Tagungsband

Computeralgebra

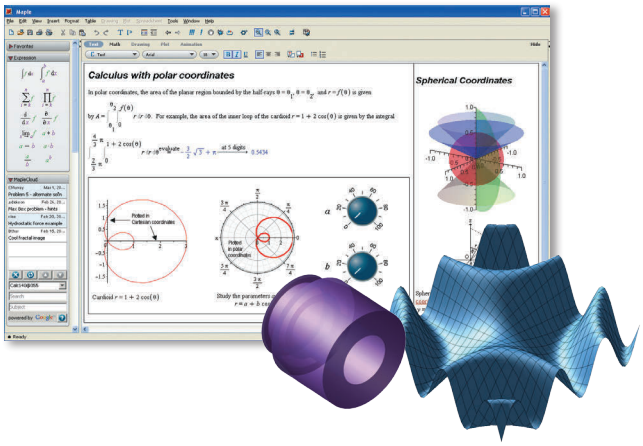
Universität Kassel

10. – 12. Mai 2012

veranstaltet von der

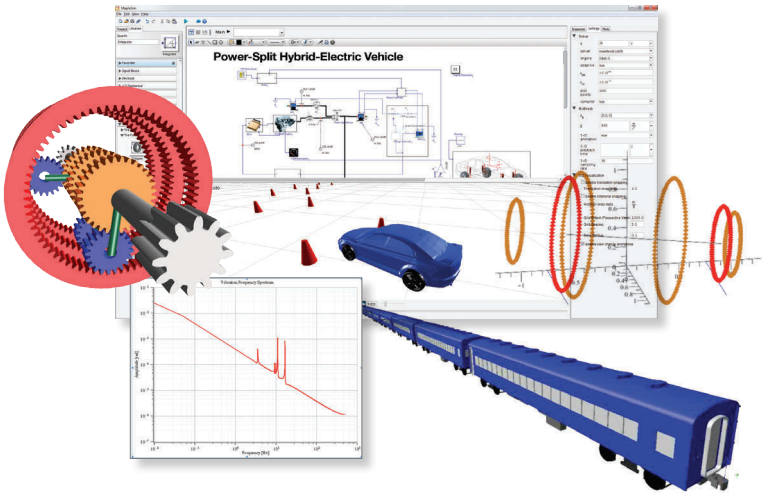
Fachgruppe Computeralgebra der DMV, GI und GAMM

Maplesoft – ComputerAlgebra-Tagung Kassel



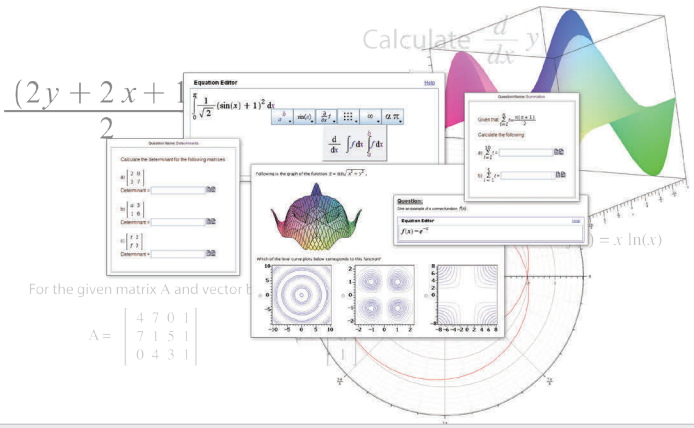
Maple™ 16

Die Mathematik spielt in unserer modernen Welt eine entscheidende Rolle. Daher vertrauen Mathematiker, Wissenschaftler und Ingenieure überall auf die Software von Maplesoft. Maple hilft Ihnen dabei, mathematische Probleme schnell, einfach und genau zu analysieren, zu erkunden, zu visualisieren und zu lösen. Mit über 5000 Funktionen, die praktisch alle Bereiche der Mathematik abdecken, bietet Maple die Tiefe, die Breite und die Leistung, um alle Herausforderungen in der Mathematik zu bewältigen. Besuchen Sie unseren Stand, und wir zeigen Ihnen gern, warum Maple für Wissenschaftler, Lehrer und Lernende in jeder mathematischen oder technischen Disziplin ein essentielles Werkzeug ist.



MapleSim™ 5

MapleSim ist ein professionelles Werkzeug zur physikalischen Modellierung und Simulation, das bei technischen Forschungseinrichtungen und Ausbildungsstätten auf der ganzen Welt eingesetzt wird. MapleSim baut auf der legendären Maple-Engine für symbolische Berechnungen auf, die Forschung und Lehre in der Mathematik revolutioniert hat. Die Software enthält einzigartige Technologie, die tiefere Einblicke in das Systemverhalten ermöglicht, Ihre Forschung beschleunigt und Ihre Lehrtätigkeit bereichert. Für Forscher reduziert MapleSim die Zeit zur Entwicklung von Modellen von Monaten auf wenige Tage. Die so erstellten Hochleistungsmodelle sind von höchster Genauigkeit. Für Lehrer und Ausbilder ist MapleSim ein praktisches Werkzeug, um schnell und verständlich den Zusammenhang zwischen Theorie und physikalischem Verhalten aufzuzeigen, und Ihre Studierenden können sich auf Entwicklungskonzepte konzentrieren, statt sich mit langwierigen mathematischen Ableitungen aufzuhalten.



MapleT.A.™ 8

Maple T.A. ist ein benutzerfreundliches web-basiertes System zur Erstellung von Tests und Aufgaben zur automatischen Prüfung von Studentenantworten und zur Leistungsbeurteilung. Es unterstützt komplexe Freiformeingabe von mathematischen Gleichungen und eine intelligente Auswertung von Antworten, was es zu einem idealen Werkzeug macht für Wissenschaft, Technologie, Ingenieurwesen, Mathematik oder für beliebige Kurse, die Mathematik-Kenntnisse erfordern.

Besuchen Sie den Stand von Maplesoft und fragen Sie nach einer individuellen Vorführung von MapleSim und dem neuen Maple 16. Dort erfahren Sie auch mehr über die kostenlosen Demoversionen.

Maplesoft
Mathematics • Modeling • Simulation

www.maplesoft.com | germany@maplesoft.com

Tagungsprogramm Computeralgebra, Universität Kassel, Heinrich-Plett-Str. 40, 34132 Kassel, 10. bis 12. Mai 2012

Uhrzeit	Donnerstag, 10. Mai 2012			Freitag, 11. Mai 2012			Samstag, 12. Mai 2012
09:15 - 09:45					**Andreas Paffenholz** Examples of Kähler-Einstein Manifolds with polymake	**Felix Noeske** Computergestützte lokale Darstellungstheorie	09:15 - 10:15 **HV 4: Gabor Wiese** Modulare Galois-Darstellungen und Computeralgebra
09:45 - 10:20					Pause	Pause	
10:20 - 10:50					**Benjamin Lorenz** Computing generators of toric ideals	**Konstantin Ziegler** Compositions and Collisions at degree p^2	**Verleihung des Nachwuchspreises**
11:00 - 12:00				**HV 2: Michael Cuntz** Klassifikation der kristallographischen Arrangements			**HV 5: Andreas Klein** RSA Protokollfehler, LLL und Gröbnerbasen
12:15 - 13:45	Registrierung			Mittagspause			Abschluss
13:45	Begrüßung			Tagungsfoto			
14:00 - 15:00	**HV 1: Daniel Andres** Algorithmische Aspekte der D-Modultheorie			**HV 3: Anne Frühbis-Krüger** Singularitäten und Computeralgebra			
15:15 - 15:45		**Simon King** Completeness Criteria for Machine Computations in Group Cohomology	**Hassan Errami** Berechnung von Hopf-Bifurkation in komplexen Reaktionsnetzwerken		**Severin Neumann** Parallele Algorithmen zur Berechnung von Gröbnerbasen	**Christian Gorzel** Kleine Polynome mit einer großen A_k-Singularität	
16:00 - 16:30	Pause			Pause			
16:30 - 17:00		**Viktor Levandowskyy** Stratifizierung des affinen Raums mittels D-Modulen	**Steffen Müller** Algorithmische arithmetische Schnitttheorie und kanonische Höhen		**Thomas Kahle** Gröbner-free computations with binomial ideals	**Johannes Hahn** W-Graph representations of Hecke algebras	
17:15 - 17:45		**Max Horn** Computing Schur multipliers of p-groups and nilpotent Lie rings	**Simon Hampe** Algorithmische tropische Schnitttheorie		**Albert Heinle** Zu Faktorisierungen in graduierten nichtkommutativen Algebren	**Sandra Weigl** Modulare Abelsche Varietäten, L-Reihen und ETNC	
18:00 - 18:30			**Eva Zerz** Neuigkeiten aus der Fachgruppe	**Thomas Richard** Neue Features in Maple 16			
19.00 Uhr				Gemeinsames Abendessen			
	R. 1409	**R. 2404**	**R. 1403**	**R. 1409**	**R. 2404**	**R. 1403**	**R. 1409**

Inhaltsverzeichnis

Algorithmische Aspekte der D-Modultheorie

Daniel Andres

daniel.andres@math.rwth-aachen.de
RWTH Aachen

Unter *D*-Moduln versteht man Moduln über Ringen von Differentialoperatoren. Im Vortrag wird ausschließlich die Weylalgebra betrachtet, d. h. der (nicht-kommutative) Ring linearer partieller Differentialoperatoren mit polynomiellen Koeffizienten über einem Körper der Charakteristik null.

In den letzten 15 Jahre wurden auf dem Gebiet der algorithmischen *D*-Modultheorie massive Fortschritte erzielt.

Gröbnerbasen, sowohl in der Weylalgebra selber als auch in gewissen Abwandlungen dieser, kommt eine besondere Bedeutung bei jeglichen konkreten Berechnungen zu.

Im Vortrag soll ein kurzer Überblick über die wichtigsten Konzepte, wie z. B. sogenannte Bernstein-Sato-Polynome (auch als *b*-Funktionen bekannt), sowie einige Anwendungen gegeben werden.

Completeness Criteria for Machine Computations in Group Cohomology

Simon King
simon.king@uni-jena.de
FSU Jena

Let G be a finite group whose order is divisible by a prime *p*. We are interested in computing the *mod-p cohomology ring* $H^*(G; \mathbb{F}p)$. That is a classical topic, with relations both in topology and modular representation theory.

Impressive computations of cohomology rings have been obtained without the help of a computer by topological methods, on the one hand, and application of spectral sequences, on the other hand. However, these methods are often restricted to special classes of examples.

The first exhaustive computation of the mod-2 cohomology of all groups of order 32 by D. Rusin was obtained using the Eilenberg-Moore spectral sequence. But the same method would not work for all groups of order 64.

Therefore, J. F. Carlson devised a different way to compute cohomology rings: Compute a degree-*d* ring approximation (i.e., find all minimal generators and relations out to degree *d*), and use a *completeness criterion* to test whether the ring approximation is actually isomorphic to the cohomology ring. Even though Carlson's original criterion relies on an unproven conjecture, he succeeded with computing the mod-2 cohomology of all groups of order 64. He needed several months of computation time, and thus the cohomology for the groups of order 128 or 243 seemed out of reach.

D. Benson suggested a different criterion. It relies on a filter regular homogeneous system of parameters for the cohomology ring that can be constructed in the ring approximation. The degree *d* in which the criterion applies depends crucially on the degrees of the parameters — which are often unreasonably large. Also the test whether the given parameters are indeed filter regular (which would not be the case in an incomplete approximation) can be very time consuming.

Together with D. Green, we improved the construction of filter regular parameters, yielding parameters in smaller degrees. In addition, we could improve the criterion by using the mere existence of parameters in *smaller* degrees after extending the coefficient field. With the improved Benson criterion, we provided the first exhaustive mod-2 cohomology computation of all groups of order 128, and also the mod-3 cohomology for all but six groups of order 243.

P. Symonds provided yet another criterion. Again, the degrees of parameters play an important role. Here, one cannot use existence results for parameters over field extensions. But it is not needed to focus on *filter regular* parameters, and thus the degrees can be lower, and the computational difficulty in testing filter regularity can be avoided.

In the case of finite groups that are not of prime power order, we formulated a criterion that mainly involves to study the Poincare series of the ring approximation and the degree of parameters over a finite field extension (one can use an existence result). Hence, it combines the advantages of the improved Benson criterion and of Symonds' criterion.

We implemented the different criteria in an optional package for the open source computer algebra system Sage. Depending on the example, different criteria are used to detect completeness of the ring approximation. With our Sage package, we computated the mod-p cohomology rings (for different primes *p*) of some sporadic simple groups, including several of the Mathieu and Janko groups, the McLaughlin group and the Higman-Sims group, and the third Conway group. Some of these cohomology rings have not been computed before.

Computing Hopf Bifurcations in Complex Reaction Networks

Hassan Errami

errami@cs.uni-bonn.de

Universität Bonn

The analysis of dynamic of chemical reaction networks by computing Hopf bifurcation is a method to understand the qualitative behavior of the network due to its relation to the existence of oscillations. For low dimensional reaction system without additional constraints Hopf bifurcation can be computed by reducing the question of its occurrence to quantifier elimination problems on real closed fields. However deciding its occurrence in high dimensional system has proven to be difficult in practice. We will present a fully algorithmic technique to compute Hopf bifurcation fixed point for reaction systems with linear conservation laws using reaction coordinates instead of concentration coordinates, a technique that extends the range of networks, which can be analyzed in practice, considerably.

STRATIFIZIERUNG DES AFFINEN RAUMS MITTELS *D*-MODULN

VIKTOR LEVANDOVSKYY
LEVANDOV@MATH.RWTH-AACHEN.DE

RWTH Aachen

Sei $\mathbb{K} = \mathbb{C}$. Betrachten wir eine Hyperfläche in $\mathbb{K}^n$, gegeben durch ein Polynom $f(x) \in R := \mathbb{K}[x_1, \ldots, x_n]$. Ein berühmter Satz von J. Bernstein besagt, dass für beliebiges *s* die Funktionalgleichung $P(s) \bullet f^{s+1} = b_f(s) \cdot f^s$ gilt, wobei • für die übliche Wirkung des Differentialoperators steht. Sei $D_n := D(R)$ die Weylalgebra, mit anderen Worten die Algebra der $\mathbb{K}$-linearen partiellen Differentialoperatoren mit Polynomkoeffizienten. Die Weylalgebra ist nichtkommutativ mit Relationen $\partial_j x_i = x_i \partial_j + \delta_{ij}$ zwischen den Erzeugern $x_1, \ldots, x_n, \partial_1, \ldots, \partial_n$. Dann $P(s) \in D_n[s]$ und $b_f(s) \in \mathbb{K}[s]$. Falls $b_f(s)$ normiert ist, wird es das globale Bernstein-Sato Polynom genannt. Bernstein zeigte, dass $b_f(s)$ kein Nullpolynom ist. Kashiwara bewies, dass die Wurzeln von $b_f(s)$ negative rationale Zahlen sind $\text{und } (s+1) \mid b_f(s)$ gilt. Es gibt auch eine lokale Version des Satzes von Bernstein. Dann wird das normierte Polynom $b_{f\,p}(s)$ auf der rechten Seite *das lokale Bernstein-Sato Polynom in* $p \in \mathbb{K}^n$ genannt.

Es stellte sich heraus, dass Bernstein-Sato Polynome sensitiv bezüglich Singularitäten von $V(f)$ sind. Im glatten Punkt $p \in V(f)$ ist das lokale Bernstein-Sato Polynom gleich *s* + 1. Es ist bekannt, dass $b_{f\,p}(s) \mid b_f(s)$ und $b_f(s) = \text{kgV}_{p \in \mathbb{K}^n} b_{f\,p}(s)$. Es gibt Algorithmen und Implementierungen (z. B. von mir und meinen Kollegen in SINGULAR:PLURAL) für die Berechnung aller Daten, die in der Bernsteinschen Funktionalgleichung erscheinen. Die Algorithmen sind aber von hoher Komplexität. Gröbnerbasen in $D_n[s]$ spielen dabei eine sehr wichtige Rolle.

Zusammen mit J. Martin-Morales (Zaragoza, Spanien) haben wir einen Algorithmus präsentiert, um eine endliche Stratifizierung von $\mathbb{K}^n$ zu berechnen, sodass das lokale Bernstein-Sato Polynom von f auf jedem Stratum konstant ist. Weiterhin, zu jedem Stratum wird noch ein $Dn[s] - Modul\, M_i$ assoziiert, wobei $D_n[s]/(Ann_{D[s]} f^s + f) = \sum_i M_i$ gilt. Es stellt sich heraus, dass M_i auch ein holonomer $D_n - Modul$ ist. Die verwendeten Techniken und Ergebnisse werden anhand von Beispielen demonstriert.

Eine weitere Verallgemeinerung der Stratifizierung wäre die Situation von Bernstein-Sato Polynomen von affinen Varietäten, die von Budur, Mustata und Saito eingeführt wurden.

Algorithmische arithmetische Schnitttheorie und kanonische Höhen

Steffen Müller

jan.steffen.mueller@uni-hamburg.de

Universität Hamburg

In diesem Vortrag werde ich zunächst arithmetische Schnittzahlen auf regulären Modellen algebraischer Kurven einführen. Diese lassen sich in nicht-archimedische und archimedische Schnittzahlen unterteilen. Anschließend stelle ich Algorithmen vor, die es ermöglichen, die nicht-archimedischen Schnittzahlen mittels Gröbnerbasen sowie die archimedischen Schnittzahlen in gewissen Situationen mittels Thetafunktionen zu berechnen. Diese Algorithmen sind im Fall hyperelliptischer Kurven in Magma implementiert worden. Schließlich möchte ich auf die derzeit wichtigste Anwendung eingehen, nämlich die Berechnung kanonischer Höhen und damit die Berechnung des in der Vermutung von Birch und Swinnerton-Dyer auftretenden Regulators der Jacobischen einer algebraischen Kurve.

Computing Schur multipliers of *p*-groups and nilpotent Lie rings

Max Horn
mhorn@tu-bs.de
TU Braunschweig

Let G be a group. Its second homology group $M(G) := H_2(G, Z)$ is called the *Schur multiplier* of G. We describe how to compute $M(G)$ for p-groups of nilpotency class c less than $p-1$ (note that this by itself is nothing new; indeed, algorithms that compute the Schur multipliers of arbitrary polycyclic groups exist). For this, we exploit the Lazard correspondence, which associates (via the Baker-Campbell-Hausdorff formula) to G a nilpotent Lie ring L with certain properties, from which G can be recovered. It turns out that $M(G)$ is isomorphic to $M(L) := H_2(L, Z)$.

We explain how to algorithmically compute $M(L)$ for any nilpotent Lie ring L using linear algebra. Combined with the Lazard correspondence, this yields are a method for computing the Schur multiplier of most p-groups G.

The novel advantage of our approach is the following: Let $c, n \in N$ and let $\{G_p \mid p \text{ is a prime greater than } c+1\}$ be a family of *p*-groups of nilpotency class c with $G_p = p^n$ with a shared parametrized presentation (e.g. $n = 3, c = 2$ and $G_p = \langle g_1, g_2, g_3 \mid [g_2, g_1] = g_3 [g_3, g_1] = [g_3, g_2] = g_1^p = g_2^p = g_3^p = 1 \rangle$).

Then we are able to compute $M(G_p)$ simultaneously for all primes $p > c+1$. As an application, we employ this to compute the Schur multipliers of all groups of order p^5.

Algorithmische tropische Schnitttheorie

Simon Hampe

hampe@mathematik.uni-kl.de

TU Kaiserslautern

In der tropischen Geometrie werden algebraische Varietäten durch einen Diskretisierungsprozess in Polyederkomplexe überführt. Diese Objekte können dann mit rein kombinatorischen Methoden studiert werden und enthalten noch genügend Informationen über die ursprüngliche Varietät, um Rückschlüsse auf deren Eigenschaften zuzulassen. So konnten beispielsweise Resultate der enumerativen Geometrie rein kombinatorisch, d.h. elementar bewiesen werden.
Dieser Vortrag gibt eine (sehr) kurze Einführung in tropische Geometrie. Anschließend werden die Grundlagen der polyedrischen tropischen Schnitttheorie sowie die damit verbundenen algorithmischen Probleme diskutiert und mithilfe von a-tint beispielhaft erläutert. a-tint ist eine Erweiterung für polymake, ein Software-Paket für polyedrische Rechnungen.

Construction of examples for Kähler-Einstein toric Fano manifolds with *POLYMAKE*

Andreas Paffenholz
paffenholz@mathematik.tu-darmstadt.de
TU Darmstadt

Classifications of polytopes allow efficient search for examples or counter-examples to open questions using appropriate software tools. In my talk I will show applications of this using the system polymake for polyhedral computations. In particular, I will show the construction of examples of non-symmetric toric Fano manifolds that admit a Kähler-Einstein metric. This answers a question first posed by V.V. Batyrev and E. Selivanova. The results are based on joint work with Benjamin Nill and Benjamin Lorenz.

Introduction

There is a powerful correspondence between n-dimensional projective toric varieties and complete n-dimensional polyhedral fans. A large dictionary translates between algebraic properties of the variety X and combinatorial properties of the polyhedral fan Σ [Ewa96]. Varieties X, X' are isomorphic if and only if the associated lattice polytopes P, P' can be identified by a lattice preserving affine transformation. Torus invariant Cartier divisors on X correspond to lattice polytopes P with normal fan Σ. Here, a lattice polytope P is the convex hull of a finite set of points in the integer lattice $\mathbb{Z}^n \subset \mathbb{R}^n$. Cones of the normal fan are sets of linear functionals that define the same face of the polytope. This correspondence of a toric variety to a polyhedral fan can be used for efficient classifications of toric varieties and computations of properties of a toric variety.
Since 2009 algorithms for polyhedral cones and fans, lattice polytopes, and their connection to toric geometry have been implemented in the software system **polymake [JMP09]**, available at **polymake.org**. The project was started already in 1996 by Gawrilow and Joswig as a tool for computations in geometric combinatorics and related areas. Interactive computations in polymake can be done with a perl-based interface, while larger projects can be implemented as a **C++**-extension using **polymake's C++**-library. Thus, **polymake** can be used for fast and reliable implementation of new algorithms, and checks of properties of examples, also on large classes. This has been successfully applied in various applications.
In the following I will explain one particular application where I used a classification of low-dimensional smooth Fano polytopes to obtain counter-examples to a question about Kähler-Einstein manifolds.

Non-symmetric Kähler-Einstein manifolds. We introduce further notation to explain our application. A lattice polytope Q is called *Fano polytope* if it contains the origin strictly in its interior, and the vertices of any facet of Q define a lattice basis of n. In particular, Q is simplicial. Its *polar polytope i*s given by

$$P := Q^* := \{y \in \mathbb{Z}^n : (y,x) \geq -1 \ \ \forall x \in Q\}.$$

As Q is Fano, the polytope P is again a lattice polytope (in the lattice dual to $\mathbb{Z}^n$). In the correspondence given above, Fano polytopes P correspond to smooth toric Fano varieties X_P (a smooth projective toric variety whose anticanonical divisor is Cartier).

For a Fano polytope P let $S(P)$ be the sub-group of lattice automorphisms that map P onto itself. We say that is symmetric if the origin is the only lattice point in P fixed by all elements of $S(P)$. We say that the toric variety X_P is symmetric if its polytope P is symmetric. A smooth toric variety is a *Kähler-Einstein variety* if it admits a Kähler-Einstein metric. The following theorem gives a relation symmetry and the existence of a Kähler-Einstein metric on a smooth toric variety.

Theorem 0.1 (Batyrev & Selivanova [BS99]). *A symmetric smooth toric Fano variety is a Kähler-Einstein variety.*

It was a long open question whether the converse of the theorem is also true [BS99]. A similar questions was also asked by Song [Son05] and others. Using **polymake** for an exhaustive search of symmetric polytopes and Kähler-Einstein varieties in a classification of smooth Fano polytopes allowed us to answer this question.

Theorem 0.2 (Nill & Paffenholz [NP11]). *Any Kähler-Einstein variety in dimension $n \geq 6$ is symmetric.*
There is exactly one non-symmetric Kähler-Einstein variety in dimension 7, and 2 in dimension 8.

In dimension 7, the one exception $X^{(7)}$ is a P^1-bundle over $(P^1)^3 \times P^3$. The two exceptions in dimension 8 are $X^7 \times P^1$ and S_6-bundle over $(P^1)^3 \times P^3$. Given these examples it is easily seen that $X^{(n)} := (P^1)^{n-7} \times \mathrm{X}^7$ generates a family of non-symmetric Kähler-Einstein varieties in any dimension $n > 7$. Subsequently, Ono et al. [OSY09] used our example to construct the first example of an asymptotically Chow unstable manifolds with constant scalar curvature.
We sketch how these examples can be found using **polymake**. 0bro [0br07] described an algorithm to generate smooth Fano polytopes in fixed dimensio n and applied it up to dimension 8. Joint with Benjamin Lorenz I have used new implementation in **polymake** to extend this to dimension 9 (see polymake.org/polytopes/paffenholz/www/fano.html for the data in **polymake** format).
polymake knows how to compute the combinatorial automorphism group of a polytope (using an interface to nauty (http://cs.anu.edu.au/~bdm/nauty/). We can adapt this to extract the group $S(P)$ of lattice automorphisms and its fixed space. This allows us to check whether a given smooth Fano polytope is symmetric. Actually, for the above examples a simpler check suffices, as the vertex barycenter is fixed by any automorphism, so this must be the origin for symmetric examples.
By a result of Wang and Zhu [WZ04] any smooth toric Fano variety X_p admits a Kähler-Einstein metric if and only if the barycenter b_p of P is 0. This translates the existence of a Kähler-Einstein metric into a combinatorial criterion that can be checked efficiently with **polymake**.

Other applications. Using the above classification and **polymake** we can also try to attack similar questions. For example, we can compute the α-invariant introduced by Tian [Tia87]. For the examples above we obtain $\alpha = \frac{1}{2}$, which shows that Tian's results do not predict the Kähler-Einstein structure. **polymake** has also proved successful in applications to other areas in mathematics.

REFERENCES

[BS99] V. Batyrev and E. Selivanova, Einstein-Kahler metrics on symmetric toric Fano manifolds, J. Reine Angew. Math. **512** (1999), 225-236.
[Ewa96] G. Ewald, Combinatorial convexity and algebraic geometry, Graduate Texts in Mathematics, vol. 168, Springer-Verlag, New York, 1996.
[JMP09] M. Joswig, B. Müller, and A. Paffenholz, Polymake and lattice polytopes.
[NP11] B. Nill and A. Paffenholz, Examples of Kahler-Einstein toric fano manifolds associated to non-symmetric reflexive polytopes, Beitr. Alg. Geom. **52** (2011), 297—304.
[0br07] M. Obro, Classification of smooth fano polytopes, Ph.D. thesis, Univ. of Aarhus, 2007.
[OSY09] H. Ono, Y. Sano, and N. Yotsutani, An example of asymptotically chow unstable manifolds with constant scalar curvature.
[Son05] J. Song, The a-invariant on toric Fano manifolds, Am. J. Math. **127** (2005), no. 6, 1247—1259.
[Tia87] G. Tian, On Kähler-Einstein metrics on certain Kähler manifolds with $C_1(M) > 0$, Invent. Math. **89** (1987), 225—246 (English).
[WZ04] X. Wang and X. Zhu, Kahler-Ricci solitons on toric manifolds with positive first Chern class, Advances in Mathematics 188 (2004), no. 1, 87—103.

TU Darmstadt, Fachbereich Mathematik, Dolivostr. 15, 64293 Darmstadt
E-mail address: paffenholz@mathematik.tu-darmstadt.de URL: http://mathematik.tu-darmstadt.de/~paffenholz

Computergestützte lokale Darstellungstheorie

Felix Noeske

felix.noeske@math-rwth-aachen.de

RWTH Aachen

Ein zentrales Thema in der Darstellungstheorie endlicher Gruppen ist der Beweis zahlreicher Vermutungen, die einen Zusammenhang zwischen den Darstellungen einer Gruppe und gewissen ihrer Untergruppen herstellt. Hierunter ist Broues abelsche Defektgruppenvermutung von besonderem Interesse. In diesem Vortrag wollen wir den erfolgreichen Rechnereinsatz bei dieser Vermutung am Beispiel der sporadischen Gruppe 2. HS vorstellen.

Dies ist eine gemeinsame Arbeit mit J. Müller und S. Koshitani.

Computing generators of toric ideals

David Ditter, Christian Haase, Benjamin Lorenz

blorenz@math.uni-frankfurt.de

Johann Wolfgang Goethe-Universität Frankfurt

1 Introduction

The study of toric varieties has attracted research from several different areas. In algebraic statistics, for example, Markov bases, i.e. special generator sets, of the ideals defining toric varieties are used for Fisher's exact test to analyze contingency tables. But even for rather small models the corresponding Markov bases are unknown.

Moreover, there is also a very close connection to the theory of integer polytopes. Many properties of projective toric varieties, such as smoothness, projective normality or very ampleness, can equivalently be defined in a purely geometric manner for the associated integer polytope. Based on this geometric perspective, I will present a work-in-progress algorithm to compute generator sets of toric ideals. Its main ingredients are the semigroup defining the variety, viewed as subset S of $\mathbb{Z}^d$, and special graphs associated to the points of S. An extension of the algorithm could also be used to compute higher betti numbers of the toric ideal.

There are several open questions concerning projective toric varieties. Of particular interest in this context are degree bounds on the generators of the ideals. So far it is known that the ideal of a projectively normal toric variety is generated by binomials of degree at most d, still open is whether this bound can be reduced to degree 2 in the smooth case [Batyrev, Sturmfels].

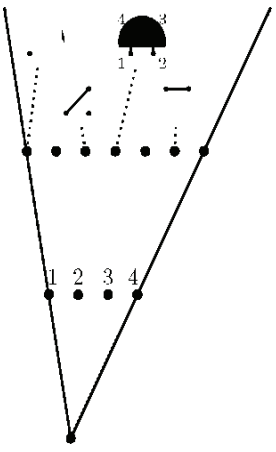
2 Algorithm

We start the description of the algorithm with the definition of the graphs, which is followed by some notes on the termination and the results of a first evaluation.

Graphs Let $\boldsymbol{A} \subset \mathbb{Z}^{\mathrm{d}}$ be a finite set of integer points contained in a common affine subspace, say last coordinate is equal to one, and let $\boldsymbol{S} = \mathbb{N}\boldsymbol{A}$ be the semigroup generated by $\boldsymbol{A}$. The toric ideal defined by $\boldsymbol{A}$ can be written as

$$IA = (\mathrm{x}^{\mathrm{u}} - \mathrm{x}^{\mathrm{v}} \in \mathbb{K}[\mathrm{x} = (\boldsymbol{x_1}, \ldots, \boldsymbol{x_n})] \mid Au = \mathrm{Av}),$$

where the columns of $\boldsymbol{A} \in \mathbb{Z}^{dxn}$ equal $\boldsymbol{A}$. The semigroup defines a multigrading on $\boldsymbol{I_A}$, which refines usual degree grading. The degree of a generator $\mathbf{x^u - x^v}$ is defined as $\mathbf{b} = \boldsymbol{Au}$. Additionally there is a $\mathbb{Z}$-grading given by the last coordinate of **b**. Now, for an arbitrary point $\mathbf{b} \in \boldsymbol{S}$, define a vertex set and an edge set as follows:



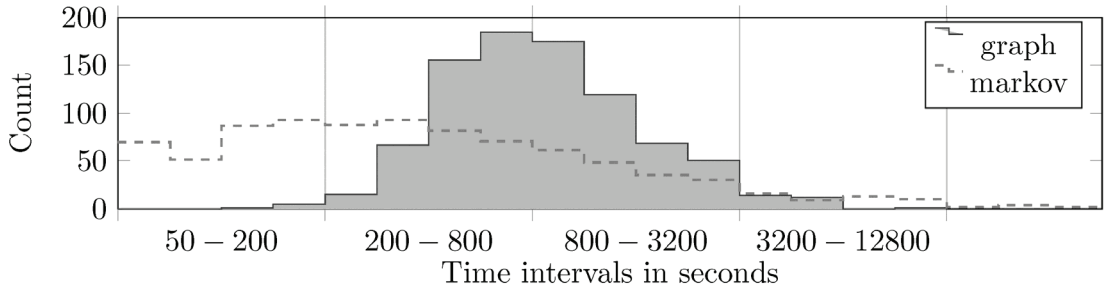
$\boldsymbol{V_h}$ **:= {a** $\in \boldsymbol{A}$ **| b - a** $\in \boldsymbol{S}$**}** $\quad$ $\boldsymbol{E_h}$ **:= {(a, a')** $\in \boldsymbol{A}$ x $\boldsymbol{A}$ **|** $\boldsymbol{b}$ **- a - a'** $\in \boldsymbol{S}$}

Theorem (Hochster, Stanley) *The number of connected components of the graph G_b = $G(V_b,E_b)$ minus one is equal to the zeroth betti number* β_0(A, **b),** *which is the same as the minimal number of generators of multidegree b in a Markov basis.*

Hence, by enumerating a still to be determined subset of the semigroup and checking the corresponding graphs we can determine all generators of the toric ideal. By definition, the vertex set $V_{b'}$ of $G_{b'}$ is the same as the adjacency list of **a** in G_b = b′ + a, and V_b can be written as $\{\boldsymbol{a} \in A \mid]\boldsymbol{b'} \in S : \boldsymbol{b} = \boldsymbol{b'} + \boldsymbol{a}\}$**.** Thus, these graphs can be constructed inductively in a very efficient manner, starting from the generators A of the semigroup.

Termination If, by chance, we do know that the embedding is projectively normal, then, by the result mentioned in the beginning, we can stop the graph generation when the last coordinate equals d. A general criterion for stopping the algorithm can be deduced from the inductive structure of the graphs: If G_b is connected and $V_b = V_{b+\boldsymbol{b'}}$ for **b'** ∈ S, then $G_{b+\boldsymbol{b'}}$ is also connected.

Testruns To evaluate the algorithm, I implemented a first version inside the **polymake** framework **[polymake.org]** and compared the runtime to **markov** from 4ti2 **[4ti2.de].** The examples used for the testruns are the semigroups generated by the integer point sets of all 866 smooth Fano polytopes in dimension 5, all of which are projectively normal [0bro].The plot shows the number of examples which finished in the given time intervals for each of the programs. For one example, **markov** crashed after exhausting all 12 gigabytes of available memory, while the graph algorithm within **polymake** never exceeded 2 gigabytes [Øbro].



Conclusion

These first results show that this is indeed a feasible and quite stable algorithm to compute Markov bases. As shown in the logarithmic runtime plot, the maximal runtime of the graph algorithm is less extreme. The most time consuming example took almost 3 hours, whereas markov needed more than 3 hours for 10 examples, reaching runtimes of about 10 hours. Moreover, there is still some room for improvement as many of the graphs could be stored in a more condensed form and lots of the connectivity checks could be skipped.

So far we only compute the zeroth betti number. But these graphs can be extended to simplicial complexes with $\Delta_b^k = \{(\boldsymbol{a_{i1}}, \ldots, \boldsymbol{a_{ik}}) \in \mathrm{A}^k \mid \boldsymbol{b} - \sum_{j=1}^{k} = a_{ij}\}$, which also carry a nice inductive structure. Computing their homology would allow us to also compute higher betti numbers of the toric ideals.

Compositions and collisions at degree p^2

Konstantin Ziegler
(joint work with Raoul Blankertz and Joachim von zur Gathen)
ziegler@bit.uni-bonn.de
Universität Bonn

The *composition* of two polynomials $g, h \in F[x]$ over a field F is denoted as $f = g \circ h = g(h)$, and then (g, h) is a *decomposition* of f, and *f* is *decomposable* if g and h have degree at least 2. In the 1920s, Ritt, Fatou, and Julia studied structural properties of these decompositions over $\mathbb{C}$, using analytic methods. A breakthrough result of Kozen & Landau (1989) was their polynomial-time algorithm to compute decompositions. A fundamental dichotomy is between the *tame case*, where the characteristic p does not divide $\deg g$ and this algorithm works, see von zur Gathen (1990a), and the *wild case*, where divides $\deg g$, see von zur Gathen (1990b). In the wild case, considerably less is known, both mathematically and computationally.
The task of counting compositions over a finite field of characteristic p was first considered in Giesbrecht (1988). Von zur Gathen (2009) presents general approximations to the number of decomposable polynomials. These come with satisfactory (rapidly decreasing) relative error bounds except when p divides $n = \deg f$ exactly twice. The main result of the present work determines exactly the number of decomposable polynomials in one of these difficult cases, namely when $n = p^2$ and hence $\deg g = \deg h = p$.
Our contribution is fourfold:

- We provide explicit constructions for collisions at degree r^2, where r is a power of the characteristic $p > 0$.
- We provide a classification of all collisions at degree p^2, linking every collision to a unique explicit construction.
- We use these two results to obtain an exact formula for the number of decomposable polynomials at degree p^2.
- The classification yields an efficient algorithm to test whether a given polynomial has a collision or not.

Klassifikation der kristallographischen Arrangements

Michael Cuntz
cuntz@mathematik.uni-kl.de
Universität Kaiserslautern

Simpliziale Arrangements wurden 1940 von Melchior entdeckt und in der Lösung vieler Probleme über Arrangements verwendet. Zum Beispiel waren sie die zentralen Objekte in Delignes Lösung der Vermutung von Brieskorn. Im dreidimensionalen sind simpliziale ArrangementsTriangulierungen der Sphäre durch Geraden.

Die Entdeckung des Weyl-Gruppoids als Symmetriestruktur gewisser Hopf-Algebren hat in den letzten Jahren zur Klassifikation einer großen Klasse von simplizialen Arrangements geführt, den sogenannten kristallographischen Arrangements.

Wir wollen im Vortrag auf die grundlegenden Eigenschaften der Weyl-Gruppoide eingehen und die algorithmischen Methoden vorstellen, die zur Klassifikation geführt haben. Außerdem wollen wir über Zusammenhänge zu torischen Varietäten, Cluster-Algebren und orientierten Matroiden berichten.

Singularitäten und Computeralgebra

Anne Frühbis-Krüger
anne@math.uni-hannover.de
Universität Hannover

Bei der Untersuchung von Singularitäten kommen Techniken aus verschiedensten Gebieten der Mathematik zusammen, aus der Algebra, der Algebraischen Geometrie und der Topologie ebenso wie der Analysis. In diesem Vortrag werde ich verschiedene Facetten der Singularitätentheorie beleuchten, in denen sich der Einsatz algorithmischer Methoden etabliert hat, angefangen von der einfachen phänomenologischen Untersuchung gegebener Singularitäten über Modulraumprobleme bis hin zur Desingularisierung.

Parallele Algorithmen zur Berechnung von Gröbnerbasen

Severin Neumann

neumans@fim.uni-passau.de

Universität Passau

Gröbnerbasen sind eines der mächtigsten Werkzeuge, welches die Computeralgebra zur Verfügung stellt. Sie können vielfältig eingesetzt werden, beispielsweise für die Berechnung von Syzygien, von Idealdurchschnitten oder von Lösungen für polynomiale Gleichungssysteme. Aber auch in anderen Bereichen der Mathematik, Informatik und Naturwissenschaften kommen sie zum Einsatz. Sie werden im Software Engineering bei der automatischen Programmverifizierung für das Finden von invarianten Schleifeneigenschaften verwendet. Mit ihnen können kryptographische Systeme angegriffen werden und sie können bei der Optimierung der Ölproduktion von Bohrplattformen eingesetzt werden. Darüber hinaus können Gröbnerbasen in der Festkörperphysik, der Halbleiterentwicklung, der Signalverarbeitung und der Biophysik helfen Lösungen für verschiedenste Probleme zu finden.

Der große Nachteil ist die Komplexität der Gröbnerbasenberechnung, die im schlimmsten Fall doppelt exponentiell in der Zahl der Elemente der Gröbnerbasis ist. Deswegen werden stets Verbesserungen gesucht oder neue Verfahren entwickelt, die schneller und speicherplatzsparender sind. Meist wird mathematisches Wissen genutzt, um unnötige Rechenschritte zu vermeiden. Kombiniert mit der stetig steigenden Computerleistung konnten so immer wieder neue schwere Probleme gelöst werden.

In diesem Vortrag soll als eine weitere Möglichkeit zur Beschleunigung der Berechnungen die Parallelisierung der Gröbnerbasenberechnung vorgestellt werden. Bei der Parallelisierung werden Schritte des Algorithmus auf mehrere Prozessoren aufgeteilt und gleichzeitig abgearbeitet. Anwendbar ist diese Verbesserung, wenn für einzelne Operationen die Reihenfolge der Ausführung nicht relevant ist. Begrenzt ist sie durch die Zahl der zur Verfügung stehenden Prozessoren. Diese wächst jedoch durch das Aufkommen von Mehrkernprozessoren seit einigen Jahren.

Nach einer kurzen Einführung in die Parallelprogrammierung wird im Vortrag gezeigt, wie sich Buchbergers Algorithmus zur Berechnung von Gröbnerbasen schrittweise parallelisieren lässt und sich schließlich in eine parallele Variante des Verfahrens F_4 [1] überführen lässt. Bei diesem werden die Reduktionen der S-Polynome in einer Matrixtransformation zur reduzierten Zeilenstufenform zusammengefasst. Zur parallelen Berechnung von reduzierten Zeilenstufenformen gibt es bereits viele Verfahren, beispielsweise lässt sich das Gauß'sche Eliminationsverfahren auf mehrere Prozessoren verteilen. Diese Verfahren berücksichtigen jedoch nicht die spezielle Struktur der Matrix, die sich aus den S-Polynomen und den Reduktionspolynomen ergibt. Durch Ausnutzung dieser Struktur lässt sich die Matrix in drei Schritten parallel reduzieren: Zunächst wird eine obere Dreiecksmatrix, die aus den Subtrahenden der S-Polynome und allen Reduktionspolynome besteht, vollständig reduziert. Anschließend werden diese Zeilen auf die verbleibenden Zeilen der Matrix angewendet. Zuletzt wird dieser Rest mittels Gauß'schem Eliminationsverfahren ebenfalls in reduzierte Zeilen-Stufenform gebracht. Alle Zeilen, die nach dem letzten Schritt ungleich Null sind, werden als neue Elemente in die gesuchte Gröbnerbasis eingefügt. Insbesondere für den ersten Schritt, bei dem der Großteil der Matrix verarbeitet wird, soll gezeigt werden, wie sich durch eine Auswahl der Reihenfolge, in der die Operationen ausgeführt werden, eine massive Parallelisierung erreichen lässt.

Abschließend wird eine C++-Implementierung des Verfahrens vorgestellt, die mit Hilfe der Programmierschnittstelle "Open Multi Processing" (OpenMP) und "Streaming SIMD Extensions" (SSE) parallelisiert wurde. Um die Beschleunigung durch die Parallelisierung des Verfahren zu messen wurden für große Polynomialsysteme über dem endlichen Körper mit 32003 Elementen **DegRevLex**-Gröbnerbasen auf einem

System mit 48 AMD Opteron™ 6172 Prozessoren und 64 Gigabyte Arbeitsspeicher mit steigender Prozessorenzahl berechnet. So konnte unter anderem für Katsura-13 die Berechnung von 41 auf 5 Minuten beschleunigt werden und für Cyclic-9 wurden mit einem Prozessor 3 Stunden benötigt, wohingegen mit 36 Prozessoren die Gröbnerbasis in 19 Minuten gefunden wurde. Die Implementierung ist auf GitHub unter der Adresse **https://github.com/svrnm/parallelGBC** frei verfügbar.

Literatur

[1] FAUGERE, JEAN CHARLES: *A new efficient algorithm for Computing Gröbner bases (F4).* Journal of Pure and Applied Algebra, 139(1-3):61-88, Juni 1999.

[2] FAUGERE, JEAN-CHARLES UND SYLVAIN LACHARTRE: *Parallel Gaussian Elimination for Gröbner bases computations in finite fields.* In: *Proceedings of the 4th International Workshop on Parallel and Symbolic Computation,* PASCO'10, Seiten 89-97, New York, USA, Juli 2010.

[3] NEUMANN, SEVERIN: *Effiziente parallele Implementation von Algorithmen zur Berechnung von Gröbnerbasen.* Masterarbeit. Universität Passau, 2011.

Kleine Polynome mit einer großen A_k-Singularität

Christian Gorzel
gorzelc@uni-muenster.de
Universität Münster

Die Frage, welche A_k-Singularitäten auf einer ebenen Kurve vom Grad *d* existieren, ist erst für $d \leq 6$ vollständig beantwortet. Schon für $d = 6$ ist dies ein schweres Problem aus dem Bereich „Computational algebraic geometry". Im Fall $d = 7$ war erst maximal die Existenz einer A_{25}-Singularität bekannt, wobei als obere Schranke *k* = 28 gilt, und *k* = 27 vermutlich optimal ist. Im Vortrag wird berichtet, unter welchen Vereinfachungen es mit Hilfe von SINGULAR gelang, eine Septik mit einer A_{27}-Singularität zu konstruieren.

Gröbner-free computations with binomial ideals

Thomas Kahle
thomas.kahle@math.ethz.ch
ETH Zürich

Binnomial ideals are inherently combinatorial objects. Indeed, a binomial tells us that one monomial is a scalar multiple of another monomial. Forgetting about the scalar, each binomial ideal defines a graph - in fact a congruence - on the monoid of exponents of the ambient ring and questions about connectivity in the graph can be formulated as ideal membership problems. This combinatorial view has lead to both significant theoretical advances in the theory of decompositions of binomial ideals, and applications in statistics, combinatorial game theory, and optimization.

Going in the other direction, that is studying ideal membership via connectivity properties of the graph, is useful for computational purposes. At this point the only computation with binomial ideals that still relies on Gröbner bases is computing the colon ideal $I:x$, where I is a binomial ideal and x a variable. We will discuss how to replace this Gröbner basis computation with a graph theoretic computation.

Balancierte Darstellungen und W-Graphen

Johannes Hahn
johannes.hahn@uni-jena.de
Universität Jena

Sei (W, *S) ein* Coxeter-System. Die Hecke-Algebra *H* = *H*(*W*, *S)* ist eine Deformation des Gruppenrings $\mathbb{Z}[W]$, deren Darstellungstheorie und Kombinatorik enge Beziehungen z.B. zu den Eigenschaften der zugehörigen algebraischen Gruppe, falls W eine Weyl-Gruppe ist. Um Berechnungen mit den H-Moduln durchzuführen, stellt man sie normalerweise als Menge von Matrizen über dem Körper der rationalen Funktionen $\mathbb{Q}(v)$ dar. Für praktische Zwecke muss man sicherstellen, dass diese Matrizen nicht zu viel Speicherplatz verbrauchen.

Es gibt verschiedene Möglichkeiten, die „Komplexität" solcher Matrizen zu messen. In diesem Vortrag werden die vorkommenden Exponenten der Unbekannten v als Komplexitätsmaß benutzt und „balancierte“ Darstellungen als Darstellungen minimaler Komplexität eingeführt.

Ein W-Graph ist ein kombinatorisches Objekt, das eine Darstellung von H kodiert. Es wird bewiesen, dass balancierte W-Graphen zusätzlich die Komplexität der kanonischen, invarianten Bilinearform minimieren, die zu dieser Darstellung gehört.

Zu Faktorisierungen in graduierten nichtkommutativen Algebren

Albert Heinle

albert.heinle@rwth-aachen.de
RWTH Aachen

1. Einleitung

Dies ist eine gemeinsame Arbeit mit Viktor Levandovskyy (RWTH Aachen). In dem Vortrag werden wir uns mit dem Faktorisierungsproblem für die erste Weyl- und die erste *q*-Weyl-Algebra beschäftigen, die wie folgt definiert sind:

Definition 1.1. Für einen Körper $\mathbb{K}$ definieren wir die erste Weyl-Algebra durch

$$A_1 := \mathbb{K}\langle x, \partial \mid \partial x = x\partial + 1\rangle$$

und erste *q*-Weyl-Algebra durch

$$Q_1 := \mathbb{K}\langle x, \partial \mid \partial x = qx\partial + 1\rangle$$

für eine Einheit $q \in \mathbb{K}$.
Auf beiden Algebren lässt sich eine nichttriviale Graduierung definieren, die durch die Gewichtung von ∂ mittels einem $z \in \mathbb{Z} \setminus \{0\}$ und die Gewichtung von x mittels $-z$ induziert wird. Der Einfachheit halber verwenden wir $z := 1$.

Die Stärke der von uns entwickelten Verfahren liegt in der Faktorisierung von homogenen Polynomen im Sinne dieser Graduierung. Wir werden kurz einen Einblick in die Funktionsweise unserer Algorithmen geben und dann auf die Weiterentwicklung eingehen. Diese besteht darin, dass wir uns um eine Verbesserung des Algorithmus für die Faktorisierung von inhomogenen Polynomen bemüht haben, der derzeit rein kombinatorischer Natur ist. Es werden sowohl neue Heuristiken gezeigt werden, als auch verbesserte Verfahren zum Finden aller Faktorisierungen (Bemerkung: Faktorisierungen von Polynomen in A_1 und Q_1 sind eindeutig bis auf eine schwache Form von Assoziiertheit).
Ein weiterer Schwerpunkt wird das Faktorisierungsproblem für Ore-Lokalisierungen von den oben genannten Algebren sein. Auch werden wir auf die Fragestellung eingehen, inwiefern man das Gausssche Lemma für nichtkommutative Ringe verallgemeinern kann. Für kommutative Ringe hat es folgende Formulierung:

Lemma 1.2 (Lemma von Gauss). Sei R ein kommutativer faktorieller Ring und $R[x]$ der Polynomring über R in einer Variablen. Sei f in $R[x]$ irreduzibel, dann ist f über Quot $(R)[x]$ auch irreduzibel.

Unter anderem ist die Frage interessant für den Fall der rationalen $(q-)$Weyl-Algebra, d.h. $\mathbb{K}(x)\langle \partial \mid \partial x = x\partial + 1\rangle$ bzw. $\mathbb{K}(x)\langle \partial \mid \partial x = qx\partial + 1\rangle$.

2. **NCFACTOR.LIB** - EIN ÜBERBLICK

Seit Version 3-1-3 ist die von uns entwickelte Bibliothek **ncfactor.lib** fester Bestandteil des Computeralgebra Systems SINGULAR. Sie beinhaltet Implementierungen unserer Faktorisierungsverfahren. Vergleiche mit den Implementierungen in MAPLE und REDUCE zeigten, dass wir im homogenen Fall (bezüglich der Graduierung in obiger Definition) sehr schnelle Berechnungen durchführen können. Es existiert auch eine Klasse von Fällen, in denen unser Algorithmus als Einziger Faktorisierungen in annehmbarer Zeit finden kann.

Derzeit finden sich in **ncfactor.lib** Funktionen zur Faktorisierung von

- der ersten Weyl-Algebra,
- der ersten Shift-Algebra und
- homogenen Polynomen in der ersten q-Weyl-Algebra.

Die genaue Funktionsweise dieser Algorithmen lässt sich in [H] und dem Online Manual von SINGULAR nachlesen.

Den Flaschenhals bilden noch Faktorisierungen nicht homogener Polynome und teilweise die Handhabung von Parametern wie z.B. in Q_1. Die Zeiten für die Berechnung sind vergleichbar mit denen anderer Computeralgebrasysteme, aber wir sehen hier viel Potenzial für Verbesserungen. Die Ideen und bis dahin evtl. eine erste Implementierung dieser sind Bestandteil unseres Vortrages.

Wir planen auch eine Schnittstelle für SAGE zu schreiben, so dass man auch von SAGE heraus auf die Bibliothek zugreifen kann. SINGULAR selbst ist spezialisiert auf polynomielle Algebren, und mit Hilfe von SAGE erhoffen wir uns eine gute rationale Darstellung für die oben erwahnten Lokalisierungen entwickeln zu können.

LITERATUR

[S] M. Saito, B. Sturmfels and N. Takayama. *Grobner deformation of hypergeometric differential equations. Algorithms and Computation in Mathematics* 6. Springer Verlag, 1999

[M] Maplesoft. *Maple Online Help.* http://www.maplesoft.com**,** 2011

[MA] H. Melenk and J. Apel. *NCPOLY: Computation in non-commutative polynomial ideals*. www.reducealgebra.com/docs/reduce.pdf

[GL] G.-M. Greuel, V. Levandovskyy, A. Motsak and H. Schönemann. PLURAL. *A* SINGULAR *3.1 Subsystem for Computations with Non-commutative Polynomial Algebras. Centre for Computer Algebra*. University of Kaiserslautern, 2010, http://www.singular.uni-kl.de

[H] A. Heinle. *Factorization in a Class of Noncommutative Algebras*. Bachelor Thesis, RWTH Aachen University, 2010, available at http://www.math.rwthaachen.de/~Albert.Heinle/LehrstuhlDWebsite/Welcome_files/bachelor_thesis-1.pdf

LEHRSTUHL D FÜR MATHEMATIK, RWTH AACHEN UNIVERSITY, TEMPLERGRABEN 64, 52062 AACHEN

*E-mail address***:** albert.heinle@rwth-aachen.de

E-mail address: viktor.levandovskyy@math.rwth-aachen.de

Modulare abelsche Varietäten, L-Reihen und ETNC

Sandra Weigl
weigl@math.lmu.de
Ludwig-Maximilians-Universität München

Sei f eine Neuform von Gewicht 2, A_f die zugehörige modulare abelsche Varietät, $L(A_f,s)$ deren *L*-Reihe und Ω_{A_f} das reelle Volumen von A_f. Zudem sei *K* eine endliche abelsche Galoiserweiterung von $\mathbb{Q}$ mit Galoisgruppe G. Gegenstand des Vortrags ist die Äquivariante Tamagawazahlvermutung für $(A_f)_K$, der Basiswechsel von A_f. Ein Hauptbestandteil dieser Vermutung ist $L^*((A_f)_K,1)$, der führende Koeffizient der Taylorentwicklung von $L(A_f)_K$ an der Stelle 1, bzw. $(L^*(A_f,\chi,1))_{\chi\in\mathrm{Irr}(G)}$.

Mit Hilfe der Theorie modularer Symbole lässt sich für jeden Dirichlet-Charakter χ der Quotient $L(A_f,\chi,1)/\Omega_{A_f}$ exakt berechnen. Und somit, im Falle (anal.) Rangs Null, auch der führende Koeffizient der Taylorentwicklung bei 1 (modulo Ω_{A_f}).

Unter zusätzlichen Voraussetzungen an G ermöglicht dies die exakte Verifizierung obiger Vermutung für modulare abelsche Varietäten von Rang Null.

New Features in Maple 16

Thomas Richard
trichard@maplesoft.com
Maplesoft Europe GmbH

We present an overview of the most important new features in Maple 16, including:
- new symbolic and numeric routines (e.g. in differential equations and physics)
- performance (memory management changes, speedups in polynomial arithmetic)
- language features (coercion, object-oriented programming)
- visualization enhancements (e.g. rubber-band zooming, new plot types)
- eBook Publisher preview
- new Clickable Math features (Smart Pop-ups, Drag-to-Solve)
- miscellaneous changes

Modulare Galois-Darstellungen und Computeralgebra

Gabor Wiese
gabor.wiese@uni.lu
Universität Luxemburg

Ein herausragendes Resultat der Arithmetischen Geometrie der letzten Jahre stellt zweifelsohne der Beweis von Khare und Wintenberger der Modularitätsvermutung von Serre dar. Diese impliziert unter anderen die verallgemeinerte Taniyama-Shimura-Vermutung (die den großen Satz von Fermat zur Folge hat) und neue Fälle der Artin-Vermutung.

Für die Computeralgebra ist die Serresche Modularitätsvermutung auch von großer Bedeutung. Denn sie erlaubt in vielen Fällen die Übertragung von sehr harten zahlentheoretischen Fragen in Fragen über Modulformen.

Letztere sind aber gut mittels Computeralgebra berechenbar, so dass oft auch für die Zahlentheorie interessante Rückschlüsse gezogen werden können.

Der Vortrag wird die Objekte der Serreschen Modularitätsvermutung erläutern und mit Beispielen illustrieren.

RSA Protokollfehler, LLL und Gröbnerbasen

Andreas Klein
klein@cage.ugent.be
Gießen

Das bekannte RSA-Verfahren hat verschiedene schwache Instanzen. Diese können in der Praxis leicht vermieden werden. Doch dazu ist es nötig, dass der Anwender die potenziellen Gefahrenquellen kennt. Einige der interessantesten Angriffe gegen schwache RSA-Instanzen nutzen klassische Computeralgebratools wie den LLL-Algorithmus oder Gröbnerbasen.

In diesem Vortrag werden jeweils ausgehend von einem konkreten kryptographischen Problem solche Angriffe und die dahinter stehende Mathematik vorgestellt.

			Teilnehmerverzeichnis	
Nr.:	**Name:**	**Vorname:**	**Anschrift:**	**E-Mail:**
1	Andres	Daniel	RWTH Aachen, Lehrstuhl D für Mathematik	daniel.andres@math.rwth-aachen.de
2	Beuerle	Karsten	München, Wilhelm-Busch-Straße 42	karsten.beuerle@live.de
3	Bley	Werner	Mathematisches Institut der Uni München	bley@math.lmu.de
4	Böttcher	Anna	Liebenau	aboettch@mathematik.uni-kassel.de
5	Cuntz	Michael	Universität Kaiserslautern, FB Mathematik	cuntz@mathematik.uni-kl.de
6	Dück	Natalia	TU Hamburg-Harburg	natalia.dueck@tu-harburg.de
7	Errami	Hassan	Universität Bonn, Institut für Informatik II	errami@cs.uni-bonn.de
8	Fetzer	Matthias	Universität Kassel, Institut für Mathematik	Fetzer@mathematik.uni-kassel.de
9	Frühbis-Krüger	Anne	Leibniz-Universität Hannover	fruehbis-krueger@math.uni-hannover.de
10	Gorzel	Christian	Universität Münster	gorzel@uni-muenster.de
11	Grelak	Felix	Universität Duisburg-Essen	felix_grelak@uni-due.de
12	Haase	Christian	Goethe-Universität Frankfurt	haase@math.uni-frankfurt.de
13	Hahn	Johannes	Universität Jena	johannes.hahn@uni-jena.de
14	Hahn	Thomas	Max-Planck-Institut für Physik	hahn@feynarts.de
16	Heinle	Albert	RWTH Aachen	Albert.Heinle@rwth-aachen.de
17	Heß	Florian	Universität Oldenburg	florian.hess@uni-oldenburg.de
18	Himstedt	Frank	TU München, Garching	himstedt@ma.tum.de
19	Horn	Max	TU Braunschweig	mhorn@tu-bs.de
20	Hornecker	Achim	Freiburg, Leo-Wohleb-Str. 6	achim@hornecker.de
21	Kahle	Thomas	ETH Zürich, Forschungsinstitut Mathematik	Thomas.Kahle@math.ethz.ch
22	Kemper	Gregor	TU München, Garching	kemper@ma.tum.de
23	King	Simon	Friedrich-Schiller-Universität Jena	simon.king@uni-jena.de
24	Klein	Andreas	Gießen	Klein@cage.ugent.be
25	Klüners	Jürgen	Universität Paderborn	klueners@math.uni-paderborn.de
26	Koepf	Wolfram	Universität Kassel, Institut für Mathematik	Koepf@mathematik.uni-kassel.de
27	Lakhal	Anen	Universität Kassel, Institut für Mathematik	alakhal@uni-kassel.de
28	Levandovskyy	Viktor	RWTH Aachen, Lehrstuhl D für Mathematik	Levandov@math.rwth-aachen.de
29	Lorenz	Benjamin	Goethe-Universität Frankfurt	blorenz@math.uni-frankfurt.de
30	Müller	Jan Steffen	Universität Hamburg, FB Mathematik	jan.steffen.mueller@uni-hamburg.de
31	Neumann	Severin	Universität Passau, Eduard-Hamm-Str. 18	neumans@fim.uni-passau.de
32	Noeske	Felix	RWTH Aachen, Lehrstuhl D für Mathematik	Felix.Noeske@math.rwth-aachen.de
33	Paffenholz	Andreas	TU Darmstadt, Fachbereich Mathematik	paffenholz@mathematik.tu-darmstadt.de
34	Petersen	Sebastian	Universität Kassel, Institut für Mathematik	Petersen@mathematik.uni-kassel.de
35	Quedenfeld	Frank-M.	Universität Kassel, Institut für Mathematik	frank.quedenfeld@mathematik.uni-kassel.de
36	Richard	Thomas	Maplesoft Europe GmbH, Aachen	Trichard@mapelsoft.com
37	Rück	Hans-Georg	Universität Kassel, Institut für Mathematik	rueck@mathematik.uni-kassel.de
38	Schweinfurter	Michael	Universität Kassel, Institut für Mathematik	michael.schweinfurter@mathematik.uni-kassel.de
39	Seiler	Werner	Universität Kassel, Institut für Mathematik	seiler@mathematik.uni-kassel.de
40	Sprenger	Torsten	Universität Kassel, Institut für Mathematik	sprenger@mathematik.uni-kassel.de
41	Trei	Wilke	Universität Oldenburg	wilke.trei@uni-oldenburg.de
42	Weigl	Sandra	Mathematisches Institut der Uni München	Sandra.Weigl@mathematik.uni-muenchen.de
43	Wiese	Gabor	Universität Luxemburg	Gabor.Wiese@uni.lu
44	Zerz	Eva	RWTH Aachen, Lehrstuhl D für Mathematik	eva.zerz@math.rwth-aachen.de
45	Ziegler	Konstantin	Universität Bonn, b-it	zieglerk@bit.uni-bonn.de

Hinweise:

- Für alle Teilnehmer wurde ein Gast-Account eingerichtet

  login: guest
  password: cat12

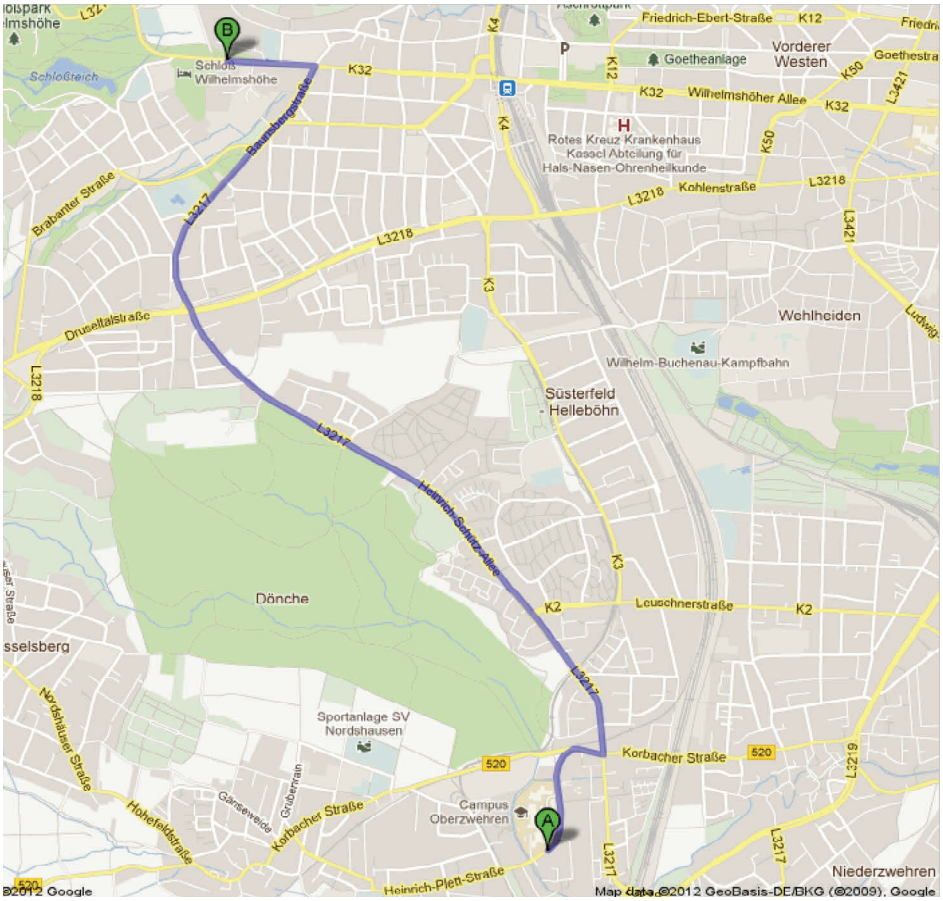
  Dieses Passwort kann nicht geändert werden. Die Home-Quota beträgt 50 MB und 500 Dateien. Alle Rechner haben eine Internetanbindung, so dass Mail auch remote über ssh bzw. Webmail möglich ist.

  Terminals befinden sich im Raum 2421/2422 (Nutzung Donnerstag und Freitag ab 15 Uhr) und im Raum 3321 (Nutzung ganztägig möglich).

- In den Räumen des Instituts ist ein Tagungs-WLAN verfügbar, die SSID des Netzes lautet „CA2012“. Die Zugangsdaten werden zu Beginn der Veranstaltung bekannt gegeben.
- Am Freitag, dem 11. Mai 2012, findet um 19:15 Uhr ein gemeinsames Abendessen im „Restaurant Gutshof“ statt. (Restaurant Gutshof, 34131 Kassel, Wilhelmshöher Allee 347a, Tel.: 0561 / 32 52 5).

  Für die gemeinsame Anfahrt besteht die Möglichkeit, um 18:56 Uhr mit der Tram 0 ab der Haltestelle „Korbacher Straße/Universität“ bis zur Haltestelle „Hessischer Rundfunk“ zu fahren. Von hier aus ist das Restaurant Gutshof in 5 Minuten zu Fuß zu erreichen.

  Anfahrt zum Restaurant Gutshof, siehe auch http://www.restaurant-gutshof.de



Weinempfehlung

2010er Weißer Burgunder Spätlese

Weinolsheimer Hohberg, Weingut Gröhl,
Erzeuger-Abflg.
Pikante Aromen vollreifer Birnen
und Anklänge von Melone,
sehr saftig und mit brillanter Frische.
- trocken -

2009er Rupestro Rosso

Für den Rupestro werden Trauben vom
Merlot und Sangiovese verwendet. Frisch,
rubinrot mit violetten Reflexen funkelt er im
Glase. Die Nase spürt Kirschen und
verschiedene andere rote Früchte, etwas
Vanille, aber auch das Aroma bitterer
Mandeln. Angenehm jugendlich, trocken, voll
und sauber im Mund, anhaltende Tannine,
kraftvoller Körper, sehr komplex.
- trocken -

Menüauswahl

Tomatensuppe Kalabrese
mit italienischen Kräutern & Olivenöl zubereitet 4,40

oder

Spargel-Rieslingsüppchen 5,70

* * * * * * *

Gutshof - Spezial
gebratene Medaillons vom Schweine- und Rinderfilet,
sowie Truthahnmignons, dazu Rahmpilze, Sc. Hollandaise,
frische Saisongemüse & Bratkartoffeln 16,80

oder

Schnitzel „Försters Tochter“
mit Rahmpilzen, Bratkartoffeln & Salat 13,70

oder

Pochiertes Lachsfilet - Ikarimi -
auf leichter Riesling-Sahnesauce, Salzkartoffeln & Salat 17,60

oder

Gefüllte Kartoffelgnocchis - in Butter gebraten -
mit frischem Rucola, Parmesan und Avocadoöl serviert 14,80

* * * * * * *

Crème Brûlée
nach französischer Rezeptur im Ofen pochiert
& mit braunem Rohrzucker karamellisiert 5,40

oder

Holunder - Waldbeerengrütze
mit Vanilleeis 4,90