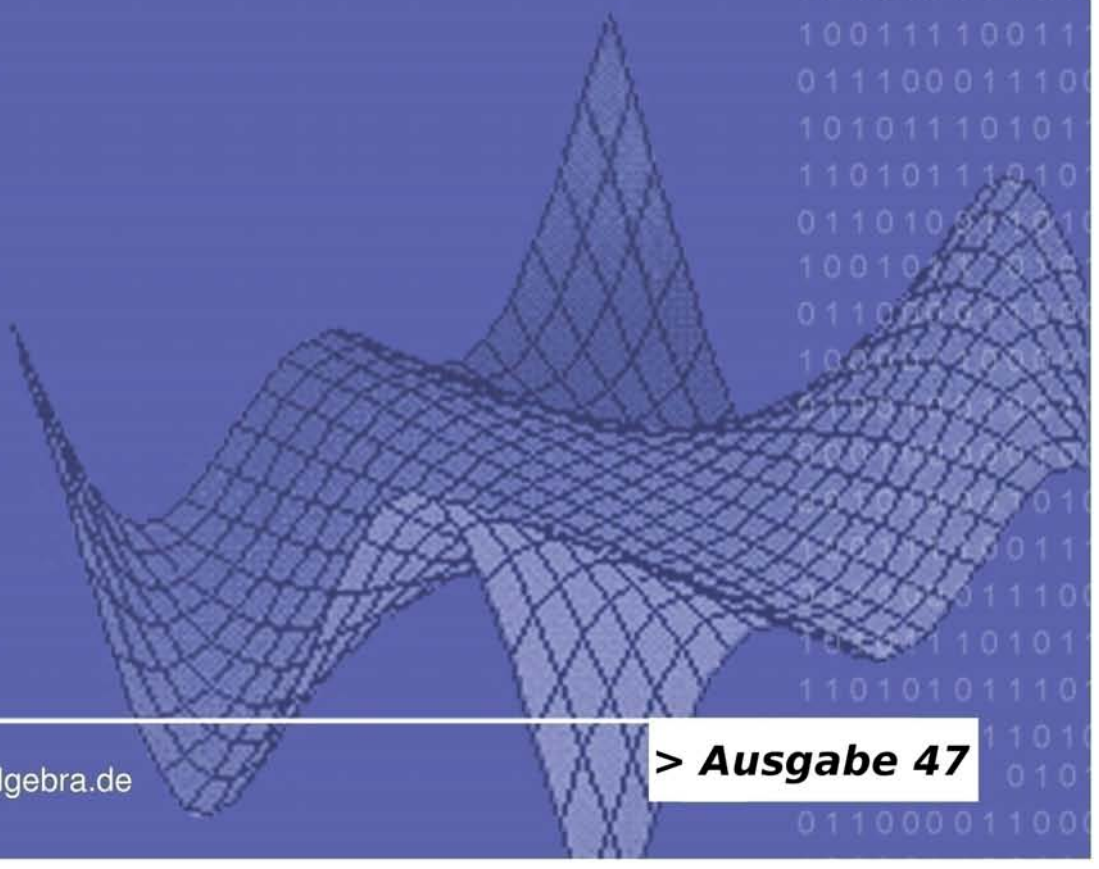
Oktober 2010

Computeralgebra Rundbrief

GI_DMV_GAMM

- ISSAC 2010 in München
- Serre-Vermutung und CA
- CA in Schule und Lehre
- DFG-Schwerpunkt SPP 1489



www.fachgruppe–computeralgebra.de

> Ausgabe 47

Rundbrief Computeralgebra Nr. 47

Werbeseite Vieweg-Teubner

Computeralgebra-Rundbrief

Nr. 47 Oktober 2010

Inhaltsverzeichnis

Impressum

Der Computeralgebra-Rundbrief wird herausgegeben von der Fachgruppe Computeralgebra der GI, DMV und GAMM (verantwortlicher Redakteur: Prof. Dr. Markus Wessler, markus.wessler@hm.edu).

Der Computeralgebra-Rundbrief erscheint halbjährlich, Redaktionsschluss 28.02. und 30.09. ISSN 0933-5994. Mitglieder der Fachgruppe Computeralgebra erhalten je ein Exemplar dieses Rundbriefs im Rahmen ihrer Mitgliedschaft. Fachgruppe Computeralgebra im Internet: http://www.fachgruppe-computeralgebra.de.

Konferenzankündigungen, Mitteilungen, einzurichtende Links, Manuskripte und Anzeigenwünsche bitte an den verantwortlichen Redakteur.

Die Geschäftsstellen der drei Trägergesellschaften:

GI (Gesellschaft für Informatik e.V.)
Wissenschaftszentrum
Ahrstr. 45
53175 Bonn
Telefon 0228-302-145
Telefax 0228-302-167
gs@gi-ev.de
http://www.gi-ev.de

DMV (Deutsche Mathematiker-Vereinigung e.V.)
Mohrenstraße 39
10117 Berlin
Telefon 030-20377-306
Telefax 030-20377-307
dmv@wias-berlin.de
http://www.dmv.mathematik.de

GAMM (Gesellschaft für Angewandte Mathematik und Mechanik e.V.)
Technische Universität Dresden
Institut für Statik und Dynamik der Tragwerke
01062 Dresden
Telefon 0351-463-34386
Telefax 0351-463-37061
GAMM@mailbox.tu-dresden.de
http://www.gamm-ev.de

Mitteilungen der Sprecher

Liebe Mitglieder der Fachgruppe Computeralgebra,

die Amtszeit der derzeitigen Fachgruppenleitung läuft im Frühjahr 2011 aus. Zur Wahl der neuen Fachgruppenleitung haben Sie mit diesem Rundbrief auch die Wahlunterlagen erhalten. Ausführliche Informationen zum Wahlverfahren und zu den Kandidaten finden Sie weiter unten in dieser Rubrik.

Die Fachgruppenleitung traf sich am Samstag, dem 2. Oktober, in Kassel zu ihrer Herbstsitzung. Themen der Sitzung waren natürlich u. A. die ISSAC 2010, eine geplante Industrietagung sowie die Wahl der Fachgruppenleitung.

Der vorliegende Rundbrief enthält auf S. 30 einen ausführlichen Bericht zur ISSAC-Tagung 2010 in München (`http://www.issac-conference.org/2010`), die von der Fachgruppe durchgeführt wurde. Herzlichen Dank für die gelungene Tagung an das gesamte Organisationskomitee!

Die Fachgruppe verlieh drei Preise: Für das Beste Paper eines Fachgruppenmitglieds *wurden Manuel Kauers und Veronika Pillwein für ihre Arbeit „*When Can We Detect that a P-Finite Sequence is Positive?*“ ausgezeichnet. Dieser Preis war mit 500 € dotiert. Die Preisträger waren im Umlaufverfahren von der gesamten Fachgruppenleitung ermittelt worden. Für die* Beste Software-Demonstration *wurden Felix Effenberger und Jonathan Spreer für ihre Software-Demo* simpcomp: A GAP toolbox for simplicial complexes *ausgezeichnet. Beide Autoren erhielten von der Fachgruppe Computeralgebra jeweils 100 € Preisgeld. Dies wurde vor Ort von Johannes Grabmeier, Thomas Hahn, Gerhard Hiß, Wolfram Koepf, Ernst Mayr, Markus Wessler und Eva Zerz entschieden.*

Der lokale Organisator Ernst Mayr bei der Eröffnung der ISSAC-Tagung 2010

Tagungsausflug auf dem Ammersee

Das Posterkomitee wählte die zwei besten Poster aus, welche die Fachgruppe Computeralgebra jeweils mit einem Preisgeld von 100 € pro beteiligtem Autor ausstattete. Gewonnen haben Sonia L. Rueda für ihr Poster Linear Differential Implicitization and Differential Resultants *sowie Seyed Mohammad Mahdi Javadi und Michael Monagan für ihr Poster* On Sparse Interpolation over Finite Fields. *Die Fachgruppe Computeralgebra vergab einen zusätzlichen Preis für das Poster* Nullspace Computation over Rational Function Fields for Symbolic Summation *von Burçin Eröcal und Arne Storjohann. Die Siegerposter sind auf S. 32–34 abgedruckt.*

Weitere Preise wurden von unserer amerikanischen Partnerorganisation SIGSAM verliehen, s. S. 30. Die Fachgruppenleitung legte auf der Herbstsitzung fest, auch auf den zukünftigen ISSAC-Tagungen, die in Europa stattfinden, jeweils Preise für die besten Poster und Software-Demonstrationen zu vergeben.

Wir beschlossen außerdem, eine neue Rundbrief-Rubrik Promotionen in der Computeralgebra *zu begründen, die im nächsten Heft beginnen soll. Daher bitten wir alle Doktoranden und ihre Betreuer, uns sämtliche Computeralgebra-Promotionen der Jahre 2009 und 2010 mit den relevanten Informationen wie Autor, Titel, Fachbereich und Universität, Betreuer, Datum und ggfs. einem Abstract zur Veröffentlichung im Rundbrief an `eva.zerz@math.rwth-aachen.de` zuzusenden.*

Die nächste ISSAC-Tagung findet am 8.–11. Juni 2011 im kalifornischen San Jose als Teil der ACM Federated Computing Research Conference *statt (`http://www.issac-conference.org/2011`), s. S. 38.*

Der DFG-Schwerpunkt Algorithmic and Experimental Methods in Algebra, Geometry, and Number Theory, *der im vorletzten Heft vorgestellt wurde, ist nun auf der Internetseite `www.computeralgebra.de` zu finden, s. S. 40. Ferner hat die DFG an der RWTH Aachen das Graduiertenkolleg 1632* Experimentelle und konstruktive Algebra *(`http://www.rwth-aachen.de/go/id/zhe`) eingerichtet.*

Nun zur Neuwahl der Fachgruppenleitung: Die Fachgruppenleitung hat zwölf Mitglieder, von denen drei von den beteiligten Trägergesellschaften als deren Vertreter bestimmt werden. Die restlichen neun Leitungsmitglieder werden von allen Mitgliedern der Fachgruppe gewählt. Die Amtszeit der Fachgruppenleitung beträgt nach unserer Ordnung drei Jahre.

Von den von Ihnen zu dieser Wahl vorgeschlagenen Kollegen haben sich 14 bereit erklärt zu kandidieren. Sie werden Ihnen im Folgenden kurz vorgestellt:

- **Dr. Anne Frühbis-Krüger**, *40, wissenschaftliche Mitarbeiterin und apl. Professorin am Institut für Algebraische Geometrie der Leibniz Universität Hannover, Arbeitsgebiete: Algorithmische Singularitätentheorie, Algorithmische Algebraische Geometrie, insbesondere Desingularisierung und deren Anwendungen, seit 1996 Mitarbeit an der Entwicklung des Computeralgebrasystems SINGULAR.*

- **Dr. Hans-Gert Gräbe**, *54, wissenschaftlicher Mitarbeiter, apl. Professor am Lehrstuhl Betriebliche Informationssysteme des Instituts für Informatik der Universität Leipzig. Derzeitige Arbeitsgebiete: Softwaretechnik, E-Learning, Wissen in der modernen Gesellschaft. Erfahrungen und Publikationen zur Computeralgebra in Forschung und Lehre, u. A.* Mathematica 6 *mit M. Kofler (Pearson Studium, 2007). In der Computeralgebra aktiv seit 1988.*
  `http://bis.informatik.uni-leipzig.de/HansGertGraebe`

- **Dr. Thomas Hahn**, *39, wissenschaftlicher Mitarbeiter am Max-Planck-Institut für Physik, München. In der Fachgruppenleitung seit 2002 als Fachexperte Physik, Autor der Computeralgebra-Softwarepakete FeynArts und FormCalc für Rechnungen im Bereich der Teilchenphysik.*
  `http://wwwth.mppmu.mpg.de/members/hahn`

- **Prof. Dr. Elkedagmar Heinrich**, *60, Hochschule für Technik, Wirtschaft und Gestaltung Konstanz. DMV-Mitglied. Arbeitsgebiete: Auswirkungen der Computeralgebra auf die Mathematikausbildung sowie die Anwendung von Computeralgebra im Bereich Simulation. Organisation des CA-Symposiums Konstanz 2000, 2003, 2007, lokale Mitorganisation von CASC 2001. Mitglied des Lenkungsausschusses Hochschuldidaktik an Fachhochschulen in Baden-Württemberg, Lehrbücher zu Mathematica und Maple.*

- **Prof. Dr. Florian Heß**, *40, Professor am Institut für Mathematik der Carl von Ossietzky Universität Oldenburg. Arbeitsgebiete: Algorithmische algebraische Zahlentheorie und Geometrie, speziell algebraische Funktionenkörper, Kurven und Anwendungen auf Kryptographie und Codierungstheorie. Seit 1994 umfangreiche Mitarbeit an den Computeralgebrasystemen Kash und Magma, ferner Mitwirkung an IEEE und ISO Kryptographiestandards und Organisation des Algorithmic Number Theory Symposiums VII in Berlin. Mitglied der Fachgruppenleitung seit 2008 als Fachreferent Themen und Anwendungen. Einwerbung von fünf Beiträgen der Rubrik Themen und Anwendungen des Rundbriefs.*
  `http://www.staff.uni-oldenburg.de/florian.hess`

- **Prof. Dr. Gregor Kemper**, *47, Professor für algorithmische Algebra an der TU München. Arbeitsgebiete: Invariantentheorie, algorithmische kommutative Algebra, Computeralgebra.*
  `http://www-m11.ma.tum.de/~kemper`

- **Prof. Dr. Jürgen Klüners**, *40, Professor für Computeralgebra und Zahlentheorie an der Universität Paderborn. Arbeitsgebiete: Computeralgebra, Galois- und Zahlentheorie. Mitentwickler der*

Computeralgebrasysteme Kant und Magma sowie einer Datenbank für Zahlkörper. Mitglied der Koordinatorengruppe des DFG-Schwerpunktprogramms 1489.
`http://www2.math.uni-paderborn.de/people/juergen-klueners.html`

- **Dr. Axel Kohnert**, *48, Privatdozent am Lehrstuhl für Computeralgebra der Universität Bayreuth. Arbeitsgebiete: algebraische Codierungstheorie, symmetrische Funktionen, algebraische Kombinatorik, Mitarbeit am Computeralgebrasystem Magma, Entwicklung der Bibliothek SYMMETRICA für symmetrische Funktionen und Darstellungstheorie der symmetrischen Gruppen.*
`http://www.algorithm.uni-bayreuth.de/de/team/kohnert_axel`

- **Prof. Dr. Martin Kreuzer**, *48, Universitätsprofessor, Lehrstuhl für Symbolic Computation, Fakultät für Informatik und Mathematik, Universität Passau. Arbeitsgebiete: Computeralgebra, insbesondere Gröbnerbasen und Randbasen, industrielle Anwendungen der Computeralgebra, algebraische Kryptographie, algebraische Geometrie. Leiter des Entwicklerteams des Computeralgebrapakets ApCoCoA. Leiter des Industrieprojekts „Algebraic Oil“.*
`http://staff.fim.uni-passau.de/~kreuzer/`

- **Prof. Dr. Gunter Malle**, *50, Professor für Algebra an der TU Kaiserslautern. Arbeitsgebiete: computergestützte und experimentelle Mathematik, insbesondere Gruppen- und Darstellungstheorie, konstruktive Galoistheorie und Invariantentheorie. Mitautor des Chevie-Pakets sowie von Datenbanken zu Gruppendarstellungen, Galoiserweiterungen und Invariantenringen.*
`http://www.mathematik.uni-kl.de/~malle/de/index.html`

- **OStR Jan Hendrik Müller**, *42, Schuldienst seit 1996, seit 2003 Lehrauftrag für Didaktik der Mathematik an der TU Dortmund (IEEM bei Prof. Dr. Hans-Wolfgang Henn). Schwerpunkte: Seit 6 Jahren im Bereich internationaler Comenius Bildungsprojekte tätig, Computereinsatz und freie Arbeitsformen im Mathematikunterricht. Fachdidaktische Veröffentlichungen seit 2003, seit 1998 in MINT-Initiativen aktiv, Unterrichtserfahrung mit CAS (TI-92, TI-Nspire, WXMaxima).*
`http://www.mathebeimueller.de`

- **Prof. Dr. Reinhard Oldenburg**, *43, Studium der Mathematik in Frankfurt (Main), Promotion in Mathematik in Göttingen, Lehramtsstudium für Mathematik, Physik und Informatik, 6 Jahre Lehrer, seit 2006 Professor für Didaktik der Mathematik und Informatik erst an der Pädagogischen Hochschule Heidelberg, seit 2008 an der Universität Frankfurt (Main); Entwicklung des computeralgebrabasierten dynamischen Geometrieprogramms FeliX.*
`http://www.math.uni-frankfurt.de/~oldenbur`

- **Dr. Hans Schönemann**, *48, wissenschaftlicher Assistent an der TU Kaiserslautern. Arbeitsgebiete: Computeralgebra in der algebraischen Geometrie, Gröbnerbasen und verwandte Algorithmen, Gröbnerbasen für nichtkommutative Algebren, Implementierung von CAS, Integration von/Parallelisierung mit verschiedenen CAS-Instanzen; Mitautor des CAS Singular.*
`http://www.mathematik.uni-kl.de/~hannes`

- **Prof. Dr. Eva Zerz**, *43, Professorin für Algebra am Lehrstuhl D für Mathematik der RWTH Aachen. Arbeitsgebiete: mathematische Kontrolltheorie, algebraische Systemtheorie, Netzwerktheorie, Anwendungen von computeralgebraischen Methoden, insbesondere Gröbnerbasen, in diesen Gebieten, z. B. Singular Control Library.*
`http://www.math.rwth-aachen.de/~Eva.Zerz`

Die Wahlleitung für diese Wahl haben die Herren Koepf sowie Mayr übernommen, die als offizielle Vertreter der DMV bzw. der GI Mitglieder der Fachgruppenleitung sind.

Bitte kreuzen Sie auf Ihrem Stimmzettel bis zu neun Namen *an und senden ihn im verschlossenen Wahlumschlag zusammen mit der unterschriebenen „Versicherung zur Briefwahl“ im beigefügten Rücksendeumschlag bis zum*

Freitag, 3. Dezember 2010, Eingang beim Wahlleiter !

an den Wahlleiter der Fachgruppe Computeralgebra, Prof. Dr. Wolfram Koepf, Universität Kassel, Heinrich-Plett-Str. 40, 34132 Kassel, zurück. Bitte machen Sie von Ihrer Wahlmöglichkeit Gebrauch!

Die konstituierende Sitzung der neuen Fachgruppenleitung wird im Februar 2011 stattfinden. Wir hoffen, Sie mit dem vorliegenden Heft wieder gut zu informieren.

Wolfram Koepf *Elkedagmar Heinrich*

Tagungen der Fachgruppe

ISSAC 2010, 25. – 28.07.2010, München
`http://www.issac-conference.org/2010`

Im Juli 2010 fand in München die internationale Tagung *ISSAC 2010* statt. Ernst W. Mayr von der TU München war Local Arrangements Chair und Wolfram Koepf General Chair dieser Tagung.

Einen ausführlichen Bericht zur *ISSAC 2010* finden Sie auf Seite 30 dieses Rundbriefs.

Die Serresche Modularitätsvermutung und Computeralgebra

Gabor Wiese
(Universität Duisburg-Essen)

gabor.wiese@uni-due.de

In den Jahren 2004 bis 2007 wurde die Serresche Modularitätsvermutung von Chandrashekhar Khare, Jean-Pierre Wintenberger und Mark Kisin ([9], [10], [12]) bewiesen. In meinen Augen stellt dies einen wichtigen Meilenstein in der arithmetischen Geometrie und Zahlentheorie dar. Dieses Resultat muss als eine weit reichende Verallgemeinerung des Satzes von Wiles und Taylor zur Modularität von rationalen elliptischen Kurven angesehen werden, der den großen Satz von Fermat impliziert. Auch für die Computeralgebra ist die Serresche Modularitätsvermutung, kurz: Serre-Vermutung, von großer Bedeutung, wie wir in diesem Artikel ausführen wollen.

Ganz grob gesprochen stellt die Serre-Vermutung eine explizite Korrespondenz zwischen bestimmten komplexen Funktionen, den *Modulformen*, und *Zahlkörpern* einer bestimmten Bauart her. Da Modulformen mittels Computeralgebra berechnet werden können, ergibt sich so ein Zugang, auch Eigenschaften der Zahlkörper, die mit anderen Methoden nicht zugänglich sind, explizit zu bestimmen.

Modulformen

Modulformen wurden bereits im 19. Jahrhundert in der Funktionen- und der Zahlentheorie u. A. von Jacobi, Kronecker, Eisenstein und Weierstraß und später von Poincaré und Klein studiert. Ein berühmtes, wunderschönes Resultat dieser Zeit ist eine Formel für die Anzahl der Möglichkeiten, eine gegebene natürliche Zahl als Summe von vier Quadraten darzustellen. Man liest sie sofort durch Koeffizientenvergleich aus der auf Jacobi zurückgehenden Identität

$$\begin{aligned}\left(\sum_{n=-\infty}^{\infty} q^{n^2}\right)^4 &= \sum_{a,b,c,d\in\mathbb{Z}} q^{a^2+b^2+c^2+d^2} \\ &= 1 + 8\sum_{m=1}^{\infty}\left(\sum_{d|m,4\nmid d} d\right) q^m\end{aligned} \tag{1}$$

ab. Die linke Seite ist eine Theta- und die rechte eine Eisenstein-Reihe. Beides sind Modulformen, und die Gleichheit folgt aus der Eindimensionalität des zugehörigen Vektorraums der Modulformen.

Die Definition einer Modulform ist sehr einfach. Jede Modulformen hat zwei Invarianten; zunächst benötigen wir nur das *Gewicht*, eine ganze Zahl. Eine Modulform vom Gewicht k ist eine holomorphe (d. h. differenzierbare) komplexwertige Funktion f auf der oberen Halbebene $\mathbb{H} := \{z = x + iy \in \mathbb{C} \mid y > 0\}$, also $f : \mathbb{H} \to \mathbb{C}$, die die Transformationseigenschaft

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z) \tag{2}$$

für alle ganzzahligen Matrizen $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ mit der Determinante 1 erfüllt und die darüber hinaus auch in den Spitzen holomorph ist, was wir sofort erklären. Die Transformationsformel für $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ ergibt $f(z+1) = f(z)$, also eine Periodizität mit Periode 1, weshalb sich f in eine Fourier-Reihe

$$f(z) = \sum_n a_n(f)\, e^{2\pi i n z} = \sum_n a_n(f)\, q^n \tag{3}$$

mit Fourier-Koeffizienten $a_n(f) \in \mathbb{C}$ entwickeln lässt, wobei wir $q = q(z) = e^{2\pi i z}$ als Abkürzung einführen. Die Holomorphie in den Spitzen bedeutet einfach, dass alle Koeffizienten $a_n(f)$ für negative n gleich 0 sind. Ist zudem $a_0(f) = 0$, dann nennt man f eine *Spitzenform*.

Die zweite Invariante einer Modulform ist ihre *Stufe*. Man verallgemeinert obige Definition, die der Stufe 1 entspricht, wie folgt zu Stufe N: Die Transformationsformel (2) wird nur für solche Matrizen gefordert, bei denen N sowohl c als auch $d-1$ teilt; außerdem muss die Holomorphie in den Spitzen etwas anders formuliert werden.[1]

[1] Für die allgemeine Definition sei auf die Vielzahl an Lehrbüchern zu Modulformen verwiesen.

Hecke-Operatoren

Erich Hecke führte in der ersten Hälfte des 20. Jahrhunderts eine wichtige algebraische Struktur auf Räumen von Modulformen ein, indem er lineare Operatoren definierte, die wir heute *Hecke-Operatoren* nennen. Für jede natürliche Zahl n gibt es einen Hecke-Operator T_n. Dieser kann durch eine einfache Formel auf den Koeffizienten der Fourier-Reihe definiert werden, hat aber auch eine geometrische Erklärung. Da die Hecke-Operatoren untereinander vertauschen, gibt es Modulformen, die Eigenfunktionen für alle Hecke-Operatoren sind. Diese nennen wir *Hecke-Eigenformen*. Ist f eine Hecke-Eigenform, so ist der Eigenraum zu den Eigenwerten der Hecke-Operatoren auf f eindimensional, wird also von f erzeugt. Wir nennen f normiert, falls $a_1(f) = 1$ gilt. Bemerkenswert ist, dass dann der Eigenwert von T_n gleich dem Fourier-Koeffizienten $a_n(f)$ ist. Für das Folgende wollen wir uns merken:

> **Die Kenntnis der Hecke-Operatoren ist äquivalent zur Kenntnis der Modulformen.**

Modulsymbole: Modulformen auf dem Computer

Die angenehmste Form, eine Modulform auf dem Computer darzustellen, ist, die ersten Koeffizienten der Fourier-Enwicklung abzuspeichern. Da für festes Gewicht und feste Stufe der Vektorraum der Modulformen endlichdimensional ist, ist dies auch genug, und einfache Formeln geben an, wieviele Koeffizienten man höchstens abzuspeichern braucht.

Es gibt mehrere Methoden, Modulformen auszurechnen, von denen ich die am weitesten verbreitete hier kurz einführen möchte: *Modulsymbole*. Diese gehen auf Bryan Birch zurück; einen richtigen Aufschwung erlebten sie durch John Cremona, der sie zur Berechnung modularer elliptischer Kurven verwendet hat [6]. Der Hintergrund hierzu ist, dass die Hodge-Zerlegung einen Isomorphismus zwischen dem Vektorraum der ersten Homologie der sogenannten Modulkurve zur Stufe N und zwei Kopien des Raumes der Modulformen derselben Stufe und Gewicht 2 ergibt. Durch Einführung eines lokalen Systems kann man auch beliebiges größeres Gewicht erreichen.

Die oben erwähnte geometrische Beschreibung der Hecke-Operatoren lässt sie auch auf der Homologie linear operieren. Da die Kenntnis der Hecke-Operatoren ja genügt, um Modulformen zu beschreiben, brauchen wir also nur die Hecke-Operatoren auf der Homologie zu berechnen. Die erste Homologie hat eine kombinatorische Beschreibung mittels des Modulsymbolformalismus (siehe zum Beispiel [13]), die zu einer Darstellung des Vektorraums der ersten Homologie auf dem Computer verwendet wird. Hier sind zwei Punkte zu betonen:

> **Hecke-Operatoren sind explizit gegebene lineare Abbildungen auf dem Vektorraum der Modulsymbole.**

Homologie kann man mit rationalen Koeffizienten definieren, genauso wie Modulsymbole. Daraus kann man zum Beispiel schließen, dass der Vektorraum der Modulformen zu beliebigem Gewicht und beliebiger Stufe eine Basis bestehend aus Modulformen besitzt, deren sämtliche Fourier-Koeffizienten rationale Zahlen sind. Dies hat zur Konsequenz:

> **Alle Rechnungen können mit rationalen Zahlen, also exakt, durchgeführt werden.**[2]

Modulformen in MAGMA und SAGE

Die Berechnung von Modulformen mittels Modulsymbolen ist in den Computeralgebrasystemen MAGMA und SAGE implementiert. Beide Implementationen gehen auf William Stein, den Hauptinitiator von SAGE, zurück. In seinem Lehrbuch [13] beschreibt er sehr detailliert die verwendeten Algorithmen und gibt eine große Anzahl an Beispielen. Kilfords Lehrbuch zu Modulformen [11] enhält ebenfalls viele Beispiele zur Berechnung von Modulformen in MAGMA und SAGE.

Zahlkörper

Ein frühes Beispiel zur zahlentheoretischen Bedeutung von Modulformen haben wir oben bereits gesehen. Weitergehende Bedeutung erlangten Modulformen in der zweiten Hälfte des 20. Jahrhunderts, da sie zahlentheoretische Strukturen auf eine sehr tief liegende Weise beschreiben. Diese kann man leicht formulieren. Um dies zu tun, müssen wir allerdings etwas ausholen.

Ein ganz wichtiges Hilfsmittel der algebraischen Zahlentheorie sind sogenannte *Zahlkörper*. Man erhält einen Zahlkörper als diejenigen komplexen Zahlen, die sich als Linearkombination mit rationalen Koeffizienten von Potenzen der Nullstelle eines rationalen Polynoms schreiben lassen. Jeder Zahlkörper ist ein endlichdimensionaler $\mathbb{Q}$-Vektorraum; die Dimension nennt man den *Grad* des Zahlkörpers. Der berühmteste Zahlkörper ist wohl der der Gaußschen Zahlen, den man aus $\mathbb{Q}$ und $i = \sqrt{-1}$ erhält. Mit seiner Hilfe kann man u. A. zeigen, dass es genauso viele Primzahlen gibt, die beim Teilen durch 4 den Rest 1 lassen, wie solche, deren Rest 3 ist.

Beim Rechnen in Zahlkörpern muss man aber etwas aufpassen, da man keine eindeutige Primzerlegung mehr hat. Wir erinnern uns an die Aussage des Hauptsatzes der elementaren Zahlentheorie, dass sich jede natürliche Zahl auf bis auf die Reihenfolge eindeutige Art als Produkt von Primzahlen darstellen lässt. Kummer hat, um diesem Mangel in Zahlkörpern abzuhelfen, sogenannte *Ideale* eingeführt und gezeigt, dass sich jedes Ideal eindeutig als Produkt von Primidealen schreiben lässt. Das ist dann so: Für jede Primzahl p gibt es ein oder mehrere eindeutig bestimmte paarweise verschiedene Primideale

[2] Das ist bei den reellen Analoga, den Maaß-Formen, nicht der Fall.

$P_1, \ldots, P_r$, so dass sich das Hauptideal zu p als Produkt

$$(p) = P_1^{e_1} \cdot \ldots \cdot P_r^{e_r} \tag{4}$$

faktorisiert. Der Normalfall ist $e_1 = \ldots = e_r = 1$; diesen nennt man *unverzweigt*. In den Gaußschen Zahlen gilt zum Beispiel $(p) = P_1 P_2$ mit zwei verschiedenen Idealen genau dann, wenn p beim Teilen durch 4 den Rest 1 lässt; ist der Rest 3, dann gibt es genau ein Ideal; nur $p = 2$ ist verzweigt. Eine wichtige Frage der *Arithmetik eines Zahlkörpers* ist:

Wie faktorisiert (p) als Produkt von Primidealen in einem Zahlkörper?

Galois-Symmetrien

In diesem Artikel möchte ich Selbstabbildungen eines Zahlkörpers als *Galois-Symmetrien* (nach Evariste Galois) bezeichnen. Die Gruppe aller Galois-Symmetrien heißt *Galois-Gruppe*.[3]

Um jetzt den Bezug zur Frage herzustellen, betrachten wir *Frobenius-Symmetrien*: Für jedes unverzweigte Primideal P im Zahlkörper gibt es die Galois-Symmetrie Frob_P: Wenn wir die ganzen Zahlen des Zahlkörpers modulo P nehmen, erhalten wir eine endliche Erweiterung des Körpers mit p Elementen, und die Galois-Symmetrie Frob_P ist dadurch charakterisiert, dass sie auf dem endlichen Körper als p-te Potenz operiert. Da Frob_P durch p bis auf Konjugation bestimmt ist, schreiben wir einfach Frob_p. Es gilt, dass die Anzahl r aus Gleichung (4) mal der Ordnung von Frob_p den Grad des Zahlkörpers ergibt.

Die Frobenius-Symmetrien Frob_p in der Galois-Gruppe eines Zahlkörpers beschreiben, wie sich Primzahlen im Zahlkörper in Primideale faktorisieren.

Das wollen wir wissen, und das können wir in bestimmten Fällen mittels Modulformen ausrechnen! Dazu kommen wir in Kürze. Für das Weitere bezeichne $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ die Galois-Gruppe des algebraischen Abschlusses von $\mathbb{Q}$ in $\mathbb{C}$: Es ist die Gruppe aller Galois-Symmetrien.

Galois-Darstellungen

Um Gruppen zu studieren, benutzt man Darstellungen. Ist die Gruppe eine Galois-Gruppe, so spricht man von einer *Galois-Darstellung*. Die Spur einer Darstellung nennt man *Charakter*, und der Charakter bestimmt irreduzible Darstellungen eindeutig. Wir erinnern uns, dass die Spur einer Matrix als die Summe ihre Diagonaleinträge definiert ist und dass sie unter Konjugation invariant ist. Daher können wir nun eindeutig vom Wert bei Frob_p des Charakters einer Galois-Darstellung reden. Man weiß, dass diese Werte den Charakter eindeutig festlegen, wenn p die Primzahlen durchläuft.[4]

Der Satz von Shimura und Deligne

Um die Verbindung zu den Modulformen herzustellen, blicken wir zurück auf deren Berechnung. Dazu werden, wie oben erwähnt, Modulsymbole, also die erste Homologie der entsprechenden Modulkurve, verwendet. Betrachtet man die Modulkurve genauer, stellt man fest, dass sie als Lösungsmenge von Polynomen mit rationalen Koeffizienten geschrieben werden kann. Somit ergibt jede Galois-Symmetrie, also jedes Element von $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, insbesondere Frob_p, eine Selbstabbildung der Modulkurve. Weiter hat dies zur Folge, dass Methoden der arithmetischen Geometrie, die auf Grothendieck zurückgehen, greifen und man statt Homologie auch ℓ-adische Etale-Kohomologie verwenden kann.[5] Insgesamt haben wir somit auf den Modulsymbolen zwei lineare Operationen: die der Hecke-Operatoren und die von $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

Sei f eine normierte Hecke-Eigenform.[6] Da der Eigenraum zu den Hecke-Eigenwerten auf f im Raum der Modulformen eindimensional ist, folgt, dass der entsprechende Eigenraum in der ersten Homologie die Dimension 2 hat. Da die Hecke-Operatoren mit den Galois-Symmetrien vertauschen, erhält man eine stetige lineare $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-Operation auf diesem Raum, also eine (ℓ-adische) Galois-Darstellung

$$\rho_{f,\ell} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{Q}}_\ell). \tag{5}$$

Durch Analyse der Reduktion der Modulkurve modulo p konnten Eichler, Shimura und Deligne zeigen, dass der Charakter $\Theta_{f,\ell}$ dieser Darstellung für alle unverzweigten p die bemerkenswert einfache Formel

$$\Theta_{f,\ell}(\mathrm{Frob}_p) = a_p(f) \tag{6}$$

erfüllt, dass er also durch die Koeffizienten der Modulform f gegeben ist! Weiter gilt, dass $\Theta_{f,\ell}$ bei der komplexen Konjugation den Wert 0 annimmt. Man sagt dann, dass die Galois-Darstellung *ungerade* ist. Wir halten fest:

Jede Hecke-Eigenform beschreibt eine ungerade ℓ-adische Galois-Darstellung.

Zahlkörper zu residuellen Galois-Darstellungen

Für den Rest dieses Artikels beschränken wir uns auf

[3] Wir nehmen in diesem Artikel stets an, dass die Zahlkörper so viele Galois-Symmetrien haben wie ihr Grad, dass sie also *galoissch über* $\mathbb{Q}$ sind.

[4] Es dürfen sogar endlich viele Primzahlen ausgelassen werden.

[5] Hier und im Folgenden sei ℓ eine Primzahl.

[6] Wir sehen im Folgenden ihre Koeffizienten als Elemente von $\overline{\mathbb{Q}}_\ell$ via einer fixierten Einbettung $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_\ell$.

eine Konsequenz hiervon: Durch Reduktion modulo ℓ erhalten wir die (residuelle) Darstellung

$$\overline{\rho}_{f,\ell} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell). \tag{7}$$

Galois-Theorie zeigt, dass es dann einen Zahlkörper $K_{f,\ell}$ gibt, dessen Galois-Gruppe eine Untergruppe von $\mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ ist. Dieser Zahlkörper ist vollständig durch f bestimmt, seine Galois-Gruppe kann einfach berechnet werden, und für die meisten p kann man aus $a_p(f)$ modulo ℓ bestimmen, in wieviele Primideale p in K_f faktorisiert.

Die Fourier-Koeffizienten der Hecke-Eigenform f beschreiben für jede Primzahl ℓ die Arithmetik des Zahlkörpers $K_{f,\ell}$.

Normalerweise stellt man einen Zahlkörper als Quotienten des Polynomringes über $\mathbb{Q}$ modulo einem rationalen Polynom dar. Wir bezeichnen mit $\phi_{f,\ell}$ ein Polynom zu $K_{f,\ell}$. Die Zahlkörper $K_{f,\ell}$ und somit auch die Polynome $\phi_{f,\ell}$ werden allerdings sehr schnell sehr groß. Zum Beispiel würde selbst unter der Annahme, dass alle Koeffizienten nur 0 oder 1 sind, also durch ein Bit beschrieben werden können, das Polynom $\phi_{f,2}$ zu einer bestimmten Eigenform f in Stufe 3313 und Gewicht 2 bereits 10^{28} GB Speicher einnehmen. Ginge man weiter, überschritte man so sicherlich die Anzahl der Atome im Universum recht schnell. Um so erstaunlicher ist, dass wir mittels der Modulform über den Zahlkörper doch wichtige arithmetische Aussagen treffen können!

Der Algorithmus von Edixhoven et. al.

Umgekehrt, wenn man in kleinem Grad ist und ein Polynom $\phi_{f,\ell}$ zum Zahlkörper $K_{f,\ell}$ kennt, dann kann man es benutzen, um Modulformen modulo ℓ auszurechnen. Macht man dies für genügend viele ℓ, erhält man Koeffizienten der Modulform aus dem chinesischen Restsatz, da die Koeffizienten beschränkt sind. Die Berechnung von $a_p(f)$ aus dem Polynom besteht im Wesentlichen aus der Faktorisierung des Polynoms modulo p.

Die neueste sehr wichtige Entwicklung in diesem Gebiet ist ein Algorithmus, der in den letzten Jahren von Edixhoven, Couveignes und anderen [8] entwickelt und in einer Variante von Johan Bosman implementiert wurde: Zu einer Eigenform f und einer Primzahl ℓ wird das Polynom $\phi_{f,\ell}$ berechnet. Dieses erlaubt also insbesondere die Berechnung der Koeffizienten von Modulformen. In seiner gerade verteidigten Doktorarbeit beweist Peter Bruin [2], dass (unter der technischen Annahme quadratfreier Stufe und der verallgemeinerten Riemannschen Vermutung) die Komplexität der Berechnung von $a_p(f)$ mit dieser Methode polynomial in der Bitlänge von p, also $\log(p)$, ist. Die Komplexität im Modulsymbolalgorithmus ist polynomial in p, also exponentiell in $\log(p)$. Die obige Speicherabschätzung zeigt aber bereits, dass trotz des theoretischen Vorteils bei diesem Verfahren praktische Probleme auftreten.

Man kann den neuen Algorithmus als einen Schritt hin zur Verallgemeinerung konstruktiver Klassenkörpertheorie auf GL_2 ansehen. Als kleine Illustration kann dienen, dass Johan Bosman [1] mit seiner Implementierung das erste bekannte Polynom mit Galois-Gruppe $\mathrm{SL}_2(\mathbb{F}_{16})$ gefunden hat.

Die Serresche Modularitätsvermutung

Nach diesem Exkurs über die Berechnung der Galois-Darstellungen zu einer Eigenform kommen wir jetzt zur Serre-Vermutung, also dem Satz von Khare, Wintenberger und Kisin:

Jede irreduzible[7] ungerade Galois-Darstellung $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ kommt von einer Eigenform f, ist also von der Form $\overline{\rho}_{f,\ell}$.

Der Satz ist sogar noch viel stärker: Er gibt Formeln für die Stufe und das Gewicht der zugehörigen Modulform an. Die Stufe berechnet sich dabei aus der Verzweigung in Primzahlen ungleich ℓ und das Gewicht aus der Verzweigung bei ℓ. Eine Umformulierung ist, dass Hecke-Eigenformen zweidimensionale irreduzible ungerade Galois-Darstellungen parametrisieren.

Konsequenzen

Eine Motivation für Serre bei seiner Vermutung war, dass sie den *großen Satz von Fermat* impliziert. Somit gibt es jetzt auch einen neuen Beweis dieses Satzes.[8] Der Startpunkt ist auch hierbei die Idee von Gerhard Frey, einer hypothetischen ganzzahligen Lösung der Gleichung $a^p + b^p = c^p$ die elliptische Kurve $y^2 = x(x - a^p)(x + b^p)$ zuzuordnen; ihre p-Teilungspunkte geben eine irreduzible ungerade Galois-Darstellung. Nach der Serre-Vermutung gehört hierzu eine Hecke-Eigenform von Stufe 2 und Gewicht 2. Eine solche gibt es aber nicht, somit gibt es auch nicht die hypothetische Lösung. Von diesem Beweistyp sind viele Variationen mit ähnlichen Gleichungen möglich.

Die Serre-Vermutung hat aber auch die *Taniyama-Shimura-Vermutung*, die von Wiles und Taylor im Spezialfall semistabiler elliptischer Kurven für den ursprünglichen Beweis des Satzes von Fermat gelöst worden ist, samt ihrer Verallgemeinerung auf rationale abelsche Varietäten vom GL_2-Typ zur Folge: *Diese sind modular*, d. h. ihre L-Reihe stimmt mit der einer Modulform überein. Eine weitere Konsequenz der Serre-Vermutung ist die berühmte *Artin-Vermutung*, also die analytische Fortsetzbarkeit der L-Reihe von komplexen Galois-Darstellungen, im Spezialfall ungerader Darstellungen $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{C})$.

[7] Irreduzibilität ist keine Einschränkung, da reduzible halbeinfache Galois-Darstellungen vollständig durch Klassenkörpertheorie beschrieben werden können.

[8] Da die Methoden zum Beweis der Serre-Vermutung Weiterentwicklungen derer von Wiles sind, kann man aber nicht von einem grundsätzlich verschiedenen Beweis reden.

Bedeutung in der Computeralgebra

Die wichtigsten Konsequenzen der Serre-Vermutung für die Computeralgebra wollen wir noch einmal auflisten:

1. **Modulformen, die mit Computeralgebra berechnet werden können, parametrisieren Galois-Darstellungen obigen Typs.**
2. **Wichtige arithmetische Eigenschaften dieser Galois-Darstellungen lassen sich durch Rechnungen mit Modulformen bestimmen.**

Eine theoretische Konsequenz der Serre-Vermutung ist der Satz, dass es für jede Primzahl ℓ nur endlich viele Isomorphieklassen von irreduziblen ungeraden und außerhalb von ℓ unverzweigten Darstellungen $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ gibt. Mit Hilfe der Computeralgebra kann man also all diese auflisten und das Wachstum ihrer Anzahl als Funktion von ℓ studieren (siehe [5] und [4] für neue Arbeiten).

Ich beschäftige mich derzeit u. A., theoretisch und mittels Computeralgebra, mit der Rolle von Modulformen von Gewicht eins und arbeite zusammen mit Panagiotis Tsaknias daran, Eigenschaften ℓ-adischer Galois-Darstellungen durch Modulformen modulo ℓ^n zu bestimmen.

Ausblick

Mit dem Beweis der Serre-Vermutung wurde zwar ein Kapitel abgeschlossen; es ist aber nur das erste Kapitel eines großen Buches, dessen Umfang wir noch nicht abschätzen können. Emerton versteht die Serre-Vermutung als eine Lokal-Global-Kompatibilitätsaussage im mod-p-Langlands-Programm von Breuil und Colmez. Auch gibt es Formulierungen von „Serre-Vermutungen“ für Hilbertsche Modulformen [3] und für Modulformen über imaginärquadratischen Zahlkörpern [14]. Für all diese gibt es einige numerische Evidenz, die mittels Computeralgebra gewonnen wurde (z. B. [7]). Wir dürfen gespannt sein, wie die Entwicklungen fortschreiten. Die Computeralgebra wird dabei ihre Rolle spielen.

Literatur

[1] Johan Bosman. *A polynomial with Galois group* $\mathrm{SL}_2(\mathbb{F}_{16})$. LMS J. Comput. Math. 10 (2007), 378-388.

[2] Peter Bruin. *Modular curves, Arakelov theory, algorithmic applications.* Dissertation, Universiteit Leiden, 2010.

[3] Kevin Buzzard, Fred Diamond and Frazer Jarvis. *On Serre's conjecture for mod l Galois representations over totally real fields.* arXiv:0810.2106.

[4] Tommaso Giorgio Centeleghe. *Computing the number of certain Galois representations mod p.* arXiv:1008.2059.

[5] Craig Citro and Alexandru Ghitza. *Enumerating Galois representations in Sage.* arXiv:1006.4084v2.

[6] J. E. Cremona. *Algorithms for modular elliptic curves.* Second edition. Cambridge University Press, Cambridge, 1997. Online-Version: `http://www.warwick.ac.uk/~masgaj/book/fulltext/index.html`

[7] Lassina Dembélé. Anhang zum Artikel *Sur une question de compatibilité local-global modulo p* von Christophe Breuil. Preprint, 2009.

[8] Bas Edixhoven, Jean-Marc Couveignes, Robin de Jong, Franz Merkl, Johan Bosman. *Computational aspects of modular forms and Galois representations.* Erscheint als Buch in der Serie *Annals of Mathematics Studies* bei Princeton University Press, arXiv:math/0605244v3.

[9] Chandrashekhar Khare and Jean-Pierre Wintenberger. *Serre's modularity conjecture. I.* Invent. Math. 178 (2009), no. 3, 485-504.

[10] Chandrashekhar Khare and Jean-Pierre Wintenberger. *Serre's modularity conjecture. II.* Invent. Math. 178 (2009), no. 3, 505-586.

[11] L. J. P. Kilford. *A classical and computational introduction.* Imperial College Press, London, 2008.

[12] Mark Kisin. *Modularity of 2-adic Barsotti-Tate representations.* Invent. Math. 178 (2009), no. 3, 587-634.

[13] William Stein. *Modular forms, a computational approach.* With an appendix by Paul E. Gunnells. Graduate Studies in Mathematics, 79. American Mathematical Society, Providence, RI, 2007.

[14] Rebecca Torrey. *On Serre's Conjecture Over Imaginary Quadratic Fields.* PhD thesis, King's College London, 2009.

Was Schüler über CAS wissen – was Schüler über CAS wissen sollten

Reinhard Oldenburg
(Goethe-Universität Frankfurt)

oldenbur@math.uni-frankfurt.de

Einleitung

Wenn Mathematik mit Hilfe von Werkzeugen betrieben wird, ist das nicht ohne Rückwirkung auf die Mathematik selbst: Die symbolische Schreibweise erlaubte zunächst nur, Sachverhalte, die bereits in der Antike bekannt waren, prägnanter auszudrücken, führte dann aber rasch dazu, dass neue Einsichten gewonnen und – noch wichtiger – neue mathematische Objekte wie Wurzeln und imaginäre Zahlen anerkannt wurden. In der Geometrie wandelt sich der Konstruktionsbegriff mit den zugelassenen Zeichenwerkzeugen. Der Einfluss verschiedener Werkzeuge ist dabei unterschiedlich. Der übliche Taschenrechner dürfte weniger bewirken als Computeralgebrasysteme. Sie sind die komplexesten der bisher im Mathematikunterricht eingesetzten Softwareprodukte. Sie kompetent nutzen zu können, ist eine Herausforderung für Schüler wie Lehrer, die zu einem langen Instrumentationsprozess [3] führt. In diesem Beitrag soll diskutiert werden, was Schüler über CAS wissen sollten – und was sie nach Beobachtungen tatsächlich wissen.

Modellvorstellungen

Erklärung ist eine wichtige Funktion von Modellen. Geeignete Modellvorstellungen (siehe z. B. [2]) können dem Benutzer das Verhalten des Computers erklären und damit Hilfen zu seiner korrekten Benutzung geben. Solche Modellvorstellungen geben das Gefühl eines Verständnisses und erhöhen damit die emotionale Akzeptanz des Werkzeugs. Selbst wiederum ein Modell für diese Sachverhalte gibt die folgende Modellvorstellung zur numerischen Nullstellensuche, wie sie beispielsweise von grafikfähigen Taschenrechnern angeboten wird: Bei der numerischen Nullstellenberechnung handelt es sich um eine rechnerische Suche, bei der, beginnend mit einem Startwert, ein schrittweises Herantasten erfolgt, bis der Funktionswert sehr klein ist.

Dieses einfache Modell erklärt:

1. Nullstellen werden evtl. nicht exakt gefunden.
2. Es können auch fälschlich Nullstellen gefunden werden, z. B. weil der Funktionswert unter der Toleranzgrenze liegt.
3. Es kann höchstens eine Nullstelle gefunden werden.
4. Zum Finden weiterer Nullstellen muss man von anderer Stelle (dazu ist Wissen über die Funktionstypen wichtig) neu starten.

Nach Beobachtungen im Unterricht zerfallen die Schüler in der Sekundarstufe II in zwei Gruppen: Diejenigen, die diese Modellvorstellungen erworben haben, benutzen die numerische Nullstellensuche kompetent, während die anderen diese als nicht nützlich empfinden und ablehnen. Damit stellt sich in Bezug auf CAS die folgende Aufgabe: Es sollte identifiziert werden, welche Modellvorstellungen zur Arbeit von Computeralgebrasystemen in der Lage sind, die kompetente CAS-Nutzung anzuleiten.

CAS – geeignete Modellvorstellungen

Hier soll, analog zum obigen Modell, ein einfaches Modell zur technischen Basis von CAS vorgestellt werden. Es umfasst folgende Komponenten:

1. Trennung: Rechenzentrale – Darstellung (EVA). Dies erklärt, dass das, was auf dem Bildschirm steht, erst durch die Verarbeitung wirksam wird.
2. CAS haben eine Variablen-Wert-Tabelle; darin darf die Wertespalte leer sein. Vorhandene Werte werden immer eingesetzt, aber es gibt keine automatische Variablenbelegung z. B. bei solve. Dies erklärt, wie man zwischen Zuweisung und Substitution wählt, und dass

   ```
   x:=y; y:=x
   ```

   unzulässig ist.

3. Alle Objekte sind (verallgemeinerte) Terme, aufgebaut aus einem Kopf und einer Anzahl von Operanden (Baumdarstellung). Dies erklärt u. A. die Wirkungslosigkeit (bei einigen CAS) von

```
subs(sqrt(x^2+y^2+z^2),
     x^2+y^2=r^2)
```

4. Operationen werden durch Regelbefolgung durchgeführt, d. h., wenn die Form passt, wird ausgeführt: In Maxima kann man beispielsweise 0 zu einer Zeichenkette addieren.

5. Die Auswertung ist ein Ersetzen von Teiltermen nach Regeln. Diese sind teilweise nur eingeschränkt gültig:

```
sqrt(x^2)
```

wird in der Regel nicht vereinfacht.

6. Sonderfälle werden in der Regel nicht beachtet. Das erklärt z. B., dass

```
subs(int(x^n,x), n=-1)
```

falsch ist.

7. Die Art der Daten legt mögliche Operationen fest (z. B. Menge und Liste nicht verwechseln, Term oder Funktion angeben).

Dieses Modell lässt noch vieles unspezifiziert. Allein zum Teilbereich des Gleichungslösens muss ein detailliertes Modell noch viel mehr umfassen:

1. Lösungen sind Substitutionen, die die Ausgangsgleichung zur Identität machen.

2. Sonderfälle werden i. A. nicht beachtet, z. B. in $a * x = b$.

3. Die Variablennamen sind bedeutungslos, man kann $a * x = b$ nach a auflösen.

4. Für Polynomialgleichungen über Grad 4 gibt es evtl. keine Darstellung mit Wurzeln: Darstellung durch algebraische Zahlen (RootOf-Objekte).

5. Lineare und polynomielle Gleichungssysteme sind immer lösbar.

6. Transzendente Gleichungen können nur in Ausnahmefällen symbolisch gelöst werden.

Dies demonstriert die angesprochene Komplexität und zeigt, dass man nicht davon ausgehen kann, dass durchschnittliche Schüler ein so detailliertes Modell aufbauen werden.

Schülervorstellungen

Besitzen Schüler nach längerer Arbeit mit einem CAS angemessene Vorstellungen, die dem skizzierten Modell nahe kommen? Um diese Frage zumindest in Ansätzen zu beantworten, wurde den 18 SchülerInnen (8 weiblich, 10 männlich) eines Mathematik-Leistungskurses kurz vor dem Abitur ein Fragebogen vorgelegt. Die Schüler benutzen den CAS-Taschenrechner TI92+ seit Beginn der elften Jahrgangsstufe.

In einem ersten Teil wurden affektive Items durch Zustimmung zu vorgelegten Aussagen auf einer Skala von -3 bis $+3$ erhoben (mit Mittelwert μ und Standardabweichung σ):

Nr.	Item	μ	σ
1	Ich arbeite gerne mit dem TI89 bzw. mit dem TI92.	1,0	0,7
2	Der TI hilft, eigene Ideen bis zu Ende zu verfolgen.	0,76	1,0
3	Ich kenne mich mit dem TI ganz gut aus.	0,66	0,8
4	Ich vertraue den Ergebnissen des Rechners.	0,44	0,98
5	Die Bedeutung der Ausgaben ist immer klar.	0,11	1,1
6	In Situationen ohne den Rechner fühle ich mich unsicher.	-0,67	1,14

Ergebnisse: Items 1 und 3 korrelieren fast signifikant ($p = 0,057$), Items 3 und 6 korrelieren interessanterweise signifikant negativ. Es gibt keine Korrelation zwischen Items 1 und 4: $r = -0,078, p = 0,76$. Varianzaufklärung zeigt, dass die Leistungsvarianz zu 51% von affektiven Variablen erklärt wird; besonders wichtig sind dabei die Items 2 und 5. Dagegen ist Item 4 (Vertrauen) praktisch unwichtig (Schlussfolgerung: Die Schüler und Schülerinnen vertrauen oft zu unrecht!).

Schülerleistungen

In einem Testteil ohne Zugang zum CAS sollten die Schüler einige CAS-Ausgaben interpretieren (in Klammern die Anteile der Nennungen):

Item 1: Gibt der TI bei der Eingabe

```
factor(1+x+x^2+x^3+x^4)
```

die Ausgabe

```
1+x+x^2+x^3+x^4,
```

dann bedeutet dies:

1. Der TI konnte keine Produktdarstellung finden. (50%)

2. Es gibt definitiv keine Produktdarstellung nur mit rationalen Zahlen. (50%)

Item 2: Gibt der TI bei der Eingabe

```
solve(x^2-y^2/2+2*x=5 and
        x^2+2*x-5/3+1/3*y^2-4/3*y=0,
      {x,y})
```

die Ausgabe

```
false,
```

dann bedeutet dies:

1. Der TI konnte keine Lösung finden. (28%)
2. Es gibt definitiv keine reelle Lösung. (28%)
3. Es ist bewiesen, dass es überhaupt keine Lösung gibt. (56%)

Item 3: Gibt der TI bei der Eingabe

```
solve(e^x-x=0,x)
```

die Ausgabe

```
e^x-x=0,
```

dann bedeutet dies:

1. Der TI konnte keine Lösung finden. (66%)
2. Es gibt definitiv keine reelle Lösung. (28%)
3. Es ist bewiesen, dass es überhaupt keine Lösung gibt. (0%)

Item 4: Zeigt die folgende Rechnung einen Fehler des Computeralgebrasystems?

```
int(1/x^2,x) -> F
```

Antwort: F=-1/x

```
(F|x=1) - (F|x=-1)
```

Antwort: -2

```
int(1/x^2,x,-1,1)
```

Antwort: Unendlich

Zu diesem Item haben erfreuliche 61% eine gute und korrekte Lösung angegeben. Das zeigt, dass die Verwendung eines CAS nicht zu Lasten der mathematischen Kritikfähigkeit gehen muss.

Es gab auch Aufgaben, in denen das CAS zugelassen war:

Item 5: Die Eingabe `expand(log(3*a))` liefert eine Summenschreibweise, `expand(log(a*b))` dagegen nicht. Woran liegt das? Kann man den zweiten Term trotzdem mit dem TI in Summenform schreiben lassen? Korrekte Lösung: 0%

Schlussfolgerungen: Schüler können nur bedingt verlässlich einschätzen, ob negative Antworten mathematische oder technische Gründe haben. Immerhin gibt es dazu offensichtlich gewisse Vorstellungen, obwohl diese Fragen im Unterricht nicht thematisiert wurden.

Perspektiven für die Lehre

CAS stellen ein didaktisches Problem dar, denn geeignete Modellvorstellungen sind wesentlich komplexer als beim GTR. Der Informatikunterricht könnte, wo er erteilt wird, hier Wesentliches zuliefern: Es ist möglich, die Grundfunktionen eines Computeralgebrasystems in einem Modell-System zu rekonstruieren. Mit einem noch überschaubaren Code-Umfang von 200 bis 300 Zeilen lassen sich simple Vereinfachungen, Substitution und Differenzieren umsetzen. Allerdings besteht derzeit seitens der Informatikdidaktik kein großes Interesse an einer solchen fächerverbindenden Zusammenarbeit, und außerdem erreicht Infomatikunterricht nur einen Bruchteil der Schüler und Schülerinnen.

Man kann aber Leistung und Grenzen von CAS auch ohne Programmieren zum Unterrichtsgegenstand machen. Zum Einen kann auf mathematischer Ebene geklärt werden, welche Problemklassen algorithmisch berechenbar sind (und in CAS typischerweise implementiert sind), so dass man z. B. aus einer negativen Antwort des CAS schließen kann, dass keine Lösung existiert. Dies sollte meines Erachtens zumindest das Wissen umfassen, dass Polynome über den rationalen Zahlen, wenn sie faktorisierbar sind, auch zerlegt werden, dass „leere Menge“ als Lösung eines polynomiellen Gleichungssysteme tatsächlich aussagt, dass es keine Lösung gibt, und dass bei transzendenten Termen und Gleichungen nur sehr kleine Teilklassen algorithmisch beherrscht sind. Dies sind auch wichtige Erkenntnisse für die Lehrerausbildung. Eine Lehrkraft sollte wissen, dass schon die schlichte Aufgabe „Vereinfache einen vorgelegten Term, der die Sinusfunktion enthalten kann, zu 0, wenn möglich“ algorithmisch nicht entscheidbar ist, denn daraus folgt einerseits eine Relativierung der Bedeutung der beliebten „Vereinfache“-Aufgaben, andererseits versteht man so, warum man sich bei komplexen symbolischen Rechnungen oft nicht sicher sein kann, ob das Ergebnis gilt, denn im Laufe der Rechnung könnte ja (trotz Vereinfachung) unbemerkt durch 0 dividiert worden sein.

Zum Anderen kann man die Arbeitsweise eines CAS auch mit Papier, Bleistift und Radiergummi nachspielen. Dazu müssen zunächst CAS-übliche Termdarstellungen behandelt werden, z. B.

```
x+y+5
```

als

```
(+ x y 5)
```

und

```
x^2+3x-y/z
```

als

```
(+ (^ x 2) (* 3 x)
    (* -1 (* y (^ z -1))))
```

Diese aus Lisp entlehnte Schreibweise macht das Assoziativitätsgesetz überflüssig, erlaubt ein Sortieren der Terme, und außerdem werden − und / als Operatoren unnötig! An der ersten Stelle jeder Klammer erkennt man sofort, um welche Art Operator es sich handelt, ohne auf Vorrangregeln achten zu müssen. Damit dürfte plausibel sein, dass diese Termdarstellung eine gute Grundlage bietet, um das mechanische Abarbeiten von algebraischen Algorithmen zu beschreiben. Die CAS-Regeln kann man explizit aufschreiben, z. B.:

```
(expand (* A (+ B1 B2))) =>
  (+ (* A B1) (* A B2))

(diff (* A B) X) =>
  (+ (* A (diff B X))
     (* (diff A X) B))
```

und auf Papier ausführen. Dies kann ein Gefühl geben für die Arbeitsweise eines CAS und wesentliche Teile der im dritten Abschnitt beschriebenen Modellvorstellung hervorbringen.

Reflektionen zum aktuellen Stand der CAS-Nutzung

Die obigen Überlegungen zeigen, dass CAS sinnvollerweise nicht nur zum Unterrichtsmittel sondern auch zum Unterrichtsgegenstand gemacht werden sollten, wie dies auch in [4] nahe gelegt wird. Dieser Forderung stehen zwei Argumente entgegen:

Ein Einwand lautet, dass die CAS in ihrem Verhalten immer näher an intuitive Vorstellungen herankommen. Je besser beispielsweise bei Substitutionen oder beim Pattern Matching die Assoziativität von Operatoren umgesetzt wird, um so weniger braucht man über Termdarstellungen wissen. Ich hege allerdings Zweifel, ob diese Sicht korrekt ist: Wenn man beispielsweise mit einem wenig technisch erscheinenden CAS einen Teilterm mit der Maus auswählt, stellt man fest, dass man bestimmte Teile auswählen kann, andere dagegen nicht und darin zeigen sich eben auch an der Oberfläche die internen Strukturen.

Ein anderer Einwand lautet, dass Mathematik gelehrt werden solle, nicht ihre technische Umsetzung. Auch hier habe ich Zweifel, ob das stichhaltig ist, denn die Erfahrung, dass und wie Mathematik maschinisierbar ist, kann durchaus den Anspruch erheben, allgemeinbildend zu sein.

Vor allem aber ist zu befürchten, dass durch die Verkürzung der Schulzeit und die Reduktion auf Kernlehrpläne die Bedeutung von CAS für die Schule zurückgehen wird. Denn CAS lohnt sich nur, wenn mit substantiellen und interessanten algebraischen Objekten gearbeitet wird. Ein schönes Beispiel schon für die Sekundarstufe I wurde von Paul Drijvers [1] gegeben: die Linsengleichung. Diese verschwindet aber gerade aus der Schule.

Die zukünftige Bedeutung von CAS in der Schule und die Art der Behandlung liegen heute ebenso im Ungewissen wie vor 10 oder 20 Jahren. Es gibt hier immer noch ein riesiges Betätigungsfeld für die Didaktik.

Literatur

[1] Drijvers, P.: *Die variable Unbekannte. Facetten des Variablenbegriffs mit Computeralgebra erkunden.* In: Mathematik lehren, Heft 136 (2006).

[2] Gentner, D., Stevens, A.: *Mental Models.* Lawrence Erlbaum 1980.

[3] Guin, D., Ruthven, K., Trouche, L.: *The Didactical Challenge of Symbolic Calculators.* Springer 2005.

[4] Hischer, H.: *Mathematikunterricht und Neue Medien – Hintergründe und Begründungen in fachdidaktischer und fachübergreifender Sicht.* Franzbecker 2002.

CAS-Einsatz im betriebswirtschaftlichen Umfeld

Markus Wessler
(Hochschule für angewandte Wissenschaften München)

markus.wessler@hm.edu

Zusammenfassung

Seit dem Wintersemester 2009/2010 wird in der Erstsemestervorlesung *Wirtschaftsmathematik* an der betriebswirtschaftlichen Fakultät der Hochschule für angewandte Wissenschaften München der Taschenrechner TI-*n***spire CAS** von Texas Instruments eingesetzt. Dieser Beitrag ist ein Erfahrungsbericht über die ersten beiden Semester.

Einführung

Wer an der betriebswirtschaftlichen Fakultät einer Hochschule mit der Vermittlung von Mathematik zu tun hat, der weiß, dass hier häufig großer Unmut über den mathematischen Lehrstoff geäußert wird, ein Unmut, der sich auf die falsche, aber weit verbreitete Meinung gründet, dass der vermittelte Stoff doch für die Praxis gar nicht relevant sei: „Das brauchen wir doch nie wieder!“ Als Lehrender kämpft man an mehreren Fronten: Die Studierenden, von denen erstaunlich viele der Meinung sind, die Betriebswirtschaft komme gänzlich ohne Mathematik aus, müssen eines Besseren belehrt, motiviert und durch die Prüfungen geschleust werden; gleichzeitig muss die Notwendigkeit eines mathematischen Grundwissens manchmal selbst vor Kollegen verteidigt werden.

Die Vorlesung *Wirtschaftsmathematik*, die im ersten Semester des Bachelor-Studiengangs Betriebswirtschaft vierstündig angeboten wird, soll die für die Anwendungen in den Wirtschaftswissenschaften relevanten mathematischen Methoden bereitstellen. Hierzu gehören u. A. das Lösen linearer Gleichungssysteme, die Differential- und Integralrechnung in einer reellen Variablen, die Differentialrechnung in mehreren reellen Variablen inklusive nichtlinearer Optimierung sowie die lineare Optimierung. Im Wesentlichen handelt es sich also bei den Inhalten um Schulstoff, und zwar nicht nur gymnasialen Schulstoff, sondern auch den Stoff der Fachoberschulen (FOS) oder auch der Berufsoberschulen (BOS), zumindest derjenigen mit wirtschaftlicher Ausrichtung.[1]

Warum CAS-Einsatz?

Orientiert man sich an der sehr praxisbezogenen Ausrichtung des betriebswirtschaftlichen Studiums an der Hochschule München, so wird schnell klar, dass bei den in der Vorlesung behandelten Problemstellungen der Modellierungsaspekt im Vordergrund stehen muss; und dies ist auch vernünftig. Wir gehen üblicherweise in drei Schritten vor: Ein Praxisproblem wird vorgestellt und muss zunächst in ein mathematisches Problem übersetzt werden. Dieses wird dann gelöst und schließlich in einem letzten Schritt wieder im Sinn der Aufgabenstellung interpretiert. In der Praxis werden die Studierenden später Probleme mit Hilfe entsprechender Programme lösen; somit kommt dem ersten und dritten dieser Schritte sicher die größte Bedeutung zu, während das „Rechnen“ in den Hintergrund treten darf. Aufgrund der großen Zahl der Studierenden (rund 200), die auch leider – aus personaltechnischen Gründen – nicht in die eigentlich vorgesehenen Semestergruppen (derzeit vier an der Zahl) eingeteilt werden konnten, musste hierfür eine Lösung gefunden werden, die keinen PC erfordert. So fiel die Wahl auf einen CAS-Rechner, und zwar auf den TI-*n***spire CAS** von Texas Instruments. Der Einsatz war zunächst nur in der Wirtschaftsmathematik geplant; es wurde dementsprechend ein Semestersatz angeschafft. Die Finanzierung erfolgte durch Studiengebühren.

Was war schlecht?

Utopisch wäre die Annahme gewesen, alles werde reibungslos verlaufen; gerade im Umfeld einer BWL-Fakultät war es ein Wagnis, sich auf den Einsatz ei-

[1] Der größte Teil der Studierenden an der Hochschule München hat einen Abschluss von FOS oder BOS; die Abiturientenquote schwankt zwischen 20 % und 30 %.

nes CAS-Taschenrechners einzulassen. Recht schnell konnte man feststellen, dass der CAS-Einsatz einmal mehr ein interessantes Licht auf die Problematik der Schnittstelle Schule/Hochschule wirft. Vieles wurde in den vergangenen Jahren – auch in diesem Rundbrief – von der Entwicklung des CAS-Einsatzes an Schulen berichtet, so etwa *Der Schulversuch CAliMERO* (H. Körner, Rundbrief Computeralgebra Nr. 43, S. 26-30) oder *CAS-Einsatz aus Sicht der Schule* (J. H. Müller, Rundbrief Computeralgebra Nr. 45, S. 24-26). Die Erfahrung mit den Studierenden der Betriebswirtschaft in München lehrt jedoch, dass hier die Realität anders aussieht. Überraschend wenige Studierende verfügten über CAS-Erfahrung aus der Schulzeit oder waren gar auf Anhieb in der Lage, mit dem TI-*n***spire CAS** umzugehen. Die Mehrheit war im Umgang mit dem Taschenrechner sehr hilflos, ja, ungeschickt. Einerseits produzierten Ungenauigkeiten bei der Eingabe (wie etwa bei Klammern) Fehlermeldungen. Tückischer noch waren andererseits syntaktisch korrekte, aber nicht zum gewünschten Ziel führende Eingaben; irgendwo zwischen Problemerfassung, mathematischer Formulierung und Rechnereingabe war dann etwas schief gegangen. Sehr häufig ging es dabei um Probleme mit Variablenbelegungen, die scheinbar unüberwindbare Hürden darstellten. War in ein und derselben Sitzung beispielweise ein Produktionsvektor x definiert worden – etwa $x = (20, 50)^T$ – und sollte im späteren Verlauf die Ableitung einer Funktion mit Variablen x – etwa $\frac{d}{dx}(x^2)$ gebildet werden, so wunderten sich viele über die Ausgabe $x = (40, 100)^T$: Hier wurde die Ableitung der Funktion $f(x) = x^2$ in der Variablen x gebildet, das Ergebnis $2x$ dann aber sogleich mit dem Wert des Vektors x ausgewertet. Hier gab es viel Klärungsbedarf und wurde viel Zeit verloren.

Aber auch als erste technische Schwierigkeiten überwunden waren, lief nicht alles glatt. Beobachten konnte man das bekannte „stumpfe Automatisieren“, das sich auf vielfache Weise manifestierte: im „Ausräumen“ einer Matrix (Anwenden des Gauß-Algorithmus), nach dessen Fertigstellung dann die Frage „... und jetzt?“ steht; im blinden Ableiten, sobald eine Funktion $f(x)$ in der Aufgabenstellung auftaucht, selbst wenn vielleicht nur deren Nullstellen gesucht sind; in der Frage, was denn nun eigentlich der Unterschied zwischen einer Matrix und einem Gleichungssystem sei; etc. Fragen, die überdeutlich machen, wie sehr es an mathematischem Verständnis, am „Gefühl für Mathematik“ mangelt.

Was war gut?

Der TI-*n***spire CAS** kann natürlich eine Hilfe sein, das eben erwähnte Verständnis, das Gefühl für mathematische Zusammenhänge zu entwickeln – und er war es für einen Teil der Studierenden auch. In der konkreten Vorlesungs- und Übungssituation soll das Rechnen zum großen Teil dem CAS überlassen werden; auf diese Weise können auch tatsächliche, realistische Probleme (mit „großen Zahlen“) behandelt werden – einer der wirklich großen Vorteile. Durch schnelle Berechnung hoher Potenzen einer Markov-Matrix etwa (Abb. 1) oder durch das wirklich sehr fruchtbare Zusammenspiel der graphischen, tabellarischen und kalkulatorischen Elemente konnte den Studierenden in vielen Situationen ein gutes Gefühl für die ablaufenden Prozesse vermittelt werden. Ein tieferes Verständnis eben dieser Prozesse ist gerade für angehende Betriebswirte unerlässlich.

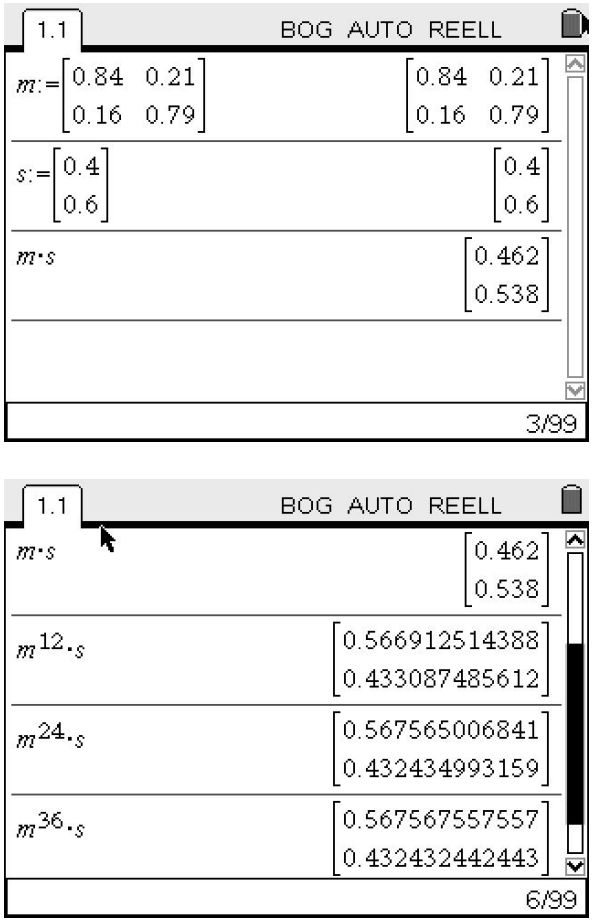


Abbildung 1 – *Eine Markov-Matrix m und ein Startvektor s (Marktaufteilung zu Beginn) werden definiert (oben). Dann werden Potenzen von m mit s multipliziert; der Prozess wird langsam stationär (unten)*

Mit dem TI-*n***spire CAS** war es möglich, in vielen konkreten Situationen schneller zum Ziel zu kommen, sich eben nicht in zu detaillierten Rechnungen zu verlieren, sondern eher den Blick für das Ganze zu schärfen. Die einzelnen Schritte einer Kurvendiskussion etwa per Hand durchführen zu können und sich mühsam den Funktionsgraphen zu konstruieren, dabei aber kaum über ganzrationale Funktionen hinauszukommen: wenig sinnvoll. Viel sinnvoller dagegen: Differentialkalkül und graphische Tools zu nutzen, um den Verlauf vieler Typen von Funktionen zu verstehen und auch zu beobachten, was etwa die Änderung dieses oder jenes Parameters ausmacht. Das konnte mit dem Rechner sehr gut umgesetzt werden, und hier beobachtete man dann auch – und zwar mit Fortschreiten der Vorlesung immer mehr – die so wichtige „Freude am Herumspielen“.

Konkrete Problemlösungen

Nach der Auflistung der eher allgemein gehaltenen Vor- und Nachteile wenden wir uns nun beispielhaft einigen „typischen“ Problemen aus dem betriebswirtschaftlichen Kontext zu, die mit Hilfe des TI-*n***spire CAS** bearbeitet werden können.

Einfache Markov-Prozesse können etwa verkleidet in einen Marketing-Kontext eingeführt werden, bei dem für eine Stichprobe von Verbrauchern das „Abwanderungsverhalten“ zwischen einer gewissen Menge von Konkurrenzprodukten mit Hilfe einer Markov-Matrix beschrieben werden kann. Zentral ist hierbei wieder die Modellierung: Idealerweise kommen die Studierenden von selber auf die Tatsache, dass das Problem mit Hilfe einer Matrix angegangen werden kann. (Sehr hilfreich dafür ist ein tieferes Verständnis der Matrizenmultiplikation; ein solches wird an früherer Stelle in der Vorlesung bereits im Rahmen mehrstufiger Produktionsprozesse hergeleitet.) Die Studierenden sollen sich nun überlegen, wie diese Matrix dann konkret aussieht und welche ihrer Eigenschaften typische Eigenschaften sind (etwa: Spaltensumme ist stets gleich 1). Dann folgt der Rechenschritt, schnell und unkompliziert mit dem Rechner durchzuführen: Die längerfristige Marktentwicklung ergibt sich durch Multiplikation eines Startvektors mit hohen Potenzen der Markov-Matrix. Dies kann – auch für große Matrizen und hohe Potenzen – schnell durchgeführt werden. Dabei stellen die Studierenden wiederum etwas fest, nämlich dass sich irgendwann die Marktaufteilung nicht mehr ändert – allerdings nur sofern die Übergangsmatrix konstant bleibt. Hier werden die Studierenden nahezu spielerisch an eine Art Grenzwertbegriff herangeführt, der den meisten aus der Schulzeit eher ein wenig unheimlich ist. Anschließend kann die Realitätstauglichkeit eines solchen einfachen Modells mit konstanter Übergangsmatrix diskutiert und können mögliche Varianten überlegt werden.

Der Umgang mit Matrizen wird natürlich auch im Zusammenhang mit linearen Gleichungssystemen ausführlich eingeübt. In der Vorlesung wird hier großer Wert darauf gelegt, die strukturellen Feinheiten zu verstehen – so etwa die Formulierung eines solchen Systems als Matrixgleichung $A \cdot x = b$, die Abhängigkeit der Lösungsmenge von der Koeffizientenmatrix A und im quadratischen Fall die Bedeutung der inversen Matrix A^{-1} in diesem Zusammenhang – dass nämlich durch $x = A^{-1} \cdot b$, also das „Auflösen“ der Matrixgleichung nach x, eine eindeutige Lösung geliefert wird. Das Matrizenkalkül des TI-*n***spire CAS** ist hier syntaktisch sehr konsistent und leicht verständlich. Neben dem Rechnen mit inversen Matrizen steht mit dem Befehl `rref` („reduced row echelon form“) auch eine Möglichkeit zur Verfügung, die erweiterte Koeffizientenmatrix nach weitestmöglicher Durchführung des Gauß-Algorithmus und somit unmittelbar die Lösung zu bestimmen.

In Abb. 2 (unten) sieht man zwei Beispiele für die Verwendung von `rref`: den Fall eindeutiger Lösbarkeit (hier mit $x_1 = -9$ und $x_2 = 4$) sowie den Fall nicht eindeutiger Lösbarkeit, erkennbar an der Nullzeile. Hier kann außerdem eine mögliche Parametrisierung der Lösungsmenge einfach abgelesen werden: Die Nullzeile ermöglicht eine freie Wahl für x_3, und die beiden anderen Komponenten ergeben sich in Abhängigkeit davon: $x_2 = 1 - 2x_3$ und $x_1 = x_3 - 1$.

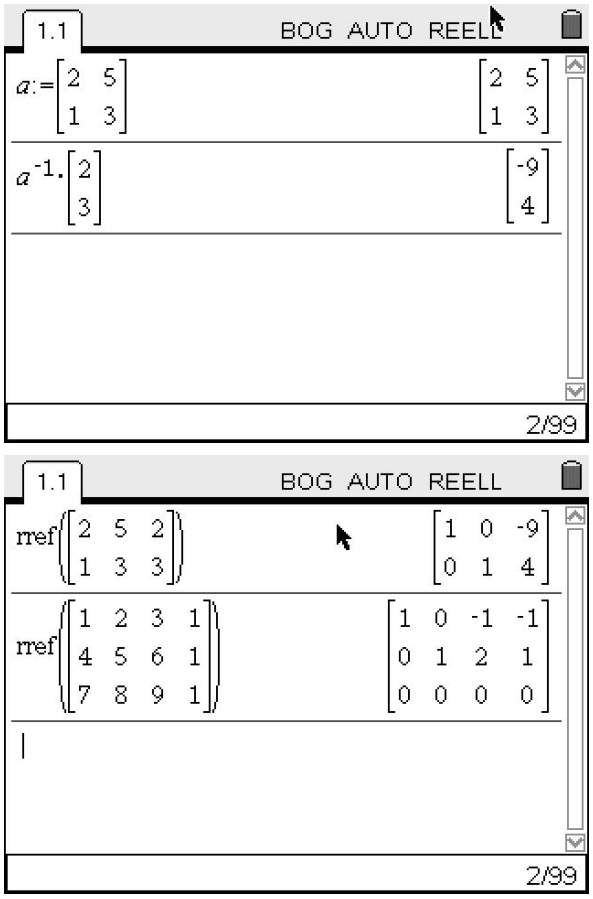


Abbildung 2 – *Das Lösen eines linearen Gleichungssystems mit Hilfe von Matrizen: mit der inversen Koeffizientenmatrix (oben) oder mit dem Befehl* `rref` *(unten)*

Auch das Optimieren von Funktionen in mehreren Variablen lässt sich schnell und bequem durchführen. Bei einer Standardaufgabe geht es etwa darum, bei einer Produktion von zwei Gütern, die in x und y gemessen werden, den Gewinn $g(x, y)$ zu maximieren, der etwa durch

$$g(x, y) = 70x - x^2 + 50y - y^2 - 10xy - 1.000$$

gegeben ist. Dieses Optimieren kann frei durchgeführt werden, was als Lösung $x = 3,75$ Mengeneinheiten (ME) und $y = 6,25$ ME ergibt. Praxisrelevanter ist der Fall, bei dem unter einer Nebenbedingung maximiert wird. Sollen etwa von beiden Produkten gemeinsam 12 ME hergestellt werden – eine Bedingung, die das globale Maximum eben nicht erfüllt – so kommt man hier mit einer Variablensubstitution an die Lösung $x = 4,75$ ME und damit $y = 7,25$ ME. Beides ist in Abb. 3 (oben) dargestellt. Anhand dieses einfachen Beispiels kann übrigens auch die Lagrange-Methode gut eingeführt werden (siehe Abb. 3 (unten)). In beiden Fällen greift man hier auf das Lösen eines Gleichungssystems mit Hilfe von `solve` zurück.

Die Unterscheidung zwischen freiem und gebundenem Optimieren – also zwischen dem globalen Maximum, das die Funktion $g(x, y)$ besitzt, und dem an die Nebenbedingung $x + y = 12$ geknüpften Maximum – ist ein zentraler Punkt in der Vorlesung. Die Studierenden sind nach entsprechenden wegbereitenden Überlegungen in der Lage zu erkennen, dass es sich bei dem Graphen zu $g(x, y)$ um ein nach unten geöffnetes Paraboloid handelt. Solche Flächen sind im Vorfeld mit Hilfe von *Mathematica* gezeigt worden, und interessanterweise steht der größte Teil der Studierenden diesen geometrischen Aspekten recht offen gegenüber – eine Tatsache, die bei weitem in einer betriebswirtschaftlichen Vorlesung nicht offensichtlich ist. So kann man ganz anschaulich – zumindest im Zwei-Variablen-Fall – darstellen, wie die Ebene der linearen Nebenbedingung (in unserem Fall $x + y = 12$) aus dem Paraboloid zur Gewinnfunktion eine Parabel „ausschneidet", deren Maximum existiert und sich dann als Maximum von $g(x, y)$ unter der Nebenbedingung herausstellt.

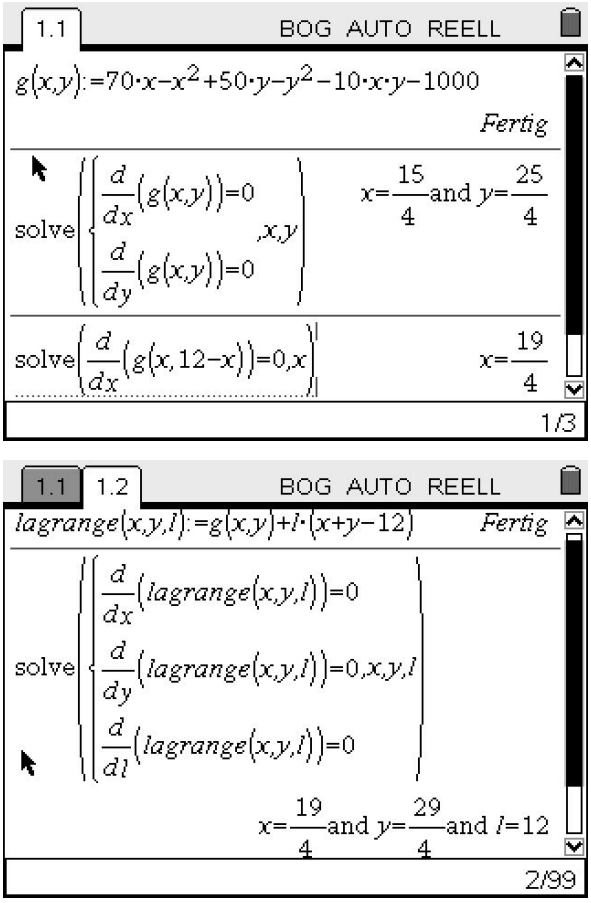


Abbildung 3 – *Optimieren einer Gewinnfunktion in zwei Variablen: frei sowie unter der Nebenbedingung $x + y = 12$ mit Variablensubstitution (oben) oder mit der Lagrange-Methode (unten)*

Leider stößt der TI-*n***spire CAS** hier mit seinen Graphik-Fähigkeiten an seine Grenzen. Darstellungen im Dreidimensionalen wären sehr wünschenswert, müssen aber wie gesagt durch den (dann leider nur frontalen) Einsatz eines zusätzlichen CAS geleistet werden. Aber auch bei zweidimensionalen Darstellungen, zumindest beim Zeichnen von Funktionsgraphen, erweist sich die Graphik-Fähigkeit des TI-*n***spire CAS** als noch nicht vollendet. Das Hinein- und Heraus-Zoomen oder auch die vielgerühmte Grab-Funktion sind in der Praxis sehr umständlich zu handhaben.

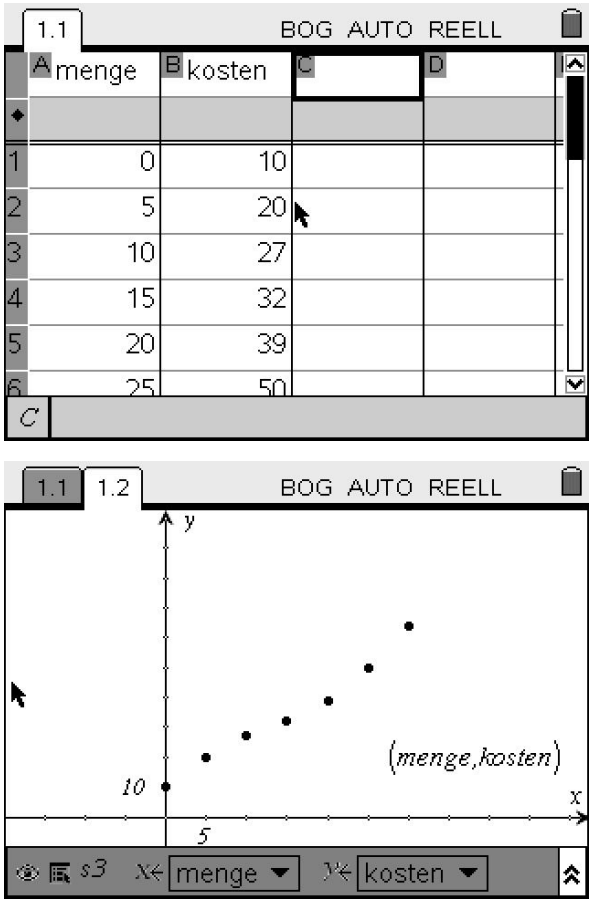


Abbildung 4 – *Eingabe der Mengen und Kosten in die Tabelle (oben) und Darstellung der entsprechenden Punkte durch einen Streuplot (unten)*

Ein weiterer interessanter Punkt ist die sogenannte *Lists-and-Spreadsheet*-Anwendung, eine Tabellenkalkulation. Die hier implementierten statistischen Funktionen etwa bieten eine breite Palette dessen, was angehende Betriebswirtschaftler besonders interessieren sollte. In der Anfängervorlesung zur Statistik lernen die Studierenden beispielsweise das lineare Regressionsmodell kennen, das im Rahmen der Wirtschaftsmathematikvorlesung mit praktischen Berechnungen aufgegriffen und erweitert wird: so etwa bei der Modellierung einer Kostenfunktion. Ausgehend von einer gegebenen Tabelle mit Kostenwerten sollen die Studierenden entscheiden, von welchem Typ die Kostenfunktion wohl ist: linear, quadratisch oder – ein wichtiges Standardmodell – kubisch-ertragsgesetzlich. Den typischen Verlauf einer solchen ertragsgesetzlichen Funktion (streng monoton wachsend mit einem Wendepunkt, bei dem degressives in progressives Wachstum übergeht) kennen die Studierenden teils bereits aus der Schule. Anhand der graphischen Darstellung mittels eines Streuplots durch Punkte im Koordinatensystem überlegen sich die Studierenden, welches Modell wohl am besten zutrifft; dann kann die entsprechende Regression durchgeführt werden: linear, kubisch, exponentiell, logistisch usw. In Abb. 4

ist ein solches Tabellenblatt mit zugehörigem Streuplot dargestellt. Hier wird aus der Graphik ersichtlich, dass die Wachstumsraten zunächst zurückgehen und dann ab einem gewissen Punkt zunehmen. Die Studierenden schließen daher auf das Modell einer ertragsgesetzlichen Kostenfunktion dritten Grades und führen mit dem TI-*n***spire CAS** die entsprechende Regression durch.

Fazit

Das (vorläufige) Fazit aus zwei Semestern CAS-Einsatz ist ein gemischtes. Dass nicht alle Studierenden überzeugt werden konnten, lag sicher zum Teil mit an einem bisher noch nicht erwähnten technischen Aspekt, der natürlich mehr in den Strukturen an der Hochschule begründet ist: Da die konkrete Zahl der Erstsemester-Studierenden sehr großen Schwankungen unterworfen ist, war die Einschätzung der Zahl der zu bestellenden Rechner schwierig; tatsächlich wurden zunächst zu wenige bestellt, und die Nachbestellung während des laufenden Semesters wurde durch Verwaltungsakte verzögert. Einige Studierende mögen sich vielleicht aus diesem Grund zögernder auf den Rechner eingelassen haben.

Was ursprünglich beabsichtigt war, nämlich bei den Studierenden ein größeres Interesse für die Analyse, ja durch die Programmierbarkeit mancher Problemstellungen vielleicht sogar Freude eben am Programmieren selber zu wecken, ist nur zum Teil gelungen. Der Anspruch, hier alle Studierenden zu erreichen, erwies sich als deutlich zu hoch. Bemerkenswert aber ist durchaus, dass sich, gerade bei fortschreitender Vorlesung, doch mehr und mehr Studierende auf den Rechner einließen. Die Vermutung lag jedoch recht nahe (und bestätigte sich dann auch), dass es sich hierbei um die „besseren“ Studierenden handelt. Einmal mehr gilt hier das oft zitierte Klischee: „Computeralgebrasysteme machen die Guten besser und die Schlechten schlechter...“ Das zu ändern und auch die weniger Starken mit dem CAS zu erreichen, ist das Ziel; der CAS-Einsatz in der Wirtschaftsmathematik jedenfalls geht weiter.

Publikationen über Computeralgebra

- Beutelspacher, A., Neumann, H. B., Schwarzpaul, T., *Kryptografie in Theorie und Praxis*, Vieweg+Teubner Verlag, 2010, 324 Seiten, ISBN 978-3-8348-0977-3, € 26,95. (Eine Besprechung finden Sie auf Seite 23.)
- Büchter, A., Henn, H. W., *Elementare Analysis: Von der Anschauung zur Theorie*, Spektrum Verlag, 2010, 340 Seiten, ISBN 978-38274-2091-6, € 22,95. (Eine Besprechung finden Sie auf Seite 24.)
- Karpfinger, C., Kiechle, H., *Kryptologie – Algebraische Methoden und Algorithmen*, Vieweg+Teubner Verlag, 2010, 261 Seiten, ISBN 978-3-8348-0884-4, € 24,90. (Eine Besprechung finden Sie auf Seite 25.)
- Seiler, W., *Involution. The Formal Theory of Differential Equations and its Applications in Computer Algebra*, Springer Verlag, 2010, 650 Seiten, ISBN 978-3-642-01286-0, € 106,95. (Eine Besprechung finden Sie auf Seite 26.)

Weitere Bücher können auf der Seite `http://www.fachgruppe-computeralgebra.de/Buecher` oder direkt bei Eva Zerz (`eva.zerz@math.rwth-aachen.de`) zur Besprechung angefordert werden.

Besprechungen zu Büchern der Computeralgebra

Albrecht Beutelspacher, Heike B. Neumann, Thomas Schwarzpaul Kryptografie in Theorie und Praxis

Vieweg+Teubner Verlag, 2010, 324 Seiten, ISBN 978-3-8348-0977-3, € 26,95

Der Untertitel des Buches lautet *Mathematische Grundlagen für Internetsicherheit, Mobilfunk und elektronisches Geld*. Ein Blick ins Inhaltsverzeichnis, das sich in die Teile *Symmetrische Verschlüsselungen*, *Asymmetrische Verschlüsselungen* und *Anwendungen* gliedert, bestätigt, dass das Buch eine enorme Breite an Themen abdecken und dabei keinen Verzicht üben will. So findet man hier auch Stromchiffren, Pseudo-Zufallsgeneratoren mit Schieberegistern, Kryptographische Zufallsgeneratoren von Blum-Micali und Blum-Blum-Shub, Statistische Tests, Blockchiffren DES und AES, Elliptische Kurven sowie Kryptosysteme, die auf Codes oder kombinatorischen Problemen beruhen. Damit ist aber nur etwas mehr als die Hälfte des Buches gefüllt, denn der weitaus größte Teil ist den *Anwendungen* vorbehalten. In diesem Abschnitt geht es um Authentizität von Nachrichten, Zero-Knowledge-Protokolle, Schlüsselinfrastrukturen und Authentifizierung von Teilnehmern, Secret-Sharing, Anonymität, bis hin zur Sicherheit von Internet-Standards, Mobilfunk und zur Quantenkryptografie.

Diese Themen werden auch tatsächlich angesprochen, allerdings bleibt das Buch dabei verständlicherweise an der Oberfläche. Mathematische Grundlagen findet man nur zu einem gewissen Teil, und wenn sie vorhanden sind, ist der Grad der Vertiefung eher inkonsistent. So startet das Buch z. B. mit hohem Anspruch an mathematische Präzision, wenn etwa das Sicherheitskonzept der Ununterscheidbarkeit mit Hilfe von Komplexitätstheorie, Erfolgswahrscheinlichkeiten von Angreifern und (asymptotisch) vernachlässigbaren Funktionen eingeführt wird, wie man es aus Goldreichs *Foundations of Cryptography* erwarten würde. Wenige Seiten später wird auf einen dreizeiligen Beweis der Bayes-Formel verzichtet und stattdessen ein Lehrbuch der Stochastik zitiert.

Dass verschiedene Grundlagen nicht bewiesen werden, zieht sich durch das ganze Buch. Wenn statt eines trivialen Beweises ein Lehrbuch zitiert wird, ist das nicht schön, aber verkraftbar. Wenn gar keine Referenzen gegeben werden (und das kommt vor), hat ein unbedarfter Leser allerdings keine Chance einzuschätzen, ob hier nur eine Kleinigkeit fehlt oder etwas Substanzielles. Hinzu kommt eine gewisse Frustration mit gelegentlich schlampiger mathematischer Darstellung. Bereits im Kapitel über Schieberegister, der ersten Gelegenheit zu etwas technischeren Rechnungen, stolpert man über vergessene Voraussetzungen in Definitionen und Bemerkungen. Da das Buch fast alles anspricht – ein Thema, das ausgespart wurde, sind Faktorisierungsmethoden – wird auch auf forschungsrelevante Themen eingegangen. Erstaunlicherweise sind gerade hier die Literaturverweise recht ausführlich, so dass das Buch über ein langes Verzeichnis an Zeitschriften- und Konferenzartikeln verfügt.

Vom Stil her versuchen die Autoren möglichst leicht verständlich und textorientiert zu erklären. Dies geht zu Lasten der Übersicht und zu Lasten des

Tiefgangs. Je nach Geschmack kann der Stil entweder leicht zugänglich erscheinen, oder aber auch der Verständlichkeit selbst abträglich sein. Mit Wiederholungen ist zu rechnen.

Als Zielgruppe des Buches kommen Leser in Frage, die sich einen erstmaligen Überblick über Kryptografie und ihre aktuellen Anwendungen verschaffen wollen und dabei weniger Wert auf Beweise legen. Für diese ist das Buch leicht zugänglich und besticht sicherlich durch seine enorme Themenabdeckung. In der mathematischen Darstellung gibt es dagegen bessere Bücher.

Timo Hanke (Aachen)

Andreas Büchter, Hans Wolfgang Henn
Elementare Analysis: Von der Anschauung zur Theorie

Spektrum Verlag, 2010, 340 Seiten, ISBN 978-38274-2091-6, € 22,95

Das Buch gliedert sich in acht Kapitel, wobei das erste Kapitel eine ausführliche Einleitung ist. Ein vorangestelltes Vorwort sowie ein nachgestelltes Literaturverzeichnis und abschließendes Schlagwortverzeichnis (Index) rahmen die Abhandlung ein. Im Vorwort wird noch auf einen Anhang zu diesem Buch hingewiesen, der unter einer angegebenen Internetadresse gefunden werden kann. Bereits im Vorwort beschreiben die Autoren die beabsichtigte Ausrichtung: Aus der Sicht der Hochschulmathematik soll ein inhaltlicher Zugang zur Analysis ermöglicht werden. Die Autoren haben hierbei auch die Vorlesungen „Elementarmathematik vom höheren Standpunkt aus“ von Felix Klein im Blick, die dieser „ganz besonders den Lehrern der Mathematik an unseren höheren Schulen“ unterbreitete, und sie verweisen auf das von ihm beschriebene Ziel (Zitat):

> *... dem Lehrer – oder auch dem reiferen Studenten – Inhalt und Grundlegung der im Unterricht zu behandelnden Gebiete vom Standpunkt der heutigen Wissenschaft in möglichst einfacher und anregender Weise überzeugend darzulegen.*

Damit ist die verfolgte Absicht festgelegt und die zu erwartende Vorgehensweise in diesem Buch auch durch den Untertitel in einer Weise beschrieben, die den Leser neugierig machen dürfte auf die inhaltliche Ausgestaltung.

Zum Leserkreis gehören also konform zur Zielsetzung des Buches Studierende des Fachs Mathematik für ein Lehramt in den Sekundarstufen, aber auch Referendare und Lehrer. Studierenden der Mathematik soll es auch dazu dienen, einen für weiterführende Analysisvorlesungen inhaltlichen Zugang zu ermöglichen.

In der Einleitung werden nun noch einmal die im Vorwort bereits genannten Absichten dieses Buches beschrieben und unter Bezug auf Heinrich Winters „Grunderfahrungen“ (Heinrich Winter: *Mathematikunterricht und Allgemeinbildung*, Mitteilungen der Gesellschaft für Didaktik der Mathematik Nr. 61 (1996), 37–46) auf eine mathematikdidaktische Grundlage gestellt. Der Aufbau des Buchs wird erläutert, und spezifische Ratschläge zur Lektüre dieses Buchs werden gegeben.

Dem ersten Kapitel („Einleitung“) folgt dann ein mit 70 von insgesamt 336 Seiten besonders breit angelegtes zweites Kapitel („Funktionale Zusammenhänge und Funktionen“). Hier werden Funktionen sowohl hinsichtlich der Begrifflichkeit als auch hinsichtlich verschiedener Grundvorstellungen und Darstellungsarten problematisiert, und es werden die aus der Schule bekannten elementaren Funktionen und ihre Charakteristika vorgestellt. Ein Exkurs zum Thema „Funktionen und Kurven“ schließt dieses Kapitel ab.

Der im dritten Kapitel vorgestellte anschauliche Zugang zur Differential- und Integralrechnung erscheint dann mit 24 Seiten äußerst knapp. Sind hier doch sowohl der Ableitungsbegriff als auch das Integral und der Zusammenhang zwischen „Ableiten“ und „Integrieren“ bis hin zum Hauptsatz der Differential- und Integralrechnung vorgestellt. Unter dem Aspekt der anschaulichen Vorbereitung einer noch zu entwickelnden Theorie ist aber dieser knappe Platz durchaus angemessen.

Die Kapitel vier, fünf, sechs und sieben gehen nun auf die theoretische Fundamentierung der Analysis ein: So werden im Kapitel vier („Mathematische Grundlagen der Analysis“) u. A. die Vollständigkeit der reellen Zahlen, Grenzwerte von Folgen und Grenzwerte von Funktionen sowie die Stetigkeit von Funktionen abgehandelt. Cauchy-Folgen werden kurz erwähnt. Der strategische Nutzen im Zusammenhang mit der Reihenlehre (z. B. absolute Konvergenz $\Rightarrow$ Konvergenz) bleibt offen. Zwischenwertsatz und Satz über das Maximum und Minimum stetiger Funktionen auf einem kompakten Intervall werden im Rahmen der bereitgestellten Theorien behandelt. Das Kapitel fünf („Grenzwerte von Differenzenquotienten: die Ableitung“) behandelt die Differenzierbarkeit mit den üblichen Rechenregeln bis hin zu einer Regel von L'Hospital. Den Satz von Rolle und den Mittelwertsatz findet der Leser im Unterkapitel „Anschauung und Differenzierbarkeit“. Der Zusammenhang zwischen dem Satz von Rolle und dem Mittelwertsatz wird formal über die bekannte Hilfsfunktion vorgestellt, ohne auf den geometrischen Zusammenhang einzugehen, der

den Beweisansatz erklärt. Geht doch der Mittelwertsatz aus dem Satz von Rolle durch eine Scherung an der y-Achse hervor. Das Kapitel sechs („Grenzwerte von Riemannschen Summen: das Integral“) behandelt eine gut lesbare und auf das Wesentliche beschränkte Einführung des Riemann-Darboux-Integrals nebst Kriterien der Integrierbarkeit sowie den Zusammenhang zwischen Monotonie bzw. zwischen Stetigkeit und Integrierbarkeit. Im Kapitel sieben („Zusammenhang von Differenzial- und Integralrechnung“) wird u. A. der Hauptsatz der Differential- und Integralrechnung abgehandelt. Dabei hätte der Bezug zum Mittelwertsatz vielleicht deutlicher herausgearbeitet werden können. Der Hauptsatz wird in zwei Teilen formuliert, und jeder Teil wird unabhängig vom anderen Teil bewiesen, obwohl beide Teile logisch äquivalent sind und dies auch von den Verfassern bekundet wird (S. 244, Aufgabe 7.1). Es folgt ein achtes Kapitel („Anwendungen in Theorie und Praxis“), in dem nicht nur auf die bekannte Kurvendiskussion eingegangen wird. Reizvoll sind die Betrachtungen zu den „Änderungsraten bei geometrischen Maßen“ oder das „Wechselspiel von Theorie und Anwendungen“.

Zusammenfassung: Die Verfasser haben sich bemüht, den für den Schulunterricht relevanten Teil der Analysis vom Standpunkt der heutigen mathematischen Wissenschaft durch eine auf Anschauung basierte Theorie zu erarbeiten. Sie liefern hierbei eine Vielzahl von Beispielen, skizzieren ihre Überlegungen ausführlich und schaffen insgesamt ein Werk, das dem angesprochenen Personenkreis hilfreich eine Brücke bauen wird, um die auch für den angehenden Lehrer in der Sekundarstufe benötigte Theorie der Analysis, wie sie auf jeder Universität gelehrt wird, mit dem Auftrag einer verantwortungsvollen Unterrichtstätigkeit an der Schule im Sinne Felix Kleins zu verbinden, der den Verfassern mit seinen berühmten Vorlesungen „Elementarmathematik vom höherem Standpunkt aus“ vor Augen stand. Mir drängt sich ein weiteres Zitat aus diesen Vorlesungen auf:

> *Wissenschaftlich unterrichten kann nur heißen, den Menschen dahin bringen, dass er wissenschaftlich denkt, keineswegs aber, ihm von Anfang an mit einer kalten, wissenschaftlich aufgeputzten Systematik ins Gesicht springen* (Felix Klein: Elementarmathematik vom höheren Standpunkt aus; Bd. 1 Arithmetik, Algebra, Analysis; anschließende Bemerkungen über den Schulunterricht).

Dieses Werk könnte jedem Studierenden der Mathematik als Ergänzung seiner Ausbildung im Fach Analysis empfohlen werden.

Wolfgang Spiegel (Wuppertal)

Ch. Karpfinger, H. Kiechle
Kryptologie – Algebraische Methoden und Algorithmen

Vieweg+Teubner Verlag, 2010, 261 Seiten, ISBN 978-3-8348-0884-4, € 24,90

Das Buch stellt die Ausarbeitung einer Vorlesung der Autoren dar, die sich an Studierende der Mathematik oder Informatik ab dem 3. Semester richtet. Vorausgesetzt werden nur wenige Grundlagen aus linearer Algebra und Analysis, wohingegen die benötigte elementare Zahlentheorie und Wahrscheinlichkeitstheorie im Buch selbst entwickelt werden.

Das Buch erhebt nicht den Anspruch, ein vollständiges Lehrbuch zur Kryptologie zu sein. Stattdessen haben die Autoren eine subjektive Stoffauswahl getroffen, die sich in einer vierstündigen Vorlesung unterbringen lässt. Diese Auswahl ist durchaus gelungen, konsequent im Aufbau und von angebrachtem Umfang. So wurden zum Beispiel weniger relevant gewordene Themen wie DES (Data Encryption Standard) weggelassen, dagegen etwa der AKS-Primzahltest mit aufgenommen.

Im Einzelnen findet man folgende Themen: Klassische Chiffren und ihre Analyse; Perfekte Sicherheit nach Shannon auf Grundlage elementarer Wahrscheinlichkeitstheorie, ohne Verwendung von Informationstheorie/Entropie; Block-Chiffren am Beispiel von AES (Advanced Encryption Standard); Komplexität inklusive Analyse einiger arithmetischer Algorithmen; Symmetrische Authentifikation mit Message Authentication Codes (MAC); Exponentiationschiffren und das RSA-Verfahren inklusive Wiener-Angriff; Primzahltests von Miller-Rabin und AKS; Diffie-Hellman, ElGamal und Rabin-Verfahren; Diskretes Logarithmusproblem mit Baby-Step-Giant-Step und Pollard-ρ; Faktorisierungsmethoden mit Pollard-ρ, Kettenbrüchen und quadratischem Sieb; Signaturverfahren und Digital Signature Standard (DSS); Elliptische Kurven sowie deren Verwendung für ElGamal, Signatur und Faktorisierung. Die Grundlagen werden dabei über die Kapitel verteilt an den Stellen eingeführt, an denen sie benötigt werden.

Der Autorenauswahl zum Opfer gefallen ist die Erzeugung von Pseudozufalls-Sequenzen. Als Folge davon kommt das Buch allerdings ohne Stochastik aus und verzichtet auch auf weiterführende Zahlentheorie in Richtung quadratischer Reste. Es fehlt die Diskussion von Sicherheitsmodellen (Ununterscheidbarkeit und

semantische Sicherheit). Wie von einer vierstündigen Vorlesung nicht anders zu erwarten, können lineare und differentielle Kryptoanalyse nicht ausgeführt werden. Auf die Darstellung anwendungsorientierter Protokolle, Public-Key-Infrastruktur und aktueller Standards wird komplett verzichtet. Erstaunlicherweise wird die Existenz des Index-Calculus-Algorithmus für das Diskrete Logarithmusproblem in endlichen Körpern nicht erwähnt, wodurch die Verwendung elliptischer Kurven unmotiviert bleibt.

Die Autoren legen sichtbar Wert auf Vollständigkeit in den Beweisen; Lücken, die nur durch andere Lehrbücher zu schließen wären, treten praktisch nicht auf. Dies wird bemerkenswerterweise auch beim Thema elliptischer Kurven weitgehend durchgehalten, wo andere Lehrbücher Abstriche machen. So findet man hier auch eine Einführung in die Geometrie projektiver Ebenen. Die im Untertitel versprochene Betonung algebraischer Methoden und Algorithmen wird erfüllt.

Der Stil des Buches ist durch Ausführlichkeit, aber auch durch Präzision geprägt, und durchaus für Studierende im zweiten Jahr zum Selbststudium geeignet. Als Zielgruppe des Buches sind somit einerseits Studierende im Erstkontakt mit Kryptographie auszumachen, denen ein gut lesbares, geschlossenes und übersichtliches Lehrbuch vorliegt. Für die weiterführende Beschäftigung nach der ersten Vorlesung oder als Nachschlagewerk werden Studierende allerdings zusätzliche Literatur benötigen. Dem Dozenten bietet sich eine gute Vorlage für die eigene Vorlesung. Möchte er sich komplett an dem Buch orientieren, so ist nur noch eine geringe Eigenauswahl zu treffen, um den Umfang etwas zu reduzieren. Möchte er nur einzelne Teile in seine Vorlesung übernehmen, so wird dies dadurch vereinfacht, dass alle benötigten Grundlagen weitgehend an der entsprechenden Stelle im Buch finden sind. Übungsaufgaben werden (ohne Lösungen) bereitgestellt. Das Buch befreit uns dankenswerterweise von Alice und Bob.

Timo Hanke (Aachen)

Werner M. Seiler
Involution: The Formal Theory of Differential Equations and its Applications in Computer Algebra

Springer Verlag, 2010, 650 Seiten, ISBN 978-3-642-01286-0, € 106,95

Among the most fundamental mathematical results in the theory of partial differential equations (PDEs) is the Cauchy-Kovalevskaya theorem on the existence and uniqueness of analytical solutions to the initial-value problem for systems of PDEs in normal or Cauchy-Kovalevskaya form. This was generalized to other classes of PDE systems by Cartan, Kähler, Riquier, Janet, Thomas and led to the so-called formal theory of differential equations (FTDE), whose main contributors were Spencer, Goldschmidt, Kuranishi and Quillen. The main notion of FTDE is involution, and involutive systems of PDEs just generalize those of Cauchy-Kovalevskaya form. A transformation of a PDE system into the involutive form is called completion.

Involutive systems of PDEs play in FTDE the role similar to that of Gröbner bases in the theory of polynomial equations. Moreover, constructive ideas used by Riquier and Janet for completion of PDEs to involution provided a new algorithmic platform for the construction of Gröbner bases. The latter are called involutive bases when they satisfy the involutivity conditions, and the completion algorithms applied to polynomial systems are called involutive. The structure of an involutive basis is fully determined by the type of the chosen restricted monomial division, called involutive division.

Involution is the first book that provides a self-contained treatment of constructive and algorithmic ideas and methods in FTDE and those in the theory of polynomial involutive bases (TPIB) together with a number of important applications. The author singles out involutive bases of special type (Pommaret bases) due to their sensitivity to δ-regularity of a coordinate system, a concept that plays a principal role in FTDE.

Contents: The distinctive property of the book is that it successfully combines a differential-geometric formalism, which is the most adequate to FTDE, with the standard algebraic formalism of the theory of polynomial ideals and modules. Such combination provides much deeper insight into the concepts and methods of FTDE and TPIB than any of the two formalisms exploited separately. In particular, the geometric approach to differential equations is intrinsic and allows to study them in a coordinate-independent way, whereas the algebraic approach is much more constructive and algorithmic.

Chapter 2 introduces a reader to the jet-bundle techniques for geometric study of differential equations by prolongation and projection and defines differential equations as fibred manifolds of jet bundles. Integrability conditions and formal integrability are defined, analyzed and illustrated by examples including the classical differential equations such as Maxwell, Yang-Mills, Navier-Stokes equations.

Chapter 3-4 describe basics of TPIB. The cornerstone concept of this theory is the underlying involutive monomial division induced by partition of variables into multiplicative and nonmultiplicative ones. An axiomatic definition and properties of involutive division are considered. Two involutive divisions, namely, Janet and Pommaret division are particularly investigated. Unlike the former the latter division is not Noetherian, and by this reason (finite) Pommaret bases need not exist. There is a deep interconnection between the existence of a Pommaret basis and δ-regularity of a coordinate system. Interrelation of Gröbner and involutive bases is analyzed and computational aspects of completion of polynomial systems to involution are discussed including some algorithmic optimizations. TPIB is extended from commutative algebras to algebras of solvable type.

Chapter 5 is devoted to the application of TPIB to the structural analysis of modules over commutative polynomial rings $\mathcal{P}$. The most important feature of involutive division is that a monomial may have at most one involutive divisor among elements in an involutively reduced monomial set. This makes involutive bases a useful tool in constructing combinatorial decompositions and their analysis. For instance, in the case of a homogeneous ideal $\mathcal{I}$ it is shown that by means of a finite Pommaret basis it is easy to verify whether the graded algebra $\mathcal{P}/\mathcal{I}$ is Cohen-Macaulay. The last sections of the chapter reveal the relation of Pommaret bases to the construction of Noether normalizations, to the study of free resolutions and to the determination of Castelnuovo-Mumford regularity.

Chapter 6-7 are the central ones for the most general aspects of FTDE. Chapter 6 introduces homological foundations for the combinatorial invariants considered in the previous chapter by means of TPIB. According to Spencer's criterion of involutivity, a PDE system is involutive if and only if its symbol is involutive and its first prolongation and projection does not reveal new integrability conditions. Thus completion to involution is reduced to prolongations and projections. In Chapter 7, the author considers first completion of ordinary differential systems to involution and indicates the relevance of such completion for the Dirac theory of constrained dynamical systems. Then general Cartan-Kuranishi completion is described with the main statement on the finiteness of the completion procedure.

Chapter 8 deals with arbitrariness in the formal solution space of differential equations. It can be characterized by means of Cartan characters and the Hilbert function. An important application of the given analysis is the study of PDEs possessing gauge symmetries, which is important for field theories relevant to physics. Maxwell's equations and the $U(1)$ Yang-Mills equations are considered in this context.

The existence and uniqueness of solutions to initial value problems for PDEs are discussed in Chapter 9. The Cauchy-Kovalevskaya theorem and its extension to an arbitrary quasi-linear first-order involutive system solved with respect to the highest ranking partial derivative (the Cartan-Kähler theorem) are proven. For involutivity analysis of more general nonlinear systems, one can use either the Cartan formalism based on the exterior calculus or the dual vector field approach by Vessiot. The author of the book prefers the last approach and describes it in detail.

The last chapter is devoted to the involutivity analysis of linear PDE systems. Both geometric FTDE and algebraic TPIB are applied to equations of elliptic and hyperbolic types. It is argued that classification of linear PDEs into elliptic and parabolic ones based on their completion to involution is more natural than that known from the literature. By examining the proof of the Cartan-Kähler theorem specialized to linear systems, it is shown that existence and uniqueness are valid also for continuously differentiable solutions. It is also shown that one can solve the inverse syzygy problem, i.e., to verify whether a given differential equation is a compatibility condition of another equation. For the constant coefficient case a solution is constructed fully algorithmically. Appendices A-C contain auxiliary material with some basics from commutative algebra and differential geometry.

General remarks: Surprisingly, the book addresses in a rather complete way quite a number of topics from two apparently different, and each very wide, research areas: the differential-geometric theory of differential equations and algorithmic commutative algebra with generalization to "weakly noncommutative algebras". This completeness is mainly due to a universal algorithmic approach – completion to involution – that unifies and connects the topics of both areas as presented in the book.

For all that, there are interesting topics that cannot be addressed in a complete way even in a book of this size. Such a topic of principal interest, to my opinion, is the careful comparative analysis of differential-geometric completion algorithms, especially for nonlinear PDEs, based on exterior calculus, like that implemented in the paper by Hartley and Tucker (Ref. [194] in the bibliography list) and those based on Riquier-Janet theory extended by Thomas and its modifications done in TPIB. It is clear, and it was emphasized in the book, that the former algorithms are "much more" coordinate independent but "much less" algorithmic. However, the latter algorithms, like all those designed for Gröbner bases, crucially depend on term orderings (rankings). Thus, it is not clear at all for which classes of PDEs, if any, the algorithms of one group are more appropriate or/and more efficient than those of the other group.

To conclude, the book *Involution* is unique, self-contained, rather complete and, in addition, well-written with numerous instructive examples and comprehensive bibliography devoted to the constructive differential-geometric and computer-algebraic aspects of involutivity analysis of differential and polynomial equations and their applications. It can be recommended to researchers, postgraduate and advanced graduate students.

Vladimir P. Gerdt (Dubna)

Berichte von Konferenzen

1. SCC 2010 – Second International Conference on Symbolic Computation and Cryptography

London, Großbritannien, 23. – 25.06.2010

http://scc2010.rhul.ac.uk/

Diese Tagung war (nach Beijing 2008) die zweite in einer Reihe von internationalen Konferenzen, die sich mit Anwendungen der Computeralgebra in der Kryptographie befassen. Sie schloss sich unmittelbar an den *Workshop on Tools for Cryptanalysis 2010* an, der am gleichen Ort stattfand.

Die Hauptvorträge hielten V. Gerdt (über involutive Basen), A. Myasnikov (über gruppenbasierte Kryptographie) und A. May (über Angriffe auf RSA). Daneben gab es 20 eingeladene Vorträge, die von Gröbnerbasis-Methoden über nichtkommutative symbolische Berechnungen bis hin zu Anwendungen unter Zuhilfenahme der diskreten Optimierung, Wahrscheinlichkeitstheorie oder Logik reichten. Das Programm wurde von einer *Dinner Cruise* auf der Themse abgerundet.

Auf Grund der sehr positiven Resonanz ist geplant, die Veranstaltungsreihe mit einer Tagung in Bochum fortzusetzen.

Martin Kreuzer (Passau)

2. ACA 2010 – 16th International Conference on Applications of Computer Algebra

Vlore, Albanien,
24. – 27.06.2010

http://aca2010.info/index.php/aca2010/aca2010

The ACA series of conferences is devoted to promoting all manner of computer algebra applications, and encouraging the interaction of developers of computer algebra systems and packages with researchers and users (including scientists, engineers, educators, etc.). Additional information and a listing of previous and future conferences can be found at http://math.unm.edu/~aca/.

ACA 2010 was held at the University of Vlora, Albania, with Jacques Calmet and Tony Shaska as chairs. Sponsors were Department of Mathematics, College of Technical Sciences, and the Office for Research and Development at the University of Vlora. There were 129 attendees. Special sessions covered the following topics:

Algebraic and Numerical Computation for Engineering and Optimization Problems, Approximate Algebraic Computation, Coding Theory, Computational Algebraic Geometry, Computer Algebra in Education, Non-Standard Applications of Computer Algebra, Numerical Algebraic Geometry, Symbolic Symmetry Analysis and Its Applications. The Proceedings will be published as a special issue of the Albanian Journal of Mathematics.

Tony Shaska (Vlora, Albania)

3. Symbolic Computation and its Applications

Maribor, Slowenien,
30.06. – 02.07.2010

http://www.camtp.uni-mb.si/camtp/SCA

Im slowenischen Maribor fand vom 30.06. bis zum 02.07.2010 zum ersten Mal die Konferenz „Symbolic Computation and its Applications“ (kurz SCA) statt. Organisiert wurde sie vom Center for Applied Mathematics and Theoretical Physics (CAMTP) der Universität Maribor und vom Institute of Mathematics, Physics and Mechanics (IMFM). Die Tagung fand im Hotel „Pyramida“ statt.

Das Programm war so konzipiert, dass es erstens keine parallelen Sektionen gab und zweitens die Mehrheit der Vorträge von renommierten internationalen Wissenschaftlern gehalten wurde. Als Ergebnis bot diese Tagung viel Zeit für Diskussionen und Austausch, was von über 40 registrierten Teilnehmern als sehr angenehm empfunden und gerne genutzt wurde. Die Hauptredner mit 50-minütigen Vorträgen waren Herbert Wilf, Douglas Shafer, Peter Paule, Maoan Han, Vladimir Gerdt und Marko Petkovšek. Die weiteren Vorträge waren 40 oder 30 Minuten lang, jeweils mit lebhaften Diskussionen.

Thematisch lagen die Schwerpunkte der Tagung bei Anwendungen des symbolischen Rechnens auf Differential- und Differenzengleichungen, dynamische Systeme, algorithmische Kombinatorik und Probleme aus der Biologie. Auch kommutative Algebra, algebraische Geometrie, D-Moduln und Kryptoanalysis wurden angesprochen. An Computeralgebrasystemen wurden Singular, Mathematica, Maple, CoCoa, GAP und GINV oft erwähnt.

Zur selben Zeit fand in Maribor das „Festival Lent“ statt, was den Teilnehmern der Tagung zahlreiche Möglichkeiten zum Kennenlernen sowohl slowenischer als auch internationaler Künstler bot. Außerdem rundeten eine Exkursion zum berühmten Weinkeller der Stadt Maribor und ein klassisches Konzert des Duos „Fla-Via“ (Querflöte und Violine) als Auftakt zum Konferenzdinner das Konzept der Tagung ab. Möglicherweise wird die Tagung „Symbolic Computation and its Applications“ auch weiterhin in ein- oder zweijährigem Abstand stattfinden.

Viktor Levandovskyy (Aachen)

4. ANTS 2010 – Ninth Algorithmic Number Theory Symposium

Nancy, Frankreich,
19. – 23.07.2010

`http://ants9.org/`

Die Tagung ANTS IX fand vom 19. bis zum 23. Juli 2010 am INRIA (Institut National de Recherche en Informatique et en Automatique) in Nancy in Frankreich statt und wurde von den lokalen Organisatoren Anne-Lise Charbonnier, Jérémie Detrey, Pierrick Gaudry, Emmanuel Thomé und Paul Zimmermann vorzüglich geleitet.

ANTS IX war die 9. Ausgabe der bewährten zweijährlichen ANTS-Tagungsreihe, auf der seit ihrer Gründung neueste Resultate in der Algorithmischen Zahlentheorie vorgestellt werden. Offiziell nahmen 135 Personen aus allen Teilen der Welt teil, die meisten aus Frankreich und etwa 15 aus Deutschland.

Im Sinne früherer ANTS-Tagungen gab es Vorträge aus einem breitgefächerten Spektrum zahlentheoretischer Anwendungen, u. A. aus der elementaren Zahlentheorie, der arithmetischen Geometrie, der Geometrie der Zahlen, der analytischen Zahlentheorie und der Kryptographie.

Zu den fünf eingeladenen Plenarvorträgen: Gabriele Nebe (Rheinisch-Westfälische Technische Hochschule Aachen) startete die Tagung mit einem interessanten Einblick in *Lattices and Spherical Designs*. Am zweiten Tag sprach Jean-François Mestre (Université de Paris 7, Frankreich) über *Curves of Genus 3 With a Group of Automorphisms Isomorphic to* S_3 und am dritten Tag Carl Pomerance (Dartmouth College, USA) über *Fixed Points for Discrete Logarithms*. Oded Regev (Tel-Aviv University, Israel) erklärte dann das Thema *Learning with Errors over Rings*. Schließlich diskutierte Henri Darmon (McGill University, Kanada) die Problematik von *Putting the Hodge and Tate Conjectures to the Test*. Zusätzlich gab Michael Stoll (Universität Bayreuth) einen eingeladenen Spezialvortrag zu Ehren des kürzlich verstorbenen Fritz Grunewald.

Das akademische Programm wurde durch 25 eingereichte Vorträge von jeweils 30 Minuten, Posterpräsentationen und einer informellen Rump Session komplettiert. Carl Pomerance (Dartmouth College) überreichte den *Selfridge Prize in computational number theory* für den besten eingereichten Artikel an John Voigt (University of Vermont) für seinen Beitrag *Computing automorphic forms on Shimura curves over fields with arbitrary class number*.

Im Business Meeting wurde beschlossen, dass ANTS X im Juni oder Juli 2012 in San Diego, USA, stattfinden wird. Es wurde sogar über ANTS XI in Auckland, Neuseeland, nachgedacht. Des Weiteren gab es Diskussionen über die offizielle Benennung eines Steering Committees und über einen möglichen Wechsel des Verlages für zukünftige Proceedings von ANTS.

Das detaillierte Programm der Tagung inklusive der sozialen Aktivitäten ist auf der oben angegebenen Webseite zu finden. Die Proceedings sind in Springer Lecture Notes in Computer Science, Band 6197, erschienen.

Andreas Stein (Oldenburg)

5. ISSAC 2010 – International Symposium on Symbolic and Algebraic Computation

Technische Universität München, 25. – 28.07.2010

http://www.issac-conference.org/2010

Die ISSAC-Konferenz 2010 fand vom 25. bis zum 28. Juli 2010 auf dem innerstädtischen Campus der Technischen Universität München statt. (Mit)organisiert von der Fachgruppe Computeralgebra lag die Leitung in den Händen von Ernst W. Mayr (Local Arragements) und Wolfram Koepf (General Chair). Der Vorsitzende des Programmkomitees und zugleich Herausgeber des Tagungsbandes war Stephen Watt (London, Kanada).

Campus der TUM

Die Konferenz war gut besucht; es waren 188 Teilnehmer registriert. Das mag zu einem Teil an einer guten Aneinanderreihung der ‚related conferences' liegen. Zum anderen ist München auch als Reiseziel für viele Teilnehmer sehr attraktiv. Der Tagungsbeitrag konnte aufgrund eines großzügigen DFG-Zuschusses relativ niedrig gehalten werden. Gedankt werden sollte in diesem Zusammenhang auch den Sponsoren Maplesoft und TI. Eine gute Idee war das Angebot von Tageskarten für den öffentlichen Nahverkehr. In einer Stadt dieser Größe mit einem komplexen System des Nahverkehrs ist das sicher hilfreich.

Es wurden 45 Paper (leider ein no-show) und 33 Poster vorgestellt. Die Titel der Paper und Poster finden sich auf der Webseite der Konferenz.

Leider wurden anders als in vorherigen Jahren die Paper nicht auf einem ‚hands-on' elektronischen Medium wie DVD oder Stick verteilt. Sie sind jedoch für die Konferenzteilnehmer auf der Tagungs-Webseite zum Download verfügbar und stehen auch in der ACM Digital Library zur Verfügung.

Eingeladene Vorträge wurden von Evelyne Hubert, Siegfried M. Rump und Ashish Tiwari präsentiert:

Evelyne Hubert (INRIA Sophia Antipolis): Algebraic Invariants and their Differential Algebras

Siegfried M. Rump (Hamburg University of Technology and Waseda University): Verification Methods: Rigorous Results using Floating-point Arithmetic

Ashish Tiwari (SRI International): Theory of Reals for Verification and Synthesis of Hybrid Dynamical Systems

Tutorials waren von Sergey Tsarev, Jürgen Gerhard und Moulay A. Barkatou geplant. Sergey Tsarev musste sein Tutorial leider aus gesundheitlichen Gründen absagen. An seiner Stelle sprang dankenswerterweise Gregor Kemper (TU München) kurzfristig ein.

So kam es zu folgenden Tutorials:

Moulay A. Barkatou (Limoges University): Symbolic Methods for Solving Systems of Linear Ordinary Differential Equations

Jürgen Gerhard (Maplesoft): Asymptotically Fast Algorithms for Modern Computer Algebra

Gregor Kemper (TU München): Algorithmic Invariant Theory

In diesem Jahr waren erstmals die Gebühren der Tutorials in der Registrierungsgebühr eingeschlossen. Das ist sicherlich eine gute Idee für die nächsten Konferenzen, zumal die zusätzlichen Kosten nicht allzu hoch sind. So lag die Teilnehmerzahl bei den Tutorials etwa bei 100, weit höher als die sonst üblichen ca. 30 Teilnehmer. Zum Vergleich: Die ISSAC 2009 in Seoul hatte *insgesamt* nur knapp über 100 Teilnehmer.

Es fanden auch einige (eher wenige) Software-Demonstrationen statt, allerdings mit doch sehr speziellen Themen. Die Fa. Maplesoft stellte die neue Maple Version (14) vor.

Die SIGSAM und die Fachgruppe Computeralgebra prämierten die besten Tagungsbeiträge. Die Gewinner des

ISSAC 2010 Distinguished Paper Award der SIGSAM waren Ioannis Z. Emiris, Bernard Mourrain und Elias Tsigaridas für ihr Paper *The DMM bound: Multivariate (Aggregate) Separation Bounds*, der Gewinner des *ISSAC 2010 Distinguished Student Author Award* der SIGSAM war Pierre-Jean Spaenlehauer für *Computing Loci of Rank Defects of Linear Matrices using Gröbner Bases and Applications to Cryptology*, einer gemeinsamen Arbeit mit Jean-Charles Faugère und Mohab Safey El Din.

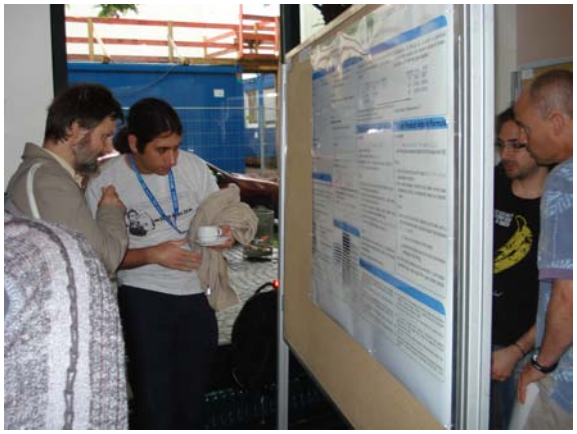
Auch die Fachgruppe stellte diesmal einige Preise zur Verfügung. Für das *Beste Paper eines Fachgruppenmitglieds* wurden Manuel Kauers und Veronika Pillwein für ihre Arbeit *When Can We Detect that a P-Finite Sequence is Positive?* ausgezeichnet. Dieser Preis war mit 500 € dotiert. Für die *Beste Software-Demonstration* wurden Felix Effenberger und Jonathan Spreer für die Software-Demo *simpcomp: A GAP toolbox for simplicial complexes* ausgezeichnet. Beide Autoren erhielten von der Fachgruppe Computeralgebra jeweils 100 € Preisgeld.

Manuel Kauers und Veronika Pillwein

Das Posterkomitee wählte die zwei besten Poster aus, welche die Fachgruppe Computeralgebra jeweils mit einem Preisgeld von 100 € pro beteiligtem Autor ausstattete. Gewonnen haben Sonia L. Rueda für ihr Poster *Linear Differential Implicitization and Differential Resultants* sowie Seyed Mohammad Mahdi Javadi und Michael Monagan für ihr Poster *On Sparse Interpolation over Finite Fields*. Die Fachgruppe Computeralgebra vergab einen zusätzlichen Preis für das Poster *Nullspace Computation over Rational Function Fields for Symbolic Summation* von Burçin Eröcal und Arne Storjohann.

Siegerin im Posterwettbewerb Sonia Rueda

Alle Software- und Postersieger erhielten außerdem eine Maple-Lizenz von der Firma Maplesoft. Wir haben die preisgekrönten Poster auf S. 32–34 abgedruckt.



Sieger im Posterwettbewerb Burçin Eröcal

Das Conference Banquet verbunden mit einem Ausflug zum Ammersee fand im Kloster Andechs statt. Es gab eine kurze Einführung in die Geschichte und künstlerische Gestaltung des Klosters und der Klosterkirche, ein kurzes Orgelkonzert und ein ausgiebiges Bankett mit bayrischen Spezialitäten (Schmankerln). (Neulich traf der Autor dieses Berichts einige der Teilnehmer des Banketts und die Erinnerungen waren zwar etwas verschwommen aber auch nach 6 Wochen noch sehr angenehm.) Das Wetter zum Ausflug war grenzwertig, aber nach furiosem Auftakt mit Starkregen hatten alle Gelegenheit zum Trocknen bei einer Busfahrt.

Bankett im Klostergasthof Andechs

ISSAC Business Meeting:

André Galligo, dessen Amtszeit im ISSAC Steering Committee endet, wurde während des ISSAC Meetings gedankt. Als neues Mitglied im ISSAC Steering Committee wurde Marc Moreno Maza gewählt.

Für die Konferenz ISSAC 2012 hatten sich Canterbury (Kent, England) und Grenoble (Frankreich) beworben. Die Wahl fiel deutlich zugunsten von Grenoble aus. Allerdings müssen die Briten nicht zu traurig sein, denn außer der PASCO 2012 (voraussichtlich in St. Andrews) werden sie 2012 auch die Olympischen Spiele in London austragen können.

Als Veranstaltungsort für die ISSAC 2011 war bereits im letzten Jahr San Jose in Kalifornien ausgewählt worden, siehe `www.issac-conference.org/2011`.

Winfried Neun (ZIB Berlin)

Supported by the Spanish
"Ministerio de Ciencia e Innovación"
under the Project MTM2008-04699-C03-01

Linear differential implicitization and differential resultants

SONIA L. RUEDA
Universidad Politécnica de Madrid

July 26, 2010

Dpto de Matemática Aplicada, E.T.S. Arquitectura
Univ. Politécnica de Madrid
Avda. Juan de Herrera 4
Madrid 28040, Spain

1 Linear differential implicitization

The implicitization results for unirational varieties in terms of resultants are well known. On the contrary, the development of similar techniques in a differential setting is a field of research at an initial stage.

Let $\mathbb{K}$ be an ordinary differential field with derivation ∂, (e.g. $\mathbb{Q}(t)$, $\partial = \frac{\partial}{\partial t}$). Let $X = \{x_1, \ldots, x_n\}$ and $U = \{u_1, \ldots, u_{n-1}\}$ be sets of differential indeterminates over $\mathbb{K}$. Let $\mathbb{N}_0 = \{0, 1, 2, \ldots, n, \ldots\}$. Let us consider the ring of differential polynomials $\mathbb{K}\{X\} = \mathbb{K}[x_i, x_{ik} = \partial^k x_i \mid i = 1, \ldots, n, k \in \mathbb{N}_0]$, analogously $\mathbb{K}\{U\}$. We consider the system of linear DPPEs

$$\mathcal{P}(X, U) = \begin{cases} x_1 = P_1(U) \\ \quad \vdots \\ x_n = P_n(U) \end{cases} \tag{1}$$

where $P_1, \ldots, P_n \in \mathbb{K}\{U\}$ with degree at most 1 and not all $P_i \in \mathbb{K}$, $i = 1, \ldots, n$. There exists $a_i \in \mathbb{K}$ and an homogeneous differential polynomial $H_i \in \mathbb{K}\{U\}$ such that

$$F_i(X, U) = x_i - P_i(U) = x_i - a_i + H_i(U).$$

Given $P \in \mathbb{K}\{X \cup U\}$ and $y \in X \cup U$, we denote by $\mathrm{ord}(P, y)$ the order of P in the variable y. If P does not have a term in y then we define $\mathrm{ord}(P, y) = -1$. To ensure that the number of parameters is $n - 1$, we assume that for each $j \in \{1, \ldots, n-1\}$ there exists $i \in \{1, \ldots, n\}$ such that $\mathrm{ord}(F_i, u_j) \geq 0$.

The implicit ideal of the system (1) is the differential prime ideal

$$\mathrm{ID} = \{f \in \mathbb{K}\{X\} \mid f(P_1(U), \ldots, P_n(U)) = 0\}.$$

The more general case of differential rational parametric equations was described in terms of characteristic sets in [Gao]. Given a characteristic set $\mathcal{C}$ of ID then $n - \mid \mathcal{C} \mid$ is the (differential) dimension of ID.

If $\dim(\mathrm{ID}) = n - 1$, then $\mathcal{C} = \{A(X)\}$ for some irreducible differential polynomial $A \in \mathbb{K}\{X\}$, we call it a characteristic polynomial of ID and the implicit equation of $\mathcal{P}(X, U)$ is defined as $A(X) = 0$.

2 Differential resultant

Linear complete differential resultants were defined in [RS] as a generalization of Carra'Ferro's differential resultant [CF] (in the linear case). Let o_i be the order of F_i.

For each $j \in \{1, \ldots, n-1\}$ we define the positive integers

$$\gamma_j := \min\{o_i - \mathrm{ord}(F_i, u_j) \mid i = 1, \ldots, n\}, \quad \gamma := \sum_{j=1}^{n-1} \gamma_j.$$

Let $N = \sum_{i=1}^{n} o_i$ then $\gamma \leq N - o_i$, for all $i \in \{1, \ldots, n\}$.

The linear complete differential resultant $\partial\mathrm{CRes}(F_1, \ldots, F_n)$ is the Macaulay's algebraic resultant of the differential polynomial set $\mathrm{PS} := \{\partial^{N-o_i-\gamma} F_i, \ldots, \partial F_i, F_i \mid i = 1, \ldots, n\}$ which contains $L = \sum_{i=1}^{n} (N - o_i - \gamma + 1)$ polynomials in the set of $L - 1$ differential variables $\mathcal{V} = \{u_j, u_{j1} \ldots, u_{jN-\gamma_j-\gamma} \mid j = 1, \ldots, n-1\}$.

Example 1 $\mathbb{K} = \mathbb{Q}(t)$, $\partial = \frac{\partial}{\partial t}$, $N = 1 + 2 + 1 = 4$, $\gamma = \gamma_1 = 1$

$$\mathcal{P}_1 = \begin{cases} x_1 = u_1 + u_2 + u_{21} \\ x_2 = t u_{11} + u_{22} \\ x_3 = u_1 + u_{21} \end{cases}$$

$\partial\mathrm{CRes}(F_1, F_2, F_3) = \det(M(L))$ where $L = 8$ and

$$M(L) = \begin{array}{c} \begin{array}{ccccccc} u_{23} & u_{22} & u_{12} & u_{21} & u_{11} & u_2 & u_1 \; 1 \end{array} \\ \begin{bmatrix} -1 & -1 & -1 & 0 & 0 & 0 & 0 \; x_{12} \\ 0 & -1 & 0 & -1 & -1 & 0 & 0 \; x_{11} \\ 0 & 0 & 0 & -1 & 0 & -1 & -1 \; x_1 \\ -1 & 0 & -t & 0 & -1 & 0 & 0 \; x_{21} \\ 0 & -1 & 0 & 0 & -t & 0 & 0 \; x_2 \\ -1 & 0 & -1 & 0 & 0 & 0 & 0 \; x_{32} \\ 0 & -1 & 0 & 0 & -1 & 0 & 0 \; x_{31} \\ 0 & 0 & 0 & -1 & 0 & 0 & -1 \; x_3 \end{bmatrix} \end{array} \begin{array}{c} \\ \partial^2 F_1 \\ \partial F_1 \\ F_1 \\ \partial F_2 \\ F_2 \\ \partial^2 F_3 \\ \partial F_3 \\ F_3 \end{array}$$

$$\begin{aligned} \det(M(L)) &= (1-t)^2 x_{32} - t x_{31} + (1-t) x_2 - (1-t)^2 x_{12} \\ &= \mathcal{L}_3(x_3) + \mathcal{L}_2(x_2) + \mathcal{L}_1(x_1) \end{aligned}$$

with $\mathcal{L}_1, \mathcal{L}_2, \mathcal{L}_3 \in \mathbb{K}[\partial]$.

Theorem Given a system $\mathcal{P}(X, U)$ of linear DPPEs with implicit ideal ID. If $\partial\mathrm{CRes}(F_1, \ldots, F_n) \neq 0$ then ID has dimension $n - 1$ and

$$\partial\mathrm{CRes}(F_1, \ldots, F_n)(X) = 0$$

is its implicit equation.

3 Characterization of $n - 1$ dimensional systems

Let (PS) be the ideal generated by PS in $\mathbb{K}[\mathcal{X}][\mathcal{V}]$ and let $[\mathrm{PS}]$ be the differential ideal generated by PS in $\mathbb{K}\{X\}\{U\}$. Let $\mathbb{K}[\partial]$ be the ring of differential operators with coefficients in $\mathbb{K}$ which is left euclidean (and also right euclidean). Given a nonzero linear differential polynomial B in $[\mathrm{PS}]$ there exist differential operators $\mathcal{F}_i \in \mathbb{K}[\partial]$, $i = 1, \ldots, n$ such that

$$B(X, U) = \sum_{i=1}^{n} \mathcal{F}_i(F_i(X, U)).$$

If B belongs to $\mathrm{ID} = [\mathrm{PS}] \cap \mathbb{K}\{X\}$ then

$$B = \sum_{i=1}^{n} \mathcal{F}_i(x_i - a_i) \text{ and } \sum_{i=1}^{n} \mathcal{F}_i(H_i(U)) = 0.$$

If B belongs to (PS) then $\deg(\mathcal{F}_i) \leq N - o_i - \gamma$, $i = 1, \ldots, n$. We define the co-order of B in (PS) as the highest positive integer $\mathrm{c}(B)$ such that $\partial^{(B)} B \in (\mathrm{PS})$.

$$\mathrm{c}(B) = \min\{N - o_i - \gamma - \mathrm{ord}(B, x_i) \mid i = 1, \ldots, n\}.$$

Given a nonzero linear differential polynomial B in ID, let $\mathcal{F}$ be the greatest common left divisor $\mathrm{gcld}(\mathcal{F}_1, \ldots, \mathcal{F}_n)$. There exists $\mathcal{L}_i$ such that $\mathcal{F}_i = \mathcal{F}\mathcal{L}_i$. We define the ID-primitive part of B as $\mathrm{IDprim}(B) = \sum_{i=1}^{n} \mathcal{L}_i(x_i - a_i)$. If $\mathcal{F} \in \mathbb{K}$ then we say that B is ID-primitive.

Let S be the $n \times (n-1)$ matrix whose entry (i, j) is the coefficient of $u_{n-j\, o_i - \gamma_j}$ in F_i, $i \in \{1, \ldots, n\}$, $j \in \{1, \ldots, n-1\}$. Let M_{L-1} be the $L \times (L-1)$ principal submatrix of $M(L)$.

Theorem Given a system $\mathcal{P}(X, U)$ of linear DPPEs with implicit ideal ID. The following statements are equivalent.

1. The dimension of ID is $n - 1$.
2. $\mathrm{rank}(S) = n - 1$ and there exists a nonzero linear ID-primitive differential polynomial A in $(\mathrm{PS}) \cap \mathbb{K}\{X\}$ such that $L - \mathrm{rank}(M_{L-1}) = \mathrm{c}(A) + 1$.

In such situation $A(X) = 0$ is the implicit equation of $\mathcal{P}(X, U)$.

4 Implicitization algorithm

Let p be a differential indeterminate over $\mathbb{K}$ such that $\partial(p) = 0$. Denote by $\mathbb{K}_p = \mathbb{K}\langle p \rangle$ the differential field extension of $\mathbb{K}$ by p. A linear perturbation of the system $\mathcal{P}(X, U)$ is a new system

$$\mathcal{P}_\phi(X, U) = \begin{cases} x_1 = P_1(U) + p\,\phi_1(U) \\ \quad \vdots \\ x_n = P_n(U) + p\,\phi_n(U) \end{cases}$$

where the linear perturbation $\phi = (\phi_1(U), \ldots, \phi_n(U))$ is a family of linear differential polynomials in $\mathbb{K}\{U\}$. For $i = 1, \ldots, n$ let $F_i^\phi(X, U) = F_i(X, U) - p\,\phi_i(U)$.

We define $\phi = (\phi_1(U), \ldots, \phi_n(U))$ by

$$\phi_i(U) = \begin{cases} u_{n-i-1, o_i - \gamma_{n-i-1}} + u_{n-i}, & i = 1, \ldots, n-2, \\ u_1, & i = n-1, \\ u_{n-1, o_n - \gamma_{n-1}}, & i = n. \end{cases} \tag{2}$$

Then $\partial\mathrm{CRes}(F_1^\phi, \ldots, F_n^\phi) \neq 0$.

Let D_ϕ be the lowest degree of p in $\partial\mathrm{CRes}(F_1^\phi, \ldots, F_n^\phi)$. The coefficient A_{D_ϕ} of p^{D_ϕ} in $\partial\mathrm{CRes}(F_1^\phi, \ldots, F_n^\phi)$ is a linear differential polynomial in $(\mathrm{PS}) \cap \mathbb{K}\{X\}$ as well as its ID-primitive part A_ϕ.

Differential implicitization algorithm for linear DPPEs

- Given the system $\mathcal{P}(X, U)$ of linear DPPEs.
- Decide whether the dimension is $n - 1$ and in the affirmative case return a characteristic polynomial of ID.

1. Compute $\mathrm{rank}(S)$. If $\mathrm{rank}(S) < n - 1$ RETURN "dimension less than $n - 1$".
2. Compute $\mathcal{P}_\phi(X, U)$ with perturbation ϕ given by (2).
3. Compute $\partial\mathrm{CRes}(F_1^\phi, \ldots, F_n^\phi)$, D_ϕ and A_{D_ϕ}. If $D_\phi = 0$ RETURN A_{D_ϕ}.
4. Compute A_ϕ and $\mathrm{c}(A_\phi)$. If $D_\phi = \mathrm{c}(A_\phi)$ RETURN A_ϕ.
5. Compute $\mathrm{rank}(M_{L-1})$.
6. If $L - \mathrm{rank}(M_{L-1}) > \mathrm{c}(A_\phi) + 1$ RETURN "dimension less than $n - 1$".
7. If $L - \mathrm{rank}(M_{L-1}) = \mathrm{c}(A_\phi) + 1$ RETURN A_ϕ.

Example 2 Let $\mathbb{K} = \mathbb{Q}$, $\partial = \frac{\partial}{\partial t}$ and $\mathcal{P}_2$ providing differential polynomials in $\mathbb{K}\{x_1, x_2, x_3\}\{u_1, u_2\}$ with $o_1 = 2, o_2 = 2, o_1 = 1$.

$$\begin{aligned} F_1(X, U) &= x_1 + u_1 - u_2 + u_{11} - u_{12} - 4u_{21} - 3u_{22}, \\ F_2(X, U) &= x_2 + u_2 + u_{11} - u_{22}, \\ F_3(X, U) &= x_3 + u_2 + u_{11} + u_{21}. \end{aligned}$$

The set $\mathrm{PS}(F_1, F_2, F_3)$ contains $L = 13$ differential polynomials and $\gamma = 0$. The matrix S of $\mathcal{P}_2$ has rank 2 and equals

$$S = \begin{bmatrix} -3 & 1 \\ -1 & 0 \\ 1 & 1 \end{bmatrix}, \phi_i(U) = \begin{cases} u_{12} + u_2, & i = 1, \\ u_1, & i = 2, \\ u_{21}, & i = 3. \end{cases}$$

There exists a nonzero differential polynomial $P(X) \in (\mathrm{PS}) \cap \mathbb{K}\{X\}$ with coefficients in $\mathbb{K}[p]$ and content in $\mathbb{K}$ such that the determinant of the 13×13 matrix $M_\phi(13)$ equals

$$\begin{aligned} &\partial\mathrm{CRes}(F_1^\phi, F_2^\phi, F_3^\phi) = \det(M_\phi(13)) \\ &p\,(1 + 4\,p + 4\,p^4 - p^5 + 2\,p^7 + 11\,p^3 + p^9 - 12\,p^2 - 4\,p^6 + p^8) P(X). \end{aligned}$$

Then $D_\phi = 1$ and the coefficient of p in $\partial\mathrm{CRes}(F_1^\phi, F_2^\phi, F_3^\phi)$ is

$$A_{D_\phi} = x_{12} + x_{13} - x_2 - 3x_{21} - 4x_{22} - 2x_{23} + x_3 + 2x_{31} + 2x_{32} + 2x_{33} + x_{34}$$

We have $A_{D_\phi} = \mathcal{L}_1(x_1) + \mathcal{L}_2(x_2) + \mathcal{L}_3(x_3)$ with

$$\begin{aligned} \mathcal{L}_1 &= \partial^2 + \partial^3 = \partial^2\,(1 + \partial), \\ \mathcal{L}_2 &= -1 - 3\,\partial - 4\,\partial^2 - 2\,\partial^3 = -(\partial + 1)\,(2\,\partial^2 + 2\,\partial + 1), \\ \mathcal{L}_3 &= 1 + 2\,\partial + 2\,\partial^2 + 2\,\partial^3 + \partial^4 = (\partial^2 + 1)\,(\partial + 1)^2. \end{aligned}$$

Therefore $\mathcal{L} = \mathrm{gcld}(\mathcal{L}_1, \mathcal{L}_2, \mathcal{L}_3) = 1 + \partial$ and

$$A_\phi = x_{12} - x_2 - 2\,x_{21} - 2\,x_{22} + x_{33} + x_{32} + x_{31} + x_3$$

with $\mathrm{c}(A_\phi) = 1$. Then $D_\phi = \mathrm{c}(A_\phi)$. We conclude that the dimension of ID is $n - 1 = 2$ and its implicit equation $A_\phi(X) = 0$.

An extended version of this work can be found in [R].

5 References

[CF] G. Carra'Ferro, A resultant theory for ordinary algebraic differential equations, *Lecture Notes in Computer Science*, 1255. Applied Algebra, Algebraic Algorithms and Error-Correcting Codes. Proceedings, 1997.

[G] X.S. Gao, Implicitization of differential rational parametric equations, *J. Symbolic Comput.*, 36 (2003), 811–824.

[R] S.L. Rueda, A perturbed differential resultant based implicitization algorithm for linear DPPEs. arXiv:1003.4375v1.

[RS] S.L. Rueda and J.R. Sendra , Linear complete differential resultants and the implicitization of linear DPPEs. *J. Symbolic Comput.*, 45 (2010), 324–341.

On Sparse Interpolation over Finite Fields

Seyed Mohammad Mahdi Javadi, Michael Monagan
sjavadi@cs.sfu.ca, mmonagan@cecm.sfu.ca

The Problem

The problem of interpolating multivariate polynomials over a finite field is one of the most challenging problems in *computer algebra*. It has been of interest for a long time and has many applications and many solutions.

Let f be a multivariate polynomial in variables $x_1, \ldots, x_n$ with t non-zero terms. The problem is given a black box that on input $\alpha_1, \ldots, \alpha_n$ outputs $f(x_1 = \alpha_1, \ldots, x_n = \alpha_n)$, we want to find the *target polynomial* $f(x_1 \ldots, x_n)$ by *probing* the black box at a series of evaluation points.

Newton's Interpolation Algorithm

The classical method is Newton's algorithm:

1 Let d be a bound on the degree of f in each variable x_i
2 Choose $\beta_1, \beta_2, \ldots, \beta_{d+1}$ random points
3 Recursively interpolate $f_i = f(x_1 = \beta_i, x_2, \ldots, x_n)$ for $1 \le i \le d+1$
4 Use the Chinese remaindering algorithm to interpolate f from $f_1, \ldots, f_{d+1}$

Newton's algorithm does $(d+1)^n$ probes to the black box.

Example 1. *For $f = x_1^d + x_2^d + \cdots + x_n^d + 1$, Newton's algorithm does $(d+1)^n$ probes even though f has only $n+1$ non-zero terms.*

Zippel's Sparse Interpolation Algorithm

The number of probes in Zippel's sparse interpolation algorithm is polynomial in t, the number of non-zero terms in the target polynomial f.

Idea: After interpolating the first image $f_1 = f(x_1 = \beta_1)$, one can use the form of f_1 to compute $f_2, \ldots, f_{d+1}$. This is done by solving systems of linear equations.

Example 2. *Let $f = 4x^{13}y^2 - 3x^5 + 4y^3 - 1$. Let $\beta_1 = 2$. We first interpolate $f_1 = f(y = \beta_1) = 16x^{13} - 3x^5 + 31$ using 14 probes to the black box. We assume the form for f: $g = Ax^{13} + Bx^5 + C$. Each f_i now can be computed using 3 probes to the black box.*

Zippel's algorithm does $O(ndt)$ probes to the black box.

Problem: The number of probes in Zippel's algorithm still depends on a bound d on the degree of f in each variable.

Ben-Or/Tiwari Sparse Interpolation Algorithm

Let f be a polynomial with coefficients in $\mathbb{Z}$. In Ben-Or/Tiwari sparse interpolation algorithm, the number of probes does not depend on the degree. It only depends on T, a bound on the number of non-zero terms in f.

1 Let $p_1, p_2, \ldots, p_n$ be the first n prime numbers.
2 For $i = 0, \ldots, 2T-1$, Let b_i be the output of black box on $(p_1^i, \ldots, p_n^i)$.
3 Find the λ_i s.t. $b_{t+i} = \lambda_{t-1} b_{t+i-1} + \lambda_{t-2} b_{t+i-2} + \cdots + \lambda_0 b_i$ for all $i \ge 0$.
4 Let $\Lambda(z) = z^t - \lambda_{t-1} z^{t-1} - \cdots - \lambda_0$.
5 Compute $r_1, \ldots, r_t$, the integer roots of $\Lambda(z)$.
6 Each r_i is equal to a monomial of f evaluated at $(x_1 = p_1, x_2 = p_2, \ldots, x_n = p_n)$. Find the monomials using integer divisions.
7 Find the coefficients of f by solving a system of linear equations.

Ben-Or/Tiwari algorithm does $2T$ probes to the black box.

Example 3. *Let $f(x,y) = 4x^{13}y^2 - 3x^5 + 4y^3 - 1$. We have $p_1 = 2, p_2 = 3$. Let $T = 4$ be the bound on the number of terms in f. We have*

$$b_0 = f(p_1^0, p_2^0) = 4, b_1 = f(p_1^1, p_2^1) = 294923,$$

$$b_2 = f(p_1^2, p_2^2) = 21743271779, b_3 = f(p_1^3, p_2^3) = 1603087953277835,$$

$$b_4 = f(p_1^4, p_2^4) = 118192468620710277059, b_5 = f(p_1^5, p_2^5) = 8714094326467802463717803,$$

$$b_6 = f(p_1^6, p_2^6) = 642472746501818143233353336099,$$

$$b_7 = f(p_1^7, p_2^7) = 47368230654086048064431853086526155.$$

Using the **Berlekamp/Massey** *algorithm we find the linear generator for this sequence:*

$$\Lambda(z) = z^4 - 73788\, z^3 + 4424603\, z^2 - 68051808\, z + 63700992.$$

The roots of this polynomial are $73728 = p_1^{13} \times p_2^2$, $32 = p_1^5$, $27 = p_2^3$ and 1. Hence the monomials are $x^{13}y^2, x^5, y^3$ and 1.

Problem: Unfortunately one can not use this algorithm for a polynomial over a finite field unless the characteristic p is very large. Let $f = \sum_{i=1}^{t} C_i M_i \in \mathbb{Z}_p[x_1, \ldots, x_n]$. Choose $(\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}_p^n$ at random. One can use Steps 1 to 5 of the Ben-Or/Tiwari algorithm to find the images of the monomials $r_i = M_i(\alpha_1, \ldots, \alpha_n) \bmod p$. The problem is that we can not uniquely determine the degrees of the monomials by their images $r_1, \ldots, r_t$ using only integer divisions in $\mathbb{Z}_p$.

Our New Sparse Interpolation Algorithm

Our sparse interpolation algorithm is a modification of the Ben-Or/Tiwari algorithm for polynomials over finite fields. It costs an extra factor of $O(n)$ probes.

Idea: We choose the evaluation point $(\alpha_1, \ldots, \alpha_n, \alpha_{n+1}) \in \mathbb{Z}_p^{n+1}$ at random. We first run the first five steps of the Ben-Or/Tiwari algorithm to find the images of the monomials $r_i = M_i(\alpha_1, \ldots, \alpha_n)$. To find the degrees of the monomials in the variable x_j, we replace α_j by α_{n+1}. We run the first 5 steps again and we find $\bar{r}_i = M_i(\alpha_1, \ldots, \alpha_{j-1}, \alpha_{n+1}, \alpha_{j+1}, \ldots, \alpha_n)$.

Observation: We have

$$\frac{r_i}{\bar{r}_i} = \left(\frac{\alpha_j}{\alpha_{n+1}}\right)^{d_i},$$

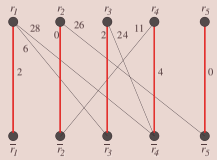
where $d_i = \deg_{x_j}(M_i)$. We will use this fact to find the degrees of all the monomials in x_j. The problem is we need to match the root r_i with the corresponding root $\bar{r}_i$. To do this, we use bipartite matching algorithm from graph theory.

Our new algorithm does $2nT$ probes to the black box.

Example 4. *Let $f = 25y^2z + 90yz^2 + 93x^2y^2z + 60y^4z + 42z^5 \in \mathbb{Z}_{101}[x,y,z]$. Here $t = 5, n = 3$. Suppose we now that the degree bound on the degree of f in each variable is $d = 40$. We choose the following evaluation points $\alpha_1 = 85, \alpha_2 = 96, \alpha_3 = 58$ and $\alpha_4 = 99$. Suppose we want to find the degrees of the monomials in y. We run the first steps of the Ben-Or/Tiwari algorithm for both $\beta_1 = (x = \alpha_1, y = \alpha_2, z = \alpha_3)$ and $\beta_2 = (x = \alpha_1, y = \alpha_4, z = \alpha_3)$. We obtain two sets of roots $R = \{36, 47, 25, 92, 87\}$ and $\bar{R} = \{30, 39, 4, 19, 87\}$. Let the graph G be a bipartite graph with nodes R and $\bar{R}$ such that r_i is connected to $\bar{r}_j$ if and only if*

$$\frac{r_i}{\bar{r}_j} = \left(\frac{\alpha_2}{\alpha_4}\right)^e,$$

for some $0 \le e \le d = 40$. We have



We try to find a perfect matching in this graph. The edges which are in the perfect matching are highlighted in red. We find that the degrees of the monomials in y are 2, 1, 2, 4 and 0.

Protobox

In 2000, Kaltofen *et al.*, presented a hybrid of Zippel and Ben-Or Tiwari algorithms which they call a racing algorithm. To interpolate the next variable, their algorithm runs a Newton interpolation and univariate Ben-Or/Tiwari algorithm, stopping when the first succeeds to reduce the number of probes. The purpose of the early termination technique is to avoid using bounds for determining the termination point in an algorithm. Instead the racing algorithm stops when the interpolated polynomial does not change after a certain number of probes to the black box.

Benchmarks

$f_i \in \mathbb{Z}_p[x_1, \ldots, x_6]$ where $p = 3037000453$. We have $\#f_i \approx 2^i$ and $d = 30$. DNF means "Did Not Finish".

i	$\#f$	New Algorithm		Zippel		ProtoBox
		Time	Probes	Time	Probes	Probes
1	2	0.00	24	0.01	496	37
2	3	0.00	36	0.01	651	59
3	8	0.00	96	0.01	1364	140
4	16	0.00	192	0.02	2511	284
5	31	0.00	372	0.05	4340	521
6	64	0.02	768	0.15	8060	995
7	127	0.06	1524	0.44	14601	1871
8	255	0.21	3060	1.51	27652	3615
9	511	0.81	6132	5.19	50530	6692
10	1016	3.10	12192	17.94	90985	12591
11	2037	12.20	24444	65.35	168299	DNF
12	4083	48.06	48996	230.60	301320	DNF
13	8151	189.21	97812	803.26	532549	DNF

References

[1] Richard Zippel. Probabilistic algorithms for sparse polynomials. In *EUROSAM '79: Proc. of the International Symposiumon on Symbolic and Algebraic Computation*, pages 216–226, London, UK, 1979.

[2] P. Tiwari M. Ben-Or. A deterministic algorithm for sparse multivariate polynomial interpolation. In *STOC '88: Proc. of the twentieth annual ACM symposium on Theory of computing*, pages 301–309, 1988. ACM.

[3] Erich Kaltofen and Wen-shin Lee. Early termination in sparse interpolation algorithms. *J. Symb. Comput.*, 36(3-4):365–400, 2003.

Nullspace Computation over Rational Function Fields for Symbolic Summation

Burçin Eröcal, RISC, Johannes Kepler University Linz, Austria
Arne Storjohann, David R. Cheriton School of Computer Science, University of Waterloo, Canada

Problem

Input: $A \in \mathbb{Z}[x]^{n\times(n+m)}$ of rank n
Output: $N \in \mathbb{Q}(x)^{(n+m)\times m}$, a right nullspace of A

Example

Input: $A = \begin{bmatrix} z & 1 & 0 & 0 \\ 0 & -y & z & 0 \\ 0 & 0 & -x & y \end{bmatrix}$

Output: canonical nullspace N

$$N = \begin{bmatrix} 1 & -z & -y & -x \end{bmatrix}^T$$

$$\begin{bmatrix} z & 1 & 0 & 0 \\ 0 & -y & z & 0 \\ 0 & 0 & -x & y \end{bmatrix} \begin{bmatrix} 1 \\ -z \\ -y \\ -x \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

Computational Issues

- n, m typically large, degree of A low
- entries in N have low degree
- e.g., $n = 112$, $m = 19$, $d = 3$, $\max_{i,j} |A|_{i,j} = 32$ entries in canonical N have
  - degree 15
  - $\max_{ij} |N|_{ij} = 32$

Outline of Approach

homomorphic imaging modulo word-size primes

1. preprocessing step reduces the problem to computing the nullspace of full row rank matrix
$$[\,A \mid B\,] \in \mathbb{Z}[x]^{n\times(n+m)},$$
where A is square nonsingular.
2. canonical nullspace basis is given by
$$\left[\frac{sA^{-1}B}{-sI}\right] \in \mathbb{Q}[x]^{(n+m)\times m},$$
where the scaling polynomial $s \in \mathbb{Q}[x]$, a factor of $\det A$, is used to clear denominators (i.e., $\mathbb{Q}(x) \to \mathbb{Q}[x]$) from $A^{-1}B \in \mathbb{Q}(x)$.
3. compute $(s, sA^{-1}B)$ modulo various word size primes p
4. recover the final result over $\mathbb{Q}[x]$ using Chinese remaindering and, if needed, rational number reconstruction.

two approaches to compute $(s, sA^{-1}B)$

(a) output sensitive x-adic lifting
(b) outer product adjoint formula

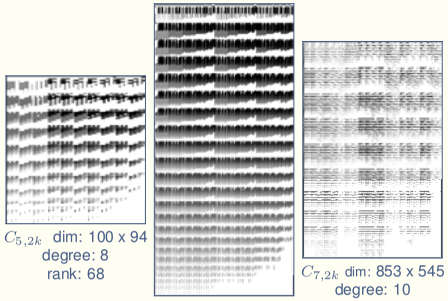
Motivation

- application to symbolic summation
  - Wilf-Zeilberger-Fasenmyer [1]
  - Karr's algorithm [2]

Example

- **Goal:** Find a recurrence relation satisfied by
$$F(k,i,j,X) = \binom{k}{j}\binom{j}{i} x^i y^{j-i} x^{k-j} = (x+y+z)^k$$
where $X = (x, y, z)$.
- **Fasenmyer's method:**
  1. Make an Ansatz for the structure set
  $$S = \{(0,0,0), (1,0,0), (1,0,1), (1,1,1)\}$$
  and write
  $$\sum_{(a,b,c)\in S} p_{(a,b,c)}(k,i,j) F(k-a, i-b, j-c, X) = 0$$
  for unknown $p(k,i,j) \in \mathbb{Q}[k,i,j]$.
  2. Divide by F(k, i, j, X) to get
  $$\sum_{(a,b,c)\in S} p(k,i,j) r_{(a,b,c)}(k,i,j,X) = 0$$
  with $r_{(a,b,c)}(k,i,j,X) \in \mathbb{Q}(k,i,j,X)$.
  3. Clear denominators to get a polynomial identity
  4. Compare coefficients of monomials in X to obtain the matrix A
  5. Plug in $p_{(a,b,c)}(k,i,j)$ from N to obtain
  $$F(k,i,j) - zF(k-1,i,j) - yF(k-1,i,j-1) - xF(k-1,i-1,j-1) = 0$$

Dataset



$C_{5,2k}$ dim: 100 x 94 degree: 8 rank: 68

$C_{6,2k}$ dim: 340 x 161 degree: 16 rank: 160

$C_{7,2k}$ dim: 853 x 545 degree: 10 rank: 401

Timings

Comparison of timings for systems generated by `MultiSum` [3] for the problems $C_{5,2k}, C_{6,2k}$ and $C_{7,2k}$ from [4]:

	lifting*	`EANullSpace`†	Maple ‡
$C_{5,2k}$	17 s	20 s	13 s
$C_{6,2k}$	42 s	> 1 hour	> 1 hour
$C_{7,2k}$	3227 s	-	-

Comparison of timings to compute a canonical nullspace for a matrix with random entries of dimension 500 x 600 with the given degree:

degree	lifting(a)	OPAF(b)
10	5341 s	5267 s
20	20461 s	20599 s
30	45879 s	45030 s

computations were done on a 2.66GHz Intel(R) Xeon(R) X7460 CPU
* output sensitive x-adic lifting in Sage [5]
† implementation by Axel Riese, timed on MMA 5.2
‡ linalg[nullspace] in Maple version 12

(a) Output sensitive x-adic lifting

- compute
$$(s, sA^{-1}B) \bmod p \in \mathbb{Z}_p[x]$$
using x-adic lifting
- s will be a monic divisor of $\det A$
- asymptotic cost of computing each image is $O\tilde{}(n^3md)$ operations modulo p.

Pros

- lifting reduced to calling the FFLAS library to perform multiply-add operations
- allows output sensitive approach for x-adic lifting and Chinese remaindering
- resulting nullspace degree much lower than bounds expected from random input.
- performs lifting up to $\max(\deg s, \deg sA^{-1}B)$ instead of the a priori degree bound nd.

Cons

- final recovery of the result over $\mathbb{Q}[x]$ requires rational number reconstruction as well as Chinese remaindering
- requires large amounts of memory

(b) Outer Product Adjoint Formula

- compute
$$(\det A, (\det A)A^{-1}B) \bmod p \in \mathbb{Z}_p[x]$$
with the outer product adjoint formula approach [6]

Pros

- cost of computing each image is $O\tilde{}(n^3d + n^2md)$ operations modulo p
- the outer product method has better worst case complexity, and is considerably faster on random input

Cons

- outer product formula requires us to work with a preconditioned matrix whose adjoint has degrees $(n-1)d$, which
  - hides the structure of the inputs
  - prevents effective use of an early termination strategy for the lifting.
- for the input matrices encountered in summation problems the x-adic algorithm gave better results

References

[1] H. S. Wilf and D. Zeilberger. An algorithmic proof theory for hypergeometric (ordinary and "q") multisum/integral identities. *Invent. Math.*, 108(3):575–633, 1992.
[2] Michael Karr. Summation in finite terms. *J. ACM*, 28(2):305–350, 1981.
[3] K. Wegschaider. Computer generated proofs of binomial multi-sum identities. Master's thesis, RISC, Johannes Kepler University, May 1997.
[4] F. Stan. On recurrences for Ising integrals. *Adv. in Appl. Math.*, 45(3):334–345, 2010.
[5] W. A. Stein et al. *Sage Mathematics Software*. The Sage Development Team. http://www.sagemath.org.
[6] A. Storjohann. On the complexity of inverting integer and polynomial matrices. Technical report, David R. Cheriton School of Computer Science, University of Waterloo, 2008.
[7] Bill Hart and David Harvey. Flint: Fast library for number theory. http://www.flintlib.org/.
[8] J.-G. Dumas, T. Gautier, and C. Pernet. Finite field linear algebra subroutines. In T. Mora, editor, *Proc. ISSAC '02*, pages 63–74. ACM Press, New York, 2002.
[9] T. Granlund. The GNU multiple precision arithmetic library, 2004. Edition 4.1.4. http://www.swox.com/gmp.
[10] David Harvey. Faster polynomial multiplication via multipoint kronecker substitution. *Journal of Symbolic Computation*, 44(10):1502 – 1510, 2009.

6. **Workshop on Complexity and Group-Based Cryptography**

Montreal, Kanada,
30.08. – 03.09.2010

http://www.crm.umontreal.ca/Complex10

Der Workshop war Teil eines thematischen Semesters über *Geometric, Combinatorial, and Computational Group Theory*, das von Juli bis Dezember 2010 am Centre de Recherches Mathematiques der Université de Montreal läuft. Neben einer Reihe von Einzelvorträgen fanden auch zwei Minikurse statt: *Algorithmic Group Theory* von Robert Gilman und Alexei Myasnikov sowie *Group-Based Cryptography* von Vladimir Shpilrain und Alexander Ushakov. Aus der Sicht der Computeralgebra besonders relevant waren die Beiträge über die Anwendung nichtkommutativer symbolischer Berechnungen, um die Sicherheit und Durchführbarkeit gruppenbasierter Kryptosysteme zu analysieren. Der Berichterstatter stellte dazu das neue Funktionspaket des ApCoCoA-Systems vor, mit dem sich Gröbnerbasis-Berechnungen in Monoid- und Gruppenringen durchführen lassen.

Die Vorträge wurden per Video aufgezeichnet und sollen über die Webseiten des *Algebraic Cryptography Center* auf http://www.stevens.edu/algebraic/ allgemein zugänglich gemacht werden.

Martin Kreuzer (Passau)

7. **CASC 2010 – 12th International Workshop on Computer Algebra in Scientific Computing**

Tsakhkadzor, Armenien, 6. – 11.09.2010

http://www14.in.tum.de/CASC2010/

The CASC 2010 participants on the Lake of Sevan

CASC 2010, the 12th international workshop on computer algebra in scientific computing, took place in Armenia in September 6-11. The workshop was organized by the Department of Informatics, Technical University, München, and by the Institute for Informatics and Automation Problems (IIAP) of Armenian Academy of Sciences. The opening with one of the invited talks given by Yury Shoukuryan (IIAP) entitled *Computational Science in Armenia* was held in Yerevan, the capital of the country, on September 7. Then the workshop participants moved to Tsakhkadzor, a city and popular health resort center in Armenia located 50 kilometers away of Yerevan, in the Teghenis Mountains, at a height of 1750 meters above see level. Two other invited talks were given by Andreas Weber, University of Bonn *Parametric Qualitative Analysis of Ordinary Differential Equations: Computer Algebra Methods for Excluding Oscillations* and by Ernst Mayr *From Petri nets to Polynomials: Modelling, Algorithms and Complexity*. Additionally, 23 regular talks were given by participants from Armenia, Belarus, Germany, France, Holland, Japan, Russia and Spain. The accepted CASC 2010 papers have been published in the Springer-Verlag series Lecture Notes in Computer Science, LNCS 6244.

Vladimir Gerdt (Dubna)

8. **28. Herbsttagung des GDM-Arbeitskreises Mathematikunterricht und Informatik**

Soest, 24. – 26.09.2010

http://didaktik-der-mathematik.de/ak/mui/

Vom 24.-26.09.2010 fand im Tagungshaus Soest die 28. Herbsttagung des Arbeitskreises statt. Diese Tagung ist auch seit diesem Jahr die Fortsetzung der Tagungsreihe Computeralgebra in Lehre, Ausbildung und Weiterbildung unserer Fachgruppe Computeralgebra. Dementsprechend war es erfreulich, dass viele Teilnehmer unserer früheren Tagungen an der Soester Tagung teilnahmen. Das diesjährige Schwerpunktsthema war „Geometrie 2030 – zwischen Kreidetafel und Holodeck“. Mehr als 20 Referentinnen und Referenten beschrieben den aktuellen Stand der Soft- und Hardware von 2D- und 3D-Geometrieumgebungen aus verschiedenen Perspektiven und entwickelten spannende Szenarien für die zu erwartenden Entwicklungen in den nächsten 20 Jahren. Etwa 50 Teilnehmerinnen und Teilnehmer aus Schule und Universität diskutierten mit den Referenten über die Zukunft des Geometrieunterrichts. In der Abschlusssitzung wurden erste Vorschläge für das Thema der nächsten Arbeitskreistagung (wieder geplant für das Wochenende 23.-25.09.2011) gesammelt; die Entscheidung wird bei der GDM-Tagung 2011 in Freiburg fallen.

Hans-Wolfgang Henn (Dortmund)

9. **13. Mitteldeutscher Computeralgebratag**

Leipzig, 01.10.2010

http://www.informatik.uni-leipzig.de/~graebe/MCAT/mcat13.html

Am 1. Oktober 2010 fand unter dem Thema „Computermathematik im Schulunterricht“ der 13. Mitteldeutsche Computeralgebratag (MCAT) als Teil des Lehrerprogramms der 40. Jahrestagung der Gesellschaft für Informatik an der Universität Leipzig statt.

Bereits in den letzten Jahren spielten Lehrer als Zielgruppe im Programm des MCAT eine größere Rolle, so beim 9. MCAT in Jena, beim 10. MCAT in Cottbus oder beim 11. MCAT in Halle/S. In diesem Jahr war das gesamte Programm speziell auf Lehrerinteressen ausgerichtet und im Vorbereitungsteam mit Ines Petzschler (Leipzig), Wolfgang Ludwicki (Stendal), Wolfgang Moldenhauer (Erfurt) und Horst Ocholt (Meissen) auch Lehrer als Multiplikatoren aus dem Schulamtsbereich der drei mitteldeutschen Bundesländer aktiv. Eine spezielle Sektion adressierte das Thema auch für Grundschullehrerinnen und -lehrer, da wir davon ausgehen, dass der zunehmende Einsatz von Technologie im Unterricht der Mittel- und Oberstufe auch an der Grundstufe nicht spurlos vorbeigehen wird.

Am Vormittag präsentierte zunächst Josef Böhm (Würmla bei Wien) mit *WIRIS* eine neue vielversprechende Plattform für Computeralgebra im Schulunterricht, die in Österreich auf dem Weg ist, das von Texas Instruments nicht mehr weiter entwickelte *Derive* abzulösen. In Deutschland kann WIRIS über das kleine Berliner Startup kapieren.de bezogen werden, das uns auch eine Desktopversion für einen

Workshop am Nachmittag zur Verfügung stellte. Der zweite Teil des Vormittagsprogramms fand in zwei Sektionen statt; in der Grundschulsektion stellte Gerd Richter (Universität Halle) Möglichkeiten einer „Computermathematik in der Grundschule“ sowohl für Unterrichtselemente als auch die Erstellung von Unterrichtsmaterialien vor, während in der Oberschulsektion Ulrich Kortenkamp (PH Karlsruhe) über das europäische Intergeo-Projekt `i2geo.net` berichtete, mit dem ein Netzwerk von Entwicklern und Anwendern von Dynamischer Geometrie-Software (DGS) geknüpft worden ist und weiter geknüpft wird, in dem auch der Einsatz von DGS im Unterricht und die Qualität entsprechender Lehrmaterialien strukturiert thematisiert wird. Kortenkamp erläuterte insbesondere die Bemühungen zur Standardisierung des Ausgabeformats von DGS mit einem neuen Format `i2g` und wies auf die GeoSkills-Ontologie hin, mit der interlinguale Beschreibungsmittel für die Qualität und den curricularen Bezug von Lehrmaterialien im DGS-Bereich zur Verfügung stehen.

Am Nachmittag wurde das Thema der Veranstaltung in fünf parallelen Workshops selektiv und zielgruppenspezifisch vertieft.

Trotzdem die Veranstaltung im Fortbildungskatalog aller drei mitteldeutschen Bundesländer gelistet und im Vorfeld intensiv beworben wurde, beteiligten sich nur etwa 60 Lehrerinnen und Lehrer sowie Interessierte aus angrenzenden Bereichen. Es entspricht der Erfahrung vergleichbarer Veranstaltungen, dass die anvisierte Zielgruppe für solche nicht unmitelbar curricular verwertbaren Veranstaltungen schwer zu mobilisieren ist.

Mit dem Blick auf das Verhältnis von Aufwand und Nutzen der MCAT der letzten Jahre stellt sich für mich die Frage nach dem Sinn dieser Veranstaltung mit neuer Schärfe, auch wenn in der Abschlussrunde der Wunsch nach Fortsetzung der Reihe deutlich artikuliert wurde. In den letzten Jahren war es zunehmend schwierig, überhaupt noch Mitorganisatoren und Finanzierungsquellen zu finden. Der 13. ist deshalb der letzte MCAT, wenigstens in der bisherigen Form. Ich bedanke mich bei allen Mitstreiterinnen und Mitstreitern, die über die Jahre dieser regionalen Computeralgebra-Aktivität nicht nur die Treue gehalten, sondern sie auch aktiv mit ausgestaltet haben, insbesondere den jahrelangen Koorganisatoren Peter Schenzel (Universität Halle) und Thomas Buchanan (FH Merseburg).

Weitere Informationen zu den Mitteldeutschen Computeralgebratagen sind unter `http://www.informatik.uni-leipzig.de/~graebe/MCAT` zu finden.

Hans-Gert Gräbe (Leipzig)

Hinweise auf Konferenzen

1. **DART IV – Workshop on Differential Algebra and Related Topics**

   Beijing, China, 27. – 30.10.2010

   `http://mmrc.iss.ac.cn/~dart4`

   Differential Algebra and Related Topics (DART) is a series of workshops which offer an opportunity for participants to present original research, to learn of research progress and new developments, and to exchange ideas and views on differential algebra and related topics. DART-IV is the fourth in this series.

2. **CASTR 2011 – Computer Algebra Systems in Teaching and Research**

   Siedlce, Polen, 02. – 06.11.2010

   `http://www.castr.pl`

   The conference is organized by the College of Finance and Management and University of Podlasie in Siedlce, Poland. It will be held at the hotel „Dwor Moscibrody“ near Siedlce from February 2, 2011 to February 6, 2011. The conference will be devoted to presentation and discussion of new developments in application of computer algebra to various mathematical and physical problems and to using computer algebra systems in education.

   Topics include applications of computer algebra systems in the theory of differential equations, applications of computer algebra to studying mathematical models in civil engineering, computer algebra methods in finance and economics, and computer algebra systems in education.

3. **3. Computeralgebratag Hannover-Braunschweig**

   Hannover, 04.11.2010

   `http://www.iag.uni-hannover.de/de/aktivitaeten/nth_compalg.php`

   Am 4. November 2010 findet der 3. Computeralgebratag Hannover-Braunschweig statt. Dieses Mal treffen wir uns an der Universität Hannover. Vortragende sind David Green (Jena), Gregor Kemper (München) und Dörte Feichtenschlager (Braunschweig).

4. **SIAM/MSRI Workshop on Hybrid Methodologies for Symbolic-Numeric Computation**

   Berkeley, Kalifornien, 17. – 19.11.2010

   `http://www.scg.uwaterloo.ca/siam-msri-hybrid`

   Hybrid symbolic-numeric computation methods, which first appeared some twenty years ago, have gained considerable prominence. Algorithms have been developed that improve numeric robustness (e.g. in quadrature or solving ODE systems) using symbolic techniques prior to, or during, a numerical solution. Likewise, traditionally symbolic algorithms have seen speed improvements from adaptation of numeric methods (e.g., lattice reduction methods). There is also an emerging approach of characterizing, locating, and solving “interesting nearby problems”, wherein one seeks an important event (for example a nontrivial factorization or other useful singularities), that in some measure is close to a given problem (one that might have only imprecisely specified data). Many novel techniques have been developed in these complementary areas, but there is a general belief that a mo-

re overarching understanding and approach will foster future progress.

Problems we are interested in are driven by applications in computational physics (quadrature of singular integrals), dynamics (symplectic integrators), robotics (global solving of direct and inverse problems near singular manifolds), control theory (stability of models), and dynamic modeling of large-scale continuous and hybrid discrete-continuous dynamical systems. Emphasis will be given to validated (certified) outputs by 1. error estimation or 2. interval techniques or 3. global optimization strategies based on semidefinite programming and exact sums-of-squares.

This workshop will provide a forum for researchers on both sides (and the middle!) of hybrid symbolic-numeric computation.

5. **Jahrestagung der Gesellschaft für Didaktik der Mathematik**

Freiburg, 21. – 25.02.2011

`http://gdm2011.ph-freiburg.de/`

Wir freuen uns, Sie zur 45. Jahrestagung der Gesellschaft für Didaktik und Mathematik vom 21.-25.02.2011 an der Pädagogischen Hochschule in Freiburg begrüßen zu dürfen. Für die Hauptvorträge konnten wir einladen: Ekkehard Klieme (Deutsches Institut für Internationale Pädagogische Forschung Frankfurt), Markus Vogel (Pädagogische Hochschule Heidelberg), Elisabeth Rathgeb-Schnierer (Pädagogische Hochschule Weingarten), Kaye Stacey (University of Melbourne), Angelika Bikner-Ahsbahs (Universität Bremen) und Alexander Renkl (Albert-Ludwigs-Universität, Freiburg). Darüber hinaus erwartet Sie ein vielfältiges Rahmenprogramm in und um Freiburg. Wir hoffen auf eine rege Beteiligung und freuen uns auf Ihren Besuch.

6. **1. Jahrestagung des DFG-Schwerpunkts Algorithmische und experimentelle Methoden in Algebra, Geometrie und Zahlentheorie**

Aachen, 21. – 25.02.2011

`http://www.computeralgebra.de`

Die erste Jahrestagung des DFG-Schwerpunktprogramms SPP1489 findet vom 21. bis zum 25.02.2011 in Aachen statt. Einen kurzen Bericht über die bisherige Arbeit des Schwerpunkts finden Sie in diesem Rundbrief auf S. 40.

7. **CAPP – Computer Algebra and Particle Physics 2011**

Berlin, 20. – 25.03.2011

`https://indico.desy.de/conferenceDisplay.py?confId=1573`

During the last years, computer algebra methods have been used widely throughout elementary particle physics. Applications of modern computer algebra are an essential and established calculational tool and, at the same time, methods and algorithms of computer algebra have become an important area of research itself.

The CAPP school combines theory and practice in advanced environment. It provides education and training of about 30 students and young researchers at graduate and Ph.D. level on central topics at the interface of modern computer algebra and particle physics. The courses include exercises and practical training with software and programs, the hands-on part being a central component of the school.

8. **GCR 2011 – Geometric Constraints and Reasoning**

Taichung, Taiwan, 21. – 25.03.2011

`http://www.lsi.upc.edu/~robert/gcr2011/gcr2011.html`

Geometric Constraints and Reasoning (GCR) is a technical track of the International Symposium on Applied Computing. For the past twenty years, the ACM Symposium on Applied Computing (SAC) has been a primary forum for applied computer scientists, computer engineers and application developers to gather, interact, and present their work.

SAC is sponsored by the ACM Special Interest Group on Applied Computing (SIGAPP), its proceedings are published by ACM in both printed form and CD-ROM; they are also available on the web through ACM's Digital Library.

As a special track of SAC, GCR is devoted to geometric reasoning taken in a broad sense. Initially, this track focused on geometric constraint solving but it appears that geometric computing and reasoning is closely related to this topic. Our aim is then to widen the audience and to make GCR a place where the communities of geometric constraint solving, computer aided deduction in geometry and related disciplines can meet and have fruitful exchanges.

GCR 2011 will be an opportunity to gather several communities involved in geometric computing and reasoning such as geometric constraints solving, dynamic geometry, pedagogical software packages, computer aided teaching of geometry, computer algebra and many more.

9. **82. Jahrestagung der GAMM**

Graz, Österreich, 18. – 21.04.2011

`http://www.gamm2011.tugraz.at/`

The GAMM (Gesellschaft für Angewandte Mathematik und Mechanik) cordially invites you to its 82nd Annual Scientific Conference in Graz, Austria. The GAMM was founded in 1922 by Ludwig Prandtl and Richard von Mises. The society promotes scientific development in all areas of applied mathematics and mechanics.

On behalf of the DGLR and the GAMM we also invite you to the 54th Ludwig Prandtl Memorial Lecture, which opens the conference program on Monday, April 18, 2011. Within the conference we invite all GAMM members to the regular General Assembly of GAMM on Wednesday, April 20, 2011.

10. **MEGA 2011 – Effective Methods in Algebraic Geometry**

Stockholm, Schweden, 30.05. – 03.06.2011

`http://www.math.kth.se/mega2011/`

The eleventh conference MEGA will be held at Stockholm University from Monday, 30 May to Friday, 3 June 2011.

MEGA is the acronym for Effective Methods in Algebraic Geometry (and its equivalent in Italian, French, Spanish, German, Russian, etc.), a series of roughly biennial conferences on computational and application aspects of Algebraic Geometry and related topics with very high standards. Previous meetings were held in 1990 (Castiglioncello, Italy),

1992 (Nice, France), 1994 (Santander, Spain), 1996 (Eindhoven, Nederlands), 1998 (St. Malo, France) 2000 (Bath, United Kingdom), 2003 (Kaiserslautern, Germany), 2005 (Porto Conte, Italy), 2007 (Strobl, Austria), and 2009 (Barcelona, Spain).

Proceedings containing a selection of the papers and invited talks presented at previous Mega conferences have been published by Birkhäuser in the series Progress in Mathematics (volumes no. 94, 109 and 143), by the Journal of Pure and Applied Algebra (volumes no. 117 and 118, 139 and 164) and by the Journal of Symbolic Computation (volumes no. 39 3-4 and 42 1-2).

11. CoCoA 2011 – International School on Computer Algebra

Passau, 06. – 10.06.2011

`http://cocoa.dima.unige.it/conference/cocoa2011/`

Die CoCoA-Schule richtet sich an Diplomanden und Doktoranden aus der ganzen Welt, die an Themen aus der kommutativen Algebra oder algebraischen Geometrie arbeiten und das Computeralgebrasystem CoCoA einsetzen wollen. Es wird zwei Kurse mit zugehörigen Tutorien geben: *Involutive Bases* (Werner Seiler, Tutorien: Eduardo Saenz de Cabezon) sowie einen Kurs von Giuseppe Valla (Tutorien: Anna Bigatti).

Die CoCoA-Schule findet bereits zum siebten Mal statt, jedoch erstmals in Deutschland. Neben den Kursen und Tutorien wird auch eine Poster-Session angeboten, in der die Teilnehmer ihre eigenen Arbeiten präsentieren können. Details zur Anmeldung und Durchführung sind ab Anfang 2011 auf der angegebenen Webseite abrufbar.

12. ISSAC 2011 – International Symposium on Symbolic and Algebraic Computation

San Jose, Kalifornien, 08. – 11.06.2011

`http://www.issac-conference.org/2011`

The International Symposium on Symbolic and Algebraic Computation (ISSAC) is the premier conference for research in symbolic computation and computer algebra. ISSAC 2011 is the 36th meeting in the series, started in 1966 and held annually since 1981, in North America, Europe and Asia. The conference presents a range of invited speakers, tutorials, poster sessions, software demonstrations and vendor exhibits with a centerpiece of contributed research papers. All areas of computer algebra and symbolic computation are of interest.

ISSAC 2011 invites the submission of original research contributions to be considered for publication and presentation at the conference. Papers should not duplicate work published or submitted for consideration elsewhere prior or in parallel to the ISSAC submission. Submission is in two stages: first the abstract is submitted by the abstract deadline, then the full paper may be submitted up to the paper deadline.

Papers must be in English and shall be reviewed by the Program Committee and external referees. Authors may be asked to respond to reviews shortly before acceptance decisions are made. Submissions cannot exceed 8 pages in the ACM sig-alternate.cls style (see `http://www.acm.org/sigs/publications/proceedings-templates`); if necessary, they can have an appendix that may be read by the reviewers and PC members, but which is not part of the Proceedings paper. Extended abstracts will not be accepted. Submission is exclusively via EasyChair. At least one author of each accepted paper must register for the conference to present the paper.

Important Dates:

Abstract submission deadline:	January 8, 2011
Full paper submission deadline:	January 13, 2011
Notification of acceptance:	March 10, 2011
Camera-ready copy due:	March 31, 2011

13. ICCSA 2011 – International Conference on Computational Science and Its Applications

Santander, Spanien, 20. – 23.06.2011

`http://www.iccsa.org`

The 2011 International Conference on Computational Science and Applications (ICCSA 2010) will be held on June 20-23, 2011, at the University of Cantabria, Santander, Spain.

ICCSA 2011 will be the next event in a series of highly successful International Conferences on Computational Science and Its Applications (ICCSA), previously held in Fukuoka, Japan (2010), Suwon, Korea (2009), Perugia, Italy (2008), Kuala Lumpur, Malaysia (2007), Glasgow, UK (2006), Singapore (2005), Assisi, Italy (2004), Montreal, Canada (2003), and (as ICCS) Amsterdam, The Netherlands (2002) and San Francisco, USA (2001).

Computational Science is a main pillar of most of the present research, industrial and commercial activities and plays a unique role in exploiting Information and Communication Technologies as innovative technologies.

The ICCSA Conference offers a real opportunity to discuss new issues, tackle complex problems and find advanced enabling solutions able to shape new trends in Computational Science.

14. IMACS-ACA 2011 – 17th International Conferences on Applications of Computer Algebra

Houston, Texas, 27. – 30.06.2009

`http://buchberger.cs.lamar.edu/ACA2011/`

The IMACS-ACA series of conferences is devoted to promoting the applications and development of Computer Algebra and Symbolic Computation. We bring together developers of computer algebra systems and packages with researchers and users including scientists, engineers, educators.

Topics include computer algebra and symbolic computation in engineering, the sciences, medicine, pure and applied mathematics, education, communication and computer science.

15. ICTMA 15 – International Conference on Teaching of Mathematical Modelling and Applications

Melbourne, Australien, 14. – 19.07.2011

`http://dlibrary.acu.edu.au/staffhome/jibrown/ictma.html`

ICTMA15 is hosted by the Australian Catholic University (Melbourne, Australia).

The community, through its membership, research and other activities, is recognised as The International Study Group for Mathematical Modelling and Applications (ICTMA) by

its affiliation with the International Commission on Mathematics Instruction (ICMI). International conferences on the Teaching of Mathematical Modelling and Applications are held biennially. This conference brings together international experts in a variety of fields as well as local and regional teachers, post-graduate students and academics. It considers modelling and applications in business, the environment, industry and the workplace, evaluation of effectiveness of such modelling, pedagogical issues for teaching and learning, applicability at different levels of schooling and in tertiary education, research into teaching and practice, innovative practices in research, teaching and practice, influences of technology, and assessment in schools and universities.

The conference will be held mainly at St Patrick's Campus of ACU (Melbourne). The campus is located in inner Melbourne. The possibility of a visit to ACU (Ballarat) for a plenary followed by a visit to the highly acclaimed Sovereign Hill, Ballarat, tourist attraction is being investigated by the organisers.

16. CASC 2011 – 13th International Workshop on Computer Algebra in Scientific Computing

Kassel, 05. – 09.09.2011

http://www14.in.tum.de/CASC2010/

The methods of Scientific Computing play an important role in the natural sciences and engineering. Significance and impact of computer algebra methods and computer algebra systems for scientific computing has increased considerably over the last decade. The topics addressed in the CASC workshops cover all the basic areas of scientific computing as they benefit from the application of computer algebra methods and software.

The 13th International Workshop on Computer Algebra in Scientific Computing, CASC 2010, will be held in Kassel (Local Arrangements Chair: Werner M. Seiler). The methods of Scientific Computing play an important role in the natural sciences and engineering. Significance and impact of computer algebra methods and computer algebra systems for scientific computing has increased considerably over the last decade.

17. ACAT 2011 – 14th International Workshop on Advanced Computing and Analysis Techniques in Physics Research

Brunel University Oxbridge, Großbritannien, 05. – 09.09.2011

http://acat.in2p3.fr/cgi-bin/twiki.source/bin/view/ACAT/WebHome

The ACAT workshop series, created back in 1990 as AIHENP (Artificial Intelligence in High Energy and Nuclear Research) has been covering the tremendous evolution of computing in its most advanced topics, trying to setup bridges between computer science, experimental and theoretical physics.

The gap between the need for adapting applications to exploit the new hardware possibilities and the push toward virtualisation of resources is widening, creating more challenges as technical and intellectual progress continues.

18. Jahrestagung der DMV

Köln, 19. – 22.09.2011

http://www.mi.uni-koeln.de/algebra/dates/dmv2011/

Die Jahrestagung der DMV 2011 findet vom 19. bis 22. September an der Universität zu Köln statt. In diesem Zeitraum findet auch die Mitgliederversammlung der DMV statt. Alle DMV-Mitglieder sind herzlich dazu eingeladen. Bitte reservieren Sie den Termin jetzt schon in Ihrem Kalender. Zu den Hauptvortragenden gehören Holger Dette (Bochum), Irene Fonseca (Pittsburgh), Bernhard Keller (Paris), Matthias Kreck (Bonn), Shrawan Kumar (Chapel Hill), Ladislav Kvasz (Prag), Christian Lubich (Tübingen), Ken Ono (Madison), Francisco Santos Leal (Cantabria) und Simone Warzel (München)

19. INFORMATIK 2011 – Jahrestagung der GI

TU Berlin, 04. – 07.10.2011

http://www.informatik2011.de

Die INFORMATIK 2011 findet an der TU Berlin statt, einer der drei großen Universitäten Berlins. Die TU Berlin versteht sich als international renommierte Universität in der deutschen Hauptstadt, im Zentrum Europas.

Das Motto „Informatik schafft Communities“ wird in Berlin aus zwei Richtungen beleuchtet. Zum einen soll es um unsere eigene Community gehen: Wie verbessern wir unsere Vernetzung sowohl innerhalb der Informatik als auch nach außen mit Politik, Wirtschaft und Gesellschaft? Zum anderen soll es um die Technologien gehen: Die Informatik ermöglicht ganz neuartige Wege des Miteinanders. Vielartige soziale Netzwerke entstehen: die Möglichkeit zur Kommunikation ist allgegenwärtig, die Raumgrenzen sind aufgeweicht.

Kurze Mitteilungen

Algorithmische und experimentelle Methoden in Algebra, Geometrie und Zahlentheorie – DFG-Schwerpunktprogramm SPP1489 nimmt Arbeit auf

Wolfram Decker
Technische Universität Kaiserslautern

decker@mathematik.uni-kl.de

Im Rahmen des oben genannten Schwerpunktprogramms hat die Deutsche Forschungsgemeinschaft Mitte des Jahres die Bewilligungsschreiben für die Projekte der ersten Periode verschickt. Eine Webpräsentation für das Programm ist im Aufbau:

http://www.computeralgebra.de

Dort finden sich Kurzdarstellungen der geförderten Projekte. Erstellte Programmpakete und Datenbanken sollen ebenfalls über den Webserver zur Verfügung gestellt werden. Ein Diskussionsforum für relevante Themen wird gerade eingerichtet.

Im Rahmen seiner Aktivitäten wird der Schwerpunkt insbesondere ein umfangreiches Programm an Schulen, Workshops und Konferenzen organisieren. Dabei sind Gäste von außerhalb des Schwerpunkts herzlich willkommen. Das gilt insbesondere für die Schulen des Typs S^2AM, die von einem Kommittee junger Nachwuchsforscher für junge Nachwuchsforscher organisiert werden und ein hervorragendes Forum zum gegenseitigen Kennenlernen bieten Die erste Edition von S^2AM hat bereits stattgefunden, die eingeladenen Vortragenden waren Jan Christophersen, Gerhard Frey und Graham Ellis (siehe http://severian.mit.edu/s2am/index.html). Die **erste Jahrestagung** des Schwerpunkts wird vom 21. bis 25. Februar 2011 in Aachen stattfinden.

In einer der nächsten Ausgaben des Computeralgebrarundbriefs werden wir ausführlich über die Aktivitäten des Schwerpunkts berichten.

Berufungen

Prof. Dr. Gebhard Böckle (Universität Duisburg-Essen) hat den Ruf auf eine W3-Professur für Computational Arithmetic Geometry am Interdisziplinären Zentrum für wissenschaftliches Rechnen der Universität Heidelberg angenommen. (http://www.iwr.uni-heidelberg.de)

Prof. Dr. Florian Heß (Universität Magdeburg) hat einen Ruf auf eine W3-Professur an die Universität Oldenburg angenommen. (http://www.staff.uni-oldenburg.de/florian.hess)

Aufnahmeantrag für Mitgliedschaft in der Fachgruppe Computeralgebra

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

Titel/Name: _____ Vorname: _____

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 201___ die Aufnahme als Mitglied in die Fachgruppe

   Computeralgebra (CA) (bei der GI: 0.2.1).

2. Der Jahresbeitrag beträgt € 7,50 bzw. € 9,00. Ich ordne mich folgender Beitragsklasse zu:

   [ ] **€ 7,50** 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.

   [ ] **€ 7,50**. 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.

   [ ] **€ 9,00** 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, so wird c. angenommen).

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

Ort, Datum: _____ Unterschrift: _____

Bitte senden Sie dieses Formular an:

Sprecher der Fachgruppe Computeralgebra
Prof. Dr. Wolfram Koepf
Institut für Mathematik
Universität Kassel
Heinrich-Plett-Str. 40
34132 Kassel
0561-804-4207, -4646 (Fax)
koepf@mathematik.uni-kassel.de

Fachgruppenleitung Computeralgebra 2008-2011

Sprecher,
Vertreter der DMV:
Prof. Dr. Wolfram Koepf
Institut für Mathematik
Universität Kassel
Heinrich-Plett-Str. 40
34132 Kassel
0561-804-4207, -4646 (Fax)
koepf@mathematik.uni-kassel.de
http://www.mathematik.uni-kassel.de/~koepf

Fachreferent Internet:
Dr. Hans-Gert Gräbe, apl. Prof.
Institut für Informatik
Universität Leipzig
Postfach 10 09 20
04009 Leipzig
0341-97-32248
graebe@informatik.uni-leipzig.de
http://www.informatik.uni-leipzig.de/~graebe

Fachexperte Physik:
Dr. Thomas Hahn
Max-Planck-Institut für Physik
Föhringer Ring 6
80805 München
089-32354-300, -304 (Fax)
hahn@feynarts.de
http://wwwth.mppmu.mpg.de/members/hahn

Fachreferent Themen und Anwendungen:
Prof. Dr. Florian Heß
Carl-von Ossietzky Universität Oldenburg
Institut für Mathematik
26111 Oldenburg
0441-798-3238, -3004 (Fax)
florian.hess@uni-oldenburg.de
http://www.staff.uni-oldenburg.de/florian.hess

Fachreferent CA-Systeme und -Bibliotheken:
Prof. Dr. Gregor Kemper
Zentrum Mathematik – M11
Technische Universität München
Boltzmannstr. 3
85748 Garching
089-289-17454, -17457 (Fax)
kemper@ma.tum.de
http://www-m11.ma.tum.de/~kemper

Fachreferent CA an der Hochschule:
Prof. Dr. Gunter Malle
Fachbereich Mathematik
Technische Universität Kaiserslautern
Gottlieb-Daimler-Straße
67663 Kaiserslautern
0631-205-2264, -3989 (Fax)
malle@mathematik.uni-kl.de
http://www.mathematik.uni-kl.de/~malle

Fachreferent Schule:
StD Dr. Jörg Meyer
Schäfertrift 16
31789 Hameln
05151-54236
J.M.Meyer@t-online.de

Redakteur Rundbrief:
Prof. Dr. Markus Wessler
Fakultät für Betriebswirtschaft
Hochschule für angewandte Wissenschaften München
Am Stadtpark 20
81243 München
089-1265-2773, -2714 (Fax)
markus.wessler@hm.edu

Stellvertretende Sprecherin,
Fachreferentin Fachhochschulen:
Prof. Dr. Elkedagmar Heinrich
Fachbereich Informatik
Hochschule für Technik,
Wirtschaft und Gestaltung Konstanz
Brauneggerstr. 55
78462 Konstanz
07531-206-343, -559 (Fax)
heinrich@htwg-konstanz.de
http://www.in.fh-konstanz.de/inhalte/de/KONTAKT/persseiten_nbc/heinrich.html

Fachreferent Computational Engineering,
Vertreter der GAMM:
Prof. Dr. Klaus Hackl
Lehrstuhl für Allgemeine Mechanik
Ruhr-Universität Bochum
Universitätsstr. 150
44780 Bochum
0234-32-26025, -14154 (Fax)
klaus.hackl@rub.de
http://www.rub.de/lam

Fachreferent Lehre und Didaktik:
Prof. Dr. Hans-Wolfgang Henn
Fakultät für Mathematik
Technische Universität Dortmund
44221 Dortmund
0231-755-2939, -2948 (Fax)
henn@math.tu-dortmund.de
http://www.wolfgang-henn.de

Fachexperte Industrie:
Prof. Dr. Michael Hofmeister
Siemens AG
Corporate Technology
Modeling, Simulation, Optimization
Otto-Hahn-Ring 6
81739 München
089-636-49476, -42284 (Fax)
michael.hofmeister@siemens.com
http://www.siemens.com

Fachreferent Jahr der Mathematik:
Prof. Dr. Martin Kreuzer
Fakultät für Informatik und Mathematik
Universität Passau
Innstr. 33
94030 Passau
0851-509-3120, -3122 (Fax)
martin.kreuzer@uni-passau.de
http://www.fim.uni-passau.de/~kreuzer

Vertreter der GI:
Prof. Dr. Ernst W. Mayr
Lehrstuhl für Effiziente Algorithmen
Fakultät für Informatik
Technische Universität München
Boltzmannstraße 3
85748 Garching
089-289-17706, -17707 (Fax)
mayr@in.tum.de
http://www.in.tum.de/~mayr/

Fachreferentin Publikationen und Besprechungen:
Prof. Dr. Eva Zerz
Lehrstuhl D für Mathematik
RWTH Aachen
Templergraben 64
52062 Aachen
0241-80-94544, -92108 (Fax)
eva.zerz@math.rwth-aachen.de
http://www.math.rwth-aachen.de/~Eva.Zerz/

Werbeseite Texas Instruments

Werbeseite Maplesoft