Tagungsband

Computeralgebra

Universität Kassel

4. – 6. Mai 2017

veranstaltet von der

Fachgruppe Computeralgebra der GI

in Kooperation mit DMV und GAMM

Tagungsprogramm Computeralgebra, Universität Kassel, Heinrich-Plett-Str. 40, 34132 Kassel, 4. bis 6. Mai 2017

Uhrzeit	Donnerstag, 4. Mai 2017			Freitag, 5. Mai 2017			Samstag, 6. Mai 2017
09:15 - 10:15				**HV 2: Christian Eder** Aktuelle Softwareentwicklungen zum effizienten und parallelen Berechnen von Gröbnerbasen			**HV 4: Meinolf Geck** Computations with structures in Lie theory
10:20 - 10:50				Pause			**Verleihung des Nachwuchspreises**
10:55 - 11:25					**Sascha Kurz** Upper bounds for partial spreads	**Henning Schatz** Kettenbruchentwicklungen von Funktionen	
11:30 - 12:00					**Yue Ren** Berechnung von tropischen Varietäten mittels Schnitten mit affinen Hyperebenen	**Melanie Gerling** Effiziente Berechnung des bivariaten chromatischen Polynoms für spezielle Graphen	**11:00 - 12:00 Uhr** **HV 5: Alice Niemeyer** Randomisierte Algorithmen in der Gruppentheorie
12:00 - 12:15						**Gregor Kemper** Neuigkeiten aus der Fachgruppe	Abschluss
12:15 - 13:45	Registrierung			**Mittagspause**			
13:45	**Begrüßung**			**Tagungsfoto**			
14:00 - 15:00	**HV 1: Daniel Robertz** Eliminationsverfahren für nicht-lineare PDE-Systeme			**HV 3: Stephan Elsenhans** Berechnungen zur Geometrie und Arithmetik algebraischer Flächen			
15:15 - 15:45		**Martin Scheicher** Gröbner Bases over Finitely Generated Affine Monoids and Applications	**Vladimir Gerdt** Computer algebra aided generation of difference approximations to quasilinear evolution equations		**Christian Neurohr** Berechnung von Periodenmatrizen algebraischer Kurven	**Hendrikje Schmidtpott-Schulz** CA-gestützte Lehre in großen Studiengängen (STACK in der Linearen Algebra)	
16:00 - 16:30	Pause			Pause			
16:30 - 17:00		**Johannes Hoffmann** Links-Saturation und weitere Abschlüsse im Rahmen von Ore-Lokalisierungen	**Jan Horáček** Automation of Algebraic Fault Attacks		**Matthias Junge** Schnelle Arithmetik in der Picardgruppe algebraischer Kurven	**Daniel Tcheutia** Mixed recurrence relations and interlacing properties for zeros of q-classical orthogonal polynomials	
17:15 - 17:45		**Christian Gorzel** Einsatz von Computeralgebra zur Klassifikation der maximierenden Sextiken	**Mathias Orth** Konstruktive Theorie Inverser Systeme		**Andreas Steenpass** Neue Algorithmen zur Lösung der Prym-Green-Vermutung für Kurven von Geschlecht 24	**Viktor Levandovskyy** Factorization in non-commutative algebras: algorithms and applications	
18:00 - 18:30		**Hans-Dieter Janetzko** CATOAndroid: Ein Zwischenbericht über die Konversion von CATO, der allgemeinen Benutzeroberfläche für CAS, auf Android	**Marek Košta** New Concepts for Real Quantifyer Elimination mby Virtual Substitution	18:15 Uhr, Abfahrt Bus zum gemeinsamen Abendessen			
18:30 - 19:00			**Thomas Richard** Neue Features in Maple 2017				
19.00 Uhr				Gemeinsames Abendessen im Lokal in den Herkulesterrassen			
	R. 1409	**R. 2404**	**R. 1403**	**R. 1409**	**R. 2404**	**R. 1403**	**R. 1409**

Inhaltsverzeichnis

Daniel Robertz	Eliminationsverfahren für nicht-lineare PDE-Systeme	1
Martin Scheicher	Gröbner Bases over Finitely Generated Affine Monoids and Applications	2
Vladimir Gerdt	Computer algebra aided generation and analysis ofdifference approximations to quasilinear evolution equations	4
Johannes Hoffmann	Links-Saturation und weitere Abschlüsse im Rahmen von Ore-Lokalisierungen	5
Jan Horáček	Automation of Algebraic Fault Attacks	6
Christian Gorzel	Einsatz von Computeralgebra zur Klassifikation der maximierenden Sextiken	7
Matthias Orth	Konstruktive Theorie inverser Systeme	8
Hans-Dieter Janetzko	CATOAndroid: Ein Zwischenbericht über die Konversion von CATO, der allgemeinen Benutzeroberfläche für CAS, auf Android	9
Marek Košta	New Concepts for Real Quantifier Elimination by Virtual Substitution	10
Thomas Richard	Neue Features in Maple 2017	11
Christian Eder	Aktuelle Softwareentwicklungen zum effizienten und parallelen Berechnen von Gröbnerbasen	12
Sascha Kurz	Upper Bounds for Partial Spreads	13
Henning Schatz	Kettenbruchentwicklungen von Funktionen	14
Yue Ren	Die Berechnung von tropischen Varietäten mittels affiner Hyperebenenschnitte	15
Melanie Gerling	Effiziente Berechnung des bivariaten chromatischen Polynoms für spezielle Graphen	16
Stephan Elsenhans	Berechnungen zur Geometrie und Arithmetik algebraischer Flächen	18
Christian Neurohr	Berechnung von Periodenmatrizen algebraischer Kurven	19
Hendrikje Schmidtpott-Schulz	CAS-gestützte Lehre in großen Studiengängen (STACK in der Linearen Algebra)	20
Matthias Junge	Schnelle Arithmetik in der Picardgruppe algebraischer Kurven	21
Daniel Tcheutia	Mixed Recurrence Relations and Interlacing Properties for Zeros of q-classical Orthogonal Polynomials	22
Andreas Steenpass	Neue Algorithmen zur Lösung der Prym-Green-Vermutung für Kurven von Geschlecht 24	24
Viktor Levandovskyy	Factorization in Non-commutative Algebras: Algorithms and Applications	25
Meinolf Geck	Computations with Structures in Lie Theory	27
Alice Niemeyer	Randomisierte Algorithmen in der Gruppentheorie	28

Teilnehmerliste

Hinweise

Eliminationsverfahren für nicht-lineare PDE-Systeme

Daniel Robertz

Universität Plymouth, Großbritannien, daniel.robertz@plymouth.ac.uk

Analog zur Korrespondenz zwischen Radikalidealen eines Polynomrings und Varietäten in der algebraischen Geometrie gibt es eine Korrespondenz zwischen Radikaldifferentialidealen und den Mengen von analytischen Funktionen, die Lösungen der zugehörigen Systeme von polynomialen partiellen Differentialgleichungen (PDE) sind. In diesem Vortrag werden algorithmische Aspekte dieser Korrespondenz untersucht. Insbesondere wird eine Einführung in die Methode der differentiellen Thomas-Zerlegung gegeben. Dabei wird ein nicht-lineares PDE-System in endlich viele sogenannte einfache Systeme zerlegt, deren Lösungsmengen eine Partition der Lösungsmenge des gegebenen PDE-Systems bilden und deren Potenzreihenlösungen sich einfach bestimmen lassen. Umgekehrt lassen sich gewisse Mengen von analytischen Funktionen implizit durch Differentialgleichungen und -ungleichungen beschreiben. Es werden Verfahren zur Lösung der sich ergebenden Eliminationsprobleme vorgestellt. Eine Implementation der differentiellen Thomas-Zerlegung als Maple-Paket ist frei erhältlich.

Literatur

[1] T. Bächler and M. Lange-Hegermann. `AlgebraicThomas` and `DifferentialThomas`: Thomas decomposition of algebraic and differential systems. Available online at `http://wwwb.math.rwth-aachen.de/thomasdecomposition`.

[2] T. Bächler, V. P. Gerdt, M. Lange-Hegermann, and D. Robertz. Algorithmic Thomas Decomposition of Algebraic and Differential Systems. *Journal of Symbolic Computation* 47(10):1233–1266 (2012).

[3] D. Robertz. *Formal Algorithmic Elimination for PDEs.* Vol. 2121 of Lecture Notes in Mathematics, Springer, Cham, 2014.

[4] J. M. Thomas. *Differential Systems.* Vol. XXI of American Mathematical Society Colloquium Publications. American Mathematical Society, New York, N. Y., 1937.

Gröbner Bases over Finitely Generated Affine Monoids and Applications

Martin Scheicher

University Innsbruck, Austria, martin.scheicher@uibk.ac.at

Let N be a finitely generated submonoid of the integer lattice $\mathbb{Z}^{1\times n}$ and let F be a field. The monoid algebra of N over F is the subalgebra

$$F[N] = \bigoplus_{\mu\in N} F\sigma^{\mu} \subseteq F[\sigma,\sigma^{-1}] = F[\sigma_1,\ldots,\sigma_n,\sigma_1^{-1},\ldots,\sigma_n^{-1}]$$

of the Laurent polynomial algebra $F[\sigma,\sigma^{-1}]$.

Gröbner bases for ideals of the polynomial ring $F[\sigma]$ are defined with respect to a term order on $\mathbb{N}^{1\times n}$. However, if N is not pointed—e.g., if $N=\mathbb{Z}$—there exist no term orders on N since a total order can either be compatible with the addition or it can have zero as minimal element but it cannot have both properties. In [2], Pauer and Zampieri solved this problem by considering generalised term orders, i.e., total orders which retain the property that $0=\min N$ while they are still compatible with the addition in a limited way, and by defining Gröbner bases for ideals of $F[N]$ with respect to these generalised term orders. In [1], Pauer and Unterkircher extended this concept to $\{1,\ldots,l\}\times N$ and gave an algorithm for computing Gröbner bases for submodules of $F[N]^{1\times l}$. These Gröbner bases can be used, for instance, for determining submodule membership in $F[N]^{1\times l}$ and also for solving the Cauchy problem for systems of linear partial difference equations.

The algorithms of [2] and [1] work directly with elements of $F[N]$ and thus they necessitate a complete re-implementation of a generalisation of the Buchberger algorithm. Furthermore, the authors did not prove that generalised term orders exist for every submonoid N, which has restricted the applicability of this theory up to now.

We use a representation $N=\mathbb{N}^{1\times m}\theta$ with a matrix $\theta\in\mathbb{Z}^{m\times n}$ to parametrise the monoid algebra $F[N]$ by the polynomial ring $F[s]=F[s_1,\ldots,s_m]$ via the algebra epimorphism

$$F[s] \longrightarrow F[N], \quad s^{\widetilde{\mu}} \longmapsto \sigma^{\widetilde{\mu}\theta}.$$

We derive a Gröbner basis of a submodule of $F[N]^{1\times l}$ by computing a Gröbner basis over $F[s]$ with respect to a special, "compatible" term order on $\{1,\ldots,l\}\times\mathbb{N}^{1\times m}$. Using this, we also present a division algorithm and a method for computing syzygy modules. This approach enables us to use existing, optimised implementations of the Buchberger algorithm. Furthermore, we show how to construct generalised term orders on $\{1,\ldots,l\}\times N$ as well as compatible term orders on the parameter space $\{1,\ldots,l\}\times\mathbb{N}^{1\times m}$ for arbitrary finitely generated submonoids N.

References

[1] F. Pauer and A. Unterkircher. *Gröbner bases for ideals in Laurent polynomial rings and their application to systems of difference equations*. Appl. Algebra Engrg. Comm. Comput., 9(4):271–291, 1999.

[2] F. Pauer and S. Zampieri. *Gröbner bases with respect to generalized term orders and their application to the modelling problem*. J. Symb. Comput., 21(2):155–168, 1996.

Computer algebra aided generation and analysis of difference approximations to quasilinear evolution equations

Vladimir Gerdt, Yu. Blinkov, K. Marinov

Joint Institute for Nuclear Research, Dubna, Russia, gerdt@jinr.ru
Saratov State University, Saratov, Russia, blinkovua@info.sgu.ru
University Dubna, Dubna, Russia, marinov.kohctahtih@gmail.com

Let ∂_x be the derivation operator w.r.t. x and $\mathscr{R} := \mathbb{Q}(a_1,\ldots,a_i)\{u\}$ be the ordinary differential polynomial ring over the parametric field $\mathbb{Q}(a_1,\ldots,a_i)$ of real constants. We consider a class of quasilinear evolution equations of the form

$$u_t = au_m + F(u_{m-1},\ldots,u_1,u)\,, \quad 0 \neq a\,, \quad m \in \mathbb{N}_{>0}\,, \tag{1}$$

where $u_k := \partial_x^k u$ $(0 \leq k \leq m)$, $u_0 := u$ and $F \in \mathscr{R}$ is a differential polynomial of the order $m-1$ in ∂_x and such that there is a differential polynomial $P \in \mathscr{R}$ satisfying $F = \partial_x P$.

The class (1) contains most of classical nonlinear evolution equations, e.g., the Korteveg-de Vries (KdV) equation, KdV hierarchy, the Burgers equation and Burgers hierarchy, the Kuramoto-Sivashinsky equation, the Burgers-Huxley equation, etc., and their various generalizations. In [1], for an equation in the class (1) and for a regular Cartesian grid, we applied the algorithmic procedure of paper [2] to generation of finite difference schemes by combining the methods of finite volumes, numerical integration and difference elimination by means of Groebner bases (cf. [3]). In this way we constructed a new implicit scheme for the KdV equation.

In the present talk we compare, on the exact soliton solution, numerical behavior of this scheme with that of two schemes of the same order of approximation used in the literature and show that our scheme provides substantially better numerical accuracy.

References

[1] V. P. Gerdt, Yu. A. Blinkov and K. B. Marinov: Computer Algebra Based Discretization of Quaslinear Evolution Equations. Programming and Computer Software, to appear.

[2] V. P. Gerdt, Yu. A. Blinkov and V. V. Mozzhilkin: Gröbner Bases and Generation of Difference Schemes for Partial Differential Equations. Symmetry, Integrability and Geometry: Methods and Applications, 2:26, 2006. arXiv:math.RA/0605334

[3] V. P. Gerdt and D. Robertz: Computation of Difference Gröbner Bases. Computer Science Journal of Moldova, 20(2), (2012), 203–226. arXiv:cs.SC/1206.3463

Links-Saturation und weitere Abschlüsse im Rahmen von Ore-Lokalisierungen

Johannes Hoffmann, Viktor Levandovskyy

RWTH Aachen, Deutschland, Johannes.Hoffmann@math.rwth-aachen.de
RWTH Aachen, Deutschland, Viktor.Levandovskyy@math.rwth-aachen.de

Das Konzept der Ore-Lokalisierung ist eine gängige Verallgemeinerung der klassischen kommutativen Lokalisierung auf nicht-kommutative Bereiche, welche die meisten bekannten Eigenschaften erhält. Der Nachteil ist, dass man nicht wie im Kommutativen an jeder multiplikativ abgeschlossenen Menge lokalisieren kann, sondern nur an solchen, die zusätzlich die Ore-Bedingung erfüllen. Unter diesen sogenannten Ore-Mengen gibt es im Normalfall mehrere, die im wesentlichen die gleiche Lokalisierung darstellen, allerdings haben manche Vertreter mehr Struktur als andere. Wie findet man nun einen "schönen" Repräsentanten?

Um dieser Frage auf den Grund zu gehen, führen wir den Links-Saturationsabschluss

$$\mathrm{LSat}(S) := \{r \in R \mid \exists\, w \in R : wr \in S\}$$

für eine Ore-Menge S in einem (nicht-kommutativen) Bereich R ein. Es stellt sich heraus, dass die von S und $\mathrm{LSat}(S)$ induzierten Lokalisierungen in der Tat isomorph sind, aber $\mathrm{LSat}(S)$ die besseren strukturellen Eigenschaften hat und sogar eine vollständige Beschreibung der Einheiten in der Lokalisierung liefert. Damit haben wir ein mächtiges theoretisches Werkzeug, hinsichtlich der Berechenbarkeit bleiben aber noch einige offene Fragen.

Eine eng verwandte Version der Links-Saturation löst in der Theorie ein weiteres wichtiges Problem, welches besonders im Kontext von linearen Operatoren von Interesse ist: Für ein Ideal I und eine Ore-Menge S in R betrachtet man den S-Abschluss I^S von I, die Kontraktion des von I erzeugten Ideals in der Lokalisierung unter der natürlichen Einbettung. Nun gilt

$$I^S = \mathrm{LSat}_S(I) := \{r \in R \mid \exists\, s \in S : sr \in I\},$$

aber auch hier hält die praktische Umsetzung noch einige Probleme bereit: Zwar gibt es Algorithmen für wichtige Spezialfälle wie etwa die Desingularisierung einzelner Operatoren und den sogenannten Weyl-Abschluss für Systeme partieller Differentialgleichungen von endlichem holonomen Rang, aber im Allgemeinen ist die Frage nach der Berechenbarkeit dieses Abschlusses weit offen.

Automation of Algebraic Fault Attacks

Jan Horáček

Universität Passau, Germany, Jan.Horacek@uni-passau.de

Fault attacks is a type of active side-channel attacks against cryptographic implementations, when an attacker is able to induce faults during the computation. The analysis of the fault propagation and the knowledge of the faulty and the faulty-free outputs can lead to the exposition of the secret key.

Most of the fault attacks are conducted by the careful analysis of the particular cipher in order to derive the *fault equations*. With this additional information provided by the fault equations, one may be able to break many strong cryptosystems that are believed to be secure against standard attacks.

In general, this approach is not automatic at all and very technical. In this talk we present a general framework for round-based symmetric ciphers, i.e., almost all of the modern block ciphers. This concept can be easily generalized to other cryptographic primitives. The fault equations are derived automatically from the *algebraic description* of the cipher and then converted to the input for a solver (e.g., *the Border Basis Algorithm*, *the Gröbner Basis Algorithm*, or a *SAT solver*, etc.). We discuss the different means of forming such equations and we present possible ways how to solve them.

Einsatz von Computeralgebra zur Klassifikation der maximierenden Sextiken

Christian Gorzel

Universität Münster, Deutschland, gorzelc@uni-muenster.de

Eine ebene algebraische Kurve vom Grad sechs ist eine *maximierende* Sextik, falls nur einfache Singularitäten auftreten und die totale Milnorzahl den maximalen Wert 19 annimmt. Diese Kurven sind über algebraischen Zahlkörpern definiert und somit für Berechnungen mit Computeralgebra Systemen zugänglich. Yang und Shimada erstellen per Computer jeweils Listen der auftretenden Dynkin-Kombinationen. Hiermit ergibt sich, dass bis auf projektive Äquivalenz die maximierenden Sextiken durch 629 verschiedene Gleichungen beschrieben werden. Es wird über die bei der Klassifizierung zur Anwendung kommenden Programme berichtet.

Konstruktive Theorie inverser Systeme

Matthias Orth

Universität Kassel, Deutschland, uk000566@uni-kassel.de

Inverse Systeme sind Beschreibungen von Idealen in Polynomringen mittels linearer Funktionale. Sie gehen zurück auf MacAulay.

Zunächst wird dargelegt, auf welche Weise sich lineare Funktionale des Polynomrings $\mathscr{P}$ durch Potenzreihen kodieren lassen. Es wird die Struktur des Raums aller linearen Funktionale als $\mathscr{P}$-Modul beschrieben.

Für null-dimensionale Ideale besteht eine Dualität zwischen den Idealen und ihren inversen Systemen. In diesem Fall ist die Basis des Inversen Systems endlich; außerdem gibt es Rechenverfahren zur Bestimmung dieser Basis aus einer reduzierten Gröbnerbasis des Ideals und umgekehrt.

Eine kleinere Beschreibung des Inversen Systems erhält man durch die Angabe eines $\mathscr{P}$-Modul-Erzeugendensystems. Es wird dargelegt, dass die Berechnung eines solchen Erzeugendensystems im monomialen Fall mit der Bestimmung maximaler Ecken des Idealkomplementes äquivalent ist.

Die Pommaretbasis des monomialen Ideals besitzt eine kompakte Beschreibung, die sowohl die minimalen Erzeuger des Ideals als auch die maximalen Ecken seines Komplementes beinhaltet.

Für homogene nulldimensionale Ideale lässt sich das minimale Erzeugendensystem des inversen Systems ebenfalls aus der Pommaretbasis bestimmen, hierfür müssen zusätzlich lineare Gleichungssysteme gelöst werden.

Dieser Vortrag ist eine Zusammenfassung meiner Masterarbeit an der Universität Kassel, die von Prof. Dr. Werner M. Seiler betreut wurde.

Literatur

[HOP] HEISS, W.; OBERST, U.; PAUER, F. 2004: *On inverse systems and squarefree decomposition of zero-dimensional polynomial ideals*, Journal of Symbolic Computation 41, 261-284

[MMM] MARINARI, M. G.; MÖLLER, H. M.; MORA, T. 1993: *Gröbner bases of ideals defined by functionals with an application to ideals of projective points* – AAECC 4, 103-145

[S] SEILER, W. M. 2012: *Effective Genericity, δ-Regularity and Strong Noether Position*, Communications in Algebra, 40:10, 3933-3949

CATOAndroid: Ein Zwischenbericht über die Konversion von CATO, der allgemeinen Benutzeroberfläche für CAS, auf Android

Hans-Dieter Janetzko

FH Lübeck, Deutschland, janetzko@mathematikbuero.de

CATO ist eine in Java geschriebene deutschsprachige Oberfläche für Windows, Unix und MacOx, die eine fast intuitive Verwendung von verschiedenen CAS (GAP, Maple, math. Toolbox vom MATLAB, Mathematica, Maxima, MuPAD, Yacas) ermöglicht, Ref. [1].

Nun ist eigentlich Android ein Betriebsystem, auf dem in Java geschriebene Programme, Apps, einfach laufen sollen und können. Was liegt also näher, als das Programm CATO den Smartphones mit Android anzupassen.

In diesem Vortrag werden Schwierigkeiten dieser „einfachen Anpassung“ beschrieben, bestimmte einschneidende Modifikationen erläutert; denn die Erscheinungsbilder von CATO auf dem PC und von CATO auf dem Smartphone sollen sich kaum unterscheiden.

Es wird der aktuelle Stand des Projektes vorgeführt und die ausstehenden Punkte kritisch beleuchtet.

Literatur

[1] H.-D. Janetzko, *The GUI CATO – how natural usage of CAS with CATO modified the mathematical lectures and the interface itself*, http://math.unm.edu/∼aca/ACA/2016/Education/Janetzko.pdf (2016).

New Concepts for Real Quantifier Elimination by Virtual Substitution

Marek Košta

Slovak Academy of Sciences, Institute of Informatics, Bratislava, Slovakia, marek.kosta@savba.sk

In this talk I focus on my recent results regarding real quantifier elimination. I present a novel and practically applicable framework for real quantifier elimination based on virtual substitution of test points. That framework has no limitations on the possible degrees of quantified variables and corresponds to a generic algorithm parameterized by finite virtual substitution tables up to a chosen degree bound.

In the first part of the talk I give a geometric intuition involved in the derivation of virtual substitution tables: For a particular degree d, virtual substitution tables are obtained by analyzing a finite number of geometric positions of a generic d-degree polynomial relative to another generic polynomial of degree strictly smaller than d. Moreover, up to degree three I show how to optimize the obtained tables using the newly developed technique of clustering.

In the second part of the talk I show how the Boolean structure of the input formula can be exploited in several ways. This involves a special treatment of equations and negated equations occurring somewhere in the input formula as well as an ILP-supported analysis of relations on contained atomic formulas. These enhancements allow one to discard redundant test points, which consequently leads to shorter computing times as well as shorter quantifier-free equivalents.

This talk is based on parts of my dissertation [1].

References

[1] M. Košta. *New Concepts for Real Quantifier Elimination by Virtual Substitution*. Doctoral dissertation, Universität des Saarlandes, Germany, 2016.

Neue Features in Maple 2017

Thomas Richard

Maplesoft Europe GmbH, trichard@maplesoft.com

Wir stellen einige der Neuerungen von Maple 2017 vor, welches seit Anfang Mai 2017 verfügbar ist:

- Neues bei symbolischen Berechnungen (z.B. PDEs, Integration und Summation)
- Appell-Funktionen
- Updates bei der Bestimmung bivariater Grenzwerte
- Performance-Steigerung bei rationalen Funktionen, Polynomarithmetik und Gröbnerbasen
- Erweiterungen der Pakete für Graphentheorie, Gruppentheorie, Zahlentheorie
- Benutzeroberfläche: Verbesserungen bei Einheiten, Gleichungs-Editor, Maple-Cloud und Paketmanager
- Einfacher Zugriff auf geografische Daten
- Neue Plots für Statistik und Datenanalyse
- Erweiterungen im Debugger
- Connectivity: z.B. SMTLIB-Paket *(Satisfiability Modulo Theories)*
- Code-Generator: neue Zielsprache Swift

Aktuelle Softwareentwicklungen zum effizienten und parallelen Berechnen von Gröbnerbasen

Christian Eder

Universität Kaiserslautern, Deutschland, ederc@mathematik.uni-kl.de

Das Berechnen von Gröbnerbasen lässt sich zu großen Teilen auf lineare Algebra zurückführen: Der Reduktionsvorgang von Polynomen entspricht der Eliminierung von speziellen Matrizen (Macaulay Matrizen, Faugères F4 Algorithmus), ein Verfahren, das auf natürliche Weise parallelisiert werden kann. Weiterhin ergibt sich durch Informationen aus der Gröbnerbasis eine bestimmte Struktur der entsprechenden Matrizen, welche wiederum zur Optimierung der Elimination ausgenutzt werden kann. Wir präsentieren, basierend auf den oben genannten Ideen, zwei quelloffene und freie Softwarepakete zum effizienten und parallelen Berechnen von Gröbnerbasen. Hierbei werden wir eingehend die Möglichkeiten von Mehrkern-CPU-Systemen sowie die Herausforderungen der Skalierbarkeit von entsprechender Software diskutieren. Abschließend geben wir einen Ausblick auf gegenwärtige Implementierungsstudien im Bereich des verteilten sowie des heterogenen Rechnens (CPU/GPU). Teile des Vortrags beruhen auf einer Zusammenarbeit mit Jean-Charles Faugère.

Upper Bounds for Partial Spreads

Sascha Kurz

University of Bayreuth, Germany, sascha.kurz@uni-bayreuth.de

A partial t-spread in $GF(q)^n$ is a collection of t-dimensional subspaces with trivial intersection such that each non-zero vector is covered at most once. How many t-dimensional subspaces can be packed into $GF(q)^n$, i.e., what is the maximum cardinality of a partial t-spread? An upper bound, given by Drake and Freeman [1], survived almost forty years without any improvement. At the end of 2015, the upper bounds started to crumble [2]. Here, the theoretical foundation is provided by the fact that the uncovered points, called holes in this context, form a projective q^{t-1}-divisible linear block code. This allows to apply the linear programming method, i.e., to utilize the so-called MacWilliams identities and the positivity of the coefficients of the weight enumerator of the corresponding dual code. In this talk we will exhibit how this well known approach from coding theory can used to obtain analytical bounds on the maximum size of partial t-spreads that form the present state-of-the-art.

References

[1] D.A. Drake and J.W. Freeman, *Partial t-spreads and group constructible* (s,r,μ)*-nets*, J. Geom. **13**, 2, pp. 210–216 (1979).

[2] S. Kurz, *Packing vector spaces into vector spaces*, Australas. J. Combin. **68**, 1, pp. 122-130 (2017).

Kettenbruchentwicklungen von Funktionen

Henning Schatz

Universität Kassel, Deutschland, hschatz@mathematik.uni-kassel.de

Taylorpolynome sind ein übliches Werkzeug, um eine Funktion f mit einer gewünschten Genauigkeit zu approximieren. Eine Schwäche dieses Ansatzes ist, dass die dazugehörige Potenzreihe in der Regel nur einen endlichen Konvergenzradius besitzt. Häufig lässt sich der Konvergenzbereich ausweiten durch Padé-Approximation, d.h. Näherung mittels rationaler Funktionen statt Polynomen. Die Padé-Approximanten stehen in enger Beziehung zu den Konvergenten der Entwicklung von f in einen C-Kettenbruch (C-Fraction), so dass sich der Kettenbruch aus den Padé-Approximanten konstruieren lässt und umgekehrt.

An Hand von Beispielen werden die Approximation gemäß Taylor und Padé einander gegenübergestellt und es werden Algorithmen vorgestellt, um zu einer gegebenen Funktion ihre Entwicklung in einen C-Kettenbruch zu konstruieren.

Die Berechnung von tropischen Varietäten mittels affiner Hyperebenenschnitte

Tommy Hofmann, Yue Ren

Technische Universität Kaiserslautern, Deutschland, thofmann@mathematik.uni-kl.de
Max Planck Institut für Mathematik in den Naturwissenschaften, Leipzig, Deutschland, yue.ren.kl@gmail.com

Tropische Varietäten werden gemeinhin als kombinatorische Schatten algebraischer Varietäten bezeichnet, und in der Tat spiegeln sich viele geometrische Eigenschaften ihrer algebraischen Gegenstücke in ihrer Kombinatorik wieder. Dies verschafft der tropischen Geometrie Anwendungen von der enumerativen Geometrie bis hin zur Computeralgebra.

Thema dieses Vortrags sind neue Entwicklungen in der Berechnung von tropischen Varietäten. Die ersten und bis dato einzigen Algorithmen – veröffentlicht von Bogart, Jensen, Speyer, Sturmfels und Thomas vor genau 10 Jahren – konzentrieren sich hierbei ausschließlich auf die algebraische Beschreibung tropischer Varietäten, als Unterfächer des Gröbnerfächers. Sie berechnen an zentralen Stellen sogenannte *tropische Prävarietäten*, Schnitte von tropischen Hyperflächen, was sich für schwierigere Beispiele als unüberwindbares Hindernis herausstellt.

Wir zeigen, wie sich diese Berechnung umgehen lässt, indem wir die geometrische Beschreibung tropischer Varietäten hinzuziehen, als Bild algebraischer Varietäten unter komponentenweise Bewertung. Die hierfür nötigen Werkzeuge sind in der Computeralgebra bereits wohlbekannt und wesentlicher Bestandteil wichtiger Algorithmen: der Schnitt mit generischen Hyperebenen in der Primärzerlegung und die Dreieckszerlegung beim Lösen von nulldimensionalen Gleichungssystemen.

Effiziente Berechnung des bivariaten chromatischen Polynoms für spezielle Graphen

Melanie Gerling

Universität Kassel, Deutschland, melanie.gerling@mathematik.uni-kassel.de

Im Jahre 2003 führten Dohmen, Pönitz und Tittmann eine bivariate Verallgemeinerung $P(G;x,y)$ des seit 1912 bekannten chromatischen Polynoms $P(G;y)$ eines Graphen $G = (V,E)$ ein. Während das gewöhnliche chromatische Polynom ausschließlich Knotenfärbungen zählt, welche für adjazente Knoten stets verschiedene Farben vorsehen, erlaubt das bivariate chromatische Polynom zusätzliche Möglichkeiten. Sei $X = Y \cup Z$ mit $Y \cap Z = \emptyset$ die Menge aller verfügbaren Farben mit $|X| = x$ und $|Y| = y$. Eine Abbildung $\phi : V \to X$, so dass für alle Kanten $\{u,v\} \in E$ mit $\phi(u) \in Y$ und $\phi(v) \in Y$ die Beziehung $\phi(u) \neq \phi(v)$ gilt, bezeichnen wir als eine verallgemeinerte echte Knotenfärbung von G. Mit anderen Worten dürfen zwei adjazente Knoten nur dann in derselben Farbe gefärbt werden, wenn diese aus Z stammt.

Die Berechnung des chromatischen Polynoms eines Graphen ist bekanntlich ein NP-vollständiges Problem. Folglich gilt dies auch für die bivariate Verallgemeinerung des chromatischen Polynoms. Eine Rekursionsformel, welche von Averbouch, Godlin und Makowsky im Jahre 2008 eingeführt wurde, besitzt eine exponentielle Komplexität. Daher ist unser Ziel das Finden effizienter Algorithmen oder Formeln zur Berechnung des bivariaten chromatischen Polynoms für spezielle Graphentypen. Folgende Ergebnisse sollen vorgestellt werden.

Wir konstruieren einen Graphen durch das Löschen der Kanten von paarweise disjunkten Sternen aus einem vollständigen Graphen und stellen eine rekursionsfreie Möglichkeit vor, das bivariate chromatische Polynom eines solchen Graphen zu bestimmen.

Weiterhin werden wir uns vollständig partiten Graphen zuwenden und einerseits eine rekursionsfreie Formel für Graphen der Form $K_{3,\ldots,3}$ vorstellen und andererseits eine Rekursionsgleichung zur Berechnung des bivariaten chromatischen Polynoms des allgemeineren Graphentyps $K_{n_1,\ldots,n_t}$ mit $t \geq 1$ und $n_i \geq 1$ für alle $i \in \{1,\ldots,t\}$ einführen.

Abschließend werden wir vollständige Trenner in Graphen betrachten. Im univariaten Fall erlaubt ein vollständiger Trenner eine Vereinfachung der Berechnung des chromatischen Polynoms. Wir werden zeigen, dass sich dies im bivariaten Fall bereits als viel komplexer erweist.

Literatur

[1] I. Averbouch, B. Godlin and J. A. Makowsky, *A most general edge elimination polynomial*, in *Graph-Theoretic Concepts in Computer Science*, Lecture Notes in Comput. Sci. **5344**, pp.31-42 (2008). `http://link.springer.com/chapter/10.1007%2F978-3-540-92248-3_4`

[2] K. Dohmen, A. Pönitz and P. Tittmann, *A new two-variable generalization of the chromatic polynomial*, Discrete Math. Theor. Comput. Sci. **6**, pp. 69-90 (2003). http://www.emis.de/journals/DMTCS/volumes/abstracts/dm060106.abs.html

[3] M. Gerling, *Eigenschaften chromatischer Polynome*, Dissertation, Universität Kassel. https://kobra.bibliothek.uni-kassel.de/handle/urn:nbn:de:hebis:34-2015110249265

Berechnungen zur Geometrie und Arithmetik algebraischer Flächen

Andreas-Stephan Elsenhans

Universität Paderborn, Deutschland, elsenhan@math.uni-paderborn.de

Algebraische Flächen werden seit über 100 Jahre in der Mathematik studiert. Sie entstehen als Lösungsmenge polynomieller Gleichungen. Ist eine solche Fläche als Nullstellenmenge von Polynomen mit ganzen Koeffizienten gegeben, so kann man diese Nullstellenmenge als komplexe Mannigfaltigkeit verstehen, aber man kann diese Polynome auch modulo einer Primzahl reduzieren und dann die Lösungsmenge betrachten. Es zeigt sind, dass diese beiden Betrachtungsweisen aufs engste verwandt sind.

Im Vortrag möchte ich zeigen, wie dieses Wechselspiel algorithmisch genutzt werden kann. D.h., ich möchte Algorithmen, die über endlichen Körpern arbeiten, vorstellen, die Aussagen über komplexe algebraische Mannigfaltigkeiten liefern. Im weiteren werden diese Algorithmen dann zur Suche von algebraischen Flächen mit speziellen Eigenschaften eingesetzt.

Literatur

[1] A.-S. Elsenhans und J. Jahnel: On the computation of the Picard group for K3 surfaces, Math. Proc. Camb. Phil. Soc. 151 (2011) 263-270

[2] A.-S. Elsenhans and J. Jahnel: Examples of K3 surfaces with real multiplication, Proceedings of the ANTS XI conference (Gyeongju 2014), LMS Journal of Computation and Mathematics 17 (2014) 14-35

[3] A.-S. Elsenhans and J. Jahnel: Point counting on K3 surfaces and an application concerning real and complex multiplication, LMS Journal of Computation and Mathematics 19 (2016), suppl. A, 12-28.

Berechnung von Periodenmatrizen algebraischer Kurven

Christian Neurohr

Universität Oldenburg - Institut fur Mathematik, Deutschland, christian.neurohr@uol.de

Explizite Berechnungen auf der Jacobischen Varietat einer algebraischen Kurve sind in der algebraischen Geometrie & Zahlentheorie von Interesse. Im Komplexen hat die (analytische) Jacobische die Struktur eines komplexen Torus, welcher bis auf Isomorphie durch eine Periodenmatrix der zugehorigen Riemannschen Flache gegeben ist. Periodenmatrizen konnen berechnet werden durch numerische Integration der holomorphen Dierentiale entlang der Homologiegruppe. Fur zahlentheoretische Anwendungen sind hierbei hohe Prazision sowie beweisbare Fehlerabschatzungen unverzichtbar. Wir haben Algorithmen (in Magma) implementiert die, unter Verwendung der doppelexponentiellen Integration, Periodenmatrizen schnell, zuverlassig und zu hoher Prazision berechnen. Insbesondere fur superelliptischen Kurven haben wir in Zusammenarbeit mit Pascal Molin einen beweisbaren Algorithmus entwickelt und implementiert (in Magma und Arb) der diesen Anforderungen genugt und alle bisher existierenden Algorithmen schlagt. Wichtige Anwendungen sind die Berechnung der Abel-Jacobi Abbildung, des Endomorphismenrings der Jacobischen, sowie von Thetafunktionen.

CAS-gestützte Lehre in großen Studiengängen (STACK in der Linearen Algebra)

Hendrikje Schmidtpott-Schulz

Universität Kassel, Deutschland, hendrikje.schmidtpott@mathematik.uni-kassel.de

Ein klassisches Problem in Studiengängen mit vielen Studierenden ist es, die Lernfortschritte einzelner Studenten zu überprüfen und sie mit Feedback sinnvoll in Ihrem Studium zu unterstützen. Bislang geschieht dies durch die Abgabe von Hausaufgaben, die mit hohem personellem Aufwand korrigiert werden müssen. Durch den Einsatz von computergestützten Aufgaben kann eine schnellere Korrektur bei deutlich geringerem Aufwand erfolgen. Das Assesmentsystem STACK, das in moodle integriert werden kann, liefert hier ein Werkzeug, mit dem individuelle Aufgaben erstellt und ausgewertet werden können. Hierzu ist ein intelligentes Aufgabendesign erforderlich um sicherzustellen, dass alle Studenten Aufgaben vom gleichen Schwierigkeitsgrad erhalten, wenn einige Parameter der Aufgabe randomisiert werden. Stack selber liefert einige Möglichkeiten, Studentenantworten direkt mit Musterlösungen zu vergleichen. Durch Rückmeldebäume und die Verwendung des CAS-Systems MAXIMA können die Antworten nicht nur auf Übereinstimmung mit einer richtigen Lösung, sondern auch auf Folgerichtigkeit aus falschen Zwischenergebnissen überprüft werden. Selbst wenn ein Testverfahren nicht direkt zur Verfügung steht, können kurze MAXIMA - Programme auf die Antworten der Studenten angewandt werden, so dass diese sinnvoll interpretiert werden können. Momentan wird der Einsatz von STACK-Aufgaben in der Linearen Algebra an der Universität Kassel vorbereitet und in diesem Vortrag sollen Möglichkeiten und Herausforderungen mit Schwerpunkt auf Gleichungssystemen und Matrizen demonstriert werden.

Schnelle Arithmetik in der Picardgruppe algebraischer Kurven

Matthias Junge

Universität Oldenburg, Deutschland, matthias.junge@uni-oldenburg.de

Wir präsentieren den asymptotisch schnellsten Algorithmus zum Rechnen in der Picardgruppe algebraischer Kurven, welche nicht notwendigerweise glatt sein müssen. Die Picardgruppe umfasst geometrische Objekte (Isomorphieklassen von Vektorbündeln vom Rang 1) und ist im Falle einer elliptischen Kurve äquivalent zu ihrer Punktgruppe. Allerdings lässt sich die Picardgruppe auch bei höherem arithmetischen Geschlecht betrachten. Wir sind dazu in der Lage, ihre Objekte als Ideale darzustellen, welche wiederum freie Moduln über einem Polynomring sind. Somit versetzen wir uns in die Position, diese durch ihre Basen (also Matrizen!) darzustellen und effiziente Arithmetik zu betreiben: Wir reduzieren das ursprünglich geometrische Problem auf die lineare Algebra über Polynomringe, sodass wir mit ihren Werkzeugen einen Algorithmus formulieren können, der die Arithmetik in der Picardgruppe umsetzt. Unser Algorithmus vereinigt die bisher schnellsten Laufzeiten für glatte Kurven konstanter Gonalität (Heß) und glatter Kurven mit Gonalität in der Größenordnung des Geschlechts (Khuri-Makdisi) und verallgemeinert diese darüber hinaus auf beliebige Kurven. Wir können diesem Problem die einheitliche Komplexität $O^{\sim}(n^{\omega-1}g)$ zuweisen, wobei g das arithmetische Geschlecht und n die Gonalität der Kurve bezeichnet.

Mixed Recurrence Relations and Interlacing Properties for Zeros of q-classical Orthogonal Polynomials

Daniel Tcheutia, Alta Jooste, Wolfram Koepf

University of Kassel, Germany, duvtcheutia@yahoo.fr
University of Pretoria, South Africa, alta.jooste@up.ac.za
University of Kassel, Germany, koepf@mathematik.uni-kassel.de

Using the q-version of Zeilberger's algorithm, we provide a procedure to find mixed recurrence relations satisfied by classical q-orthogonal polynomials with shifted parameters. As application of our recurrence equations, we investigate interlacing properties of zeros of classical q-orthogonal polynomials.

References

[1] R. Askey, *Graphs as an aid to understanding special functions*, Asymptotic and Computational Analysis, Winnipeg 1989, Lecture Notes in Pure and Applied Mathematics 124 (1990), 3–33.

[2] C. Brezinski, K.A. Driver, M. Redivo-Zaglia, *Quasi-orthogonality with applications to some families of classical orthogonal polynomials*, Appl. Numer. Math. 48 (2004), 157–168.

[3] L. Chihara, D. Stanton, *Zeros of generalized Krawtchouk polynomials*, J. Approx. Theory 60 (1990), 43–57.

[4] V.G. Drinfeld, *Quantum groups*, Proceedings of the International Congress of Math., Berkeley, 1986, Amer. Math. Sot. (1987), 798–820.

[5] K. Driver, K. Jordaan, N. Mbuyi, *Interlacing of the zeros of Jacobi polynomials with different parameters*, Numer. Algorithms 49 (2008), 143–152.

[6] G. Gasper, M. Rahman, *Basic Hypergeometric Series*, Cambridge University Press, Cambridge, 1990.

[7] P. Gochhayat, K. Jordaan, K. Raghavendar, A. Swaminathan, *Interlacing properties and bounds for zeros of ${}_2\phi_1$ hypergeometric and little q-Jacobi polynomials*, Ramanujan J. 40 (2016), 45–62.

[8] W. Hahn, *Über Orthogonalpolynome, die q-Differenzengleichungen genügen*, Math. Nachr. 2 (1949), 4–34.

[9] E. Heine, *Untersuchungen über die Reihe* $1+\frac{(1-q^{\alpha})(1-q^{\beta})}{(1-q)(1-q^{\gamma})}x+\frac{(1-q^{\alpha})(1-q^{\alpha+1})(1-q^{\beta})(1-q^{\beta+1})}{(1-q)(1-q^{2})(1-q^{\gamma})(1-q^{\gamma+1})}x^2+\cdots$, Journal für die reine und angewandte Mathematik 34 (1847), 285–328.

[10] M.E.H. Ismail, *Classical and Quantum Orthogonal Polynomials in One Variable*, Encyclopedia of Mathematics and Its Applications, vol. 98. Cambridge University Press, Cambridge, 2005.

[11] K. Jordaan, F. Toókos, *Interlacing theorems for the zeros of some orthogonal polynomials from different sequences*, Appl. Numer. Math. 59 (2009), 2015–2022.

[12] K. Jordaan, F. Toókos, *Mixed recurrence relations and interlacing of the zeros of some q-orthogonal polynomials from different sequences*, Acta. Math. Hungar. 128 (2010), 150–164.

[13] H. Joulak, *A contribution to quasi-orthogonal polynomials and associated polynomials*, Appl. Numer. Math. 54(1) (2005), 65–78.

[14] S. Karlin, J.L. McGregor, *The differential equations of birth-and-death processes and the Stieltjes Moment problem*, Trans. Amer. Math. Soc. 85 (1957), 489–546.

[15] R. Koekoek, P.A. Lesky, R.F. Swarttouw, *Hypergeometric Orthogonal Polynomials and Their q-Analogues*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2010.

[16] H.T. Koelink, T.H. Koornwinder, *The Clebsch-Gordan coefficients for the quantum group $S_\mu U(2)$ and q-Hahn polynomials*, Proceedings A 92 (1989), 443–456.

[17] W. Koepf, *Hypergeometric Summation–An algorithmic approach to summation and special function identities*, Second Ed., Springer, 2014.

[18] T.H. Koornwinder, *Orthogonal polynomials in connection with quantum groups*, in: P. Nevai (Ed.), Orthogonal Polynomials, Theory and Practice, Vol. 294, Kluwer Academic Publishers, Dordrecht, 1990, 257–292.

[19] T.H. Koornwinder, *Compact quantum groups and q-special functions*, in: V. Baldoni, M.A. Picardello (Eds.), Representations of Lie Groups and Quantum Groups, Pitman Research Notes in Mathematics series, Vol. 311, Longman Scientific & Technical, New York, 1994, 46–128.

[20] R.J. Levit, *The zeros of the Hahn polynomials*, SIAM Review 9 (1967), 191–203.

[21] D.S. Moak, *The q-Analogue of the Laguerre Polynomials*, J. Math. Anal. Appl. 81 (1981), 20–47.

[22] E.D. Rainville, *Special Functions*, The Macmillan Company, New York, 1960.

[23] R.F. Swarttouw, *The contiguous function relations for the basic hypergeometric series*, J. Math. Anal. Appl. 149 (1990), 151–159.

[24] G. Szegő, *Orthogonal polynomials*, American Mathematical Society, New York, 1959.

[25] R. Vidunas, T. Koornwinder, *Algorithmic methods for special functions by computer algebra*, Webpage of the NWO project, http://www.science.uva.nl/ t̃hk/specfun/compalg.html, 2000.

[26] S.L. Woronowicz, *Compact matrix pseudogroups*, Comm. Math. Phys. 111 (1987), 613–665.

Neue Algorithmen zur Lösung der Prym-Green-Vermutung für Kurven von Geschlecht 24

Andreas Steenpass

TU Kaiserslautern, Deutschland, steenpass@mathematik.uni-kl.de

Nach der Prym-Green-Vermutung besitzen Prym-kanonische nodale Kurven (PCNC) von geradem Geschlecht eine reine Auflösung. Wir konzentrieren uns auf eine Möglichkeit zum algorithmischen Nachweis dieser Aussage. Hierzu berechnen wir zunächst mit Hilfe des Algorithmus von Schreyer eine nicht-minimale Auflösung einer PCNC von entsprechendem Geschlecht g. Die Prym-Green-Vermutung trifft zu, falls eine in der Mitte dieser Auflösung auftretende quadratische Teilmatrix mit konstanten Einträgen vollen Rang hat. Dieses Verfahren lässt sich für $g \leq 20$ mit akzeptablem Aufwand durchführen, wobei sich die Vermutung nur für $g = 8$ und $g = 16$ als falsch erweist. Um die Reihe der Ausnahmen fortzusetzen, ist der Fall $g = 24$ von besonderem Interesse. Wesentliche Verbesserungen und eine neue Implementierung des Schreyer-Algorithmus haben diesen Fall nun in den Bereich des Machbaren gerückt, wobei die quadratische Matrix, deren Rang hierfür zu bestimmen ist, die Dimension 3.250.026 besitzt. Bei diesem Projekt, einer Zusammenarbeit mit Christian Eder, stehen mathematische Erkenntnisse und programmiertechnische Tricks in einer engen Wechselbeziehung. Es zeigt sich, dass das Hauptproblem bei der Lösung des Falls $g = 24$ nicht so sehr die Laufzeit der verwendeten Algorithmen, sondern vielmehr der von den Datenstrukturen in den Zwischenschritten benötigte Speicherplatz ist.

Factorization in Non-commutative Algebras: Algorithms and Applications

Viktor Levandovskyy

Lehrstuhl D für Mathematik, RWTH Aachen University, Aachen, Germany,
levandov@math.rwth-aachen.de

I will talk on the research direction, pursued together with A. Heinle, M. Giesbrecht and J. Bell (Univ. Waterloo, Canada), which resulted in a series of recent papers.

As in the classical commutative case, we are interested in factorizing polynomials over non-commutative rings. Let us start with a field K and a finitely presented associative K-algebra A, which is a domain, i. e. A has no nontrivial zero-divisors.

It turns out, that there are at least two distinct notions of a factorization of polynomials over A. One of them originates from the ring theory [Jacobson(1943), Cohn(2006)] and uses a weak notion of association relation (called left or right similarity), what is at the same time hard to approach algorithmically. On the contrary, in applications we'd like to use the classical association relation, i.e. when two elements differ by a factor, which is nonzero central unit.

The results from [Bell-Heinle-L.(2017)] give long-seeked conditions for a given algebra A to be a *finite factorization domain*, i. e. a domain, where every nonunit has at most finite number of factorizations. Over such domains a factorization procedure thus becomes into an algorithm. Examples, bounds and counterexamples will be given. Over the well-known class of ubiquitous G-algebras (or PBW algebras), we provide a factorization algorithm [Heinle-L.(2016)], its' smarter graded-driven version for graded algebras [Giesbrecht-Heinle-L.(2016), Heinle-L.(2017)] and a factorizing Gröbner algorithm [Heinle-L.(2016)]. All of these are implemented in SINGULAR:PLURAL [Greuel et al.(2016)]. We view a factorizing Gröbner algorithm (cf. [Czapor(1989), Gräbe(1995)] in the commutative case) as the only general possibility to obtain a weaker analogon to the primary decomposition from the commutative algebra. Applications of the mentioned algorithms will be presented as well.

References

[Bell-Heinle-L.(2017)] Bell, J. P., Heinle, A., and Levandovskyy, V. (2017). On noncommutative finite factorization domains. *Transactions of the American Mathematical Society*, 369:2675–2695.

[Cohn(2006)] Cohn, P. M. (2006). *Free ideal rings and localization in general rings*, volume 3. Cambridge University Press.

[Czapor(1989)] Czapor, S. R. (1989). Solving algebraic equations: combining Buchberger's algorithm with multivariate factorization. *Journal of Symbolic Computation*, 7(1):49–53.

[Giesbrecht-Heinle-L.(2016)] Giesbrecht, M., Heinle, A., and Levandovskyy, V. (2016). Factoring linear differential operators in n variables. *Journal of Symbolic Computation*, 75:127–148.

[Gräbe(1995)] Gräbe, H.-G. (1995). *Triangular systems and factorized Gröbner bases*. In *Proc. of 11th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, Springer.

[Greuel et al.(2016)] Greuel, G.-M., Levandovskyy, V., Motsak, A., and Schönemann, H. (2016). PLURAL. A SINGULAR 4-1 Subsystem for Computations with Non-commutative Polynomial Algebras. Centre for Computer Algebra, TU Kaiserslautern. `www.singular.uni-kl.de`

[Heinle-L.(2016)] Heinle, A. and Levandovskyy, V. A Factorization Algorithm for G-Algebras and Applications. In *Proc. of the International Symposium on Symbolic and Algebraic Computation (ISSAC'16), Waterloo, Canada*, pages 263–270, ACM Press, 2016.

[Heinle-L.(2017)] Heinle, A. and Levandovskyy, V. Factorization of Z-homogeneous Polynomials in the First (q-)Weyl Algebra, 22 pages, 2017, to appear. `http://arxiv.org/abs/1302.5674`

[Jacobson(1943)] Jacobson, N. (1943). *The Theory of Rings*. American Mathematical Society.

Computations with Structures in Lie Theory

Meinolf Geck

Universität Stuttgart, Germany, meinolf.geck@mathematik.uni-stuttgart.de

Lie algebras and Lie groups, and various algebraic structures related to them, admit combinatorial skeletons which make it possible to perform calculations in a highly efficient way. We present a number of examples and applications.

References

[1] M. Geck, G. Hiss, F. Lübeck, G. Malle, J. Michel and G. Pfeiffer, *CHEVIE—A computer algebra system for computing and processing generic character tables for finite groups of Lie type and Hecke algebras*; homepage at `http://www.math.rwth-aachen.de/~CHEVIE`.

[2] M. Geck, *Some applications of CHEVIE to the theory of algebraic groups*, Carpath. J. Math., **27** (2011), 64–94.

[3] J. Michel, *The development version of the CHEVIE package of GAP3*, J. Algebra **435** (2015), 308–336.

[4] M. Geck and A. Halls, *On the Kazhdan-Lusztig cells in type E_8*, Math. Comp. **84** (2015), 3029–3049.

Randomisierte Algorithmen in der Gruppentheorie

Alice Niemeyer

RWTH Aachen, Deutschland, alice.niemeyer@mathb.rwth-aachen.de

Gruppen beschreiben Symmetrien von Objekten und spielen daher eine wichtige Rolle in vielen Gebieten der Mathematik und der Naturwissenschaften. In vielen Situationen werden Gruppen durch eine kleine Menge von Elementen beschrieben, zum Beispiel kann eine Matrixgruppe durch wenige Matrizen erzeugt werden. Eine solche Beschreibung einer Gruppe eignet sich besonders gut, um mit der Gruppe auf einem Computer zu rechnen. In der Tat ermöglichen moderne Computeralgebrasysteme es, viele wichtige Fragen über konkrete Gruppen mit Hilfe eines Computers zu beantworten. Allerdings können selbst endliche Gruppen sehr viele verschiedene Elemente haben. So hat zum Beispiel die Gruppe aller Permutationen einer Menge der Mächtigkeit 100 schon mehr als 10^{157} Elemente, während die Gruppe der invertierbaren binären $20x20$ Matrizen mehr als 10^{119} Elemente hat. Daher ist es nicht sehr verwunderlich, dass moderne Algorithmen in der Gruppentheorie randomisiert sind. Solche Algorithmen ziehen Schlussfolgerungen aus der Betrachtung weniger zufällig gewählter Elemente. Können wir uns aber auf eine Antwort eines randomisierten Algorithmus verlassen?

Teilnehmerverzeichnis

Nr.:	*Name:*	*Vorname:*	*Anschrift:*	*E-Mail:*
1	Abbott	John	Universität Kassel, Institut für Mathematik	John.Abbott@mathematik.uni-kassel.de
2	Binaei	Hoda	Universität Kassel, Institut für Mathematik	hoda.binaei@mathematik.uni-kassel.de
3	Cuntz	Michael	Leibniz-Universität-Hannover	cuntz@math.uni-hannover.de
4	Eder	Christian	Universität Kaiserslautern	ederc@mathematik.uni-kl.de
5	Elsenhans	Stephan	Universität Paderborn	elsenhan@math.uni-paderborn.de
6	Fetzer	Matthias	Universität Kassel, Institut für Mathematik	Fetzer@mathematik.uni-kassel.de
7	Fouda	Armand	Universität Kassel, Institut für Mathematik	efoudajsa@yahoo.fr
8	Gansel	Kai	Additive GmbH, Friedrichsdorf	kai.gansel@additive-net.de
9	Geck	Meinolf	Universität Stuttgart, FB Mathematik	meinolf.geck@mathematik.uni-stuttgart.de
10	Gellien	Wolfgang	34119 Kassel, Breitscheidstraße 54	w.gellien@freenet.de
11	Gerdt	Vladimir	Joint Institute for Nuclear Research, Russia	Gerdt@jinr.ru
12	Gerling	Melanie	Universität Kassel, Institut für Mathematik	melanie.gerling@mathematik.uni-kassel.de
13	Gorzel	Christian	Universität Münster	gorzelc@uni-muenster.de
14	Hahn	Thomas	MPI für Physik, München	hahn@feynarts.de
15	Heß	Florian	Universität Oldenburg	florian.hess@uni-oldenburg.de
16	Himstedt	Frank	TU München, Garching	himstedt@ma.tum.de
17	Hoffmann	Johannes	RWTH Aachen, Lehrstuhl D für Mathematik	johannes.hoffmann@math.rwth-aachen.de
18	Horacek	Jan	94032 Passau, Auenweg 1	jenda.horacek@gmail.com
19	Janetzko	Hans-Dieter	23568 Lübeck, Bardowieker Weg 89	janetzko@mathematikbuero.de
20	Junge	Matthias	26121 Oldenburg, Alexanderstraße 95	matthias.junge@uol.de
21	Kemper	Gregor	TU München, Garching	Kemper@ma.tum.de
22	Klüners	Jürgen	Universität Paderborn	klueners@math.upb.de
23	Koepf	Wolfram	Universität Kassel, Institut für Mathematik	Koepf@mathematik.uni-kassel.de
24	Kosta	Marek	Slowakische Akademie der Wissenschaften	marek.kosta@savba.sk
25	Kreuzer	Martin	Universität Passau	martin.kreuzer@uni-passau.de
26	Kurz	Sascha	Universität Bayreuth	sascha.kurz@uni-bayreuth.de
27	Levandovskyy	Viktor	RWTH Aachen, Lehrstuhl D für Mathematik	levandov@math.rwth-aachen.de
28	Long	Ngoc Le	Universität Passau	Ngoc-Long.Le@uni-passau.de
29	Messeng Ekossono	Ange-Salomé	Universität Passau	Ange-Salome.MessengEkossono@uni-passau.de
30	Müller	Raphael	Universität Paderborn	raphael.mueller@math.upb.de
31	Müller	Steffen	Universität Oldenburg, Institut für Mathematik	jansteffenmueller@gmail.com
32	Neurohr	Christian	Universität Oldenburg	christian.neurohr@uni-oldenburg.de
33	Niemeyer	Alice	RWTH Aachen, Lehrstuhl D für Mathematik	alice.niemeyer@mathb.rwth-aachen.de
34	Orth	Matthias	34560 Fritzlar, Alte Kasseler Str. 33	j.matthias.orth@gmx.de
35	Pourkhajouei	Samira	Universität Passau	s.pourkhajooei@math.iut.ac.ir
36	Reimers	Fabian	TUM-Zentrum Mathematik - M 11	Reimers@Ma.Tum.de
37	Ren	Yue	Kaiserslautern, Peter-Bardens-Str. 5a	yue.ren.kl@gmail.com
38	Richard	Thomas	Maplesoft Europe GmbH, Aachen	Trichard@maplesoft.com
39	Robertz	Daniel	University of Plymouth, Great Britain	daniel.robertz@plymouth.ac.uk
40	Rück	Hans-Georg	Universität Kassel, Institut für Mathematik	rueck@mathematik.uni-kassel.de
41	Schatz	Henning	Universität Kassel, Institut für Mathematik	hschatz@mathematik.uni-kassel.de
42	Scheicher	Martin	Universität Innsbruck, Österreich	martin.scheicher@uibk.ac.at
43	Schmidtpott-Schulz	Hendrikje	Universität Kassel, Institut für Mathematik	hendrikje.schmidtpott@mathematik.uni-kassel.de
44	Seiß	Matthias	Universität Kassel, Institut für Mathematik	Matthias.Seiss@mathematik.uni-kassel.de
45	Steenpass	Andreas	TU Kaiserslautern	steenpass@mathematik.uni-kl.de
46	Sturm	Thomas	CNRS France	sturm@mpi-inf.mpg.de
47	Tcheutia	Daniel Duviol	Universität Kassel, Institut für Mathematik	tcheutia@mathematik.uni-kassel.de
48	Wehmeier	Stefan	The MathWorks GmbH, Paderborn	Stefan.Wehmeier@mathworks.de
49	Zerz	Eva	RWTH Aachen, Lehrstuhl D für Mathematik	eva.zerz@math.rwth-aachen.de

Hinweise:

- Für alle Teilnehmer wurde ein Gast-Account eingerichtet
  login: guest
  password: cat2017

- Dieses Passwort kann nicht geändert werden. Die Home-Quota beträgt 50 MB und 500 Dateien. Alle Rechner haben eine Internetanbindung, so dass Mail auch remote über ssh bzw. Webmail möglich ist. Terminals befinden sich im Raum 2421/2422 (Nutzung Donnerstag und Freitag ab 15:00 Uhr).

- In den Räumen des Instituts ist das eduroam-WLAN verfügbar. Die Zugangsdaten für einen Gastzugang werden zu Beginn der Veranstaltung bekannt gegeben.

- Am Freitag, dem 05. Mai 2017, findet um 19:00 Uhr ein gemeinsames Abendessen im Lokal *Herkules Terrassen* statt. Bitte wählen Sie aus der Speisekarte auf der nächsten Seite ein Gericht aus und tragen Sie Ihren Wunsch bis Donnerstag, 18:30 Uhr, in die ausgelegte Liste am Tagungungsdesk ein.

  Um 18:15 Uhr fahren wir zusammen mit einem Bus zum Lokal. Nach dem Essen fährt dieser wieder zu den Hotels zurück.

  Herkules Terrassen, Schlosspark 26, 34131 Kassel (Tel.: 0561 / 93 73 19-10).