfügbaren Mitteln an Hard- und Software die vollständig vom Computer ausgeführte Berechnung von Fehlerschranken gestattet. Grundlage bildet die Darstellung der Fehlerfunktion in Form einer Fixpunktgleichung. Als Information über die zu beurteilende Näherungslösung geht die formelmäßig berechenbare Defektfunktion bezüglich der gegebenen Aufgabe ein. Der Integraloperator benutzt die Greensche Funktion zu einer durch Linearisierung des gegebenen Differentialoperators ableitbaren linearen Ersatzaufgabe. Wenn für die dabei auftretenden nichtlinearen Restoperatoren in einer gewissen Umgebung der Näherungslösung spezielle Lipschitz-Bedingungen 2. Ordnung erfüllt sind, führen Fixpunktsätze zu den gewünschten Abschätzungen. Da die Greensche Funktion im allgemeinen nicht exakt berechenbar ist, wurden in mehreren Arbeiten Möglichkeiten für Normabschätzungen untersucht und für den gewünschten Zweck praktikabel gemacht.
Die automatische Berechnung von Fehlerabschätzungen setzt voraus, dass für die bei nichtlinearen Aufgaben auftretenden Lipschitz-Beziehungen praktikable Abschätzungen gefunden werden können. Möglich wird dies durch Implementierung eines angepaßten "Lipschitz-Kalküls" auf der Basis der speziell für diesen Zweck geeigneten Abschätzungen 2. Ordnung [10]. Es werden Lipschitz-Beziehungen für alle an der Aufgabenklasse beteiligten Basisfunktionen bereitgestellt. Gemäß der analysierten Syntaxstruktur der abzuschätzenden Formel wird daraus die Gesamtabschätzung zusammengesetzt. Anwendung finden dabei relativ komplexe Ableitungsregeln für Addition, Subtraktion, Multiplikation und Substitution von bereits abgeschätzten Teilformeln.
Die hier kurz skizzierte Anwendung von Computeralgebra-Systemen zur Berechnung analytischer Näherungslösungen für gewöhnliche Differentialgleichungen und der dazu gehörigen Fehleraussagen veranschaulicht die für Algorithmen der Computeranalytik typische Nutzung von Computern in einer gemischt symbolisch-numerischen Weise.
Im Vergleich zu den enormen Fortschritten der letzten Jahrzehnte im Bereich der Entwicklung, Implementierung und Anwendung von Algorithmen der Computeralgebra steht die Entwicklung des Konzeptes, Computeralgebra-Systeme für kontrollierte Näherungslösungen in Analogie zur Numerischen Mathematik zu nutzen, sicher erst am Anfang und bedarf weiterer intensiver Forschungs- und Entwicklungsarbeit.

Literatur:

[**1**] O. Becken. Algorithmen zum Lösen einfacher Differentialgleichungen. Rostocker Informatik-Berichte 17, Universität Rostock, 1995

[**2**] O. Becken. On adaptive approximation and D-finite functions. Dissertation Universität Rostock, 1999

[**3**] K. Hantzschmann. Implementierbare Fehlerabschätzungen für Näherungslösungen von Randwertaufgaben bei Systemen gewöhnlicher Differentialgleichungen. Studientexte Weiterbildungszentrum für Mathematische Kybernetik und Rechentechnik / Informationsverarbeitung 73, Technische Universität Dresden, 1984

[**4**] K. Hantzschmann. Probleme und Algorithmen der Computeranalytik. In Mitteilungen der MGDDR / Mathematikerkongress, Bd. 2, S. 61-67. MGDDR, 1990

[**5**] K. Hantzschmann. Concepts and algorithms of Computer Analysis for an approximate solution of ODEs. Rostocker Informatik-Berichte 21, Universität Rostock, 1998

[**6**] K. Hantzschmann, A. Jung. Adaptive Approximation zur näherungsweisen Lösung von Differentialgleichungen. Rostocker Informaitk-Berichte 18, Universität Rostock, 1995

[**7**] K. Hantzschmann, N. X. Thinh. Analytical approximate solution of singular ordinary differential equations. In D. Shirkov, V. Rostovtsev, and V. Gerdt, editors, IV. International Conference on Computer Algebra in Physical Research, Dubna, UdSSR, 22-26 May 1990, pages 169-174, Singapore, 1991. World Scientific Publishing.

[**8**] N. J. Lehmann. Fehlerschranken für Näherungslösungen bei Differentialgleichungen. Numerische Mathematik, S. 261-288,1967

[**9**] N. J. Lehmann. Computer algebra and practical analysis. In B. Buchberger, editor, EUROCAL'85, European Conference on Computer Algebra, Linz, April 1-3, 1985, Proceedings Vol. 1: Invited Lectures, volume 203 of Lecture Notes in Computer Science, pages 102-113, Berlin-Heidelberg-New York, 1985. Springer-Verlag

[**10**] N. J. Lehmann. Die Analytische Maschine - Grundlagen einer Computer-Analytik. In Sitzungsberichte der Sächsischen Akademie der Wissenschaften zu Leipzig, Mathematisch-naturwissenschaftliche Klasse, volume 118,4. Akademie Verlag, Berlin, 1985 2

Laptop zum Spicken
Erstmals durften Schüler beim Abitur Computer benutzen

Papier, Bleistift und ein bißchen was zum Essen hatte sich Fabian Hust für seine Abiturprüfung eingepackt. Der sperrigste Gegenstand in seinem Ranzen aber war ein kleiner, schwarzer Laptop. Mit den tragbaren Computern haben der 19jährige Reutlinger Gymnasiast und 59 weitere Schüler in Baden-Württemberg vor kurzem ihr Mathematik-Abitur bestritten.

Mit einem Computer-Algebra-System (CAS) hatten sie Kurvenscharen und Systeme mit sieben Gleichungen darzustellen. Die Festplatten ihrer Rechner wurden vor der Prüfung nicht kontrolliert. Grundsätzlich, so einer der betreuenden Lehrer, hätten diese Abiturienten damit über den „größten Spickzettel" der Welt verfügt.

Das „Pilotprojekt Mobiles Klassenzimmer" ist wohl die konsequenteste Erprobung des Einsatzes neuer Techniken im deutschen Schulunterricht. „Selbst europaweit einzigartig", urteilt der Leiter der Geschäftsstelle „Schulen ans Netz", Michael Drabe. Dabei hat sich der Quantensprung fast unbemerkt vollzogen, so als hätten die Beteiligten noch Angst vor der eigenen Courage. Bilanz ziehen wollen die beteiligten Projektschulen in Karlsruhe, Lörrach, Backnang und Reutlingen, die zuständigen Oberschulämter und das betreuende Staatliche Seminar für Schulpädagogik in Karlsruhe erst nach dem Abitur.

Drei Jahre lang haben die Grund- und Leistungskursschüler der vier Klassen viele Stunden ihres Mathematikunterrichts am Computer absolviert. Neidisch beäugt von ihren Mitschülern, haben sie ihre schicken Laptops mit sich herumgetragen und teilweise auch in anderen Fächern eingesetzt, zum Beispiel für das Verfassen von Deutschaufsätzen oder beim Erstellen eigener Homepages fürs Internet. Immerhin 1,2 Millionen Mark ließ sich das baden-württembergische Kultusministerium die teuren Geräte kosten und beschaffte mit dem Computerprogramm Maple eine Software, die auch in Forschung und Wissenschaft Verwendung findet.

Maple ermöglicht die Bearbeitung schwierigster mathematischer Operationen, übernimmt lästige Rechenarbeit und liefert auf Knopfdruck die Ergebnisse von gewaltigen Gleichungssystemen, Darstellungen von Funktionen und Lösungen für Differentialgleichungen, die bislang Stoff für das vierte Hochschulsemester waren. Aber darf die Arbeit mit dem Computer ein so starkes Gewicht im Mathematikunterricht gewinnen? Darüber diskutieren nun die Beteiligten. „Eine ähnliche Diskussion hatten wir schon bei Einführung des Taschenrechners", sagt Ulrich Rauscher vom Gymnasium in der Taus in Backnang. „Können Sie heute noch eine Wurzel ziehen ohne Taschenrechner?" fragt Ernestina Dittrich vom Karlsruher Helmholtz-Gymnasium, und Michael Komma, der Lehrer von Fabian und einer der Vorreiter des CAS-Einsatzes in der Schule, signiert jede seiner E-Mails mit dem Leibnizschen Satz: „Denn es ist eines ausgezeichneten Mannes nicht würdig, wertvolle Stunden wie ein Sklave im Keller der einfachen Berechnungen zu verbringen."

Während ihres Spezial-Abiturs durften die Laptop-Schüler alle Rechenschritte anwenden, die sie im Unterricht auf sogenannten Worksheets erarbeitet haben. „Das nützt aber nur dann etwas, wenn man weiß, welchen Lösungsweg man gehen muß", sagt Fabian Hust. Zur Vorbereitung auf die Prüfung hatte er seine gutsortierte Worksheet-Sammlung noch einmal durchgearbeitet. Unruhig machte ihn vor allem, daß er und seine Mitschüler als Vorboten das Neuland der elektronischen Reifeprüfung betreten. „Ein Abi mit dem Computer hat es schließlich noch nie gegeben, wer weiß, was für Aufgaben wir da kriegen", sorgte sich der Abiturient. In seinem zweiten Hauptprüfungsfach Chemie gebe es wenigstens Aufgabensammlungen, da wisse man ziemlich genau, was einen erwartet.

Für die Freigabe aller erarbeiteten Operationen spricht, daß die Schüler dann kreativ mit dem Rechner umgehen können. „Vier oder fünf verschiedene Lösungswege für eine Aufgabe habe ich bei meinen Schülern im Abitur gesehen", sagt Rauscher voller Begeisterung. Genau darin sehen alle Beteiligten den Hauptvorzug des Softwarepakets. Statt Gleichungen nach Schema F zu lösen, sollen die Schüler einen realen Sachverhalt mathematisch erfassen und in eine Gleichung umsetzen können. „Mehr mathematisches Verständnis, weniger Drill", sagt Hans Selinka vom Oberschulamt Tübingen. Im herkömmlichen Mathematikunterricht fehlt dazu häufig die Rechenmacht, mit einem CAS kann die inhaltliche Arbeit in den Vordergrund rücken.

Wie müssen Milchtüten geschnitten werden, damit das Verpackungsmaterial optimal genutzt ist? Wie verändern sich Populationen über mehrere Generationen in Abhängigkeit von verschiedenen Faktoren? Welche Phänomene ergeben sich beim Billardspiel mit gekrümmten Banden? „Die Schüler haben in Seminararbeiten Phantastisches abgeliefert", räumt Dieter Koller vom Seminar für Schulpädagogik ein, obwohl der zweite Bericht der Karlsruher Pädagogen kritisch mit dem Computereinsatz ins Gericht ging. „Es besteht schon die Gefahr, daß die Schüler das Wissen, das sie auf dem Laptop mit sich herumtragen, mit dem Wissen im Kopf verwechseln", sagt Koller. Vor allem die Abhängigkeit vom elektronischen Gehirn müsse aber vermieden werden.

Und die Abhängigkeit fängt schon bei lapidaren Dingen an: ohne Strom im Klassenraum kein digitales Abitur. Sicherungsdisketten und Ersatzgeräte für die nicht immer zuverlässigen Laptops sollten technische Probleme vermeiden helfen. Seine Arbeitspapiere hatte Fabian vorher noch auf eine CD gebrannt, für alle Fälle. Die Fehleranfälligkeit der Laptops, die dem Streß täglicher Fahrradfahrten in Rucksäcken und Ranzen kaum gewachsen waren, stellte dann auch tatsächlich eines der größten Probleme für Lehrer und Schüler dar. Am Ende des Abiturexperiments atmeten alle Beteiligten noch ein bißchen mehr auf als nach der normalen Abiturklausur.

Für die nächste Runde will die Mehrzahl der Schulen auf weniger empfindliche Tischgeräte setzen. Voraussetzung sind dann eine ausreichende Ausstattung der Schulen - im nächsten Schuljahr werden es mindestens doppelt so viele sein - und der Zugang zum Computer daheim. Die Ausbreitung in die Fläche dürfte noch ein Weilchen dauern. Geld vom Land aber gibt es für die zweite Runde nicht mehr. Walter Kinkelin, im baden-württembergischen Kultusministerium für das Projekt verantwortlich, kann sich da auch eine kleine Lösung mit billigeren programmierbaren Taschenrechnern vorstellen. Weniger Computereinsatz als im ersten Durchgang wünscht sich auch Dieter Koller. An den vier Projektschulen aber will man sich von PC und Maple nicht mehr trennen. Auch die „Abfallprodukte" Erfahrung mit Textverarbeitung, Umgang mit dem Internet bis hin zur Netzwerkbetreuung werden allseits als Schlüsselqualifikationen gelobt.

Mehr Mut fordert vor allem Michael Komma, der in seinen eigenen Zwischenbericht schrieb: „Wir müssen Chancen der Technologie voll ausloten." Dabei will er gar nicht auf Tafel und Kreide verzichten, die Lehrer keineswegs durch Computer und Internet ersetzen. Das virtuelle Klassenzimmer ist für ihn aber schon lange keine Vision mehr. Fast rund um die Uhr kann er Fragen seiner Schüler beantworten, als Fortschreibung der gemeinsam erarbeiteten Ergebnisse entsteht ein elektronisches Lehrbuch. Umsonst wird das bei allem Engagement der Lehrer nicht zu haben sein, denn selbständig lernende Schüler wollen individuell betreut werden.

Trotz aller positiven Erfahrungen des Modellversuchs: Der richtige Weg ist noch umstritten, die Fragen: „Wieviel Arbeit darf der Computer dem Schüler abnehmen?" und: „Wieviel Computer schadet dem Schüler?" sind noch nicht beantwortet. Doch Michael Komma ist überzeugt: „In der vernetzten Welt von morgen werden unsere Schüler genauso geprüft werden, es wäre falsch, sie nicht schon heute darauf einzustimmen."

Monika Ermert (`m.ermert@gmx.de`)

Computeralgebra-Systeme in der Schule
Erfahrungen in Deutschland

Vor ca. 30 Jahren wurden Werkzeuge entwickelt, die symbolische Manipulationen erlauben, seit ca. 10 Jahren wird der Einfluss von derartigen Computeralgebra-Systemen (CAS) auf den Mathematikunterricht in Deutschland diskutiert. Was zunächst wie die Diskussion von einigen Visionären aussah, hat sich in den letzten Jahren sehr stark verändert. Durch die Entwicklung kleiner Hardwaresysteme, sogenannten Taschencomputern, die eine Computeralgebra implementiert haben, ist der Druck auf Schule und Universität deutlich größer geworden, sich dem Thema „Mathematikunterricht mit CAS" ernsthaft zu stellen. Schon 1991 fragte Wilfried Herget auf der 9. Tagung des Arbeitskreises Mathematik und Informatik der GDM: „Wieviel Termumformungen, Kurvendiskussionen,... braucht der Mensch?". Eine befriedigende Antwort hierauf ist bisher noch nicht gefunden worden, doch hat diese zentrale Frage seither immer wieder sowohl Hochschuldidaktiker als auch Mathematiklehrer beschäftigt.

Der Einzug von Graphikrechnern (GTR) und Taschencomputern (TC) in den Unterricht ist in den einzelnen Bundesländern unterschiedlich realisiert worden. Einerseits sind in einzelnen Ländern (Nordrhein-

Westfalen [3], Baden-Württemberg [2], Niedersachsen [1], Sachsen [4]) hierzu offizielle Schulversuche durchgeführt und ausgewertet worden, andererseits gab es im ganzen Bundesgebiet lokale Versuche von engagierten Lehrern, CAS als Werkzeug in den Unterricht zu implementieren. Besonderes Interesse lag dabei neben der Frage, wie sich der MU mit diesem neuen Werkzeug ändert, auch die, wie Prüfungen mit CAS gestaltet werden sollen.

In Deutschland sind Kultusangelegenheiten Ländersache. Damit haben sich unterschiedliche Bedingungen für den Einsatz von GTR und CAS ergeben. Der Einsatz ist häufig von folgenden eher formalen Aspekten abhängig:

- Ist der Einsatz von TR ganz allgemein gesetzlich geregelt?
- Sind Hinweise in den Richtlinien Mathematik zum Einsatz von Hard- und Software enthalten?
- Welche Bedingungen gelten in Prüfungen, insbesondere im Abitur, für den Einsatz von Soft- und Hardware?
- Welche offizielle Unterstützung wird dem Einzug von Hard- und Software zuteil?
- Welche Möglichkeiten haben die Schulen vor Ort, individuell den Einsatz von Hard- und Software zu regeln?

Die deutlichste Wirkung auf die unterrichtenden Lehrer hat dabei die Frage, wie der Einsatz von entsprechender Hard- und Software im Abitur geregelt ist. Der Einsatz in der finalen Schulprüfung ist für viele das zentrale Argument für oder gegen den Einsatz derartiger Systeme. Dieses ist gut nachvollziehbar, weil sich mit dem Einsatz von CAS sowohl in den Inhalten als auch in den Formen des Unterrichtes vieles verändert. Wenn diese Veränderungen durch die anstehende Abiturprüfung egalisiert werden, sind massive Konflikte vorprogrammiert. In Baden-Württemberg hat man sich daher entschlossen, die im Pilotprojekt „Mobiles Klassenzimmer" [2], siehe auch Rundbrief Nr. 24, integrierten Lerngruppen aus dem allgemeinen zentralen Abitur herauszulösen und gesonderte zentrale Prüfungsaufgaben zu erstellen.

Dadurch, dass die Länder die Kultushoheit haben, haben sich unterschiedliche Formen der Abschlussprüfungen entwickelt. Die wesentlichen Unterschiede liegen darin, dass in einigen Länder beim Abitur zentral gestellte, in anderen individuell gestellte Prüfungsfragen von den Abiturienten zu bearbeiten sind. Dieses hat sowohl Auswirkungen auf den vorangehenden Unterricht als auch auf die Art der Prüfungsfragen. In Ländern mit Zentralabitur sind die Prüfungsaufgaben bisher deutlich stärker strukturiert, um allen Schülern unabhängig von der Form des vorangegangenen Unterrichtes einen entsprechenden Zugang zu den zentralen Problemen zu ermöglichen. Erste Ansätze zu einer Öffnung der Aufgaben sind z. B. in Baden-Württemberg zu beobachten. Länder ohne Zentralabitur haben hier sehr viel mehr Handlungsspielraum und können auf individuelle Schwerpunkte deutlich flexibler eingehen. Dieses macht sich auch beim Einsatz von CAS bemerkbar. Eine der Forderungen, sich von konvergenten Aufgaben hin zu mehr offenen Problemstellungen und divergenten Aufgaben zu bewegen, Modellierungsaspekte mehr einzubeziehen, lässt sich einfacher realisieren, wenn man sowohl beim Unterricht als auch in Prüfungen auf die Besonderheiten der Lerngruppe eingehen kann. Im Gegensatz hierzu haben erste Erfahrungen in Baden-Württemberg mit CAS Abitur gezeigt, dass bei zentralen Prüfungsfragen viele Aspekte neu überdacht werden müssen.

Global ist in der Bundesrepublik zu beobachten, dass Computeralgebrasysteme in den Schulen auf dem Vormarsch sind. Nach einer Erhebung im Jahr 1999 von Texas Instruments sind heute in weit mehr als der Hälfte der Bundesländer (Niedersachsen, Schleswig-Holstein, Rheinland-Pfalz, Nordrhein-Westfalen, Hessen, Hamburg, Bremen, Brandenburg, Mecklenburg-Vorpommern, Sachsen-Anhalt, Thüringen (jeweils nicht in Prüfungen); Baden-Württemberg (mit Einschränkung auf Schulversuche) Computeralgebrasysteme im Unterricht erlaubt. Gegenüber der ersten Erhebung (1996, Texas Instruments) hat sich hier ein dramatischer Wandel ergeben. Damals waren in ca. der Hälfte der Bundesländer lediglich GTR in Unterricht und Prüfung erlaubt, in den anderen Ländern waren sie in den Prüfungen und im Unterricht verboten. Der Einsatz von CAS war zu diesem Zeitpunkt in keinem Bundesland zentral geregelt.

In Niedersachsen, wo in den letzten zwei Jahren ein starker Anstieg der Schulen, die CAS im Unterricht einsetzen, zu beobachten ist, sind die Voraussetzungen für den Einsatz von GTR und CAS eher günstig:

- Es gibt keinen offiziellen Taschenrechnererlass mehr. Die Einsicht, dass man nicht bei jeder neuen Rechnergeneration die Bedingungen für den Einsatz haarklein vorgeben kann, haben dazu geführt, dass nur noch auf der Basis des Gleicheitsgrundsatzes lokal von den einzelnen Schulen über den Einsatz von Hard- und Software entschieden wird.

- In den neu zu entwickelnden Rahmenrichtlinien für die Sekundarstufe I und II wird davon ausgegangen, dass in der Sekundarstufe I alle Schülerinnen und Schüler einen graphikfähigen Taschenrechner besitzen und in den Schulen Zugang zu weiterer Software haben. In der Sekundarstufe II wird darüber hinaus der Einsatz von CAS als ein neues Werkzeug vorgesehen.

- In den neuen Einheitlichen Prüfungsanforderungen im Abitur sind alle Hard- und Software zugelassen, wenn der Gleichheitsgrundsatz gewährleistet ist. Der Einfluss dieser Werkzeuge auf die zu bearbeitenden Problemstellungen muss vom einreichenden Lehrer erläutert werden, die Problemstellungen sind entsprechend dem zur Verfügung stehenden Werkzeug auszuwählen. Darüber hinaus ist bei der Bearbeitung der Prüflinge darauf zu achten, dass sie hinreichend Raum haben, ihre Lösungsstrategien sachgerecht zu dokumentieren.

- Durch die Empfehlung der Mathematikkommission für einen zukünftigen MU am Gymnasium wird der Einsatz von Hard- und Software entsprechend unterstützt. Im Sommer 1999 hat die Kultusministerin in einem Erlass darüber hinaus den Einsatz von GTR und Taschencomputern mit CAS in den entsprechenden Schulstufen gefordert.

- Aufgrund der Erlasslage und der Diktion des Ministeriums können die Schulen auf der Basis von Rahmenrichtlinien und Einheitlichen Prüfungsanforderungen Abitur individuell den Einsatz von Hard- und Software planen und durchführen.

- Das Ministerium hat beschlossen, alle Mathematiklehrer im Gymnasium verbindlich im Sinne der Ideen der Mathematikempfehlungen in den nächsten Jahren fortzubilden. Themenschwerpunkte werden hierbei Einsatz und Einfluss von GTR, CAS und DGS im Unterricht sein.

Trotzdem nutzen z. Z. nur ein Teil der Kollegen die Möglichkeit, diese neuen Technologien im Unterricht einzusetzen. Bisher liegen erste Erfahrungen (ca. 10 Schulen) zum Einsatz von CAS im Abitur vor (2 Jahrgänge), sie sind aber noch nicht ausgewertet. Da in einigen Landesteilen GTR und TC sich zunehmend mehr an den Schulen verbreiten, ist aber damit zu rechnen, dass in den nächsten Jahren auch im Abitur diese Geräte Eingang haben werden. Durch die Ablösung des wissenschaftlich-technischen Taschenrechners durch einen GTR werden mittelfristig alle Prüfungsaufgaben auf dieser neuen Folie entwickelt werden.

Erste Ergebnisse aus einem Schulversuch in Niedersachsen zum Einsatz von TC im MU

Im Schuljahr 1996/97 hat in drei Gymnasien ein halbjähriger Schulversuch zum Thema „Einsatz des Taschencomputers TI 92 im Mathematikunterricht des Gymnasiums" stattgefunden. Die Geräte wurden in einer der beteiligten Schulen in mehreren Lerngruppen für die Dauer von jeweils ca. 4 Wochen, in den beiden anderen im gesamten Beobachtungszeitraum jeweils in nur einer Lerngruppe (LK 12) eingesetzt. Durch unterschiedliche Konzepte wurde gewährleistet, dass die Beobachtungen neben dem vollintegrierten auch den teilintegrierten Einsatz des Rechners berücksichtigten.

Aus den Beobachtungen der Kolleginnen und Kollegen und den Erfahrungen der Schülerinnen und Schüler läßt sich ein erstes vorläufiges Resümee ziehen [1]. Die hierbei gemachten Beobachtungen decken sich weitgehend mit denen aus der österreichischen Untersuchung zum Einfluss des TI 92 im MU und den Ergebnissen des Pilotprojektes „Mobiles Klassenzimmer" in Baden-Württemberg:

- Beim Einsatz des TC werden einerseits mathematische Verständnisdefizite klarer aufgezeigt, da Schülerinnen und Schüler sich durch Entlastung bei Termumformungen nicht mehr hinter der schematischen Anwendung des Kalküls verstecken können. Andererseits können durch den Einsatz des TC Mängel in der Kalkülkompetenz (Lösen von Gleichungen, korrektes Differenzieren und Integrieren) „gestopft" werden, so dass diese nicht mehr von dem Auffinden der Problemlösung ablenken. Leistungsstarken Schülerinnen und Schülern eröffnen sich durch das neue Werkzeug neue Perspektiven, die sie zu kreativem Umgang mit Mathematik anregen können. Sowohl leistungsstarke als auch leistungsschwache Schülerinnen und Schüler können dadurch von dem Rechner deutlich profitieren. Bei Schülerinnen und Schülern mit bisher befriedigenden Leistungen wird durch den Einsatz des Rechners die Tendenz ihrer Leistungsfähigkeit deutlicher: diejenigen, die gute Ideen aber Schwächen in der Umsetzung haben, werden durch das Werkzeug entlastet und können ihre Lösungsideen eher umsetzen; diejenigen, deren Leistung sich primär auf sicheren Umgang mit dem Kalkül stützt, werden durch veränderte Anforderungen im Unterricht und den Klausuren diese Leistungsstärke nicht mehr so zur Geltung bringen können.

- Durch verstärkten Einsatz des Rechners wird ohne entsprechende Gegensteuerung die Kalkülkompetenz der Schülerinnen und Schüler geringer. Andererseits kann gerade der Rechner dazu anregen, der äußeren Form nach unterschiedliche Terme mit klassischen Mitteln auf Gleichheit zu überprüfen. Die geringere Kalkülkompetenz wirkt sich aber nach den bisherigen Beobachtungen nicht auf die Fähigkeit aus, inner- und außermathematische Probleme unter Einsatz dieses Rechners zu lösen. Lösungswege sind häufiger „kreativer", da die

Besorgnis der nicht erfolgreichen Bearbeitung des algebraischen Problems gering ist. Es bleibt abzuwarten, wie sich die Forderungen an die Kalkülkompetenz durch verstärkten Einsatz von Computeralgebrasystemen in allen Lebensbereichen (vergleichbar dem des Taschenrechners) langfristig verändern werden.

- Durch den Einsatz des Rechners wird das Gespräch über Mathematik deutlich befruchtet. Unterschiedliche Ansätze und Lösungsstrategien, deren Vergleich nicht mehr durch fehlerhafte Termumformungen „belastet" ist, fordern zu Fragen und Diskussionen heraus, die weit über das bisher übliche hinausgehen. Es ist jetzt weniger das „wie" sondern eher das „warum" Zentrum der gemeinsamen Betrachtung eines Lösungsweges. Die Sprache der Schülerinnen und Schüler orientiert sich dabei stark an den kompakten Befehlen des CAS, „dann wenden wir den Solver an",.... Das Gespräch über die Sache wird auch in den jetzt andersartigen Dokumentationen über das „Tun" deutlich, die durch längere Textpassagen mit mathematischen Begründungen gekennzeichnet sind. Diese neue Qualität der Reflexion inner- und außermathematischer Probleme im Unterricht wird durch den Einsatz des TC stark forciert.
- Geschlechtsspezifische Unterschiede im Umgang und Einsatz des TC wurden um so deutlicher, je später eine Erstbegegnung mit diesem neuen Werkzeug geschah. Bei Schülerinnen und Schülern der Klassenstufe 7 und 8 waren keine Unterschiede erkennbar, das neue Werkzeug wurde in gleicher Weise zur Lösung, Kontrolle und zu weiterführenden Experimenten eingesetzt. In höheren Klassen (9 - 11) wurden Unterschiede dann deutlich, wenn auch unterschiedliche Vorerfahrungen mit Computern allgemein vorhanden waren. Bei Schülerinnen und Schülern der Grundkurse waren diese „Rollen" noch deutlicher ausgeprägt, im Leistungskurs waren dagegen geschlechtsspezifische unterschiedliche Zugänge zum Rechner nicht erkennbar.
- Im Rahmen der Untersuchung war insbesondere in Lerngruppen, in denen der TC langfristig eingesetzt wurde, zu beobachten, dass sich die Unterrichtsinhalte nicht mehr so stark am Kalkül orientierten. Innermathematische Fragestellungen konnten vielschichtiger untersucht werden (Interpolation und Extrapolation, vielschichtige Ansätze der Integralrechnung, numerische Verfahren,...), außermathematische Anwendungen waren durch den Einsatz des TC überhaupt erst sinnvoll geschlossen zu bearbeiten. Reales Datenmaterial mußte nicht erst manipuliert werden, sondern konnte in der vorgelegten Form weiterverarbeitet werden, dadurch konnten reale Problemstellungen mit mathematischen Modellen sinnvoll behandelt werden. Für die Schülerinnen und Schüler stellte sich die Frage nach der Sinnhaftigkeit des eigenen Handelns im Mathematikunterricht nicht mehr in der sonst vorhandenen Form, da sie zu realen Problemen Lösungsmodelle und Strategien weitgehend selbständig entwickeln konnten. Der Taschencomputer bietet Möglichkeiten, Probleme auf unterschiedlichen Betrachtungsebenen (graphisch, tabellarisch, algebraisch) zu bearbeiten und sich Sachverhalte vielseitig zu veranschaulichen. Diese neue Qualität des Mathematikunterrichts, problemlos auf unterschiedlichen Ebenen zu arbeiten, bietet den Schülerinnen und Schülern die Chance, ihre individuellen Lösungsstrategien umzusetzen. Die Abgrenzungen der Ebenen einerseits und ihre Verknüpfung andererseits werden durch ein derartiges Werkzeug initiiert.
- Aufgrund der Vielzahl von Variationsmöglichkeiten kommen die Schülerinnen und Schüler selbständig zu neuen Fragestellungen, erhalten eine Fülle von Anschauungsmaterial, wodurch sich die Durchdringung des Stoffes vertiefen kann.
- Bei schriftlichen Lernzielkontrollen konnte festgestellt werden, dass sich nach entsprechenden Anlaufschwierigkeiten keine wesentlichen neuen Probleme ergaben. Es konnte beobachtet werden, dass mit zunehmender Veränderung des Unterrichtes in Hinsicht auf den Umfang des Rechnereinsatzes auch die Klausuren so gestaltet wurden, dass die Benutzung des TC nur nebensächlich wurde. Statt der klassischen Anfertigung einer Zeichnung oder Skizze, die bei Einsatz des integrierten Funktionenplotters nur noch sehr eingeschränkt Sinn macht, wurden z.B. Zeichnungen vorgegeben, die entsprechend weiter zu untersuchen bzw. zu interpretieren waren. Bei Funktionsbetrachtungen z. B. wurde eine breite Untersuchung zugunsten einer starken Fokussierung auf Einzelaspekte mit anschließender Variation verworfen. Die klassische Kurvendiskussion verliert ihren Stellenwert, dennoch bleiben einzelne Aspekte erhalten und gewinnen im anderen Kontext neue Bedeutung.

Insgesamt ist festzustellen, dass der teilintegrierte Ansatz beim Einsatz des TC sich in den beobachteten Lerngruppen nur sehr eingeschränkt bewährt hat, da die Schülerinnen und Schüler sich nicht in dem gewünschten Umfang mit dem Rechner vertraut machen konnten. Der lokale Einsatz in einzelnen ausgewählten Unterrichtsstunden führt aufgrund mangelhafter Kenntnisse in der Benutzung des TC eher zu negativen Auswirkungen. Erst der vollintegrierte Ansatz, der den Einsatz des TC jederzeit im Unterricht, zu Hause und in den Klausuren vorsieht, führt dazu, dass der Rechner als natürliches Werkzeug im MU angesehen wird. Mit zunehmender Einsatzdauer der Rechner ist insgesamt zu beobachten, dass der Umfang seines direkten Einsatzes eher rückläufig ist. Dieser scheinbare Widerspruch erklärt sich daraus, dass Themen und Inhalte des Unterrichtes und der Klausuren sich von ergebnis- und kalkülorientierten Aufgaben hin zu inner- und außermathematischen Problemen orientiert. Dabei ist der Rechner im Hintergrund als mächtiges Werkzeug stets latent vorhanden, das den Unterricht in vielen Bereichen von „Berechnungen" (Differenzieren, Integrieren, Lösen von Gleichungen, Termumformungen,...) entlastet und damit den Blick für zentrale Fragestellungen freigibt. Allein die Existenz des Taschencomputers in Schülerhand fordert den Lehrer auf, sich zusammen mit seinen Schülerinnen und Schülern Problemstellungen zu widmen, deren Lösung von der sicheren Beherrschung von Termumformungen nicht mehr unmittelbar abhängig sind. Die klassische Kurvendiskussion verliert weitgehend ihren Stellenwert, da sie fast ausschließlich auf die Beherrschung im Sinne einer korrekten Durchführung des Kalküls ausgerichtet ist. Außerdem sind die im Unterrichtsalltag breit angelegten Kurvendiskussionen nur sehr eingeschränkt dazu geeignet, für die Schülerinnen und Schüler ein gültiges Bild von Mathematik zu erzeugen.

Wenn Schülerinnen und Schüler durch einen derartigen Mathematikunterricht geprägt werden, werden sie mit anderen Kompetenzen als bisher die Schule verlassen und die Universität besuchen. Hierauf muss sich auch die Universität neu einstellen.

Literatur

[1] Niedersächsisches Kultusministerium, Empfehlungen für den Mathematikunterricht an Gymnasien, MK 1998

[2] Henn, H.-W., Schulversuche zum Einsatz von CAS in Baden-Württemberg, mathematica didactica, vol. 2, p. 18-27, 1996

[3] Landesinstitut für Schule und Weiterbildung, Mathematik mit CAS, Der Schulversuch in NRW, Soest 1998, `http://www.learn-line.nrw.de`

[4] Sächsisches Staatsinstitut für Bildung und Schulentwicklung, Comenius-Institut, `http://marvin.sn.schule.de/~ci/`

Heiko Knechtel (Bückeburg, `HKnechtel@aol.com`))

The Dutch Perspective

Computer algebra has been an issue in mathematics education in the Netherlands for some years already. This does not imply that the discussion on this phenomenon has resulted in an agreement; no consensus on the role of computer algebra in the mathematics classroom has emerged so far.

Below, I describe some recent developments in my country from a personal perspective. I confine myself to mathematics education at upper secondary, pre-university level.

Firstly, I describe the Dutch situation concerning curriculum and assessment. Secondly, I briefly consider the first educational experiments with computer algebra. Thirdly, the rise of the graphics calculator is discussed. In the end, computer algebra comes into the picture again, but now in a hand-held format. I conclude with an imaginary jump into future.

Understanding the developments in my country requires some knowledge of the organisation of the curriculum and assessment.

As far as the curriculum is concerned, it is important to notice that there is no detailed curriculum that prescribes which topic should be taught when. The curriculum is defined by a description of skills and concepts that will be assessed by the end of secondary school; the schools are free to choose how they get there. They can also decide on the textbooks they want their students to use. It is because of this relative freedom that the final assessment is so important.

The final assessment at upper secondary level consists of two parts: a school set assessment and a final national examination that is externally set and internally graded. This national examination is very important for the implementation of technology; if a certain technology device is not allowed at the final examination, it will not easily become popular in the classroom. The current regulation is that the graphics calculator is required at the final examination, whereas computer algebra is excluded. Two arguments guided this legislation. Firstly, it would be hard to organize a national examination throughout the country with computer access for all the candidates; hand-held computer algebra was not yet available. Secondly, the financial aspect was important. If computer access was required at the final examination, schools would need money to buy them, whereas hand-held technology devices are supplied by the students themselves.

For the school assessment, the authorities recommend the use or partial use of a computer, but again, the schools are free to decide. I have the impression that the number of schools that use a computer in their examination is increasing. The computer is often used in combination with investigation tasks where a written or oral report forms the assessment.

Obviously, the Dutch policy on technology is a careful one. Information about the different strategies concerning technology use and assessment in other countries can be found in [4].

The first project on computer algebra at upper secondary level started in 1990. The idea of this two-year project was to develop short instructional units that were tested in pilot schools. Although the production of these materials was useful, the project as a whole was not very successful. This was caused by the lack of computer facilities at schools and by the difficulties students had with the user friendliness: they had little 'computer literacy' and a windows interface was not available. Obviously, the time was not yet ripe for the implementation of computer algebra at this level.

By the end of this project, a group of volunteering teachers decided to continue the work. This group, called CAVO, existed until 1998 and was a lively and important platform for further development and discussion (see [6]). In the mean time, however, the graphics calculator came on the market, and attracted much attention.

The development of the graphics calculator elicited discussion on which technology platform should be used in secondary education (see [1]). The Dutch authorities decided that the implementation of the graphics calculator would be the first step to take. Therefore, they supported a research project on this issue in 1992. This project was carried out by the Freudenthal Institute, a research group on mathematics education. Later it became an integrated part of a larger curriculum development project called Profi. Results of the Profi-project included student textbooks that integrated the use of the graphics calculator, and experimental examinations that required the availability of a hand-held graphing device. The role of the graphics calculator in this project is summarized in [5].

Some educators and teachers were, however, opposed to the implementation of the graphics calculator. Their arguments were that computer algebra is a much more sophisticated mathematical tool, and that a graphics calculator is only a temporary step backwards compared to the possibilities that PC's offer. In 1996, however, a questionnaire revealed that PC's were hardly ever used during mathematics lessons, although they were available in schools. This supports the idea that real implementation of technology requires that the student has direct access to the device. The limited mathematical power of the graphics calculator is not an important disadvantage: it allows teachers, textbook authors and examination boards to have sufficient time to carefully integrate a graphical and numerical tool without having to cope with computer algebra in the mean time.

The choice of the graphics calculator may be a temporary preference indeed: the symbolic calculator raises the issue again.

Nowadays, computer algebra is also available in a hand-held format. A first pilot experiment using the TI-92 revealed that the students appreciated this machine as an 'algebraic calculator', but not so much as a dynamic geometry tool [3].

When the Dutch Association of Mathematics Teachers became aware of the possible impact of symbolic calculators on secondary mathematics education, an Advisory Board on Computer Algebra and Symbolic Calculator was formed. In May, 1998, this Board concluded that:

- computer algebra should be implemented in upper secondary education;
- research was needed in order to find answers to the pedagogical and curriculum issues that will be raised by this;
- as a computer algebra platform, the PC would be preferred to the symbolic calculator, at least in the long term.

For the full report of the Board (in Dutch!) I refer to the Dutch Association of Mathematics Teachers site: `www.euronet.nl/~nvvw/`.

In the fall of 1998, the Freudenthal Institute conducted an explorative case study using the symbolic calculator. This machine turned out to be quite useful in investigation tasks. The sophisticated use of variables and parameters, however, was not always clear to the students. Furthermore, some students were reluctant to use computer algebra for the application of techniques that they had not yet mastered manually.

At present, many research questions concerning the role of computer algebra in secondary education are still unanswered (see [2]). No decisions on its implementation in the Netherlands have been made so far. In the next few years, I expect three developments to take place.

Firstly, teachers, examination boards and school book authors will get used to the graphics calculator and will take advantage of the pedagogical possibilities that these devices offer.

Secondly, research will be carried out concerning the role of computer algebra in the learning of mathematics and, more specifically, in the learning of algebraic concepts. Such a study was started recently by the Freudenthal Institute.

Thirdly, research will be carried out on the possibilities of computer algebra as a wide-range technology tool. A project that focuses on the use of a computer algebra environment in combination with a text editor (to write mathematical reports) and an Internet browser has been started at the Algemeen Pedagogisch Studiecentrum, an institute for improvement of (mathematics) education.

It is my hope that these developments will lead to a carefully considered implementation of computer algebra in secondary education.

Literatur

[1] P. Drijvers. Graphics calculators and computer algebra systems: Differences & similarities. *The International Derive Journal*, 1(1):71–82, 1994.

[2] P. Drijvers. What issues do we need to know more about: Questions for future educational research concerning CAS. In J. Berry et al., editor, *The state of computer algebra in mathematics education.* Chartwell-Bratt, Bromley, 1997.

[3] P. Drijvers. You never forget your first love ...: The TI-92 in teacher education. *The International Journal on Computer Algebra in Mathematics Education*, 4(1):69–76, 1997.

[4] P. Drijvers. Assessment and new technologies: Different policies in different countries. *The International Journal on Computer Algebra in Mathematics Education*, 5(2):81–93, 1998.

[5] P. Drijvers and M. Doorman. The graphics calculator in mathematics education. *The Journal of Mathematical Behaviour*, 14(4):425–440, 1997.

[6] P. Drijvers, A. Verweij, and E. Van Winsen. Mathematics lessons with Derive developed by the CAVO working group. *Zentralblatt für Didaktik der Mathematik*, 97(4):118–123, 1997.

Paul Drijvers (Freudenthal Institute, Utrecht, Niederlande, `P.Drijvers@fi.uu.nl`)

Der Artikel von Paul Drijvers ist ein Vorabdruck aus

J. Grabmeier, E. Kaltofen, V. Weispfenning (Eds.)
Handbook of Computer Algebra
Springer, 2000
`http://www.springer.de/math/prep/compalg.html`

Wir bedanken uns bei den Herausgebern für die freundliche Erlaubnis.

Heiko Knechtel (Bückeburg, `HKnechtel@aol.com`)
Wolfram Koepf (Leipzig, `koepf@imn.htwk-leipzig.de`)

Publikationen über Computeralgebra

- Becker, T., Weispfenning, V., *Gröbner Bases – A Computational Approach to Commutative Algebra, korrigierter Neudruck*, Graduate Texts in Mathematics, Vol. 141, Springer Verlag, Berlin, Heidelberg, New York, ISBN 3-540-97971-9, 1998
- Jungnickel, D., *Graphs, Networks and Algorithms*, Springer Verlag, Berlin, Heidelberg, New York, ISBN 3-540-63760-5, 1999, pp. 589, 98 DM.

  Das Buch wird in diesem Rundbrief auf Seite 27 besprochen.
- Kerber, A., *Applied Finite Group Actions (2nd edition, revised and expanded)*, Springer Verlag, Berlin, Heidelberg, New York, ISBN 3-540-65941-2, 1999.
- Koblitz, N., *Algebraic Aspects of Cryptography*, Springer Verlag, Berlin, Heidelberg, New York, ISBN 3-540-63446-0, 1998, DM 98,-.

  Das Buch wird in diesem Rundbrief auf Seite 28 besprochen.
- Kress, R., *Linear Integral Equations*, Springer Verlag, Berlin, Heidelberg, New York, ISBN 0-387-98700-2, 1999, DM 120,-.
- Matzat, B.H., Greuel, G.-M., Hiss, G., (Eds.), *Algorithmic Algebra and Number Theory*, Springer Verlag, Berlin, Heidelberg, New York, ISBN 3-540-64670-1, 1999.
- Mignotte, M., Stefanescu, D., *Polynomials - an algorithmic approach*, Springer Verlag, Berlin, Heidelberg, New York, ISBN 981-4021-51-2, 1999, DM 98,-.

  Das Buch wird in diesem Rundbrief auf Seite 27 besprochen.
- Pethö, A., *Algebraische Algorithmen (herausgegeben von Michael Pohst)*, Vieweg Verlagsges., Braunschweig, Wiesbaden, ISBN 3-528-06598-2, 1999.
- von zur Gathen, J., Gerhard, J., *Modern Computer Algebra*, Cambridge University Press, Cambridge, ISBN 0-521-64176-4, 1999,
- Teske, E. E., *New Algorithms for Finite Abelian Groups*, Shaker Verlag, Aachen, ISBN 3-8265-4045-X, 1999, pp. 173, 94,00 DM.

Besprechungen zu Büchern der Computeralgebra

Wolff, Manfred, Gloor, Oliver, Richard, Christoph
Analysis Alive - Ein interaktiver Mathematik-Kurs

Birkhäuser, Basel, ISBN 3-7643-5966-8, pp 392 mit CD-ROM, DM 68

Analysis Alive ist kein Buch, sondern eine „Medienkombination" (so die Bezeichnung des Verlags) bestehend aus einem gedruckten Buch und einer CD. Beide Teile dieser Kombination, Buch und CD, sind ausgesprochen gut gestaltet, sowohl inhaltlich wie auch ästhetisch: Es macht Freude sich mit Analysis Alive zu beschäftigen! Die CD enthält viele Visualisierungen, oft Animationen, mathematischer Sachverhalte; dies geschieht mit Hilfe des Computeralgebraprogramms Maple, von dem eine Demo- und eine zeitliche befristete Testversion der CD beigefügt ist. Wirklichen Nutzen wird aber nur derjenige ziehen, der auch über eine Maple-Lizenz, z.B. die preiswerte Student Edition, verfügt, da er dann eigene Varianten der Beispiele ausführen kann. Der Inhalt:

Folgen und Reihen
Einführung in die reellen Funktionen
Differentialrechnung
Integralrechnung einer Veränderlichen
Normierte Vektorräume
Funktionen mehrerer Veränderlicher
Differentialrechnung in mehreren Veränderlichen
Integration in mehreren Veränderlichen

Der behandelte Stoffumfang ist beachtlich; dabei mußten die Autoren eines 400-Seiten-Buches naturgemäß Kompromisse eingehen. Ihre Darstellung ist knapp, aber klar und präzis. Zu kurz kommen die Motivation für die verschiedenen Begriffsbildungen und deren Anwendungen. Das Buch eignet sich daher nach Meinung des Reszensenten nicht zum Selbststudium, als Begleittext zu einer Lehrveranstaltung für Mathematiker, Physiker und Informatiker ist es dagegen ausgezeichnet geeignet. Auch derjenige, der nur ein knappe und klare Darstellung der Analysis zum Nachschlagen sucht, etwa Lehrer der gymnasialen Oberstufe, ist gut bedient, zumal letztgenannter Leserkreis viele anregende Visualisierungen zur Unterrichtsgestaltung vorfindet. Ingenieurstudenten oder Naturwissenschaftler werden durch die eher theoretisch orientierte Darstellung weniger angesprochen werden; viele für die Anwendungen wichtige Themen kommen einfach zu kurz, so wird etwa die Laplace-Transformation auf weniger als zwei Seiten behandelt.

Analysis Alive erwartet vom Leser keinerlei Kenntnisse über das Computeralgebra-Programm Maple; die Beispiele sind so konzipiert und programmiert, daß sie von jedem nachvollzogen werden können. Das Buch selbst enthält keinerlei Maple-Code; Computeralgebra wird bewußt und konsequent nur als Werkzeug zum leichteren Erlernen von Mathematik benutzt. Es ist kein Ziel des Buches, irgendwelche Computeralgebra-Kenntnisse zu vermitteln.

Alles in allem: Analysis Alive ist ein sehr empfehlenswertes Mathematikbuch, das viel bietet. Man muß aber akzeptieren, daß man nicht gleichzeitig den Umfang auf rund 400 Seiten begrenzen und jeden Teilaspekt eines Themas behandeln kann. Selbst die CD alleine mit ihren zahlreichen ausgefeilten Visualisierungen der Analysis rechtfertigt die Anschaffung dieser gelungenen „Medienkombination"! Diese Aussage soll jedoch nicht die Qualität des Partners „Buch" in dieser Medienkombination schmälern.

Wilhelm Werner (Heilbronn)

Jungnickel, Dieter
Graphs, Networks and Algorithms

Springer, Berlin, ISBN 3-540-63760-5, 1999, pp. 589, 98 DM.

Das vorliegende Buch erschien nun als fünftes der Springer-Reihe *Algorithms and Computation in Mathematics*, welche von E. Becker, M. Bronstein, H. Cohen, D. Eisenbud und R. Gilman herausgegeben wird. Allerdings handelt es sich hierbei nicht um ein gänzlich neues Buch, sondern im wesenlichen um eine englische Übersetzung der dritten Auflage (1994) des in deutscher Sprache bei BI (inzwischen: Spektrum Akademischer Verlag) erschienenen Buchs *Graphen, Netzwerke und Algorithmen*.

Von einem algorithmischen Standpunkt aus gibt *Graphs, Networks and Algorithms* eine Einführung in die Grundbegriffe der Graphentheorie und der graphentheoretisch formulierbaren Probleme der kombinatorischen Optimierung. Jeder Algorithmus wird in Pseudo-Code dargestellt und auf seine asymptotische Komplexität hin untersucht. Der Autor macht klar, daß eine Komplexitätsanalyse von den verwendeten Datenstrukturen abhängig ist und bezieht diese immer in seine Ausführungen mit ein.

Die folgenden Themen werden behandelt: Kürzeste Wege, aufspannende Bäume, Greedy-Algorithmen, Flüsse, bipartite Graphen, Zirkulationen, Färbungen, Zusammenhangsfragen und Matchings. Das letzte Kapitel behandelt dann schließlich als typisches NP-vollständiges Problem das TSP (Traveling Salesman Problem = Problem des Handlungsreisenden). Hier werden sowohl praktikable Algorithmen zur Auffindung der besten Tour als auch solche zur Bestimmung guter Näherungslösungen diskutiert.

Das Buch enthält Lösungshinweise zu den zahlreichen Übungsaufgaben und einen ausführlichen Index. Es sollte (in der deutschen oder in der englischen Fassung) in keiner Bücherei fehlen.

Wolfram Koepf (Leipzig)

Mignotte, Maurice, Ştefănescu, Doru
Polynomials: An Algorithmic Approach

Springer, Singapore, ISBN 981-4021-51-2, 1999, pp. 306, 98 DM.

Ich muß zugeben, daß ich mir unter diesem Titel ein anderes Buch vorgestellt habe. In einem Buch, das eine algorithmische Theorie der Polynome verspricht, habe ich unzweifelhaft (auch) die Betrachtung von Gröbnerbasen und ihren Anwendungen vermutet. Der Autor sagt hierzu in der Einleitung: „We left out on purpose several topics, for which an extensive literature is available, such as [...] and Gröbner bases (T. Becker–V. Weispfenning, W. W. Adams–P. Loustaunau)." Schade!

Das Buch behandelt Polynomalgorithmen und ist zum Einsatz in der Lehre gedacht. Die Autoren beschränken sich hierbei im wesentlichen auf univariate Polynome. Besonders ausführlich wird die Faktorisierung ganzzahliger Polynome besprochen (Kapitel 4); man kann sagen, das Buch gipfelt in der Faktorisierungstheorie. Hierbei werden sowohl der Berlekamp-Zassenhaus-Algorithmus mit Hensel-Lifting als auch der asymptotisch schnelle LLL-Algorithmus (Lenstra, Lenstra, Lovász) durchgenommen. Als Vorbereitung hierfür werden in Kapitel 3 Polynome mit Koeffizienten in endlichen Körpern und in Kapitel 2 Eigenschaften, insbesondere a-priori-Abschätzungen, von komplexen Polynomen behandelt.

Das erste Kapitel enthält die grundlegenden Algorithmen zur Berechnung von größten gemeinsamen Teilern, Pseudodivision, Resultanten, von Interpolationspolynomen usw. und behandelt beispielsweise die Darstellung symmetrischer Funktionen. Alle Algorithmen werden in Pseudocode dargestellt, und es werden Komplexitätsbetrachtungen durchgeführt.

Leider enthält der Text nur wenige Beispiele. Jeder Algorithmus wird an *einem* „kleinen" Beispiel, das auch der Handberechnung zugänglich ist, exemplarisch vorgeführt. Dafür sind insgesamt 288 Übungsaufgaben zu bearbeiten. Der Titel des Buchs ist sicherlich ungeschickt gewählt. Wer sich aber für die Faktorisierung von Polynomen interessiert, wird das Buch mit Interesse und Gewinn lesen.

Wolfram Koepf (Leipzig)

Kamerich, Ernic
A Guide to Maple

Springer Verlag, New York, 1998, ISBN 0-387-94116-9, HC DM 69.

Auf dem Buchrücken wird der Inhalt bereits recht treffend folgendermaßen beschrieben:
Das vorliegende Buch hat das Ziel, den Leser schnell und umfassend in die Benutzung von Maple und seinen vielfältigen Möglichkeiten einzuführen. Es soll ihm einen gewissen Standard vermitteln, ihm aber auch beriets den Gebrauch weiterführender, mehr spezialisierter Techniken ermöglichen. Die Verlässlichkeit der Ergebnisse wird dabei systematisch untersucht, und es werden Wege aufgezeigt, wie man Resultate auf ihre Korrektheit überprüft,

Die ersten fünf Kapitel (basic elements, numbers and operators, names and evaluation 1, elementary calculus, names and evaluation 2) bilden die Grundlage des Buches, der Leser erhält in ihnen einen raschen Einstieg in den Gebrauch von Maple. Bereits hier fällt auf, dass der Autor neben einem systematischen Aufbau der Maple-Objekte, ihrer Bedeutung und dem Umgang mit ihnen stets auch die Anwendungen in speziellen Fachgebieten im Auge hat. Dies ist etwas gewöhnungsbedürftig, lockert die Darstellung dafür angenehm auf. Dass elementare Analysis zu den Grundlagen zählt, lineare Algebra hingegen nicht, ist für den deutschen Markt vielleicht nicht so günstig.

Der Aufbau von Maple nebst Anwendungen wird in den anschließenden Kapiteln fortgesetzt (mathematische Funktionen, Graphik, Reihenentwicklungen, Numerik, Manipulation mehrerer Objekte gleichzeitig (?), Substitution, Manipulation von Zahlen, Polynome und rationale Ausdrücke). Die letzte Überschrift macht deutlich, dass der Autor es mit den mathematischen Objekten, die behandelt werden, nicht immer ganz genau nimmt. Dies ist natürlich in erster Linie eine Schwachstelle von Maple, das einem mathematischen Elementim allgemeinen keinem entsprechenden Bereich (Gruppe, Ring, Modul, Körper) zuordnet, indem mit ihm nach fest vorgegebenen Regeln gerechnet werden kann. Überdeutlich wird dies bei der Behandlung von Parametern und deren Spezialisierungen.

Weiter geht es im Inhalt mit Polynomgleichungen und Polynomfaktorisierungen, Manipulation algebraischer Objekte (!), Lösung von Gleichungen und Ungleichungen, Lösung von Differentialgleichungen, Vektoren und Matrizen.

Bereits kurz angesprochen wurden die intensiven Bemühungen des Autors, Ergebnisse auf ihre Verlässlichkeit hin zu überprüfen. Dies ist ein wesentliches Element des vorliegenden Buches und mit Sicherheit ein sehr verdienstvolles Unterfangen. Leicht getrübt wird dieser Eindruck durch Standardbemerkungen an den Kapitelenden wie "arbeitet in der Regel korrekt" (?).

Insgesamt betrachte ich das Buch als einen gelungenen Einstieg in den Gebrauch von Maple. Bereits zu Beginn erhält der Leser eine "Short Reference List" der wichtigsten Aufrufe. Es gibt eine große Anzahl von hilfreichen Querverweisen. (Vorsicht: Verweise auf sehr viel spätere Seiten differieren dank TEX um eine Seite.) Wichtige Dinge (etwa: Gebrauch von Digits) werden zum Teil mehrfach kurz erklärt, was für eine Vertiefung günstig ist. Mittels eines "Catchword Index" kommt man leicht an gewünschte Informationen. Über weiterführende Bereiche wird allerdings nur wenig oder gar nichts gesagt (etwa: Galois groups).

Michael Pohst (Berlin)

Koblitz, N.,
Algebraic Aspects of Cryptography

Band 3 der Reihe *Algorithms and Computations in Mathematics*, Springer-Verlag Berlin-Heidelberg-New York 1998, ISBN 3-540-63446-0, pp. 206, DM 98.

Der Autor, der durch seine Bücher “Introduction to Elliptic Curves and Modular Forms” (GTM 97, Springer 1984) und “A Course in Number Theory and Cryptography” (GTM 114, Springer 1987) vielen Lesern dieses Rundbriefs gut bekannt sein wird, hat hier ein kleines Werk vorgelegt, das man wohl am Besten als “Lesebuch zu algebraischen Aspekten der Kryptographie mit öffentlichem Schlüssel” charakterisieren kann.

Bis Mitte der 70er Jahre (der Autor setzt den Schnitt im Jahr 1976) spielten derartige Verfahren in der Kryptographie im Vergleich zu symmetrischen Verfahren bekanntlich eine untergeordnete Rolle. Dies änderte sich erst unter dem Druck verschiedener Computeranwendungsmöglichkeiten. Die generelle Aufgabenstellung für den Entwurf eines Kryptosystems mit öffentlichem Schlüssel kann man wie folgt formulieren: Es ist eine (injektive) Funktion $f: X \longrightarrow Y$ von der Menge der Quelltexteinheiten X in die Menge Y der verschlüsselten Nachrichteneinheiten zu entwerfen, die für alle $x \in X$ einfach zu berechnen ist, für die aber $f^{-1}(y)$ für die meisten $y \in im(f)$ ohne zusätzliche, öffentlich nicht zugängliche Information nicht mit zumutbarem Aufwand zu ermitteln ist. Allerdings soll es eine geheime Zusatzinformation, den privaten Schlüssel, geben, mit dessen Hilfe auch die Umkehraufgabe, das Dechiffrieren, einfach wird.

Viele schwierige mathematische Probleme gaben bisher Anlass für sichere oder vermeintlich sichere Verschlüsselungsverfahren. Die von einer Kryptanalyse zu beantwortenden Fragen sind dabei vor allem komplexitätstheoretischer Natur. Allerdings fortgeschrittener Art, denn die Existenz eines privaten Schlüssels legt die Frage nahe, ob man nicht durch geschickte Kombination öffentlich erzeugbarer Zusatzinformationen diesen Schlüssel doch irgendwie berechnen kann. Die "Code-Knacker" setzen gerade hier an.

Da sich damit in der Kryptanalyse die gesamte Mathematik wie in einem Brennglas sammelt, wird man in einem Büchlein wie dem des Autors immer nur einen kleinen Ausschnitt dieses großen Gebiets einfangen können. Der Autor hat hierfür drei Themenkreise (Monomsysteme, polynomiale Gleichungssysteme und Verallgemeinerungen des Diffie-Hellman-Verfahrens auf elliptische und hyperelliptische Kurven) mit algebraischem Hintergrund gewählt, die bisher nicht in monographischer Form vorlagen.

Das Buch kann man grob in zwei (auch umfangmäßig etwa gleich große) Teile teilen. Im ersten Teil (Kap. 1 – 3) werden wichtige Begriffe und Zusammenhänge der im Weiteren benötigten mathematischen und kryptographischen Grundlagen erläutert und teilweise bewiesen. Der Umfang dieses Teils ist vor allem einer recht detaillierten Darlegung algorithmischer Aspekte geschuldet. Diese fände man zwar auch anderswo, jedoch gewinnt das Buch damit selbst für fortgeschrittene Studenten eine gewisse Abgeschlossenheit. Ein Teil des Materials wurde (für den fleißigen Leser) in eine Fülle von Übungsaufgaben ausgelagert, zu denen im Anhang Lösungen bzw. Lösungshinweise enthalten sind.

Der erste Teil umfasst im Einzelnen eine Tour durch kryptographische Fragen (Aufgabenstellung und Geschichte; das RSA-Kryptosystem; der Ansatz von Diffie-Hellman zur Verwendung von Logarithmus-Abbildungen; Anwendungen auf digitale Signaturen, Passwörter, Auswertung verdeckter Information), die Diskussion relevanter Komplexitätsklassen (polynomial vs. exponentiell; P, NP und NP-hart; Berechnungsaufgaben mit Zusatzinformationen; probabilistische Verfahren) an Beispielen aus Kombinatorik und Zahlentheorie sowie Fragen aus der Theorie endlicher Körper (Existenz- und Eindeutigkeitssatz; konstruktive Aspekte) und der Polynomringe (bis hin zu Hilberts Nullstellensatz, S-Polynomen und Gröbnerbasen).

Im zweiten Teil wird der Leser, begleitet von Alice, Bob und Catherine, durch die bereits oben genannten drei Themenkreise geführt. Der Autor legt großen Wert auf eine ausführliche und verständliche Darlegung des jeweils betrachteten kryptographischen Verfahrens, das in den zugehörigen Übungsaufgaben weiter vertieft werden kann. Die Kryptanalyse erfolgt in der Regel von einer einfach zu brechenden Variante aus, die sich verstärken, aber mit mehr Einsatz von Mathematik auch wieder brechen lässt. Der dabei gezeichnete Weg führt von einer guten Straße über unebenes Gelände bis hin zum Dickicht moderner Forschungen und (noch) ungelöster Fragen.

Kap. 4 befasst sich mit dem Imai-Matsumoto-System. Die Idee des Systems besteht darin, die Abbildung $u \mapsto u^h$ zum Verschlüsseln zu verwenden, wobei u aus einer endlichen Erweiterung von $\mathbf{F}_q$ stammt. Zusätzlich werden affine Transformationen vor- und nachgeschaltet, um "die Spuren zu verwischen". Für geeignete Exponenten h (Summen von wenigen q-Potenzen) lässt sich daraus ein polynomiales Kodierungssystem herleiten. Die Kryptanalyse zeigt, dass in einigen Fällen aus diesen Gleichungen die Existenz bilinearer Gleichungen folgt, die man zum Kodebrechen mit linearer Algebra verwenden kann.

Kap. 5 befasst sich mit dem "Polly Cracker". Hierbei ist $X = F$ ein Körper und $Y = F[T_1, \ldots, T_n]$ ein Polynomring. Eine Nachricht $x \in X$ wird durch ein zufälliges Polynom $p \in I(B)$ bzgl. eines (öffentlich bekannten) Polynomsystems $B \subset Y$ zu $c = x + p$ verfälscht. Die Dechiffrierung erfolgt mit Kenntnis einer (geheimen) Nullstelle $y \in F^n$ von B. Die Kryptanalyse muss also feststellen, wie schwierig es ist, eine solche Nullstelle allein aus den Gleichungen B zu bestimmen. Hierzu werden Gleichungssysteme betrachtet, die sich aus verschiedenen NP-harten kombinatorischen Problemen ableiten lassen, womit das Erstellen eines solchen Systems in $\mathbf{P}$, sein Knacken aber (wahrscheinlich) in $\mathbf{NP}$ liegt. Abschließend wird eine Verallgemeinerung des Polly Crackers betrachtet, wo X eine Teilmenge der Standardmonome bzgl. $I(B)$ ist. Der Autor folgt den Argumenten von T. Mora (1993), der vermutet, dass es mit Blick auf intelligente Attacken mit linearer Algebra einen solchen "Krypto-Gröbner" nicht geben kann.

Kap. 6 ist schließlich Kryptosystemen auf der Basis elliptischer und hyperelliptischer Kurven gewidmet. Diese basieren auf der Idee von Diffie-Hellman, die auf die additive Gruppe der Kurve (im elliptischen Fall) bzw. deren Jacobischer (im hyperelliptischen Fall) angewendet wird. Damit vergrößert sich der Fundus von Gruppen, wo man die Anwendung der genannten Idee studiert hat, beträchtlich. Die Ausführungen beginnen mit einer Zusammenstellung der wichtigsten Fakten aus der Theorie elliptischer Kurven, die im weiteren benötigt werden. Es schließt sich eine ausführliche Erörterung verschiedener Aspekte von Kryptosystemen an, die elliptische Kurven verwenden (subexponentielles Verhalten des Originalverfahrens von Diffie und Hellman für $G = \mathbf{F}_q^*$; Diskreter Logarithmus und "schlechte" Gruppenordnungen; ECDSA-Verfahren zur digitalen Signatur; Auswahl "guter" Kurven und Probleme der klassischen Zahlentheorie). Im abschließenden Teil werden die Fragen auf hyperelliptische Kurven übertragen. Wichtigstes neues Problem ist dabei die effiziente Ausführung der Addition auf der Jacobischen, das in einem Anhang ("An Elementary Introduction to Hyperelliptic Curves" von A.J. Menezes, Yi-Hong Wu und R.J. Zuccherato) abgehandelt wird.

Mit zunehmender Schwierigkeit des Materials werden die Ausführungen dabei skizzenhafter und beschränken sich immer stärker auf den Hinweis auf entsprechende Quellen, was den Charakter eines guten "Lesebuchs", wie ich es oben bezeichnet habe, ausmachen sollte. Das Buch eignet sich damit selbst für "advanced undergraduates", wie es im Klappentext heißt, als Einstieg und erster Überblick über ein Gebiet, in dem sich in den letzten Jahren auf überraschende Weise praktische Anwendungsmöglichkeiten für tief innermathematische Themen ergeben haben.

Hans-Gert Gräbe (Leipzig)

Lehrveranstaltungen zu Computeralgebra im WS 1999/2000

- **Rheinisch–Westfälische Technische Hochschule Aachen**
  Fachdidaktisches Seminar: Computer im Geometrieunterricht, U. Schoenwaelder, U. Bettscheider, Ü4
  Einführungspraktikum in das Formelmanipulationssystem Maple, G. Hiß, U. Klein, V. Dietrich, P2
  Praktikum: Programmieren in Maple, G. Hiß, U. Klein, P4
  Praktikum: Lineare Algebra mit Maple, H. Pahlings, U. Klein, P2
  Arbeitsgemeinschaft zu speziellen Problemen mit Maple, V. Dietrich, U. Klein, E. Görlich, Ü2

- **Universität Bonn**
  Computer-Algebra II, A. Schönhage, V4 + Ü2
  Seminar Algorithmik, Komplexität, A. Schönhage, S2

- **Universität Dortmund**
  Symbolisches Rechnen, H. M. Möller, V4 + Ü2

- **Universität Erlangen-Nürnberg**
  Zahlentheoretische und algebraische Grundlagen der Kryptographie II V2+Ü2, H. Meyn, V2

- **Technische Hochschule Hamburg-Harburg**
  Diskrete Mathematik II, K.-H.Zimmermann, A.Popp, V3+Ü2
  Programmieren in Maple, K.-H.Zimmermann, A.Popp, Ü1
  Praktische Kryptographie, K.-H.Zimmermann, A.Popp, Ü2
  Diskrete Mathematik III, F. Mayer-Lindenberg, V2

- **Universität Hannover**
  Computeralgebra, Hotje, V2

- **Martin-Luther-Universität Halle(Saale)**
  Mathematik mit Mathcad, H.Benker, S2
  Wirtschaftsmathematik mit Mathematica und Maple, H.Benker, V2+S2

- **Universität Heidelberg**
  Computeralgebra-Systeme und gewöhnliche Differentialgleichungen, A. Riede, V2
  Algorithmische algebraische Geometrie, G. Kemper, V4 + Ü2
  Computeralgebra zur Linearen Algebra 1, A. Riede, P

- **Universität Kaiserslautern**
  Einführung in die Computer Algebra, G.-M. Greuel, V2 + Ü1
  Commutative Algebra, G. Pfister, V2 + Ü1
  Singularity Theory, G. Pfister, V2 + Ü1
  Primzahltests, Primfaktorzerlegung und Kryptographie, A. Guthmann, V4 + Ü2
  Oberseminar Singularitätentheorie und Computeralgebra, G.-M. Greuel, G. Pfister S2

- **Pädagogische Hochschule Karlsruhe**
  Algorithmen - von Hammurapi bis Gödel, J. Ziegenbalg, V2
  Workshop: Algorithmen / Informatik, J. Ziegenbalg, HS2

- **Universität Karlsruhe**
  Praktikum Computer-Algebra, T. Beth, C. Ballarin, J. Calmet, W. Geiselmann, M. Rötteler, P2
  Repräsentation math. Wissens in der KI, J. Calmet, C. Ballarin, S2

- **Hochschule für Technik, Wirtschaft und Kultur Leipzig**
  Codierungstheorie und Kryptographie, Koepf, V2, Ü2
  Programmieren in Mathematica, Koepf, V1, Ü1

- **Universität Leipzig**
  Einführung in das Symbolische Rechnen, H.-G. Gräbe, V2 + S1 + P2
  Fachseminar Roboterkinematik, H.-G. Gräbe, S2

- **Universität Linz, Research Institute for Symbolic Computation**
  Einführung in die Computer-Algebra, F. Winkler, V2+Ü1
  Diskrete algorithmische Geometrie, S. Stifter, V2
  Mathematikunterricht mit DERIVE, B. Kutzler, V2
  Projektseminar (WS): Computer-Algebra, F. Winkler, S2
  Projektseminar (WS): Proving and Solving over the Reals, B. Buchberger, J. Schicho, S2
  Projektseminar (WS): Applications of Sheaf Theory, B. Buchberger, J. Schicho, S2

- **Universität Mannheim**
  Computeralgebra, Schlichenmaier, Seiler, Kredel, S2

- **Technische Universität München**
  Computeralgebra I, M. Kaplan, V4

- **Universität Oldenburg**
  Ganze Zahlen, Polynome und Matrizen, W. Schmale, V4+ 2
  Seminar Algebra und Anwendungen (CA), W. Schmale , S2

- **Universität-Gesamthochschule Paderborn**
  Computeralgebra, F. Schwarz, V4 + Ü2
  Spezielle Kapitel der Computeralgebra, B. Fuchssteiner, V2 + Ü2
  MuPAD Seminar, B. Fuchssteiner, S2

- **Universität Passau**
  Roboterkinematik, V. Weispfenning, V3
  Oberseminar Computeralgebra, V. Weispfenning, S2

- **Universität Tübingen**
  Spezifikation und Verifikation, C. Schwarzweller, V2 +Ü1

- **Universität Ulm**
  Computeralgebra Praktikum für Physiker, G.Baumann, V2+P4
  Klassische Mechanik mit Computeralgebra, G.Baumann, V4+Ü4

- **ETH Zürich**
  Computer Algebra I, T. Mulders, V2 + Ü1

Kurze Mitteilungen

- **ISSAC Steering committee**

  Auf der diesjährigen ISSAC in Vancouver fand eine Sitzung des Steering committees statt. Es schieden turnusmässig aus: Bruce Char und Hoon Hong. Neu ist als institutionelles Mitglied Rob Corless (SIGSAM) und neu gewählt (als at large Mitglied) wurde George Labahn. Corless wurde zum Vorsitzenden gewählt. Daher jetzt die Zusammensetzung des Steering committees: Rob Corless (SIGSAM) als Vorsitzender; Marc Giusti (Medicis) jetzt wiedergewählt für drei Jahre; H.M. Möller (FG CA) Amtszeit bis Juli 2000; George Labahn (at large) neu gewählt; Barry Trager (at large); David Saunders (at large).

- **D21 – eine branchenübergreifende Informationsindustrieinitiative**

Viele namhafte deutsche Unternehmen haben sich dem Gründungsaufruf der IBM Deutschland angeschlossen und die branchenübergreifende Initiative D21 `http://www.initiatived21.de` ins Leben gerufen. Ihr Ziel ist die engere Zusammenarbeit von Wirtschaft, Politik, Gesellschaft und Wissenschaft, um der Informationsgesellschaft in Deutschland zum Durchbruch zu verhelfen. Ideen und Ziele der Initiative sind in dem Memorandum *Initiative D21*
(`http://www.initiatived21.de/content/memorandum-d21.pdf`) festgelegt, das am 07.07.99 Bundeskanzler Schröder, der den Vorsitz im Beirat der D21 Initiative übernehmen wird, vorgestellt. Die folgenden Schwerpunktthemen stehen dabei im Zentrum:

- Ordnungsrahmen und Zugang zum Internet
- Vorreiterrolle des Staates beim Einsatz moderner Technologien
- Bildung und Qualifikation
- Förderung von Frauen in IT-Berufen

Am 27. Juli 1999 wurde dann in Stuttgart von 27 Gründungsmitgliedern die *Initiative D21 e.V.* ins Leben gerufen. Neben IBM gehören zu den Gründungsmitgliedern unter anderen Alcatel SEL, AOK Baden-Württemberg, Arthur D. Little, Canto Software AG, debis, Dresdner Bank, EDS, Hewlett-Packard, Siemens und Preussag. Zum Vorsitzenden der Initiative wurde Erwin Staudt, Vorsitzender der Geschäftsführung der IBM Deutschland GmbH, gewählt.

Als erstes großes Projekt steht das Thema *Internet-Klassenzimmer* an. Dabei sollen Schulen und Sponsoren zueinander finden können, damit das Ziel, daß in jedem deutschen Klassenzimmer ein internetfähiger PC steht soll, verwirklicht werden kann.

Zusätzlich gibt es zur Zeit Kontaktaufnahme und Gespräche zwischen verschiedenen Herstellern von Computeralgebra-Software und der IBM, damit auch gleich Computeralgebra-Software auf diesen Rechnern installiert werden kann. Sobald sich diese Ideen, die von der Fachgruppenleitung unterstützt werden, konkretisieren, werden wir weiter darüber berichten.

- **UMS MEDICIS**

MEDICIS is a french "Unite Mixte de Service" and is part of CNRS and the Ecole polytechnique. It's role is a centre of resources for computer algebra.

It can be used by anybody to solve scientific calculations with the tools of computer algebra and symbolic computation. It can, in effect, put at your disposal hardware resources, software and expertise.

In this way, MEDICIS can respond to your needs e.g.:
- a need for a large central memory: 2 machines in the cluster having 2 Gb of memory.
- a need for a 64-bits architecture: 8 Alpha-500 Mhz processors.
- a need for parallel calculus: 16 Pentium II-400 Mhz processors.
- a need for computer algebra software: the current list which can be completed with your demands.
- a need for contacts with knowledgeable users of computer algebra: already more than 200 users.

In total, there are
- approximately 13 Ghz of CPU
- 11 Gb of central memory
- 12 up to date large software packages of computer algebra
- a local 100 Mbs switched and secure network
- a system-network-applications administrator
- 200 experts and knowledgeable users,

who are available at your disposal.

To find out more, particularly about the activities of MEDICIS or to gain access, see the WEB server of MEDICIS:
`http://www.medicis.polytechnique.fr/medicis/cri-eng.html`

Aufnahmeantrag für Mitgliedschaft in der Fachgruppe Computeralgebra

(Im folgenden jeweils Zutreffendes bitte im entsprechenden Feld [ ] ankreuzen bzw. ____________ ausfüllen.)

Name: ______________________________ Vorname: ______________

Akademischer Grad/Titel: ______________________________

Privatadresse

Straße/Postfach: ______________________________

PLZ/Ort: ______________________________ Telefon: ______________

e-mail: ______________________________ Telefax: ______________

Dienstanschrift

Firma/Institution: ______________________________

Straße/Postfach: ______________________________

PLZ/Ort: ______________________________ Telefon: ______________

e-mail: ______________________________ Telefax: ______________

Gewünschte Postanschrift: [ ] Privatadresse [ ] Dienstanschrift

1. Hiermit beantrage ich zum 1. Januar 200___ die Aufnahme als Mitglied in die Fachgruppe

Computeralgebra (CA) (bei der GI: 2.2.1).

2. Der Jahresbeitrag beträgt DM 15,00 bzw. DM 18,00. Ich ordne mich folgender Beitragsklasse zu:

   [ ] **15,00 DM**. für Mitglieder einer der drei Trägergesellschaften
   - [ ] GI Mitgliedsnummer: ______________
   - [ ] DMV Mitgliedsnummer: ______________
   - [ ] GAMM Mitgliedsnummer: ______________

   Der Beitrag zur Fachgruppe Computeralgebra wird mit der Beitragsrechnung der Trägergesellschaft in Rechnung gestellt. (Bei Mitgliedschaft bei mehreren Trägergesellschaften wird dies von derjenigen durchgeführt, zu der Sie diesen Antrag schicken.) [ ] Ich habe dafür bereits eine Einzugsvollmacht erteilt. Diese wird hiermit für den Beitrag für die Fachgruppe Computeralgebra erweitert.

   [ ] **15,00 DM**. Ich bin aber noch nicht Mitglied einer der drei Trägergesellschaften. Deshalb beantrage ich gleichzeitig die Mitgliedschaft in der

   [ ] GI [ ] DMV [ ] GAMM.

   und bitte um Übersendung der entsprechenden Unterlagen.

   [ ] **18,00 DM** für Nichtmitglieder der drei Trägergesellschaften. [ ] Gleichzeitig bitte ich um Zusendung von Informationen über die Mitgliedschaft in folgenden Gesellschaften:

   [ ] GI [ ] DMV [ ] GAMM.

3. Die in dieses Formular eingetragenen Angaben werden elektronisch gespeichert. Ich bin damit einverstanden, daß meine Postanschrift durch die Trägergesellschaften oder durch Dritte nach Weitergabe durch eine Trägergesellschaft wie folgt genutzt werden kann (ist nichts angekreuzt wird c. angenommen).

   [ ] a. Zusendungen aller Art mit Bezug zur Informatik, Mathematik bzw. Mechanik.
   [ ] b. Zusendungen durch wissenschaftliche Institutionen mit Bezug zur Informatik, Mathematik bzw. Mechanik.
   [ ] c. Nur Zusendungen interner Art von GI, DMV bzw. GAMM.

Ort, Datum: ______________________ Unterschrift: ______________________________

Zurück an:

Gesellschaft für Informatik e.V. (GI)
Wissenschaftszentrum
Ahrstraße 45
53175 Bonn
Tel.: 0228-302-149, Fax.: -167
e-mail: gs@gi-ev.de

oder

Deutsche Mathematiker-Vereinigung e.V. (DMV)
Mohrenstraße 39, 10117 Berlin
Tel.: 030-20377-306, Fax.: -307
e-mail: dmv@wias-berlin.de

oder

Gesellschaft für Angewandte Mathematik und Mechanik e.V. (GAMM)
NWF I – Mathematik, Univ. Regensburg
Universitätsstr. 31, 96053 Regensburg

Fachgruppenleitung Computeralgebra 1999-2002

Dr. Johannes Grabmeier
IBM Deutschland Informationssysteme GmbH
Vangerowstr. 18, Postfach 10 30 68
69020 Heidelberg
Tel. 06221-59-4329,-4254(Sekr.)
Telefax: 06221-59-3500
grabm@de.ibm.com

Fachexperte Physik:
zur Zeit nicht besetzt.

Referent Lehre & Didaktik:
Prof. Dr. Wolfram Koepf
Fachbereich IMN, HTWK Leipzig
Gustav-Freytag-Str. 42 A
D-04277 Leipzig
Tel.: 0341-307-6495
Telefax: 0341-301-2722
koepf@imn.htwk-leipzig.de
http://www.imn.htwk-leipzig.de/~koepf

Stellv. Sprecher:
Prof. Dr. M. Pohst
Fachbereich 3 Mathematik MA 8-1
Technische Universität Berlin
Straße des 17. Juni 136
10623 Berlin
Tel.: 030-314-25772, -24015 (Sekr.)
Telefax: 030-314-21604
pohst@math.tu-berlin.de

Referent Computational Engineering:
Prof. Dr. Volker Strehl
c/o Lehrstuhl Informatik 8 (Künstl. Intelligenz)
Universität Erlangen-Nürnberg
Am Weichselgarten 9
D-91058 Erlangen
Tel.: 09131-29914, -29907 (Sekr.)
Telefax: 09131-29905
strehl@informatik.uni-erlangen.de

Referent Benchmarks:
Prof. Dr. G.-M. Greuel
Fachbereich Mathematik
der Universität Kaiserslautern
Postfach 3049
D-67653 Kaiserslautern
Tel. 0631-205-2850,-2339(Sekr.)
Telefax: 0631-205-3052
greuel@mathematik.uni-kl.de
http://www.mathematik.uni-kl.de/~wwwagag/D/Greuel

Referent Chemieanwendungen:
Prof. Dr. A. Kerber
Lehrstuhl II f. Mathematik
Univ. Bayreuth, 95440 Bayreuth
Tel. 0921-553387
Telefax: 0921-553385
kerber@uni-bayreuth.de
http://www.mathe2.uni-bayreuth.de

Vertreter der DMV:
Prof. Dr. B. Heinrich Matzat
Interdisziplinäres Zentrum f.
Wissenschaftliches Rechnen
Univ. Heidelberg, Im Neuenheimer Feld 368
69120 Heidelberg
Tel. 06221-54-8242, -8318 (Sekr.)
Telefax 06221-54-8850
matzat@iwr.uni-heidelberg.de

Vertreter der GAMM:
Prof. Dr. Siegfried M. Rump
Informatik III
TU Hamburg-Harburg
Eissendorfer Str. 38
21071 Hamburg
Tel. 040-42878-3027
rump@tu-harburg.de
http://www.ti3.tu-harburg.de/rump/

Prof. Dr. V. Weispfenning
Lehrstuhl für Mathematik
Universität Passau
Innstraße 33
94030 Passau
Tel. 0851-509-3120, -3121 (Sekr.)
Telefax: 0851-509-3122
weispfen@uni-passau.de
http://www.fmi.uni-passau.de/~weispfen

Vertreter der GI:
Prof. Dr. Karl Hantzschmann
Fachbereich Informatik
Universität Rostock
Albert-Einstein-Straße 21
18059 Rostock
Postanschrift: 18051 Rostock
Tel.: 0381-498-3400
Telefax: 0381/498-3399
hantzschmann@informatik.uni-rostock.de

Fachexperte Schule:
Heiko Knechtel
An der Tränke 2a
31675 Bückeburg
Tel. 05722-23628
HKnechtel@aol.com

Sprecher:
Prof. Dr. H. Michael Möller
Fachbereich Mathematik
Universität Dortmund
44221 Dortmund
Tel. 0231-755-3077
Moeller@math.uni-dortmund.de

Referent CAIS:
Prof. Dr. Gerhard Schneider
GWDG, Am Faßberg
37077 Göttingen
Tel. 0551-201-1545
Telefax: 0551-21119
Gerhard.Schneider@gwdg.de

Fachexperte Fachhochschulen:
Prof. Dr. Wilhelm Werner
FB TWK der FH Heilbronn
Außenstelle Künzelsau
Daimlerstr.35 Tel. 07940-1306-21 (Sekr.)
Telefax: 07940-1306-20
werner@fh-heilbronn.de

Verwaltungen der Fachgruppe Computeralgebra

Mitgliederverwaltung der GI, Anzeigenverwaltung:
Gesellschaft für Informatik e.V.
Wissenschaftszentrum
Ahrstr. 45
53175 Bonn
Telefon 0228-302-145 (-164 Anzeigen)
Telefax 0228-302-167
el.Adr.: gs@gi-ev.de

Mitgliederverwaltung der DMV:
Deutsche Mathematiker
-Vereinigung, Geschäftsstelle
Mohrenstraße 39
10117 Berlin
Telefon 030-20377-306
Telefax 030-20377-307, el.Adr.:
dmv@wias-berlin.de

Mitgliederverwaltung der GAMM:
Gesellschaft für Angewandte
Mathematik und Mechanik e.V.
NWF I – Mathematik,
Univ. Regensburg
Universitätsstr. 31
96053 Regensburg
http://www.uni-regensburg.de/Fakultaeten/nat_Fak_I/Mennicken/gamm/vorstand.html

Impressum

Computeralgebra–Rundbrief Herausgegeben von der Fachgruppe Computeralgebra der GI (2.2.1), DMV und GAMM, Redaktionsschluß 28.02 und 30.09. Anschrift: Dr. Ulrich Schwardmann, Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen (GWDG), Am Fassberg, 37077 Göttingen, Telefax: 0551-21119, Telefon: 0551-201-1542, Internet: uschwar1@gwdg.de , ISSN 0933-5994.
Mitglieder der Fachgruppe Computeralgebra erhalten je ein Exemplar dieses Rundbriefs im Rahmen ihrer Mitgliedschaft. Exemplare darüber hinaus bzw. außerhalb der Mitgliedschaft können über die GI bezogen werden.
WWW-Server der Fachgruppe Computeralgebra mit URL: http://www.gwdg.de/~cais,
Konferenzankündigungen, Mitteilungen und einzurichtende Links bitte an: cais@rz.uni-karlsruhe.de
Computeralgebra-Liste der Fachgruppe: cais@rz.uni-karlsruhe.de (Anm.:SUBSCRIBE CAIS-L <vorname> <nachname>)

Werbeseite der Fa. Springer Verlag