

März 2013

# Computeralgebra

## Rundbrief

> Ausgabe 52

- ▶ Die Ordnung von Tate-Shafarevich Gruppen modulo Quadrate
- ▶ Torische Geometrie mit `polymake`
- ▶ Bildverarbeitung: Mathematik arbeiten sehen

## Impressum

Der Computeralgebra-Rundbrief wird herausgegeben von der Fachgruppe Computeralgebra der GI, DMV und GAMM  
(verantwortliche Redakteure: Dr. Michael Cuntz, Dr. Gohar Kyureghyan, [car@mathematik.de](mailto:car@mathematik.de))

Der Computeralgebra-Rundbrief erscheint halbjährlich, Redaktionsschluss 15.02. und 15.09. ISSN 0933-5994. Mitglieder der Fachgruppe Computeralgebra erhalten je ein Exemplar dieses Rundbriefs im Rahmen ihrer Mitgliedschaft. Fachgruppe Computeralgebra im Internet:  
<http://www.fachgruppe-computeralgebra.de>.

Konferenzankündigungen, Mitteilungen, einzurichtende Links, Manuskripte und Anzeigenwünsche bitte an die verantwortlichen Redakteure.

Die Geschäftsstellen der drei Trägergesellschaften:

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



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



**GAMM** (Gesellschaft für Angewandte  
Mathematik und Mechanik e.V.)  
Technische Universität Dresden  
Institut für Statik und Dynamik der  
Tragwerke  
01062 Dresden  
Telefon 0351-463-33448  
Telefax 0351-463-37086  
[GAMM@mailbox.tu-dresden.de](mailto:GAMM@mailbox.tu-dresden.de)  
<http://www.gamm-ev.de>





## Inhaltsverzeichnis

<b>Impressum</b>	2
<b>Inhalt</b>	3
<b>Mitteilungen der Sprecher</b>	4
<b>Tagungen der Fachgruppe</b>	6
<b>Themen und Anwendungen der Computeralgebra</b>	7
Die Ordnung von Tate-Shafarevich Gruppen modulo Quadrate (S. Keil, R. N. Kloosterman)	7
Neuer Primzahlrekord (J. Klüners)	12
<b>Neues über Systeme</b>	13
Torische Geometrie mit <i>polymake</i> (M. Joswig, A. Paffenholz)	13
<b>Computeralgebra in der Lehre</b>	18
Bildverarbeitung: Mathematik arbeiten sehen (Bernhard Burgeth, Florian Kern)	18
<b>Besprechungen zu Büchern der Computeralgebra</b>	22
Steven D. Galbraith: <i>Mathematics of Public Key Cryptography</i> (Florian Heß)	22
<b>Ehrenpromotion in der Computeralgebra</b>	23
<b>Promotionen in der Computeralgebra</b>	24
<b>Habilitationen in der Computeralgebra</b>	25
<b>Berichte von Konferenzen</b>	26
<b>Hinweise auf Konferenzen</b>	30
<b>Fachgruppenleitung Computeralgebra 2011-2014</b>	34

---

## Mitteilungen der Sprecher

---

*Liebe Mitglieder der Fachgruppe Computeralgebra,*

*am 18. Februar 2013 fand an der Leibniz-Universität in Hannover die fünfte Sitzung der aktuellen Fachgruppenleitung statt.*

*Mit Bestürzung erfuhren die Anwesenden zu Beginn der Sitzung vom unerwarteten Tod von Prof. Dr. Michael Hofmeister nach kurzer, schwerer Krankheit. Herr Hofmeister war in der Fachgruppenleitung als Fachexperte Industrie tätig und nahm mit seinem Engagement zur Verbindung universitärer und industrieller Forschung eine wichtige Rolle ein. Sein Einsatz und Ideenreichtum, unter anderem bei der Organisation der Industrietagung der Fachgruppe, werden schmerzlich vermisst werden. Einen Nachruf für Herrn Hofmeister finden Sie auf Seite 5.*

*Im Mittelpunkt der Sitzung standen die vielfältigen Tagungsaktivitäten der Fachgruppe, der aktuelle Computeralgebra-Rundbrief sowie die Organisationsstruktur der Fachgruppe.*

*Die zweite Ausgabe der Industrietagung „Industrial Applications and Prospects of Computer Algebra“ (IAPCA 2013) der Fachgruppe findet am 16. und 17. September 2013 am Zuse-Institut in Berlin statt. Wir widmen diese Tagung dem Andenken an Herrn Hofmeister. Die Planungen sind zur Zeit in vollem Gange, nähere Informationen finden Sie auf Seite 6 und unter der dort angegebenen Webseite.*

*Eine weitere hochrangige und internationale Tagung mit Fachgruppen-Beteiligung ist die Konferenz „Computer Algebra in Scientific Computing 2013“ (CASC 2013), die vom 9. bis zum 13. September 2013 ebenfalls am Zuse-Institut Berlin stattfinden wird. General Chairs sind Ernst W. Mayr von der Fachgruppenleitung und Vladimir P. Gerdt, Program Committee Chairs sind Wolfram Koepf von der Fachgruppenleitung und Evgenii V. Vorozhtsov. Nähere Informationen zur CASC 2013 finden Sie auf der Seite 31.*

*Nach dem von Hans-Gert Gräbe von der Fachgruppenleitung veranstalteten erfolgreichen ersten Workshop zu SymbolicData im vergangenen Dezember ist ein zweiter Workshop für den Zeitraum 25.-27. Juli 2013 geplant. Hierzu finden Sie weitere Informationen unter der Webseite <http://symbolicdata.org/wiki/Events>.*

*Im Computeralgebra-Rundbrief im Herbst werden wieder die Wahlunterlagen für die nächste Legislaturperiode der Fachgruppenleitung verschickt. Wir bitten, bis dahin Vorschläge und Bewerbungen beim Sprecher Florian Heß ([florian.hess@uni-oldenburg.de](mailto:florian.hess@uni-oldenburg.de)) einzureichen. Jeder, der hier mitwirken will, ist herzlich willkommen!*

*Wir hoffen, Sie mit dem vorliegenden Heft gut zu informieren.*

*Florian Heß*

*Eva Zerz*

## Nachruf



Nach kurzer schwerer Krankheit starb am 15. Februar dieses Jahres Prof. Dr. Michael Hofmeister, der der Fachgruppe seit 2008 als Fachexperte Industrie angehörte. Das Kernziel seines Engagements in der Fachgruppe war hierbei das Überbrücken der Kluft und das Initiieren eines Dialoges zwischen der universitären Forschung in Computeralgebra auf der einen und den industriellen Anwendern von Computeralgebrasystemen auf der anderen Seite. Auf seine Initiative geht die Tagungsreihe *Industrial Applications and Prospects of Computer Algebra* der Fachgruppe zurück, die 2011 begann und in diesem Jahr fortgesetzt werden wird.

Auch sein wissenschaftlicher Werdegang und Berufsweg sind gekennzeichnet durch Aktivitäten in beiden Welten. Nach einem Studium des gymnasialen Lehramts für die Fächer Mathematik und Physik promovierte Michael Hofmeister 1986 in Köln in Mathematik. Sein Interessengebiet hier lag vor allem im Bereich der Kombinatorik, Diskreten Mathematik und Optimierung.

1990 verließ er den Hochschulbereich und ging in die Industrie, zu Siemens in München, wo er bis zu seinem Tod tätig war. Hier sammelte er vielfältige Erfahrungen im praktischen Einsatz mathematischer Methoden in Industrieprojekten und hob den Kompetenzbereich *Discrete Optimization* mit aus der Taufe, der in das später von ihm geleitete Applikationsfeld *Modeling, Simulation and Optimization* überging. Aus seiner engen Zusammenarbeit mit technischen Projekten erwuchsen dabei auch mehrere Patente.

Gleichzeitig blieb er aber auch dem Hochschulbereich verbunden und habilitierte sich 2004 in Darmstadt, wo er 2009 eine Honorarprofessur erhielt. Seit 2011 war er Honorarprofessor in Erlangen. Diese Verbindung von industrieller Tätigkeit und universitärer Lehre und Forschung nutzte er nicht nur im Angebot entsprechender Lehrveranstaltungen, sondern auch zur Nachwuchsförderung durch die Vergabe von Studierenden- und Promotionsstipendien und als Vertreter der Berufspraxis im Fachausschuss Mathematik der Akkreditierungsagentur für Studiengänge der Ingenieurwissenschaften, der Informatik, der Naturwissenschaften und der Mathematik (ASIIN). Darüberhinaus war es ihm als Gründungsmitglied des Strategiekomitees für mathematische Modellierung, Simulation und Optimierung (KoMSO) ein besonderes Anliegen, das Potenzial der Mathematik für die Industrie und für die Gesellschaft besser zu erschließen und nutzbar zu machen.

Mit ihm verliert die Fachgruppe Computeralgebra einen geschätzten Experten und engagierten Kollegen, der gerade durch seinen facettenreichen Werdegang immer wieder neue Perspektiven und Gesichtspunkte einbringen konnte. Die Industrietagung im September (siehe Seite 6), zu deren Planung er schon nicht mehr so beitragen konnte, wie er es gerne gewünscht hätte, möchte die Fachgruppe Computeralgebra seinem Andenken widmen; sie wird am ZIB in Berlin stattfinden, dessen wissenschaftlichem Beirat er ebenfalls angehörte.



*Industrial Applications and Prospects of Computer Algebra 2013, 16.–17. September 2013, Berlin*

### **Industrial Applications and Prospects of Computer Algebra 2013, 16.–17. September 2013, Berlin**

<http://www.computeralgebra.de/IndustrialApplications2013>

*in memoriam Michael Hofmeister*

Im September dieses Jahres lädt die Fachgruppe wieder zu einer Konferenz ein, deren zentrale Themen industrielle Anwendungen der Computeralgebra sind sowie bestehende und zukünftige Erwartungen, die mit einem solchen Einsatz verbunden sind. Ziel dieser Tagungsreihe ist, den Dialog zwischen den verschiedenen Interessengruppen im Umfeld industrieller Anwendungen der Computeralgebra zu fördern:

- Universitäten und Hochschulen, die formale Methoden im Umfeld von CA erforschen und zur Verfügung stellen,
- Tool-Provider, die diese Methoden zur Marktreife führen, sowie
- Unternehmen und anwendungsorientierte öffentliche Forschungseinrichtungen, die diese Methoden durch Verwendung der Tools bei der Entwicklung neuer Produkte zum Einsatz bringen.

Die Konferenz soll als Forum für alle Interessengruppen dienen, nicht nur, um Erfahrungen auszutauschen, sondern auch, um die Anforderungen an den industriellen Einsatz der Computeralgebra im Unterschied zu anderen Einsatzbereichen (wie etwa der Schule und Hochschule) zu diskutieren. Da die Initiative zu dieser Konferenzreihe auf den kürzlich verstorbenen Michael Hofmeister zurückgeht, möchte die Fachgruppe Computeralgebra ihm die diesjährige Tagung widmen.

Wie auch vor zwei Jahren ist wieder ein Vortragsprogramm aus Beiträgen der drei Interessengruppen vorgesehen, begleitet von Ausstellungen und Postern. Die Hauptvorträge in diesem Jahr beschäftigen sich unter anderem mit Kryptographie, Industrieinsatz von CAS und Algebraischer Statistik. Kurzbeiträge und Poster sind willkommen; Näheres zum Einreichen und den Deadlines entnehmen Sie bitte der Homepage.

Das Zuse Institut in Berlin bietet uns in diesem Jahr das geeignete Umfeld für die Tagung, die Organisation liegt diesmal in den Händen von Frau Baciú (Shell Oil), die kurzfristig Herrn Hofmeisters Aufgaben übernommen hat, Frau Frühbis-Krüger (Leibniz Universität Hannover) und Herrn Neun (ZIB) als lokalem Organisator.



## Die Ordnung von Tate-Shafarevich Gruppen modulo Quadrate

S. Keil, R. N. Kloosterman  
(Humboldt-Universität zu Berlin)

keil@math.hu-berlin.de  
klooster@math.hu-berlin.de



---

### Lokale und globale Lösungen

---

Eine der ältesten Problemstellungen der Zahlentheorie ist das Beschreiben der Lösungsmenge von diophantischen Gleichungen. Eine algebraische Gleichung heißt *diophantisch*, wenn alle in ihr vorkommenden Koeffizienten ganze Zahlen sind. Eine allgemeine diophantische Gleichung vom Grad 2 in zwei Variablen hat die Gestalt

$$a_1X^2 + a_2Y^2 + a_3XY + a_4X + a_5Y + a_6 = 0,$$

wobei die sechs Koeffizienten  $a_i$  aus  $\mathbb{Z}$  sind. In Grad 3 erhalten wir somit die allgemeine Formel

$$a_1X^3 + a_2Y^3 + a_3X^2Y + a_4XY^2 + a_5X^2 + a_6Y^2 \\ + a_7XY + a_8X + a_9Y + a_{10} = 0.$$

Üblicherweise interessiert man sich nun für ganzzahlige oder rationale Lösungen solcher diophantischer Gleichungen. In diesem Abschnitt werden wir uns am meisten mit diophantischen Gleichungen in zwei Unbekannten beschäftigen.

Gibt es eine rationale Lösung einer diophantischen Gleichung, so gibt es natürlich auch eine reelle Lösung für diese Gleichung, d. h., gibt es keine reelle Lösung, so kann es auch keine rationale Lösung geben. Zum Beispiel hat die Gleichung  $X^2 + Y^2 + 1 = 0$  keine rationale Lösung, was man leicht überprüft, indem man zeigt, dass es keine reelle Lösung gibt. Eine Variante der obigen Fragestellung erhält man, indem man *homogene* diophantische Gleichungen in der projektiven Ebene  $\mathbb{P}_{\mathbb{Q}}^2$  betrachtet, d. h., man sucht die Nullstellenmenge von Polynomen  $f \in \mathbb{Q}[X, Y, Z]$ , wobei die Grade der einzelnen Monome alle gleich sind. In Grad 2 erhalten wir demnach die allgemeine Formel

$$a_1X^2 + a_2Y^2 + a_3XY + a_4XZ + a_5YZ + a_6Z^2 = 0$$

mit  $a_i \in \mathbb{Q}$ . Durch entsprechendes Durchmultiplizieren mit dem Hauptnenner der Koeffizienten  $a_i$  ändert sich

die Lösungsmenge nicht und man erhält stets ein Polynom aus  $\mathbb{Z}[X, Y, Z]$ . Ist ein Tripel  $(x_0, y_0, z_0)$  eine rationale Lösung eines solchen Polynoms  $f(X, Y, Z)$ , so ist auch jedes rationale Vielfache davon eine rationale Lösung. Die so erhaltenen Tripel interpretieren wir als eine projektive Lösung  $(x_0 : y_0 : z_0)$ . Den Nullvektor wollen wir dabei allerdings nicht als gültige Lösung akzeptieren. O.B.d.A. können wir also stets für eine projektive Lösung  $(x_0 : y_0 : z_0)$  annehmen, dass  $x_0, y_0, z_0 \in \mathbb{Z}$  und  $\text{ggT}(x_0, y_0, z_0) = 1$  gilt. Dies ermöglicht uns über eine Lösung modulo  $p^n$  zu sprechen, für eine Primzahl  $p$  und ein  $n \in \mathbb{N}$ .

Umgekehrt können wir auch die Gleichung  $f \equiv 0 \pmod{p^n}$  betrachten und nach Lösungen in  $\mathbb{Z}/p^n\mathbb{Z}$  fragen. Aus Hensels Lemma lässt sich folgern, dass es für jede Primzahl  $p$  ein berechenbares  $n_p \in \mathbb{N}$  gibt, so dass für jedes  $n \geq n_p$  gilt, dass wenn  $f = 0$  eine Lösung modulo  $p^n$  hat, dann hat  $f = 0$  auch eine Lösung modulo  $p^{n+1}$ . Dabei ist die ursprüngliche Lösung aus der späteren rekonstruierbar, indem man einfach wieder modulo  $p^n$  rechnet. Man sagt, dass die Lösungen *geliftet* werden können. Gibt es für eine feste Primzahl  $p$  ab  $n = 1$  eine ununterbrochene Kette solcher Hensel-Lifte, so nennen wir dies eine *p-adische Lösung* der Gleichung  $f = 0$ . Beschreibt die Gleichung  $f = 0$  überdies eine glatte Kurve in  $\mathbb{P}_{\mathbb{Q}}^2$ , so ist  $n_p = 1$ , für alle bis auf endlich viele Primzahlen  $p$ . Mit weiteren Mitteln der algebraischen Geometrie lässt sich zeigen, dass es eine untere Schranke  $m \in \mathbb{N}$  gibt, so dass für alle Primzahlen  $p > m$  gilt, dass  $f \equiv 0 \pmod{p}$  eine Lösung hat. Dieses  $m$  lässt sich effektiv bestimmen. Für fast alle Primzahlen  $p$  weiß man also im glatten Falle bereits *a priori*, dass es eine *p-adische Lösung* gibt. Und für die endlich vielen verbleibenden Primzahlen lässt sich die Existenz einer *p-adischen Lösung* durch die Kenntnis der  $n_p$  ebenfalls in endlicher Zeit auf einem Rechner überprüfen. Hat eine Gleichung eine reelle Lösung, sowie für jede Primzahl  $p$  eine *p-adische Lösung*, so sagen wir, sie habe *überall lokale Lösungen*.

Für eine diophantische Gleichung ist es eine notwendige Bedingung überall lokale Lösungen zu haben,

um eine tatsächliche Lösung (*globale Lösung*) zu haben. (Falls eine globale Lösung existiert, dann liefert diese Lösung modulo  $p^n$   $p$ -adische Lösungen.)

**Beispiel 1** (i) Sei  $f = X^2 + Y^2 + 5Z^2 \in \mathbb{Q}[X, Y, Z]$ . Es ist klar, dass  $(0, 0, k)$  eine Lösung von  $f \equiv 0 \pmod{5}$  ist, für  $k \in \mathbb{Z} \setminus \{0\}$ . Diese können wir jedoch nicht zu einer Lösung modulo  $5^2$  liften. Da man aus einem solchen Lift  $(x_0, y_0, z_0)$  die alte Lösung rekonstruieren können muss, folgt, dass  $x_0$  und  $y_0$  beide durch 5 teilbar sein müssen. Dies impliziert sofort, dass auch  $z_0$  durch 5 teilbar sein muss, um  $f(x_0, y_0, z_0) \equiv 0 \pmod{5^2}$  zu erhalten. Damit hätten wir  $\text{ggT}(x_0, y_0, z_0) = 5$ , bzw.  $k = 0$ , und somit einen Widerspruch. Die Lösung  $(1, 2, 2)$  modulo 5 lässt sich dagegen liften, z. B. zu  $(1, 2, 7)$  modulo  $5^2$ . Nun ist hier  $n_5 = 2$ , so dass mit Hensels Lemma gefolgert werden kann, dass es eine 5-adische Lösung gibt.

(ii) Sei  $f = X^2 + Y^2 + 7Z^2 \in \mathbb{Q}[X, Y, Z]$ . Man sieht schnell, dass für jede Lösung  $(x_0, y_0, z_0)$  modulo 7 gilt, dass  $x_0$  und  $y_0$  durch 7 teilbar sein müssen. Wie im ersten Beispiel bereits gesehen, können derartige Lösungen aber nicht geliftet werden. Da jede Lösung modulo  $7^2$  stets ein Lift irgendeiner Lösung modulo 7 ist, folgt sofort, dass es gar keine Lösung modulo  $7^2$  gibt und demnach auch keine 7-adische Lösung.

Das bereits erwähnte Hasse-Prinzip beschäftigt sich mit der Frage, inwieweit die Existenz von überall lokalen Lösungen ausreicht, um die Existenz einer globalen Lösung zu garantieren. Für Gleichungen vom Grad 2 ist dies tatsächlich so:

**Satz 2 (Hasse-Prinzip / Satz von Hasse-Minkowski)**

Sei  $f \in \mathbb{Q}[X, Y, Z]$  ein homogenes Polynom vom Grad 2 und die Gleichung  $f = 0$  habe überall eine lokale Lösung. Dann hat die Gleichung  $f = 0$  auch eine globale Lösung.

Falls man eine globale Lösung einer Gleichung vom Grad 2 kennt, so kann man damit relativ einfach alle weiteren globalen Lösungen finden.

## Selmer- und Tate-Shafarevich-Gruppen

Ist der Grad gleich 3, so gilt Hensels Lemma noch immer, jedoch das Hasse-Prinzip nicht mehr. Eines der ersten Gegenbeispiele wurde durch Selmer konstruiert: die Gleichung

$$3X^3 + 4Y^3 + 5Z^3 = 0$$

hat überall lokale Lösungen. Selmer bewies, dass sie aber keine globale Lösung hat. Man benötigt also eine andere Strategie als das Hasse-Prinzip, um für Gleichungen dritten Grades entscheiden zu können, ob sie rationale Lösungen haben. Und falls es eine globale Lösung gibt, dann sagt diese Lösung auch wenig über die weiteren Lösungen der Gleichung. (Man kann aus ihr zwar oft weitere globale Lösungen konstruieren, aber dies sind im Allgemeinen nicht alle Lösungen.)

Wir beschäftigen uns nun mit dem Bestimmen aller globalen Lösungen einer diophantischen Gleichung

vom Grad 3, wenn man schon mindestens eine Lösung gefunden hat. Dazu macht man sich eine wichtige geometrische Eigenschaft zu Nutze. Derartige Gleichungen beschreiben nämlich eine Kurve in der projektiven Ebene, welche eine sogenannte elliptische Kurve  $E$  über  $\mathbb{Q}$  ist. Entscheidend ist, dass die rationalen Punkte von  $E$ , im Zeichen  $E(\mathbb{Q})$ , eine abelsche Gruppe bilden, und jede elliptische Kurve  $E/\mathbb{Q}$  lässt sich affin als folgende Weierstraß-Gleichung schreiben

$$E: Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6,$$

mit  $a_i \in \mathbb{Q}$ . In diesem affinen Modell fehlt genau ein Punkt im Unendlichen  $(0 : 1 : 0)$ , welcher der neutrale Punkt des Gruppengesetzes ist. Eine Gerade schneidet  $E$  in genau drei Punkten (mit Vielfachheit) und die Addition ist so definiert, dass die Summe solcher dreier Schnittpunkte gleich dem neutralen Punkt ist. Da wir auf  $E(\mathbb{Q})$  addieren können, gibt es also für jedes  $n \in \mathbb{N}$  eine natürliche Multiplikation-mit- $n$ -Abbildung. Nach dem Satz von Mordell-Weil ist  $E(\mathbb{Q})$  als Gruppe endlich erzeugt, somit ist der Kokern  $E(\mathbb{Q})/nE(\mathbb{Q})$  endlich. Überdies ist bei elliptischen Kurven  $E/\mathbb{Q}$  der Torsionsanteil von  $E(\mathbb{Q})$  leicht zu berechnen. Um  $E(\mathbb{Q})$  als abstrakte Gruppe zu kennen, reicht es somit aus, für ein beliebiges  $n \geq 2$  den Kokern  $E(\mathbb{Q})/nE(\mathbb{Q})$  zu bestimmen.

Folgender traditioneller Ansatz wurde für diesen Zweck versucht. Der Kokern  $E(\mathbb{Q})/nE(\mathbb{Q})$  lässt sich in die sogenannte  $n$ -Selmer-Gruppe  $\text{Sel}^{(n)}(E/\mathbb{Q})$  einbetten. Es führt hier zu weit diese Gruppe zu definieren, jedoch weiß man, dass sie endlich ist, und ihre Ordnung ist berechenbar. Die Elemente der  $n$ -Selmer-Gruppe korrespondieren mit Kurven  $C/\mathbb{Q}$ , die über einer Körpererweiterung isomorph zu  $E$  sind (sogenannte Twists von  $E$ ), und die überall lokale Punkte haben. Außerdem gilt, dass das Bild von  $E(\mathbb{Q})/nE(\mathbb{Q})$  in  $\text{Sel}^{(n)}(E/\mathbb{Q})$  genau denjenigen Kurven  $C/\mathbb{Q}$  entspricht, die mindestens einen rationalen Punkt haben. Diese Kurven erfüllen also das Hasse-Prinzip, da sie überall lokale Lösungen haben und auch eine globale Lösung. Die Einbettung von  $E(\mathbb{Q})/nE(\mathbb{Q})$  in die  $n$ -Selmer-Gruppe ist im Allgemeinen nicht surjektiv. Die Abweichung zur Surjektivität misst die sogenannte Tate-Shafarevich-Gruppe  $\text{III}(E/\mathbb{Q})$ . Die Elemente der Tate-Shafarevich-Gruppe entsprechen also den Twists aus der Selmer-Gruppe, die das Hasse-Prinzip nicht erfüllen. Es ist bekannt, dass  $\text{III}(E/\mathbb{Q})$  eine abelsche Torsionsgruppe ist, d. h., jedes Element hat endliche Ordnung. Die  $n$ -Torsion von  $\text{III}(E/\mathbb{Q})$ , im Zeichen  $\text{III}(E/\mathbb{Q})[n]$ , ist eine endliche Gruppe und ist mittels der folgenden kurzen exakten Sequenz definiert

$$\begin{aligned} 0 \rightarrow E(\mathbb{Q})/nE(\mathbb{Q}) &\rightarrow \text{Sel}^{(n)}(E/\mathbb{Q}) \\ &\rightarrow \text{III}(E/\mathbb{Q})[n] \rightarrow 0. \end{aligned}$$

Insgesamt ist über die Tate-Shafarevich-Gruppe wenig bekannt und es gibt keinen Algorithmus, um sie zu berechnen. Dies entspricht ja auch der eingangs gestellten Frage, festzustellen, ob eine Gleichung dritten Grades einen rationalen Punkt hat. Dies ist auch heute noch ein offenes Problem. Häufig kann jedoch



die Gruppenstruktur von  $E(\mathbb{Q})$  trotzdem bestimmt werden, indem man mit Hilfe eines Rechners endlich viele Punkte  $P_1, \dots, P_k$  findet, und zeigt, dass für eine natürliche Zahl  $n$  deren Bilder in  $\text{Sel}^{(n)}$  die ganze  $n$ -Selmer-Gruppe erzeugen. Es wird vermutet, dass die Tate-Shafarevich-Gruppe eine endliche Gruppe ist. Damit wäre  $\text{III}(E/\mathbb{Q})[p]$  bis auf endlich viele Primzahlen  $p$  trivial und somit  $E(\mathbb{Q})/nE(\mathbb{Q})$  fast immer identisch zur  $n$ -Selmer-Gruppe. Basierend auf dieser Vermutung kann mit dem soeben beschriebenen Verfahren die Gruppenstruktur von  $E(\mathbb{Q})$  bestimmt werden, indem für hinreichend viele  $n$  die  $n$ -Selmer-Gruppe bestimmt wird und lange genug nach Punkten gesucht wird.

Eines der bekannten Ergebnisse über die Tate-Shafarevich-Gruppe ist, dass, die Ordnung von  $\#\text{III}(E/\mathbb{Q})$ , wenn  $\text{III}(E/\mathbb{Q})$  endlich ist, immer eine Quadratzahl ist. Dies beweist man mit Hilfe einer Paarung auf  $\text{III}(E/\mathbb{Q})$ .

## Abelsche Varietäten

Wir betrachten nun die höherdimensionalen Verallgemeinerungen von elliptischen Kurven, die sogenannten *abelschen Varietäten*. Die genaue Definition ist ziemlich technisch, jedoch ist im Wesentlichen eine abelsche Varietät eine glatte projektive Varietät  $A$  (d. h. eine (glatte) Nullstellenmenge von endlich vielen homogenen Polynomen), so dass auf  $A$  eine Gruppenstruktur auf algebraische Weise definiert werden kann.

Im eindimensionalen Fall sind dies genau die elliptischen Kurven. Man erhält sofort Beispiele von  $n$ -dimensionalen abelschen Varietäten, indem man das Produkt von  $n$  elliptischen Kurven betrachtet. Zwei elliptische Kurven  $E_1$  und  $E_2$  ‘spannen’ also eine abelsche Fläche  $E_1 \times E_2$  auf. Die natürlichen Abbildungen zwischen projektiven Varietäten sind rationale Funktionen. Eine solche Abbildung zwischen zwei abelschen Varietäten gleicher Dimension, die gleichzeitig ein Gruppenhomomorphismus ist und einen endlichen Kern hat, nennen wir eine *Isogenie*. Die Definitionen der Selmer- und Tate-Shafarevich-Gruppe lassen sich für abelsche Varietäten beliebiger Dimension verallgemeinern.

Eine konkrete Bestimmung der Tate-Shafarevich-Gruppe ist, wie im Falle der elliptischen Kurven, nur in wenigen Einzelfällen möglich. Anders als im Fall der elliptischen Kurven kann jetzt die Ordnung der Tate-Shafarevich-Gruppe auch eine Nicht-Quadratzahl sein. Fälschlicherweise wurde jedoch für über 30 Jahre angenommen, dass  $\#\text{III}(A/\mathbb{Q})$  immer ein Quadrat ist (sofern endlich). Erst Ende der 1990er Jahren wurde das erste Beispiel einer endlichen Tate-Shafarevich-Gruppe mit nicht-quadratischer Ordnung gefunden [4]. Es handelt sich dabei um eine abelsche Fläche  $B/\mathbb{Q}$  mit  $\#\text{III}(B/\mathbb{Q}) = 2\Box$ , wobei wir mit  $\Box$  eine passende Quadratzahl meinen. Etwas später wurde ein Beispiel einer abelschen Fläche  $B/\mathbb{Q}$  gefunden mit  $\#\text{III}(B/\mathbb{Q}) = 3\Box$ , sowie andere Beispiele in höheren Dimensionen. Wir werden nun beschreiben, wie man mit Hilfe der Computeralgebra viele Beispiele von abelschen Flächen

konstruieren kann, deren Tate-Shafarevich-Gruppe als Ordnung keine Quadratzahl hat.

## Abelsche Flächen $B/\mathbb{Q}$ mit $\#\text{III}(B/\mathbb{Q}) = 5\Box$

Nicht nur bei der Bestimmung der rationalen Punkte einer abelschen Varietät spielt die Tate-Shafarevich-Gruppe eine entscheidende Rolle, sondern auch in einem der sieben Millennium-Probleme, der sogenannten *Vermutung von Birch und Swinnerton-Dyer* aus den 1960er Jahren. Auf die Kernaussage dieser bedeutenden Vermutung werden wir später noch eingehen. Zunächst sei erwähnt, dass Cassels und Tate bewiesen haben, dass diese Vermutung invariant unter Isogenien ist, das heißt, es ist bekannt, dass wenn sie für eine abelsche Varietät  $A$  zutrifft, so gilt sie auch für jede zu  $A$  isogene abelsche Varietät  $B$ . Dazu bewiesen Cassels und Tate eine Gleichung, in der viele wichtige Invarianten zweier isogener abelscher Varietäten zueinander in Beziehung gestellt werden. Diese Invarianten sind der Regulator  $R$ , die Periode  $P$ , die duale abelsche Varietät  $A^\vee$ , der Torsionsanteil  $A(\mathbb{Q})_{\text{tors}}$  der rationalen Punkte und für jede Primzahl  $p$  die lokale Tamagawazahl  $c_p$ . Das Produkt im nachstehenden Satz ist wohldefiniert, da  $c_p = 1$  gilt, für alle bis auf endlich viele Primzahlen.

**Satz 3 (Gleichung von Cassels und Tate) [1] [5]** Sei  $\varphi : A \rightarrow B$  eine Isogenie zwischen zwei abelschen Varietäten  $A$  und  $B$  über  $\mathbb{Q}$ . Sind  $\text{III}(A/\mathbb{Q})$  und  $\text{III}(B/\mathbb{Q})$  endlich, so lässt sich der Quotient der Ordnungen der Tate-Shafarevich-Gruppen  $\frac{\#\text{III}(A/\mathbb{Q})}{\#\text{III}(B/\mathbb{Q})}$  wie folgt berechnen:

$$\frac{R_B}{R_A} \cdot \frac{\#A(\mathbb{Q})_{\text{tors}} \#A^\vee(\mathbb{Q})_{\text{tors}}}{\#B(\mathbb{Q})_{\text{tors}} \#B^\vee(\mathbb{Q})_{\text{tors}}} \cdot \frac{P_B}{P_A} \cdot \prod_{p \text{ prim}} \frac{c_{B,p}}{c_{A,p}} \quad (1)$$

Wir haben diese Gleichung benutzt, um Beispiele von abelschen Flächen mit Tate-Shafarevich-Gruppe der Ordnung 5 mal ein Quadrat zu konstruieren. Seien dazu  $E_1$  und  $E_2$  zwei elliptische Kurven über  $\mathbb{Q}$ , die einen rationalen Torsionspunkt der Ordnung 5 haben; nennen wir diesen  $P_1$  bzw.  $P_2$ . Nun bilden wir das Produkt dieser beiden elliptischen Kurven, d. h., wir erhalten eine abelsche Fläche und betrachten die folgende Isogenie

$$\varphi : E_1 \times E_2 \rightarrow B,$$

wobei der Kern von  $\varphi$  von dem Punkt  $(P_1, P_2)$  erzeugt wird, dass heißt, er ist eine zyklische Gruppe der Ordnung 5. Die abelsche Fläche  $B/\mathbb{Q}$  ist also der Quotient  $(E_1 \times E_2)/\langle (P_1, P_2) \rangle$ . Da die Tate-Shafarevich-Gruppe eines Produktes das Produkt der beiden Tate-Shafarevich-Gruppen ist, erhalten wir dass

$$\#\text{III}(E_1 \times E_2) = \#\text{III}(E_1) \cdot \#\text{III}(E_2) = \Box,$$

sofern die Kardinalitäten endlich sind, was wir ab jetzt immer annehmen wollen. Desweiteren ist der Grad der Isogenie  $\varphi$  gleich 5, weswegen sich die Ordnung von  $\text{III}(B/\mathbb{Q})$  nur um eine 5-Potenz von der von  $\text{III}(E_1 \times E_2)$  unterscheiden kann. Somit wissen wir *a priori*, dass

$\#III(B/\mathbb{Q}) = \square$  oder  $5\square$  ist. Um dies konkret entscheiden zu können, reicht es also (1) modulo Quadraten zu bestimmen. Dazu zerlegen wir dieses Produkt erneut in zwei Teile, und zwar in den Regulator- und Torsionsquotienten

$$\frac{R_B}{R_A} \cdot \frac{\#A(\mathbb{Q})_{\text{tors}} \#A^\vee(\mathbb{Q})_{\text{tors}}}{\#B(\mathbb{Q})_{\text{tors}} \#B^\vee(\mathbb{Q})_{\text{tors}}},$$

welches wir den *globalen Quotienten* nennen, und in den Perioden- und Tamagawazahlenquotienten

$$\frac{P_B}{P_A} \cdot \prod_{p \text{ prim}} \frac{c_{B,p}}{c_{A,p}},$$

welches wir den *lokalen Quotienten* nennen. Nun nutzen wir die Tatsache, dass sich alle elliptischen Kurven  $E/\mathbb{Q}$ , die einen rationalen 5-Torsionspunkt haben, mittels einer rationalen Zahl  $d \in \mathbb{Q} \setminus \{0\}$  parametrisieren lassen. Diese elliptischen Kurven entsprechen nämlich genau den Weierstraß-Gleichungen

$$E : Y^2 + (d+1)XY + dY = X^3 + dX^2.$$

Wir identifizieren also unser Produkt  $E_1 \times E_2$  mit dem Paar  $(d_1, d_2)$ , wobei wir wiederum  $d_i = u_i/v_i$  als Quotient zweier ganzer, teilerfremder Zahlen  $u_i, v_i \in \mathbb{Z}$  schreiben. Der lokale Quotient und auch der Torsionsquotient lassen sich nun sehr einfach aus der Primfaktorzerlegung der  $u_i$  und  $v_i$  und aus dem Verhalten der  $d_i$  modulo 5-ter Potenzen bestimmen. Dafür definieren wir für alle Primzahlen  $p$  eine rationale Zahl  $\text{lokal}_p$ . Gilt  $p \mid u_1 v_1 u_2 v_2$ , so ist  $\text{lokal}_p = 1/5$ . Falls  $p \equiv 1(5)$  ist und  $p$  ist ein Teiler von  $\text{ggT}(u_1^2 + 11u_1 v_1 - v_1^2, u_2^2 + 11u_2 v_2 - v_2^2)$  dann ist  $\text{lokal}_p$  gleich 5. Falls  $p = 5$  und 25 teilt  $u_1 - 7v_1 \equiv u_2 - 7v_2$  dann ist  $\text{lokal}_5$  gleich 5. Für die übrigen Fälle gilt  $\text{lokal}_p = 1$ .

**Satz 4** [2, Thm. 4.3] *Der lokale Quotient lässt sich als folgendes endliches Produkt berechnen:*

$$\frac{1}{5} \cdot \prod_{p \text{ prim}} \text{lokal}_p.$$

Der Torsionsquotient lässt sich ebenso sehr einfach bestimmen.

**Satz 5** [2, Prop. 4.6] *Der Torsionsquotient hat den Wert*

$$\begin{cases} 1 \text{ oder } 5, & d_1, d_2 \in \mathbb{Q}^{*5}, \\ 5^2, & d_i \in \mathbb{Q}^{*5}, d_j \notin \mathbb{Q}^{*5}, i \neq j, \\ 5^2, & \langle 1 \rangle \neq \langle d_1 \rangle = \langle d_2 \rangle \neq \langle 1 \rangle \text{ in } \mathbb{Q}^*/\mathbb{Q}^{*5}, \\ 5^3, & \langle 1 \rangle \neq \langle d_1 \rangle \neq \langle d_2 \rangle \neq \langle 1 \rangle \text{ in } \mathbb{Q}^*/\mathbb{Q}^{*5}. \end{cases}$$

Der Einfachheit halber haben wir im Torsionsquotienten den Fall, dass beide  $d_i$  5-te Potenzen sind, nicht weiter spezifiziert.

**Beispiel 6** Seien  $E_1/\mathbb{Q}$  und  $E_2/\mathbb{Q}$  gegeben durch  $d_1 = u_1/v_1 = 1/11$  und  $d_2 = u_2/v_2 = 2/9$ . Mit den obigen

Sätzen rechnet man leicht nach, dass der lokale Quotient  $1/5^4$  ist: Für die drei Primzahlen  $p = 2, 3, 11$  gilt  $\text{lokal}_p = 1/5$  und für alle anderen Primzahlen gilt  $\text{lokal}_p = 1$ . Der Torsionsquotient ist gleich  $5^3$ . Mit dem Computer bestimmt man nun den sogenannten analytischen Rang der beiden elliptischen Kurven, welcher in beiden Fällen gleich 0 ist. Dies impliziert sofort, dass der Regulatorquotient gleich 1 ist. Außerdem ist dies einer der wenigen bewiesenen Fälle, bei denen wir wissen, dass die Tate-Shafarevich-Gruppen endlich sind. Wir erhalten also vollkommen unconditionell die Gleichung

$$\#III(B) = 5 \cdot \#III(E_1 \times E_2) = 5\square.$$

## Regulatorquotient & Computer-Algebra

Es bleibt somit noch übrig den Regulatorquotienten  $R_B/R_{E_1 \times E_2}$  zu berechnen. Für diesen Quotienten gibt es nach unseren Kenntnissen keine einfache Formel, wie für die anderen beiden Quotienten. Wir können allerdings einen Algorithmus angeben, mit welchem er in vielen Fällen mit Hilfe des Computers berechnet werden kann. Dazu müssen wir zunächst die Gruppen  $E_1(\mathbb{Q})$  und  $E_2(\mathbb{Q})$  bestimmen. Eine Möglichkeit wäre es hier für geeignete  $n$ , die  $n$ -Selmer-Gruppen zu bestimmen und hinreichend viele Punkte auf  $E_1(\mathbb{Q})$  zu finden, wie wir oben bereits erwähnt haben. In vielen Fällen kann man dies jedoch umgehen, indem man entweder bewiesene Fälle der Birch und Swinnerton-Dyer-Vermutung ausnutzt oder diese Vermutung annimmt. Da  $E(\mathbb{Q})$  eine endlich erzeugte Gruppe ist, gilt abstrakt  $E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus E(\mathbb{Q})_{\text{tors}}$ , für eine nicht-negative ganze Zahl  $r$ , genannt der *Mordell-Weil-Rang* von  $E/\mathbb{Q}$ . Die Kernaussage der Birch und Swinnerton-Dyer-Vermutung betrifft den analytischen Rang und besagt, dass dieser gleich dem Mordell-Weil-Rang ist. Es ist bewiesen, dass wenn der analytische Rang gleich 0 oder 1 ist, dann gleicht er tatsächlich dem Mordell-Weil-Rang. In diesem Fall weiß man zudem noch, dass die Tate-Shafarevich-Gruppe endlich ist.

Dieser analytische Rang ist die Ordnung einer Nullstelle einer holomorphen Funktion. Falls diese Ordnung höchstens drei ist (was für die meisten Beispiele gilt), so kann man diesen analytischen Rang vergleichsweise einfach und schnell (auf einem Rechner) bestimmen.

Ist der analytische Rang 0, so weiß man, dass  $E(\mathbb{Q})$  endlich ist. Falls der analytische Rang 1 ist, dann braucht unser Algorithmus einen einzigen beliebigen Punkt unendlicher Ordnung. Solch einen Punkt zu finden ist allerdings keine triviale Aufgabe, denn die Zähler und Nenner der Koeffizienten dieser Punkte können sehr groß werden. Nimmt man z. B. die elliptische Kurve mit  $d = 83/74$ , welche analytischen Rang 1 hat, so dauert es sehr lange den ersten Punkt unendlicher Ordnung zu finden, wenn man systematisch alle rationalen  $X$ -Werte durchläuft und prüft ob es da zu einen rationalen  $Y$ -Wert gibt. Der 'kleinste'  $X$ -Wert

dieses Beispiels hat einen negativen Zähler mit 44 Ziffern und einen Nenner mit 40 Ziffern. Das Berechnen von Selmer-Gruppen stellt sich hier zusätzlich als sehr hilfreich heraus, da man mit deren Kenntnis auch den Punktesuch-Algorithmus deutlich beschleunigen kann. Im Falle dass der Rang gleich 1 ist, kann auch mit der Theorie der Heegner-Punkte auf einem Computer ein Punkt unendlicher Ordnung auf der elliptischen Kurve gefunden werden.

Falls der analytische Rang größer als eins ist, dann ist die Birch und Swinnerton-Dyer-Vermutung noch offen. Für diese Kurven nehmen wir stets an, dass der analytische Rang mit dem Mordell-Weil-Rang übereinstimmt.

Hat man nun eine ‘Basis’ von  $E_1(\mathbb{Q})$  und  $E_2(\mathbb{Q})$  bestimmt, so kann daraus der Regulatorquotient  $R_B/R_{E_1 \times E_2}$  berechnet werden. Falls beide Gruppen endlich sind, so ist der Regulatorquotient gleich 1. Sonst benutzt man die Erzeuger von  $E_i(\mathbb{Q})$  (modulo Torsionspunkten) um endlich viele Zahlen in  $\mathbb{Q}^*/\mathbb{Q}^{*5}$  und in  $\mathbb{Q}(\mu_5)^*/\mathbb{Q}(\mu_5)^{*5}$  zu bestimmen. Dann muss man die Ordnung der durch diese Zahlen erzeugten Untergruppen bestimmen. Nun kann man mit Hilfe der Theorie abelscher Varietäten zeigen, dass der Regulatorquotient genau dann ein Quadrat ist, wenn das Produkt dieser Ordnungen ein Quadrat ist.

---

## Ergebnisse

---

Das oben beschriebene Verfahren haben wir auf alle Paare von elliptischen Kurven  $E_1$  und  $E_2$  angewendet, für deren Parameter  $d_1$  und  $d_2$  die Zähler und Nenner betragsmäßig durch 100 beschränkt sind. Daraus resultierten ungefähr 18,5 Millionen abelsche Flächen, wovon 49,31% eine Tate-Shafarevich-Gruppe mit

Ordnung  $5\Box$  haben. Jedoch ist dieses Ergebnis bedingt durch Annahme der Birch und Swinnerton-Dyer-Vermutung.

Betrachtet man davon nur die abelschen Flächen, so dass beide zugehörigen elliptischen Kurven analytischen Rang 0 oder 1 haben, (d. h., die Birch und Swinnerton-Dyer-Vermutung ist schon bewiesen für  $E_1$  und  $E_2$ ), so ergibt dies 14,7 Millionen abelsche Flächen von denen 49,95% eine Tate-Shafarevich-Gruppe mit Ordnung  $5\Box$  haben [3].

Insbesondere zeigt dies, dass man häufig in der Lage ist, zu unterscheiden, ob die Ordnung der Tate-Shafarevich-Gruppe ein Nicht-Quadrat ist, ohne deren Ordnung selbst zu berechnen.

## Literatur

- [1] Cassels, J. W. S. Arithmetic on curves of genus 1. VIII. On conjectures of Birch and Swinnerton-Dyer. *J. Reine Angew. Math.*, 217:180–199, 1965.
- [2] Keil, Stefan. Examples of abelian varieties with non-square Tate-Shafarevich group. Preprint 2012, *arXiv:1206.1822v1*.
- [3] Keil, Stefan and Kloosterman, Remke N. On the density of abelian surfaces with Tate-Shafarevich group of order five times a square. Erscheint in: *Algorithmic number theory, 10th international symposium, ANTS-X Proceedings*, 2013.
- [4] Poonen, Bjorn and Stoll, Michael. The Cassels-Tate pairing on polarized abelian varieties. *Ann. of Math.* (2), 150:1109–1149, 1999.
- [5] Tate, John. On the conjectures of Birch and Swinnerton-Dyer and a geometric analog. *Séminaire Bourbaki*, Vol. 9, 9:415–4401, 1995.

# Neuer Primzahlrekord

**J. Klüners**  
(Universität Paderborn)

klueners@math.uni-paderborn.de

Am 12. Februar 2013 hat Spiegel-Online<sup>1</sup> gemeldet, dass eine neue Rekord-Primzahl gefunden wurde. Die gefundene Primzahl ist  $2^{57.885.161} - 1$  und hat ausgeschrieben 17.425.170 Stellen. Damit ist sie die bisher größte bekannte Primzahl.

Die Primeigenschaft dieser Zahl wurde am 25. Januar 2013 mit Hilfe einer 39-tägigen Berechnung auf einem PC bewiesen. Bei sehr großen Zahlen ist es selbst für einen Computer schwierig zu beweisen, dass eine gegebene Zahl eine Primzahl ist. Für Zahlen von spezieller Form gibt es deutlich effizientere Algorithmen, welche einen Nachweis der Primeigenschaft erst ermöglichen. Daher ist es keine Überraschung, dass diese größte bekannte Primzahl eine sogenannte Mersenne-Primzahl ist, d. h. eine Primzahl der Form  $2^p - 1$ , wobei  $p$  selbst auch eine Primzahl sein muss. Dies ist aber nicht hinreichend, da z. B.  $2^{11} - 1 = 23 \cdot 89$  keine Primzahl ist. In vergangenen Rundbriefen [1, 2] und dem Sonderheft [3] zum Jahr der Mathematik wurde schon ausführlich über dieses Thema und die zugehörige Theorie berichtet.

Eine interessante Informationsquelle ist die Homepage<sup>2</sup> des Great Internet Mersenne Prime Search-Projekts (GIMPS). Dort kann man nachlesen, dass bisher die kleinsten 42 Mersenne-Primzahlen sowie sechs weitere bekannt sind. Die vorletzte gefundene Mersenne-Primzahl wurde übrigens 2009 gefunden, dafür wurde aber im Dezember 2012 gezeigt, dass die kleinsten 42 bekannt sind.

## Literatur

- [1] H.-M. Elvenich  $2^{37.156.667} - 1$  ist eine Primzahl. *Computeralgebra-Rundbrief*, 45:12–13, Oktober 2009.
- [2] G. M. Ziegler Primzahl-Rekordjagd. *Computeralgebra-Rundbrief*, 34:11–12, März 2004.
- [3] G. M. Ziegler Primzahltests und Primzahlrekorde. *Sonderheft, Computeralgebra-Rundbrief*, 29–31, April 2008.

$2^2 - 1$	$2^{521} - 1$	$2^{21.701} - 1$	$2^{3.021.377} - 1$
$2^3 - 1$	$2^{607} - 1$	$2^{23.209} - 1$	$2^{6.972.593} - 1$
$2^5 - 1$	$2^{1.279} - 1$	$2^{44.497} - 1$	$2^{13.466.917} - 1$
$2^7 - 1$	$2^{2.203} - 1$	$2^{86.243} - 1$	$2^{20.996.011} - 1$
$2^{13} - 1$	$2^{2.281} - 1$	$2^{110.503} - 1$	$2^{24.036.583} - 1$
$2^{17} - 1$	$2^{3.217} - 1$	$2^{132.049} - 1$	$2^{25.964.951} - 1$
$2^{19} - 1$	$2^{4.253} - 1$	$2^{216.091} - 1$	$2^{30.402.457} - 1$
$2^{31} - 1$	$2^{4.423} - 1$	$2^{756.839} - 1$	$2^{32.582.657} - 1$
$2^{61} - 1$	$2^{9.689} - 1$	$2^{859.433} - 1$	$2^{37.156.667} - 1$
$2^{89} - 1$	$2^{9.941} - 1$	$2^{1.257.787} - 1$	$2^{42.643.801} - 1$
$2^{107} - 1$	$2^{11.213} - 1$	$2^{1.398.269} - 1$	$2^{43.112.609} - 1$
$2^{127} - 1$	$2^{19.937} - 1$	$2^{2.976.221} - 1$	$2^{57.885.161} - 1$

*Die bisher bekannten Mersenne-Primzahlen.*

<sup>1</sup><http://www.spiegel.de/wissenschaft/mensch/17-4-millionen-stellen-computer-entdeckt-rekord-mersenne-primzahl-a-882646.html>

<sup>2</sup><http://www.mersenne.org/>

### Torische Geometrie mit `polymake`

M. Joswig, A. Paffenholz  
(TU Darmstadt, Fachbereich Mathematik,  
Dolivostr. 15, 64293 Darmstadt, Germany)

`joswig@mathematik.tu-darmstadt.de`  
`paffenholz@mathematik.tu-darmstadt.de`



---

### Einführung

---

`polymake` ist Software für ein weites Spektrum von Anwendungen in kombinatorischer Geometrie und benachbarten Gebieten. Der Schwerpunkt liegt auf der Polyedertheorie. Andere Aspekte betreffen Graphen und Matroide, lineare und kombinatorische Optimierung, kombinatorische und algebraische Topologie sowie torische und tropische Geometrie. Zielsetzung und Organisation folgen grundsätzlich immer noch den in [9] und [12] dargelegten Prinzipien, jedoch ist die Funktionalität seitdem in technischer und mathematischer Hinsicht erheblich erweitert worden. Der Zweck dieses Textes ist es, einen Einblick in die aktuelle Entwicklung zu geben. Diese profitiert maßgeblich von der Kooperation innerhalb des DFG-Schwerpunktprogramms 1489 „Algorithmic and Experimental Methods in Algebra, Geometry and Number Theory“, vgl. [8].

`polymake` ist quelloffen und wird unter der GNU Public License auf der Webseite

[www.polymake.org](http://www.polymake.org)

vertrieben. Das letzte `polymake`-Release 2.12 wurde im März 2012 veröffentlicht. Es kann auf Unix/Linux- und Mac OS-basierten Systemen kompiliert werden. Um Interessierten den Zugang zur aktuellen Entwicklung zu ermöglichen, kann seit Januar 2013 ein direkter Abzug aus unserem Subversion-Repository bezogen werden.

---

### Interfaces

---

Wie viele Computeralgebra-Systeme besitzt auch `polymake` ein interaktives Shell-basiertes Interface. Als Eingabesprache kommt ein Perl-Dialekt zum Einsatz. Die Algorithmen sind überwiegend in Perl und C++ implementiert. So lassen sich die Vorteile einer interpretierten Sprache mit denen einer kompilierten kombinieren. Für die Visualisierung wird in erster Linie

`jreality` [13] über dessen Java-API verwendet; siehe hierzu [10].

Zusätzlich zu zahlreichen direkt in `polymake` implementierten Verfahren spielen Interfaces zu anderen Systemen eine wichtige Rolle. In jüngster Zeit hinzugekommen sind ein bidirektionales Interface zu `Singular` [4], ein Interface von `GAP` [7], das ebenfalls bidirektional ausgebaut werden soll, sowie Interfaces von `polymake` zu `normaliz` [2], `bliss` [14], `Gfan` [11], `permlib` und `sympol` [20]. Seit der Version 2.12 existiert `polymake` auch in einer Version als C++-Bibliothek, das zugehörige API wird von `GAP` und `Singular` verwendet.

---

### Regeln und Erweiterungen

---

Grundsätzlich erfolgt die Kommunikation zwischen Benutzer und System regelbasiert. Typische Objekte wie etwa ein konvexes Polytop, sind auf der höchsten Abstraktionsebene innerhalb `polymake` als Listen von *Eigenschaften* (*properties*) codiert. Zu jedem Zeitpunkt sind einige bekannt, andere noch nicht, und eine Menge von *Regeln* (*rules*) legt fest, aus welchen Kombinationen bekannter Eigenschaften neue ausgerechnet werden können. Der zentrale *Scheduler* legt fest, in welcher Reihenfolge Regeln ausgeführt werden, um eine Benutzeranfrage zu befriedigen. Der Benutzer kann das Verhalten des Schedulers durch verschiedene Mechanismen beeinflussen und die gesamte Regelbasis modifizieren.

Die Regelbasis ist auf zweierlei Weise modularisiert. Einerseits sind Objekte und zugehörige Regeln in *Anwendungen* (*applications*) organisiert, die sich im weitesten Sinn ähnlich wie *name spaces* verhalten. Die wichtigsten Standardanwendungen sind derzeit `polytope` (für konvexe Polyeder), `fan` (für polyedrische Fächer und Komplexe) und `topaz` (für Topologie). Andererseits existiert ein hierzu orthogonales Konzept von *Erweiterungen* (*extensions*). Eine Erweiterung kann zu einer oder mehreren bestehenden Anwendungen neue Objekte oder neue Regeln hinzufügen. Alternativ kann eine Erweiterung auch eine vollständige neue

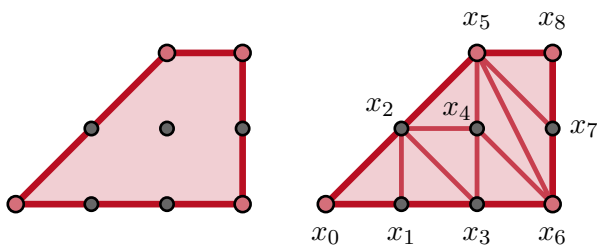
Anwendung begründen mit gänzlich eigenen Objekten und Regeln.

Die aktuelle SVN-Version macht bereits in der zentralen Codebasis vom Erweiterungskonzept Gebrauch. Für das Rechnen mit Graphenautomorphismen stehen beispielsweise Interfaces zu `nauty` [17] und `bliss` bereit, die sich alternativ konfigurieren lassen. Das Interface von `polymake` zu `Singular` ist ebenfalls in eine Erweiterung ausgelagert, die nicht zwingend konfiguriert werden muss, so dass es möglich bleibt, `polymake` auch ohne `Singular` zu nutzen; allerdings fehlt dann ein Teil der Funktionalität. Erweiterungen innerhalb der `polymake`-Distribution werden *bundled extensions* genannt.

## Beispiel: Hirzebruchflächen

Wir wollen die Benutzung von `polymake` an zwei einfachen Beispielen aus der algebraischen Geometrie demonstrieren. Eine *projektive torische Varietät*  $X$  korrespondiert zu einem *vollständigen rationalen polyedrischen Fächer*  $\Sigma_X$ , also einer Familie rationaler polyedrischer Kegel, die sich paarweise in Seiten schneiden und den gesamten Raum überdecken; für einen Überblick siehe [3]. Besonders wichtig ist die folgende Konstruktion. Es sei  $P$  ein *Gitterpolytop*, das heißt, die konvexe Hülle endlich vieler ganzzahliger Punkte in  $\mathbb{R}^d$ . Für jede Seite  $F$  von  $P$  ist der zugehörige *Normalenkegel* die Menge derjenigen linearen Funktionale, die auf  $F$  ihren Maximalwert annehmen. Die Menge aller Normalenkegel bildet den *Normalenfächer* und hierdurch eine projektive torische Varietät. In `polymake` sind die relevanten Methoden auf die beiden Anwendungen `polytope` und `fan` verteilt.

In unserem ersten Beispiel wollen wir *Hirzebruch-Flächen* betrachten. Die Hirzebruchfläche  $\mathcal{H}_a$  für ein  $a \in \mathbb{Z}_{\geq 0}$  ist eine 2-dimensionale projektive torische Varietät. Der Fläche  $\mathcal{H}_a$  ist der Fächer  $\Sigma_a$  mit den durch  $(-1, 0)$ ,  $(0, 1)$ ,  $(1, -a)$ , und  $(0, -1)$  erzeugten Strahlen zugeordnet. Bestimmte Gitterpolytope  $H_a$  mit diesem Normalenfächer erzeugen eine Einbettung von  $\mathcal{H}_a$  in den projektiven Raum  $\mathbb{CP}^{n-1}$ , wobei  $n = \#(H_a \cap \mathbb{Z}^2)$  die Anzahl der Gitterpunkte des Polytops ist. Ein geeignetes Gitterpolytop ist in Abbildung 1 links dargestellt. Das *Stanley-Reisner-Ideal* einer regulären und unimodularen Triangulierung ergibt ein Erzeugendensystem des Initialideals des definierenden Ideals der Varietät [21].



**Abbildung 1:** Links: Gitterpolytop  $H$ , dessen Normalenfächer die Hirzebruchfläche  $\mathcal{H}_1$  liefert. Rechts: unimodulare Triangulierung.

Wir wollen dieses Ideal mit `polymake` bestimmen. Nach dem Aufruf in einem Terminal erhalten wir den `polymake`-prompt zur Anwendung `polytope`, die als Standard eingestellt ist.

```
polytope> $V=new Matrix<Rational>([
  [1,0,1],[1,1,1],[1,1,-1],[1,-2,-1]]);
polytope> $H=new Polytope<Rational>(POINTS=>$V);
polytope> print $H->FACETS
1 1 -1
1 0 1
1 -1 0
1 0 -1
```

Wir haben das Polytop  $\$H$  als konvexe Hülle der vier Punkte

$$(0,1) \quad (1,1) \quad (1,-1) \quad (-2,-1)$$

definiert und uns die irredundante Ungleichungsbeschreibung ausgeben lassen. In `polymake` wird ein Polytop  $P$  durch seine Homogenisierung  $\{1\} \times P$  dargestellt, daher wird bei der Eingabe allen Punkten eine 1 vorangestellt. Listen von Vektoren werden zeilenweise ein- und ausgegeben. `polymake` unterscheidet zwei Darstellungen von Punktmengen. Die Eingabe `POINTS` darf redundant sein; dagegen listet die Eigenschaft `VERTICES` nur die Ecken des Polytops. Ein Objekt vom Typ `Polytope` darf auch ein unbeschränktes Polyeder sein; die Eigenschaft `LINEALITY_SPACE` gibt eine Basis des Linealitätsraums an (die redundante Form zur Eingabe heißt `INPUT_LINEALITY`). Das Paar aus `INEQUALITIES` und `EQUATIONS` erlaubt die redundante Beschreibung eines Polytops durch Ungleichungen. Die nicht-redundanten Entsprechungen sind `FACETS` bzw. `AFFINE_HULL`. `polymake` kennt verschiedene Algorithmen um von `POINTS` zu `FACETS` zu gelangen. Welcher zum Einsatz kommt, hängt von der lokalen Konfiguration der Regelbasis ab.

Fast alle Datentypen, wie oben `Matrix` und `Polytope`, können von anderen Datentypen abhängen. In unserem Fall haben wir den Typ der Koordinaten auf `Rational` festgelegt, was rationalen Zahlen mit exakter Arithmetik entspricht. Es sind auch komplexere Varianten möglich, z. B. ergibt `new Array<Vector<Integer>>(5)` einen Array von fünf ganzzahligen Vektoren. Die Notation bildet das *template*-Konzept der C++-Klassen ab, das den Datentypen zugrunde liegt.

Bei der Erzeugung eines Objekts z. B. vom Typ `Polytope` können beliebig viele Eigenschaften in der Form `property=>value` angegeben werden. Dabei liegt es in der Verantwortung des Benutzers, dass die Eingabe gültig ist, `polymake` überprüft dies bewusst nicht — aus Gründen der Effizienz bzw. wegen Grenzen der Entscheidbarkeit. Nach der Definition des Polytops können Eigenschaften berechnet werden, die sich mit Hilfe der Regelbasis ableiten lassen. Neben der direkten Konstruktion durch Eigenschaften kennt `polymake` viele Standardkonstruktionen. Beispiele sind `cube(d)` für einen  $d$ -dimensionalen Würfel oder `product($P,$Q)` für das Produkt zweier Polytope  $\$P$  und  $\$Q$ .



Nun testen wir, ob unser Polytop eine Einbettung ergibt, bestimmen eine reguläre Triangulierung und speichern sie in einem neuen Objekt vom Typ `SimplicialComplex` aus der Anwendung `topaz`.

```
polytope> $T=new topaz::SimplicialComplex(FACETS=>
  placing_triangulation($H->LATTICE_POINTS));
polytope> print $T->FACETS;
{0 1 2}
{1 2 3}
{2 3 4}
{2 4 5}
{3 4 6}
{4 5 6}
{5 6 7}
{5 7 8}
polytope> $I=ideal::stanley_reisner($T);
polytope> print $I->GENERATORS;
x0*x3 x0*x4 x0*x5 x0*x6 x0*x7 x0*x8 x1*x4
x1*x5 x1*x6 x1*x7 x1*x8 x2*x6 x2*x7 x2*x8
x3*x5 x3*x7 x3*x8 x4*x7 x4*x8 x6*x8
```

Die Triangulierung ist in Abbildung 1 rechts dargestellt. Nach der Definition haben wir uns die Liste der maximalen Simplexes der Triangulierung ausgeben lassen. Die Numerierung (ab 0) der Ecken der Triangulierung entspricht dabei der Reihenfolge in der Liste aller Gitterpunkte `$H->LATTICE_POINTS`. Anschließend haben wir das *Stanley-Reisner-Ideal* der Triangulierung bestimmt und uns die Erzeuger anzeigen lassen. Da unser Polytop `$H` eben ist, ist die Triangulierung unimodular. Im Stanley-Reisner-Ideal entspricht jeder Gitterpunkt einer Variablen, und die Monome entsprechen minimalen Teilmengen von Punkten, die keine Seite der Triangulierung bilden. Das zugehörige torische Ideal und Gröbnerbasen können mit der Erweiterung `polymake_algebra` weiter untersucht werden [16].

## Beispiel: Polyedrische Adjunktion

In diesem Abschnitt wollen wir die Erweiterung `PolyhedralAdjunction` vorstellen [18]. Jedes *rationale*  $d$ -dimensionale Polytop  $P$  lässt sich in der Form

$$P := \{x \in \mathbb{R}^d \mid \langle a_i, x \rangle \leq b_i \text{ für } 1 \leq i \leq n\}$$

beschreiben, wobei  $a_i \in (\mathbb{Z}^d)^*$  ein primitiver ganzzahliger Vektor ist, und keine der  $n$  Ungleichungen weggelassen werden kann, ohne das Polytop zu verändern (das System ist *irredundant*). Das zu  $P$  mit Parameter  $c > 0$  *adjungierte* Polytop ist dann

$$P^{(c)} := \{x \in \mathbb{R}^d \mid \langle a_i, x \rangle \leq b_i - c \text{ für } 1 \leq i \leq n\},$$

siehe auch [5]. Vor der ersten Verwendung muss eine Erweiterung mit `import_extension` initialisiert werden,

```
polytope> import_extension("/path/to/extension");
```

wobei `/path/to/extension` durch den korrekten Pfad ersetzt werden sollte.

```
polytope> $P=new Polytope(INEQUALITIES=>
  [[4,-1,1],[0,1,0],[0,0,1],[3,0,-1],[5,-1,0]]);
polytope> $adj_P1=adjoint_polytope($P,1);
polytope> print $adj_P1->VERTICES;
1 1 1
1 1 2
1 4 2
1 4 1
```

Hier haben wir ein durch fünf Ungleichungen bestimmtes Polytop definiert und in der Variablen `$P` gespeichert. Dabei werden Ungleichungen in `polymake` in der Form  $0 \leq b + \langle a, x \rangle$  interpretiert, der Vektor  $(4, -1, 1)$  entspricht also der Ungleichung  $x_1 - x_2 \leq 4$ .

Anschließend haben wir via `adjoint_polytope` aus der zuvor geladenen Erweiterung das Polytop  $P^{(1)}$  berechnet und uns die Ecken ausgeben lassen. Das Polytop und sein Adjungiertes für  $c = 1$  sind in folgender Abbildung dargestellt.

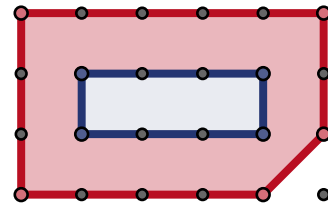


Abbildung 2: Ein Gitterpolygon und sein Adjungiertes für  $c = 1$

Wie zu sehen ist, kann das Polytop  $P^{(c)}$  weniger Facetten haben als  $P$ ; und für ausreichend großes  $c$  ist es leer. Das führt zu zwei interessanten Invarianten. Der *nef-Wert* von  $P$  ist das Inverse des kleinsten  $c$ , für das die Normalenfächer von  $P$  und  $P^{(c)}$  nicht mehr übereinstimmen und der  *$\mathbb{Q}$ -Kograd* ist das Inverse des größten  $c$ , für das  $P^{(c)}$  nicht leer ist.

```
polytope> print $P->NEF_VALUE;
1
polytope> print $P->Q_CODEGREE;
3/2
```

Die Motivation für das Studium dieser Invarianten kommt aus der algebraischen Geometrie. Wie bereits oben bei den Hirzebruchflächen definiert der Normalenfächer eines Gitterpolytops  $P$  eine projektive torische Varietät  $X$ . Zusätzlich legt die konkrete Wahl des Polytops auch noch ein Geradenbündel auf  $X$  fest. Die adjungierten Polytope gehören dann zu den adjungierten Geradenbündeln  $K_X + cL$ , siehe [1, 5]. Diese Korrespondenz zwischen algebraischer und kombinatorischer Geometrie ermöglicht es, algebraische Fragen mit kombinatorischen Methoden zu untersuchen. Auf diesem Weg konnte kürzlich z. B. die Spektralvermutung von Fujita im torischen Fall bewiesen werden [19].

Wir wollen den Normalenfächer unseres Polytops  $P$  weiter untersuchen. Die meisten Methoden liegen in der Anwendung `fan`. Daher wechseln wir zunächst dorthin.

```
polytope> application "fan";
fan> $nf=normal_fan($P);
fan> print $nf->Q_GORENSTEIN;
1
fan> print $nf->Q_GORENSTEIN_INDEX;
1
```

Die Variable `$nf` enthält nun den Normalenfächer unseres Polygons. Mit der nachfolgenden Abfrage haben wir `polymake` ausrechnen lassen, ob unsere Varietät die  *$\mathbb{Q}$ -Gorenstein-Eigenschaft* besitzt, ob es also eine positive ganze Zahl  $r$  gibt, so dass das  $r$ -fache des kanonischen Divisors  $K_X$  ein Cartier-Divisor ist. Die Ausgabe ist ein boolescher Wert, 1 steht hier für *wahr* (bei *falsch* bliebe die Ausgabe leer). Wir können uns mit `Q_GORENSTEIN_INDEX` die Zahl  $r$  berechnen lassen. Unsere Varietät ist sogar nichtsingulär, wie wir mit

```
fan> print $nf->SMOOTH_FAN;
1
```

verifizieren können. Der Fächer wird durch seine Strahlen und deren Inzidenzrelation vollständig bestimmt. Hier zeigen wir, wie man die implizite Numerierung der Strahlen sichtbar machen kann.

```
fan> print rows_numbered($nf->RAYS);
0: -1  1
1:  1  0
2:  0  1
3:  0 -1
4: -1  0
fan > print $nf->MAXIMAL_CONES;
{1 2}
{0 2}
{0 4}
{3 4}
{1 3}
```

`MAXIMAL_CONES` listet die inklusionsmaximalen Kegel, wobei für jeden Kegel der Index der Strahlen in der Liste `RAYS` angegeben wird, der ein Strahl des Kegels ist. Für weitere Eigenschaften, insbesondere für Rechnungen mit Divisoren auf der torischen Varietät steht die Erweiterung `polymake_toric` zur Verfügung [15].

Die hier vorgestellten Methoden bilden nur einen sehr kleinen Teil der Funktionalität von `polymake` ab. In den Tutorials und der Dokumentation auf `polymake.org` finden sich viele weitere. Dort findet sich auch eine Liste mit wissenschaftlichen Arbeiten, die `polymake` verwendet haben. Weitere Projekte, die `polymake` benutzen, stehen auch auf der Seite `computeralgebra.de`. Direkte Hilfe in der Shell gibt es mit `help "<item>"` zu fast allen Funktionen und Eigenschaften, z. B.

```
polytope> help "CANONICAL";
objects/LatticePolytope/properties/CANONICAL:
The polytope is canonical if there is
exactly one interior lattice point.
```

Für weitergehende Fragen verweisen wir auch auf unser Forum unter `forum.polymake.org`.

## Literatur


- [1] M.C. Beltrametti und A.J. Sommese, The adjunction theory of complex projective varieties, Band 16 in *Expositions in Mathematics*, Walter de Gruyter & Co., Berlin, 1995.
- [2] W. Bruns, B. Ichim und C. Söger, Normaliz. Algorithms for rational cones and affine monoids, [www.math.uos.de/normaliz](http://www.math.uos.de/normaliz).
- [3] D.A. Cox, J.B. Little und H.K. Schenck, Toric varieties, *Graduate Studies in Mathematics*, Band 124, American Mathematical Society, Providence, RI, 2011.
- [4] W. Decker, G.-M. Greuel, G. Pfister und H. Schönemann, SINGULAR 3-1-6 — A computer algebra system for polynomial computations, 2012, [www.singular.uni-kl.de](http://www.singular.uni-kl.de).
- [5] S. DiRocco, C. Haase, B. Nill und A. Paffenholz, Polyhedral Adjunction Theory, preprint, Mai 2011, [arxiv:1105.2415](https://arxiv.org/abs/1105.2415).
- [6] T. Fujita, On Kodaira energy and adjoint reduction of polarized manifolds. *Manuscr. Math.*, 76:59–84, 1992.
- [7] The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.5.7, 2012, [www.gap-system.org](http://www.gap-system.org).
- [8] [github.com/Singular/Sources/wiki/Gap-Polymake-Singular-Applications](https://github.com/Singular/Sources/wiki/Gap-Polymake-Singular-Applications)
- [9] E. Gawrilow und M. Joswig, `polymake`: a framework for analyzing convex polytopes, *Polytopes—combinatorics and computation* (Oberwolfach, 1997), Birkhäuser, Basel, 2000, pp. 43–73.
- [10] E. Gawrilow, M. Joswig, T. Rörig und N. Witte, Drawing polytopal graphs in `polymake`, *Comput. Vis. Sci.*, 2010:13, 99–110.
- [11] A.N. Jensen, Gfan, a software system for Gröbner fans and tropical varieties, [home.imf.au.dk/jensen/software/gfan/gfan.html](http://home.imf.au.dk/jensen/software/gfan/gfan.html).
- [12] M. Joswig, `polymake`, *Computeralgebra-Rundbrief* 2003:33, 15–16.
- [13] The jReality team, jReality, [www3.math.tu-berlin.de/jreality/](http://www3.math.tu-berlin.de/jreality/)
- [14] T. Junttila und P. Kaski, bliss: A Tool for Computing Automorphism Groups and Canonical Labelings of Graphs, [www.tcs.hut.fi/Software/bliss/](http://www.tcs.hut.fi/Software/bliss/), 2012.
- [15] L. Kastner, B. Lorenz, A. Paffenholz und A. Winz, `polymake_toric` (eine `polymake` Erweiterung), [github.com/lkastner/polymake\\_toric](https://github.com/lkastner/polymake_toric).
- [16] L. Kastner, B. Lorenz und A. Winz, `polymake_algebra` (eine `polymake` Erweiterung), [github.com/lkastner/polymake\\_algebra](https://github.com/lkastner/polymake_algebra).
- [17] B. D. McKay, Practical graph isomorphism, *Congressus Numerantium* 1981:30, 45–87.
- [18] A. Paffenholz, PolyhedralAdjunction (eine `polymake` Erweiterung), [github.com/apaffenholz/polymake\\_polyhedral\\_adjunction](https://github.com/apaffenholz/polymake_polyhedral_adjunction).
- [19] A. Paffenholz, Finiteness of the Polyhedral  $\mathbb{Q}$ -Co-degree Spectrum, preprint, Januar 2013, [arxiv:1301.4967](https://arxiv.org/abs/1301.4967).

[20] T. Rehn und A. Schürmann, C++ Tools for Exploiting Polyhedral Symmetries, *Lecture Notes in Computer Science*, 2010, Band 6327/2010

[21] B. Sturmfels, Gröbner bases and convex polytopes, *University Lecture Series*, 8. American Mathematical Society, Providence, RI, 1996.

**mathemas ordinate**  **www.ordinate.de**

 0431 23745-00/  -01 , info@ordinate.de → Software for mathematical people !

 **Mathematische Software u. Consulting, MathType, Optica, ExtendSim, KaleidaGraph, Intel-Software, Fortran, NSBasic, @Risk, Chemistry, Satellitensteuerung u.a.**  $\infty + \mu < \heartsuit$

mathemas ordinate, Dipl. Math. Carsten Herrmann, M. Sc.  
Königsbergerstr. 97, 24161 Altenholz

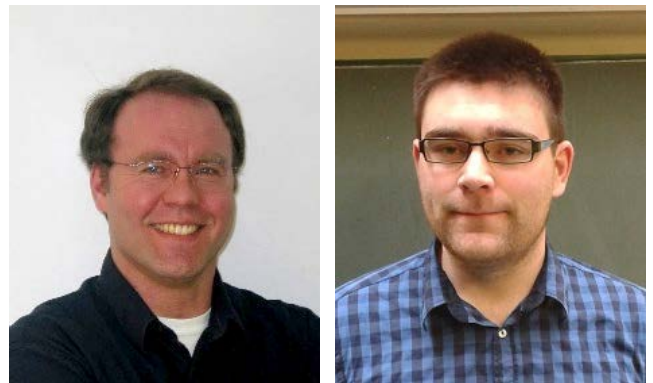
Fast 30 Jahre Erfahrung mit Software-Distribution !

$$\int_{x_1}^{x_2} \frac{1}{\sigma \sqrt{2\pi}} e^{-\frac{1}{2} \left( \frac{x-\mu}{\sigma} \right)^2} dx$$

### Bildverarbeitung: Mathematik arbeiten sehen

**B. Burgeth, F. Kern**  
(Universität des Saarlandes)

burgeth@math.uni-sb.de  
florkern@math.uni-sb.de



---

### Bildverarbeitung, wozu?

---

Der Mensch ist ein visuelles Wesen, der den weitaus größten Teil der Informationen über seine Umwelt durch seinen Sehsinn erhält. Umgekehrt verbreitet er auch gezielt Wissen und Kenntnisse an andere über Zeichen („Lesen“) und Bilder, vor allem in neuerer Zeit, da ihm die Segnungen des modernen Technologie- und Medienzeitalters zur Verfügung stehen. Auch Schüler haben oft schon wie selbstverständlich Zugriff auf Computer und Digitalkamera (integriert im „Handy“). Damit sind ihnen auch schon die Möglichkeiten gegeben, Bilder zu machen, zu speichern und, vor allem, zu verändern. Diese Manipulation von Bildern geschieht mit mathematischen Methoden, und was kann deswegen näher liegen als die Wirkungsweise elementarer Mathematikkonzepte an Bildern zu veranschaulichen, mit Bildern einsehbar zu machen?

Um die Verdeutlichung einfacher mathematischer Konzepte an Bildern soll es in diesem Artikel gehen. Dabei werden wir uns auf folgende Fragen konzentrieren:

Was sind Bilder, wie können sie mathematisch beschrieben werden? Wie werden sie im Computer repräsentiert? Was bedeuten dabei Diskretisierung und Quantisierung? Wie kann man Bilder untersuchen, analysieren und auf einfache Weise gezielt verändern?

Die Verarbeitung aller Bilder und die Erstellung sämtlicher Graphiken in diesem Beitrag ist mit Hilfe des Computeralgebrasystems MAPLE15 [3] geschehen. Es bietet mit seinem *ImageTools Package* eine recht bequeme Möglichkeit verschiedene Bildfile-Formate, wie z. B. das bekannte .jpg-Format und fast kompressionsfreie .tif-Format, als Files ein- und auszulesen und ins ascii-format, also in eine Datei mit lesbaren Zahlen, umzuwandeln. Mit seinen anderen Funktionalitäten, z. B. dem *Statistics Package*, und dem *LinearAlgebra Package* gelingt dann eine statistische Analyse und die Verarbeitung der Bilddaten. Wer schon ein wenig Erfahrung mit MAPLE hat, wird durch die Hilfe-Funktion einen schnellen Einstieg in die Handhabung des Bildverarbei-

tungsmoduls finden. Zweifelsohne gibt es noch weitere leistungsfähige Computeralgebrasysteme, die Werkzeuge zur Bildverarbeitung anbieten. Dass die Wahl der Autoren auf Maple fiel, ist Zufall.

---

### Repräsentationen von Bildern

---

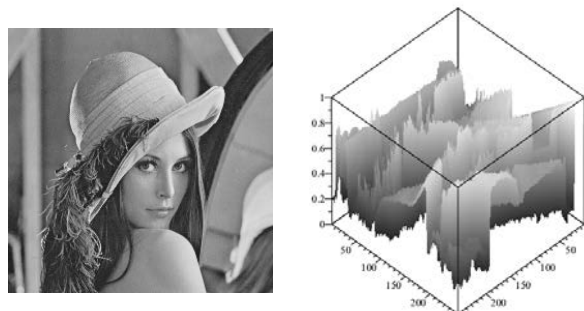
#### Bilder als Funktionen

Wir betrachten hier so genannte Grauwertbilder, da diese grundlegenden Charakter auch für Farbbilder haben, und letztere konzeptionell für einen Einstieg ungeeignet erscheinen.

Ein kontinuierliches Grauwertbild kann als eine Funktion von zwei Veränderlichen betrachtet werden, also als Abbildung  $f$  vom Definitionsbereich  $\Omega = [0, a] \times [0, b]$  in den Zielbereich  $\mathbb{R}$ :

$$f : \mathbb{R}^2 \supset \Omega \longrightarrow \mathbb{R}.$$

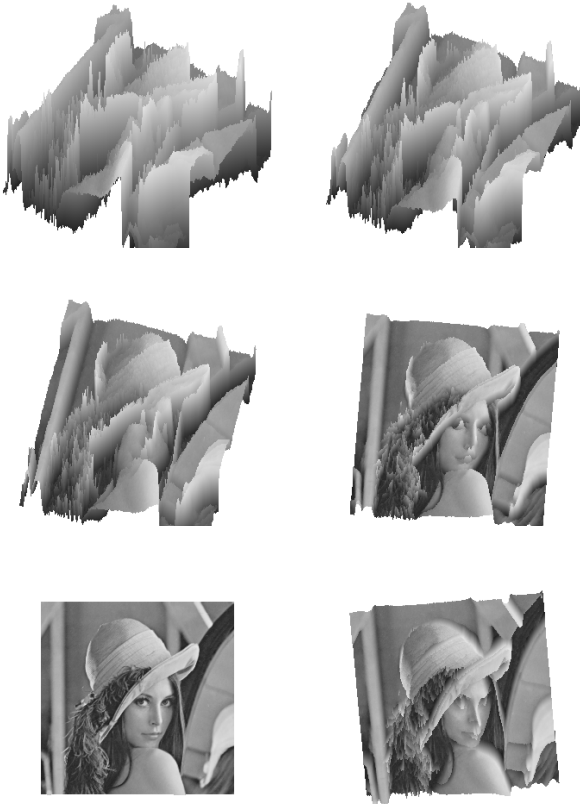
Ihre Definitionsmenge, der rechteckige Bereich  $\Omega$  heißt Bildbereich oder auch, etwas missverständlich, Bildebene. Der Wertebereich dieser Funktion ist die Menge aller Grauwerte des Bildes. Dabei werden niedrige Grauwerte dunkel, hohe Grauwerte hell dargestellt.



**Abbildung 1:** *Lena, eines der bekanntesten Testbilder in der Bildverarbeitung. Links: Original. Rechts: Als Funktionsgraph einer Funktion in zwei Veränderlichen.*

In dieser Seitenansicht des dreidimensionalen Graphen  $G_f$  ist Lena nur schwer zu erkennen. Eine schrittweise Rotation des Graphen, so dass man

am Ende von oben auf ihn blickt, bringt Klarheit.



**Abbildung 2:** Von links oben nach rechts unten: Schrittweise Rotation.

### Diskretisierung 1: Bilder als Matrizen

Natürlich kann man keinen Funktionsterm angeben, dessen Graph das Bild von Lena darstellt. Man kann das Bild nur in Form einer recht umfangreichen Wertetabelle im Computer abspeichern. Das Erstellen dieser Wertetabelle nennt man abtasten und meint die Diskretisierung des Bildbereiches. Die Bilddaten sind dann nur auf den Punkten  $(i, j)$  eines Rechteckgitters in  $\Omega$  gegeben und wir haben auf diese Weise ein **digitales Bild** erzeugt

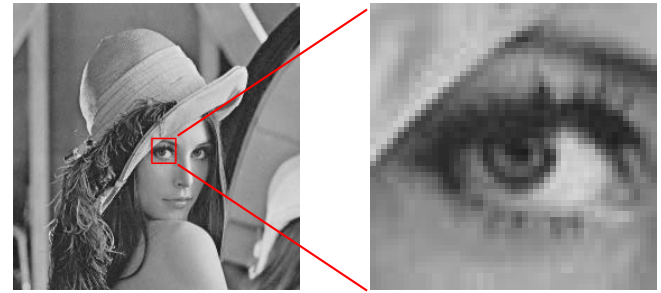
$$\{f_{i,j} = f(i, j) \mid i = 1, \dots, N, j = 1, \dots, M\},$$

das auch als Matrix angesehen werden kann:

$$(f_{i,j})_{i,j} = \begin{bmatrix} 0.38 & 0.48 & 0.51 & 0.73 & 0.43 & 0.55 & 0.91 & 0.20 \\ 0.38 & 0.75 & 0.44 & 0.72 & 0.81 & 0.67 & 0.17 & 0.63 \\ 0.39 & 0.82 & 0.57 & 0.46 & 0.73 & 0.69 & 0.65 & 0.59 \\ 0.44 & 0.58 & 0.30 & 0.41 & 0.74 & 0.25 & 0.62 & 0.50 \\ 0.45 & 0.60 & 0.63 & 0.61 & 0.81 & 0.14 & 0.57 & 0.81 \\ 0.48 & 0.34 & 0.25 & 0.36 & 0.25 & 0.61 & 0.45 & 0.19 \\ 0.58 & 0.18 & 0.40 & 0.55 & 0.68 & 0.56 & 0.86 & 0.36 \\ 0.37 & 0.29 & 0.42 & 0.54 & 0.61 & 0.46 & 0.29 & 0.42 \end{bmatrix}$$

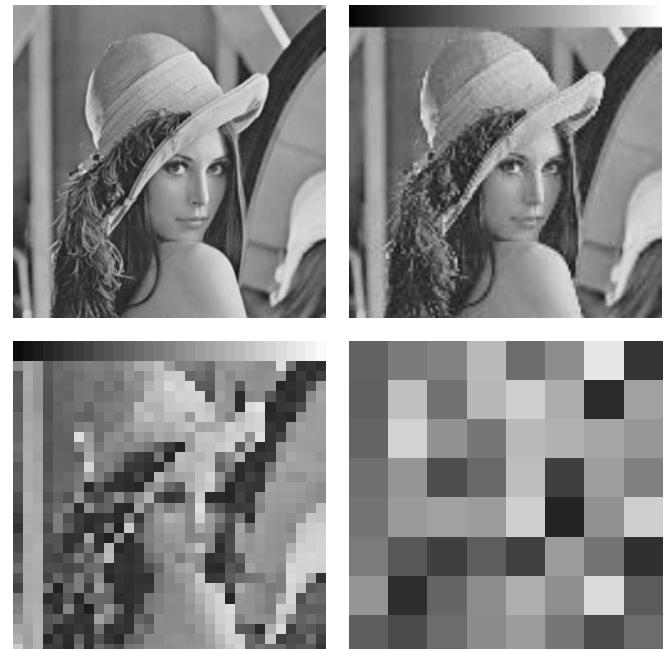
Die Gitterpunkte (man spricht auch von Gitterzellen)  $(i, j)$  heißen **Pixel**. Es ist in der Bildverarbeitung aus Gründen der Einfachheit üblich den Abstand der Gitterpunkte (bzw. Gitterzellenseitenlängen) auf 1 zu normieren. Dies bringt auch eine vereinfachte und sparsamere Speicherung der Bilder auf dem Computer mit sich,

da keine expliziten Gitterpunktkoordinaten gespeichert werden müssen. Wenn man einen Ausschnitt eines digitalen Bildes stark vergrößert, tritt die Pixelstruktur deutlich sichtbar hervor.



**Abbildung 3:** Links: Lena. Rechts: Auge vergrößert.

Tastet man beispielsweise die Funktion auf einem größeren Gitter ab, so erhält man eine kleinere Matrix, die durch dieses **Vergrößern** (engl. down sampling) allerdings als „verpixeltes“ Bild interpretiert wird, bei dem viele Details verlorengehen.



**Abbildung 4:** Auflösung in  $n \times n$  Pixel. Links oben:  $512 \times 512$ . Rechts oben:  $128 \times 128$ . Links unten:  $32 \times 32$ . Rechts unten:  $8 \times 8$ .

Man sieht sofort: bei einer Auflösung von  $8 \times 8$  Pixel ist Lena nicht mehr zu erkennen. Das letzte Bild entspricht übrigens gerade der eben genannten  $8 \times 8$ -Matrix  $(f_{i,j})$ . Es sei noch angemerkt, dass es sich bei dem Streifen am oberen Bildrand um kein Diskretisierungsartefakt handelt, es ist vielmehr ein Teststreifen, der eine gleichmäßig von null (schwarz) nach eins (weiss) ansteigende lineare Funktion darstellt. Dies wird bei noch folgenden Ausführungen noch eine Rolle spielen.

### Diskretisierung 2: Quantisierung

Mit **Quantisierung** meint man in der Bildverarbeitung die Diskretisierung des Wertebereichs  $f(\Omega)$ . Das führt im Extremfall zu binären Bildern, also Schwarz-Weiss-Bildern:  $f(\Omega) = \{0, 1\}$ . Als Speicherplatz noch kostbar war, benutzte man auch noch die byte-Codierung der Grauwerte, die eine Unterteilung in 256 Graustufen



erlaube:  $f(\Omega) = \{0, 1, \dots, 255\}$ . Dies ist völlig ausreichend, da Menschen durch ihre Physiologie bestimmt nur etwa 40 verschiedene Grauwerte unterscheiden können. In den Zeiten leistungsfähiger Computer findet man heute oft einen quasi-kontinuierlichen Wertebereich bei Bildern:  $f(\Omega) = [0, 1]$ . Dies wollen wir auch für diesen Aufsatz annehmen, falls nicht anderweitig angemerkt.



**Abbildung 5:** Quantisierung beim Bild Kameramann. Links: 256 Grauwertstufen. Rechts: 4 Grauwertstufen, mit deutlichem Effekt auch auf den Teststreifen.

## Wann ist ein Bild ein Bild? Verteilung von Grauwerten

Ein digitales Bild ist eine Art diskretisierte Funktion und kann als Matrix betrachtet werden, deren Einträge Zahlen aus dem Intervall  $[0, 1]$  sind. Ordnet man diese Einträge in einer fest vorgegebenen Reihenfolge (etwa Zeile für Zeile der Matrix) hintereinander an, so erhält man einen Vektor, aber einen sehr hochdimensionalen: das  $256 \times 256$  Bild von Lena ergibt einen Vektor der Dimension  $256 \cdot 256 = 65536$ ! Ein Schüler, dem das klar geworden ist, wird dem allgemeinen Konzept eines  $n$ -dimensionalen Vektors im Mathematikunterricht wohl etwas offener gegenüber stehen.

Die in einem Bild enthaltene Information steckt in der räumlichen Verteilung der Grauwerte, und diese können wir uns „in Schichten“ ansehen, in Form von **Niveaumengen**. Dazu denken wir uns ein digitales Bild mit 256 Graustufen gegeben  $f : \Omega \rightarrow \{c_0, \dots, c_{255}\} \subset [0, 1]$ . Mit dem Begriff der Niveaumenge haben Schüler und Anfänger im Studium in der Regel Schwierigkeiten. Dieses und verwandte Konzepte lassen sich an einem Bild sinnfällig veranschaulichen. Wie zu erwarten ist die **Niveaumenge** zum Grauwert  $c_k \in \{c_0, \dots, c_{255}\}$  als die Menge

$$\{(i, j) \in \Omega \mid f(i, j) = c_k\} = f^{-1}(c_k)$$

definiert, also als Teilmenge des Bildbereichs, mathematisch eine Urbildmenge. Anders das **Niveaubild**:

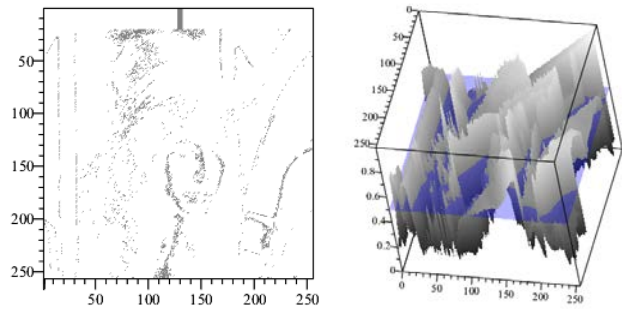
$$I_{c_k}^f(i, j) = f(i, j) \cdot \mathbf{1}_{f^{-1}(c_k)}(i, j) = c_k \cdot \mathbf{1}_{f^{-1}(c_k)}(i, j)$$

mit  $\mathbf{1}_M$  als der Indikatorfunktion einer Menge  $M$ ,

$$\mathbf{1}_M(x) = \begin{cases} 1 & \text{falls } x \in M \\ 0 & \text{falls } x \notin M \end{cases}$$

Das Niveaubild hat einen bestimmten Grauwert (nämlich  $c_k$ , siehe Abb. 2) und ist eine Teilmenge des Graphen der (diskretisierten) Funktion.

Auch die Wirkungsweise der Indikatorfunktion als wichtiges Instrument einer Fallunterscheidung kann damit demonstriert werden.



**Abbildung 6:** Räumliche Verteilung von Grauwerten. Links: Niveaubild zum Grauwert 0.5 in 2D. Rechts: Niveaubild zum Grauwert 0.5 in 3D.

Diese Schichten eines Bildes lassen sich auch wieder zusammensetzen, man hat die interessante Zerlegung:

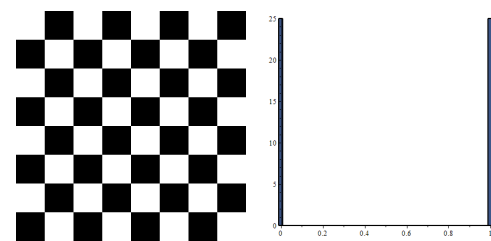
$$f = \sum_{k=0}^{255} I_{c_k}^f = \sum_{k=0}^{255} c_k \cdot \mathbf{1}_{f^{-1}(c_k)}.$$

Einen ganz anderen Blick auf ein Bild gewinnt man, wenn die **Häufigkeitsverteilung der Grauwerte** betrachtet wird. Dies bietet einen anwendungsnahen Einstieg zum Thema **Histogramme** über der Menge der Grauwerte eines Bildes.

Es geht also darum, wie oft ein Grauwert in einem diskreten Bild  $f : \Omega \rightarrow [0, 1]$  vorkommt, genauer: Die Zuordnung

$$H : c \mapsto |f^{-1}(c)| = \text{Anzahl}(f^{-1}(c))$$

liefert das Histogramm  $H$  zur Verteilung der Grauwerte,  $H : [0, 1] \rightarrow \{0, \dots, |\Omega|\}$ . Da es nur um Anzahlen geht, ist die räumliche Anordnung der Pixel in  $\Omega$  ohne Bedeutung für das Histogramm. Und gerade die Chance, an einem Objekt, dem Bild, diese beiden Aspekte von „Verteilung“ gegenüber stellen zu können macht den Reiz dieser Betrachtungsweise aus. Das Histogramm selbst kann in Form eines Punkte-, Stäbchen- oder, am häufigsten, in der Gestalt eines Balkendiagramms dargestellt werden. Die folgenden Abbildungen zeigen einige Beispiele.

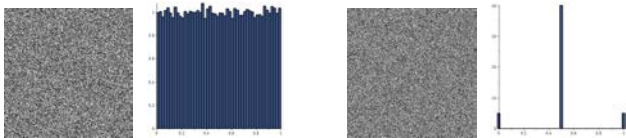


**Abbildung 7:** Häufigkeitsverteilung von Grauwerten bei einem binärem Bild. Links: Schachbrettmuster. Rechts: Zugehöriges Histogramm.

Und manchmal zeigt ein Histogramm doch mehr als ein Blick auf das Bild, zum Beispiel beim sogenannten



„Rauschen“.



**Abbildung 8:** Häufigkeitsverteilung von Grauwerten bei zwei häufig auftretenden Arten von Rauschen. Oben: Gleichverteiltes Rauschen mit Histogramm. Oben: „Salz und Pfeffer“-Rauschen mit Histogramm.

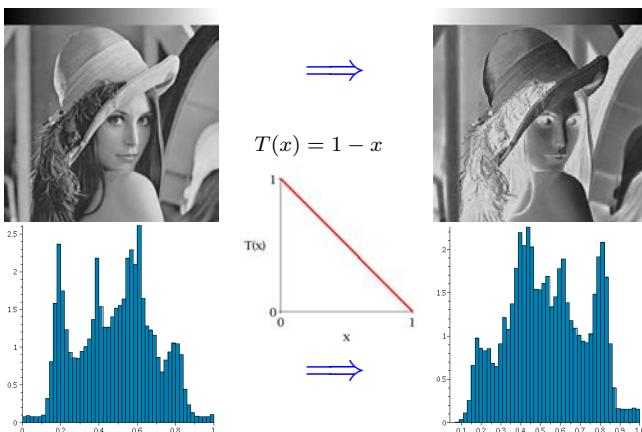
Auch solche Bilder, die nur Rauschen, d. h., von einem Pixel zum anderen einen starken und zufälligen Wechsel in den Grauwerten zeigen, sind Bilder. Am zugehörigen Histogramm wird deutlich, um welche Art von Rauschen es sich handelt, was wichtig sein kann zur Entwicklung von „Entrauschungsalgorithmen“.

## Nicht nur schauen: Verarbeiten von Bildern

Bis jetzt haben wir Bilder mehr oder weniger nur analysiert. Jetzt geht es um die tatsächliche Verarbeitung von Bildern und wir stellen uns die Frage, ob man reellwertige Funktionen  $T : D \supset \mathbb{R} \rightarrow \mathbb{R}$  auf Bilder anwenden und sie auf diese Art transformieren kann. Die Antwort ist, wie zu erwarten, ja, denn diese Anwendung läuft auf eine Verknüpfung von  $T$  mit der Funktion  $f$  hinaus, deren dreidimensionaler Graph  $G_f$  das Bild darstellt (vgl. Abschnitt 1). Allerdings taugt nicht jede Funktion als transformierende Abbildung  $T$ , genauer: zu einem Bild repräsentiert durch  $f : \Omega \rightarrow [0, 1]$  und der Funktion  $T : [0, 1] \rightarrow [0, 1]$  (!) liefert die Verknüpfung  $T \circ f$  von Transformation  $T$  und Bild  $f$  das **transformierte Bild**,

$$T \circ f : \Omega \rightarrow [0, 1].$$

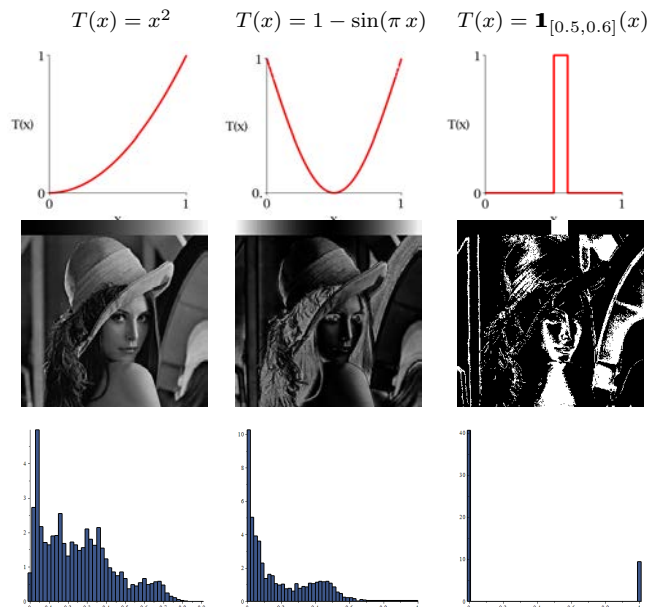
Im ersten Beispiel werden wir sehen, dass der Begriff des „Negativs“ eines Bildes nicht völlig zutreffend ist.



**Abbildung 9:** Transformationen von Bildern. Rechte Spalte: Lena (Bild  $f$ ) und zugehöriges Histogramm. Mittlere Spalte: Transformation  $T$  und Graph. Rechte Seite: „Transformierte“ Lena (Bild  $T \circ f$ ) mit (gespiegeltem) Histogramm.

Die Transformation verändert auch die Häufigkeitsverteilung der Grauwerte, d. h. die Histogramme. An den folgenden Beispielen wird „sichtbar“ wie sich

Monotonie- und Stetigkeitseigenschaften von  $T$  im Ergebnisbild und -histogramm widerspiegeln.



**Abbildung 10:** Beispiele (spaltenweise gelesen) von Transformationen. Die angegebenen Transformationen werden jeweils auf das originale Lena-Bild angewandt. Aus dem Teststreifen läßt sich die Gestalt des Graphen  $G_T$  der Transformation  $T$  ableiten.

Man darf hoffen, dass die/der interessierte Schüler/in vielleicht von sich heraus versucht, mit verschiedenen Transformationen ansprechende Effekte zu erzielen (und z. B. aus einer Bildergeschichte mit selbstaufgenommenen Fotos ein Comic-Strip zu machen). Es ergeben sich auch didaktisch interessante Fragestellungen:

Bei gegebenem  $T$ , kann man grob voraussagen, wie Bild und Histogramm verändert werden wird? Wann kann ein transformiertes Bild wieder rekonstruiert werden? Das führt zu einer sinnhaften Auseinandersetzung mit dem Konzept der Umkehrfunktion in Form der Umkehrabbildung  $T^{-1}$ . Was ist zu tun, wenn der Wertebereich einer Funktion  $T$  nicht von vorne herein in  $[0, 1]$  enthalten ist,  $T([0, 1]) \not\subset [0, 1]$ ? Welches Funktionsdesign ist dann nötig, stauchen, „klippen“,...?

### Rückblick

Wir hoffen mit diesem Aufsatz wenigstens ansatzweise aufgezeigt zu haben, welches Potenzial die mathematische Bildverarbeitung bietet, zahlreiche Zusammenhänge und Konzepte der (Schul-)Mathematik vernetzt darzustellen und visuell erfahrbar zu machen. Als Bücher, die allgemein von Bildverarbeitung handeln, seien hier [1] und [2] genannt.

## Literatur

- [1] Rafael C. Gonzalez und Richard E. Woods. *Digital Image Processing*, 2008.
- [2] Milan Sonka, Vaclav Hlavac und Roger Boyle. *Image Processing, Analysis and Machine Vision*, 1999.
- [3] *Maple 15*. [www.maplesoft.com](http://www.maplesoft.com) (zuletzt aufgerufen am 14.02.2013)

### Steven D. Galbraith Mathematics of Public Key Cryptography

Cambridge University Press, 2012,  
630 pp., ISBN-13: 9781107013926 , € 51,30

Das vorliegende Buch behandelt die mathematischen Grundlagen der Kryptographie mit öffentlichem Schlüssel. Im Vordergrund der Darstellung liegen die Mathematik und die Algorithmen aus Algebra, Zahlentheorie und Geometrie, mit Hilfe derer aktuelle, in der Praxis verwendete Kryptosysteme mit öffentlichem Schlüssel und solche der nächsten Generation implementiert oder angegriffen werden können. Algebraischen Kurven und der kurvenbasierten Kryptographie wird ein besonderes Gewicht gegeben, aber die auf dem Faktorisierungsproblem beruhende Kryptographie und die gitterbasierte Kryptographie werden ebenfalls ausführlich behandelt. Einige der Themen erscheinen hier erstmalig gebündelt und in Lehrbuchform.

Die an den Leser gestellten Voraussetzungen sind ein Grundwissen über Gruppen, Ringe, Körper sowie Kryptographie, Algorithmen und Komplexität, wie sie in Veranstaltungen eines Bachelorstudiums vermittelt werden. Der Autor räumt in seiner Darstellung Gründlichkeit und Präzision einen höheren Stellenwert ein als einer größtmöglichen Allgemeinheit oder Optimalität

der beschriebenen Algorithmen. Zudem sind in den laufenden Text zahlreiche Übungsaufgaben eingearbeitet. Damit eignet sich das Buch sowohl als Begleitmaterial zu einer Vorlesung, als auch zum Selbststudium. Vom Inhalt her umfaßt das Buch das Kernwissen, welches für einen Start in die eigene Forschung im Rahmen einer Promotion im Bereich der mathematischen Kryptographie erforderlich ist.

Das Buch ist mit 630 Seiten und über 600 Literaturreferenzen umfangreich ausgefallen. Es unterteilt sich in die folgenden Teile: „Background“, „Algebraic Groups“ und „Exponentiation, Factoring and Discrete Logarithms“, „Lattices“, „Cryptography Related to Discrete Logarithms“, „Cryptography Related to Integer Factorisation“ und „Advanced Topics in Elliptic and Hyperelliptic Curves“ mit Abschnitten zu Isogenien und Paarungen. Weitere Details zum Inhalt sind unter <http://www.math.auckland.ac.nz/~sgal018/crypto-book/crypto-book.html> zu finden.

*Florian Heß (Oldenburg)*

Weitere Bücher können auf der Seite <http://www.fachgruppe-computeralgebra.de/Buecher> oder direkt bei Anne Frühbis-Krüger ([fruehbis-krueger@math.uni-hannover.de](mailto:fruehbis-krueger@math.uni-hannover.de)) zur Besprechung angefordert werden.

### Verleihung des Ehrendokortitels an Anthony C. Hearn

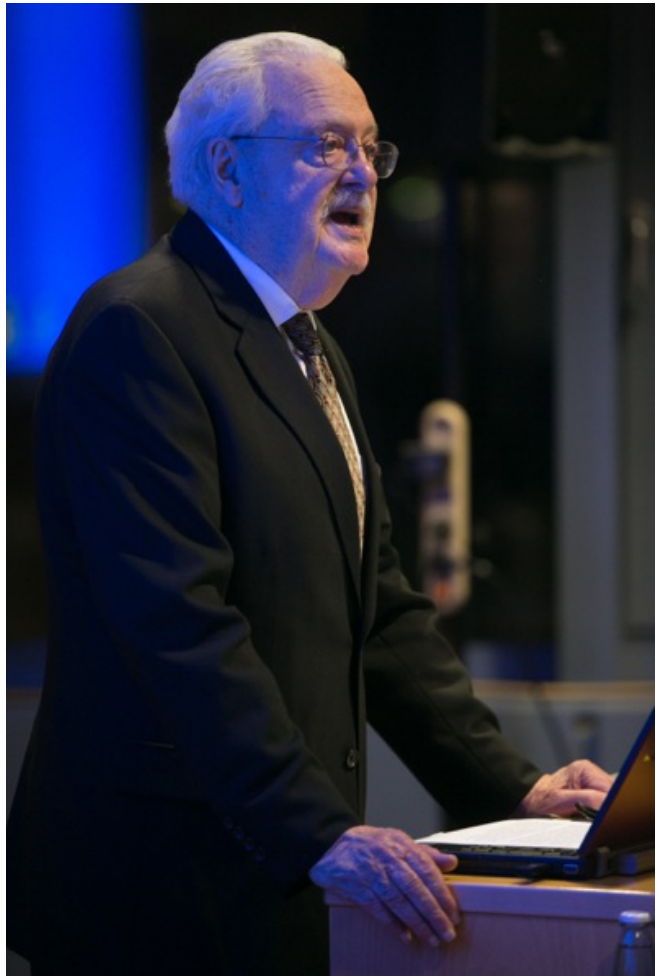
Erlangen, 30. November 2012



*Ehrendoktor Anthony C. Hearn, Dekanin Marion Merklein, Laudator Herbert Stoyan.  
(Foto: Erich Malter, Erlangen)*

Im Rahmen ihrer Jahresabschlussfeier am 30. November 2012 hat die Technische Fakultät der Friedrich-Alexander-Universität Erlangen-Nürnberg den Grad und die Würde eines Doktors der Ingenieurwissenschaften Ehren halber (Dr.-Ing. E. h.) an Anthony C. Hearn, Ph.D., verliehen. Die Verleihung wurde von der Dekanin, Frau Prof. Dr.-Ing. Marion Merklein, Inhaberin des Lehrstuhls für Fertigungstechnologie, vorgenommen. Die Laudatio hielt Prof. i.R. Dr. Herbert Stoyan, vormaliger Inhaber des Lehrstuhls für Künstliche Intelligenz am Department Informatik, der als LISP-Experte seit langer Zeit eine besondere Beziehung zu Anthony Hearn, seinem Computeralgebrasystem REDUCE und dem von ihm entwickelten Standard Lisp hat. In seiner Würdigung ging er auf den Werdegang von Anthony Hearn und seine wissenschaftlichen und organisatorischen Leistungen rund um REDUCE ein, betonte aber auch dessen weltweiten Einsatz als „Wissenschaftsorganisator“ und „Wissenschaftsdiplomat“ zu Zeiten, als dies politisch und technisch noch erheblich schwieriger und weniger selbstverständlich war als heute. Als „Urgestein der Computeralgebra“ hat es Anthony Hearn geschafft, ein Programmsystem mit einem fachlich und international breiten Spektrum von Anwendern zu etablieren, das nunmehr über fast ein halbes Jahrhundert weiterentwickelt wird, was einen absoluten Ausnahmecharakter haben dürfte. Die Offenheit des Codes und seiner Entwicklung kennzeichnet zudem Hearn's frühen und konsequenten Einsatz für frei zugängliche, offene Software.

Die Ehrung für Anthony Hearn schließt sich übrigens an die gleiche Ehrung an, die im Jahre 2000 John McCarthy, dem Schöpfer der Programmiersprache LISP, zuteil geworden war. Es waren Begegnungen zwischen dem Physiker Anthony Hearn und dem Logiker und Informatiker John McCarthy im Stanford des Jahres 1963, die den Ausgangspunkt von Hearn's Projekt der Programmierung eines Systems zur „Formelmanipulation“ zur Bearbeitung (seiner) physikalischer Fragestellungen (Feynman-Diagramme) und damit den Ausgangspunkt für die Entwicklung von REDUCE markieren.



*Anthony C. Hearn bei seiner Dankesrede.  
(Foto: Erich Malter, Erlangen)*

Anthony Hearn bedankte sich in einer kurzen, prägnanten Antwort für die ihm zuteil gewordene Ehrung. Am Nachmittag des gleichen Tages hatte er bereits in einem Kolloquiumsvortrag am Department Informatik seine persönliche Geschichte, verwoben mit der Entwicklung von REDUCE, dessen vielseitigen Anwendungen und Anwendern, bis hin zu seiner Sicht auf aktuelle Entwicklungen des wissenschaftlichen Rechnens dargestellt. Der andauernde Erfolg von REDUCE war und ist ja auch einer der vielen Nutzer, die zu diesem offenen System wesentliche Beiträge geleistet haben. Besonders betonte er, dass Kollegen aus Deutschland qualitativ und quantitativ besonders aktiv waren und weiterhin sind. Mit besonderer Genugtuung konnte Anthony Hearn daher die Teilnahme etlicher deutscher REDUCE-Aktivisten registrieren, die aus Anlass seiner Ehrung nach Erlangen gekommen waren.

*V. Strehl (Universität Erlangen-Nürnberg)*

**Ehsan Ullah: New Techniques for Polynomial System Solving****Betreuer: Martin Kreuzer (Passau)****Zweitgutachter: Lorenzo Robbiano (Genua)****Juli 2012**<http://www.opus-bayern.de/uni-passau/volltexte/2012/2681/>**Zusammenfassung:**

In den letzten Jahren ist es in der algebraischen Kryptoanalyse immer wichtiger geworden, spezielle Systeme polynomialer Gleichungssysteme zu lösen: der Grundkörper ist endlich, es gibt i.A. genau eine Lösung, und diese ist über dem Grundkörper definiert. In dieser Dissertation entwickelt, implementiert und analysiert der Autor eine Reihe von Methoden, um auch große Beispiele solcher Gleichungssysteme zu lösen. Er verwendet dabei Techniken, die aus verschiedenen Gebieten der Mathematik stammen.

(1) Methoden aus der linearen Algebra basieren auf den Techniken von J. de Loera und anderen, bei der das polynomiale Gleichungssystem durch immer größere lineare Gleichungssysteme approximiert und jeweils nur die Lösbarkeit untersucht wird. Diesen Ansatz kombiniert der Autor geschickt mit der Idee der *Mutants* von J. Ding.

(2) Methoden aus der diskreten Optimierung, insbesondere Integer Programming (IP), Mixed Integer Programming (MILP) und Mixed Integer Non-Linear Programming (MINLP) werden anwendbar, indem man das Gleichungssystem in eine Menge linearer Ungleichungen über  $\mathbb{Z}$  umwandelt. Hierzu werden eine Reihe von Konversionsalgorithmen entwickelt und miteinander verglichen. Wie zu erwarten haben sie einen großen Einfluß auf das Laufzeitverhalten der verwendeten IP-Solver.

(3) Weitere betrachtete Methoden sind die Umwandlung in ein SAT-Problem und anschließende Verwendung eines SAT-Solvers, Umwandlung in ein lineares Diophantisches Gleichungssystem über  $\mathbb{Z}$  mit Berechnung der Smith Normalform, und die Umwandlung in ein reelles oder komplexes Gleichungssystem mit Verwendung von Methoden aus der numerischen Analysis, insbesondere der Newton-Methode und der Homotopie-Fortsetzungsmethoden.

Die Arbeit hat einen erheblichen Umfang und wird durch eine Vielzahl an Implementationen und Timings expliziter Beispiele aus der Kryptoanalyse ergänzt.

**Xingqiang Xiu: Non-Commutative Gröbner Bases and Applications****Betreuer: Martin Kreuzer (Passau)****Zweitgutachter: Gerhard Rosenberger (Hamburg)****Juli 2012**<http://www.opus-bayern.de/uni-passau/volltexte/2012/2682/>**Zusammenfassung:**

Während die Algorithmen zur Berechnung von Gröbner-Basen für Ideale im kommutativen Polynomring hochentwickelt und weitgehend optimiert sind, ist die Situation für

zweiseitige Ideale im nicht-kommutativen Polynomring (also in der freien assoziativen Algebra) weit weniger erfreulich. Es gibt kein Standardlehrbuch für die theoretischen Grundlagen, es gibt nur wenige, oft nicht sehr zugängliche Implementationen, und mögliche Optimierungen der Buchberger-Prozedur sind nur ansatzweise untersucht worden. Die Dissertation von X. Xiu versucht hier etwas Abhilfe zu schaffen. Nachdem die Grundlagen ausführlich entwickelt werden, untersucht und optimiert der Autor die Buchberger-Prozedur. Dazu werden die Obstruktionen (also die nicht-kommutativen Analoga der kritischen Paare) sorgfältig minimiert und es werden nicht-kommutative Analoga der Gebauer-Möller Kriterien zur Paarvermeidung entwickelt. Auch die Art und Anzahl der notwendigen Interreduktionen wird eingeschränkt, so dass sich eine stark optimierte, performante Version der Buchberger-Prozedur ergibt.

In weiteren Kapiteln werden Anwendungen auf Berechnungen für Untermoduln freier zweiseitiger Moduln, eine nicht-kommutative Version des F4-Algorithmus, Gröbner-Basisberechnungen in Restklassenringen nicht-kommutativer Polynomringe (z. B. in Gruppenringen) und Methoden zur Bestimmung der Gelfand-Kirillov Dimension sowie der nicht-kommutativen Hilbert-Funktion beschrieben.

Der Autor hat alle Algorithmen effizient in einem C++ Paket für das Computeralgebrasystem ApCoCoA implementiert, das frei verfügbar ist. Die Dissertation enthält auch viele mit diesem Paket berechnete Beispiele und Timings.

**Stephan Ritscher: Degree Bounds and Complexity of Gröbner Bases of Important Classes of Polynomial Ideals****Betreuer: Ernst W. Mayr (TUM Informatik)****Gutachter: Gregor Kemper (TUM Mathematik), Chee Yap (New York University)****Oktober 2012**<http://mediatum.ub.tum.de/doc/1006213/1006213.pdf>**Zusammenfassung:**

Polynomial ideals have been intensely studied by computer scientists. The method of Buchberger allows to effectively solve the membership problem to which a variety of other interesting problems can be reduced. Mayr and Meyer showed, that these computations are very expensive in the worst case. As a consequence, special ideal classes have to be identified for which the membership problem can be solved more efficiently. As previous results show, the complexity of the membership problem is mainly related to the degrees of the representation problem and Gröbner bases. Thus the first part of the thesis studies degree bounds for various ideal classes. The main contributions are upper and lower bounds for Gröbner bases depending on the ideal dimension and some results for toric ideals. In the second part, these findings are applied to questions of complexity. The presentation comprises an incremental space-efficient algorithm for the computation of Gröbner bases, an algorithm in polylogarithmic space for the membership problem in toric ideals and the space-efficient computation of the radicals of low-dimensional ideals.

**Daniel Robertz:**

**Formal Algorithmic Elimination for PDEs**

**Betreuer: Wilhelm Plesken (Aachen)**

**Gutachter: Dima Grigoriev (Lille), Franz Winkler (Linz)**

**Dezember 2012**

### **Zusammenfassung:**

This thesis approaches partial differential equations (PDEs) from the viewpoint of algebra and contributes algorithmic methods which allow to investigate effectively the relationship of systems of PDEs and their sets of solutions. Employing formal techniques, the focus is on polynomial differential equations and their analytic solutions.

We borrow quite a few concepts from algebraic geometry. Whenever a set of points is given by a polynomial or rational parametrization, an elimination of the parameters from the equations which express the coordinates of the points yields equations that are satisfied by the coordinates of every point of the set. If there exists an implicit description of this set as solution set of a system of polynomial equations, then elimination constructs such a description.

This thesis develops algorithmic methods which accomplish the analogous elimination task for systems of polynomial partial differential equations and their (complex) analytic solutions. It builds on work by C. Riquier, M. Janet, J. M. Thomas, J. F. Ritt, E. R. Kolchin, and others, who laid the foundation of differential algebra.

A given multivariate polynomial, whose coefficients are analytic functions, is interpreted as a parametrization of a set of analytic functions, i.e., every element of this set arises from substitution of appropriate analytic functions for the indeterminates of the polynomial. Moreover, the substitution of functions for the indeterminates also involves the composition with prescribed analytic functions. If the polynomial is linear, then the resulting set is a vector space over the field of constants. In general, however, the parametrized set is rarely

closed under addition.

As a simple example we mention that the analytic functions of the form  $F(x - t) + G(x + t)$  admit an implicit description as solution set of the wave equation  $\frac{\partial^2 u}{\partial t^2} = \frac{\partial^2 u}{\partial x^2}$ , a well-known fact when considered in the reverse direction.

An implicit description of an algebraic variety admits a straightforward check whether or not a given point belongs to the variety, namely by verifying if it is a solution of the defining equations. Similarly, if a set of analytic functions is the solution set of a system of differential equations, membership to this set reduces to the check whether or not a given analytic function is annihilated by the corresponding differential operators.

Depending on the representation of a function at hand, it may not be obvious at all whether the function has another representation of a special form, e.g., as sum of functions depending on a smaller number of arguments, etc. A prominent example, which is only loosely related to the contents of this thesis, is V. I. Arnold's solution of Hilbert's 13th problem showing that every continuous function of several variables can be represented as a composition of finitely many continuous functions of two variables. We restrict our attention to decomposition problems for analytic functions which may be answered by constructing a system of partial differential equations and inequations, whose set of solutions coincides with the set of decomposable functions.

The algorithmic methods developed in this thesis allow to improve symbolic solving of PDEs. On the one hand, membership of a solution to a family of solutions, which is implicitly described by PDEs, is decidable, so that questions regarding completeness of the family of solutions can be addressed. On the other hand, adding a PDE system characterizing analytic functions of a special form to a PDE system to be investigated, may allow to extract explicit solutions of the prescribed type. This approach generalizes the well-known method of separation of variables. A small family of explicit solutions for the Navier-Stokes equations is computed.



### 1. 16. Workshop on Elliptic Curve Cryptography (ECC 2012)

Santiago de Querétaro, 28.–31. Oktober 2012

<http://ecc2012.cs.cinvestav.mx/>

Wie schon in den Jahren zuvor bestand das Programm ausschließlich aus eingeladenen Vorträgen zu allen Themenbereichen der Kryptographie basierend auf elliptischen Kurven, von mathematischen Grundlagen und Sicherheitsaspekten bis hin zu Implementierungen. Auch Aspekte kryptographischer Paarungen waren Thema mehrerer Vorträge. Die Vorträge wurden alle als Videos aufgezeichnet und sowohl die Vortragsfolien als auch die Videos der Vorträge sind auf <http://ecc2012.cs.cinvestav.mx/program.php> online verfügbar. Die Konferenz wurde hervorragend organisiert und geleitet von Neal Koblitz (University of Washington, Seattle, USA), Francisco Rodríguez-Henríquez (CINVESTAV-IPN, Mexiko) und Horacio Tapia-Recillas (UAM-Iztapalapa, Mexiko), die tatkräftig von mehreren Doktoranden des CINVESTAV-IPN unterstützt wurden.



THE 16TH WORKSHOP ON ELLIPTIC CURVE CRYPTOGRAPHY  
ECC 2012

Anders als in den meisten Vorjahren gab es keine Summerschool für Doktoranden in der Woche vor der ECC. Anstatt dessen begann die Tagung sonntags mit drei zweistündigen einführenden Vorlesungen. Craig Costello (Technische Universität Eindhoven, mittlerweile Microsoft Research) hielt eine Vorlesung zu mathematischen Grundlagen von Kryptographie basierend auf elliptischen Kurven, Francisco Rodríguez-Henríquez (CINVESTAV Mexiko) über Implementierungsaspekte in Hard- und Software und schließlich hielt Neal Koblitz, einer der beiden Erfinder von Kryptographie basierend auf elliptischen Kurven, eine Vorlesung über Angriffe gegen Signatur- und Verschlusungsverfahren.

Neben den einführenden Vorlesungen am Sonntag und den einstündigen Vorträgen der Tagung gab es auch im Rahmen der sogenannten „Rump Session“ die Möglichkeit, in fünf bis zehnminütigen Vorträgen aktuelle Ergebnisse und laufende Projekte vorzustellen. Die Rump Session fand, wie auch der Empfang der Konferenz, bei typisch mexikanischem Essen und einer landestypischen Auswahl von Getränken statt. Die Folien der Kurzvorträge sind online auf <http://ecc.2012.rump.cr.jp.to/> verfügbar. Das Rahmenprogramm wurde abgerundet durch eine Stadtführung durch das Zentrum von Santiago de Querétaro, das Teil des UNESCO Weltkulturerbes ist, sowie dem Galadinner am Dienstag Abend.

Die Tagung war eingebettet in die 45. Tagung der Mexikanischen Gesellschaft für Mathematik, die vom 28. September bis zum 2. Oktober ebenfalls in Santiago de Querétaro stattfand. Teilnehmer der ECC hatten so auch Zugang zu den Vorträgen dieser nationalen Konferenz.

Termin und Veranstaltungsort für die kommende ECC stehen mittlerweile auch fest: Die ECC 2013 wird in Leuven, Belgien, vom 16. bis 18. September 2013 stattfinden. In der Woche vor der Konferenz wird eine dreitägige Summerschool für Doktoranden und interessierte Masterstudenten stattfinden. Informationen zur ECC 2013 sind auf <https://www.cosic.esat.kuleuven.be/ecc2013/> online zu finden.

Peter Schwabe (Radboud University Nijmegen)

### 2. Workshop on SymbolicData Design

Leipzig, 13.–14. Dezember 2012

<http://symbolicdata.org/wiki/Events.2012-12-13>

Within the E-Science Benchmarking Project we invited for a workshop and hackathon to discuss and promote different aspects of the SymbolicData Project. The workshop took place at HTWK – Hochschule für Technik, Wirtschaft und Kultur Leipzig. We had two days of intense discussions about the goals, philosophy, subprojects, links etc. of the SymbolicData Project [1].

First we discussed the current state of the project. *Hans-Gert Gräbe* (Uni Leipzig) explained in detail the work done so far towards a redesign of the Data collection according to Linked Open Data standards. Within this refactoring process we distinguish more clearly between *Data* (called *XMLResources*) and *Metadata* (called *RDFResources*; interlinking of metadata is nowadays best supported by the RDF based Semantic Web Stack [2]). Such a distinction allows to express more clearly another point: Data and its semantic meaning are managed *within* different Computer Algebra Communities, Metadata are required for *Cross Community Communication* purposes. The main future focus of SymbolicData will be on the needs of such a Cross Community Communication between different Computer Algebra Communities.

*Albert Heinle* (RWTH Aachen, now U Waterloo) presented the *SDEval* framework. It grew up from the profiling and testing needs of the Free Algebra community [3], but is generic enough to serve as a best practice how to organize automated set up, run, evaluation and comparison of dedicated computational tasks on a large amount of data. The framework is written in *python*, heavily uses UNIX process management facilities to flexibly define and set up computational environments with dedicated characteristics, and can be reused for a wide range of computational tasks with different CA software. SDEval continues the SymbolicData efforts to establish standards how to set up environments for testing and benchmarking of CA software on a larger collection of given data.

*Satya Samal* (Uni Bonn) presented the PoCaB Project [4], explained in detail structural approaches within the PoCaB Databases and how data are generated within the PoCaB framework. PoCaB mainly addresses topics around categorization of differential equation systems in mass action and non-mass action kinetics in chemical systems coming from a biological background. PoCaB is interlinked with different communities within CA (Polynomial Systems Solving and the Polymake communities) and also beyond. In particular,



it heavily exploits biological databases (BioModel Database, KEGG Database) [5] that come with their own language SML and experiences how to express semantical aspects in a computer readable way.

Johannes Waldmann (HTWK Leipzig) gave a talk about Benchmarks and Competitions in Theoretical Computer Science presenting best practices of three TCS Communities: Termination, SAT and SMT. He explained the Termination Problems Data Base [6] and their way of benchmarking: They regularly organize Termination Competitions on previously agreed data from different problem categories at a central site. This competition accompanies the annual large conference in the field. Waldmann emphasized that most communities have their own (intracommunity) infrastructure – workshops, mailing lists, wiki (to adjust a „common story“) – and domain specific

- input syntax and semantics specification,
- standards for what is an acceptable proof trace,
- methods for selecting competition problems, and
- algorithms for scoring results,

that should be reused as much as possible by efforts like SymbolicData. Waldmann is involved with the StarExec Project [7] that „has the goal to provide a domain-agnostic execution platform (software and hardware) for running competitions in computational logics and developed some meta-model of competitions that covers standards for benchmarks, tools and results“.

At the meeting we decided about the future main road of the SymbolicData Project. First, the SymbolicData Project will be refocussed to address needs and efforts of *communities* within Symbolic Computation to profile, test and benchmark implementations on larger sets of data.

There is a commonly complained misrecognition of such efforts because they are not in the focus of reputational processes of the respective communities and are in rare cases acknowledged properly. Such questions arise in other experimentally based sciences, too.

SymbolicData (v.1 and v.2) had its origin within the Polynomial Systems Community, so such a refocussing has to be processed also as a reorganization of data for SymbolicData v.3. This work is on the way. A list of communities with benchmarking activities addressed by SymbolicData will be maintained on the SymbolicData website.

For the future there should be a better interlinking between (intracommunity) sources, resources and communication structures within such a community and SymbolicData. This will be carefully studied on a number of use cases in cooperation with the SPP 1489.

SDEval as a python based generic benchmarking compute framework represents best practice to run dedicated computational tasks on a large amount of given data. This code is available from the SymbolicData Public Repository.

In the near future we focus on consolidating SymbolicData and releasing a stable v.3. As a first step we moved to git and operate a public repository at github [8]. There is a Sparql endpoint [9] for SymbolicData that serves the latest RDFData. In the second half of July there will be another workshop in Leipzig to resume current progress.

Links:

- [1] The SymbolicData Project. <http://symbolicdata.org>.
- [2] The Semantic Web Stack. [http://en.wikipedia.org/wiki/Semantic\\_Web\\_Stack](http://en.wikipedia.org/wiki/Semantic_Web_Stack).
- [3] The SD Free Algebra Subproject. <http://symbolicdata.org/wiki/FreeAlgebra>.

- [4] The PoCaB Project – Platform of Chemical and Biological Analysis Using Computer Algebra Methods. <http://pocab.cg.cs.uni-bonn.de>.
- [5] Bio Model Databases. <http://www.ebi.ac.uk/biomodels-main>.
- [6] TPBD – the Termination Problems Data Base. <http://termination-portal.org/wiki/TPDB>.
- [7] The StarExec Project. <http://www.starexec.org/starexec/public/about.jsp>.
- [8] For details, see <http://symbolicdata.org/wiki/Using.Git>.
- [9] The Sparql endpoint operates at <http://symbolicdata.ontowiki.net>.

Hans-Gert Gräbe (Leipzig)

### 3. Conference on Commutative Rings, Integer-valued Polynomials and Polynomial Functions

Graz, 19.–22. Dezember 2012

<http://integer-valued.org>



Vom 16. bis zum 22. Dezember 2012 fanden im vorweihnachtlichen Graz die „Conference on Commutative Rings, Integer-valued Polynomials and Polynomial Functions“ sowie einführende Minikurse statt. Organisiert wurde die Konferenz durch Sophie Frisch, Giulio Peruginelli und Roswitha Rissner von der TU Graz.

Die Konferenz wurde eingeleitet durch eine Reihe von Minikursen, die im Zeitraum vom 16. bis 18. Dezember stattfanden. Jean-Luc Chabert, Sarah Glaz, Alan Loper, Irena Swanson und Qifan Zhang führten in diesem Rahmen mit je drei Vorlesungen in ihre Forschungsgebiete ein. Es gelang ihnen, einen hervorragenden Überblick unter anderem zu ganzzahligen Polynomen und Abschüssen, Prüfer-Bedingungen und Ultrafiltern zu geben, der als Rüstzeug für die folgende Konferenz dienlich war.

Eingeladene Sprecher der Konferenz selbst waren die Leiter der Minikurse Jean-Luc Chabert, Sarah Glaz, Alan Loper, Irena Swanson und Qifan Zhang sowie Marco Fontana und Byung Gyun Kang. In insgesamt 41 Vorträgen wurde ein breites Spektrum an Themen abgedeckt. Einige Schwerpunkte waren ganzzahlige Polynomen über kommutativen sowie nicht-kommutativen Ringen, Implikationen verschiedener Prüfer-Bedingungen und der Einsatz von Ultrafiltern. Einige Vorträge beschäftigten sich auch mit Themen aus dem Bereich der Computeralgebra, zum Beispiel präsentierte Wolfgang Herfort einen hochinteressanten Beweis der Gleichung von Hua mit Hilfe von Shirshov-Gröbner-Basen.

Unter dem Titel „Commutative rings, integer-valued polynomials, and polynomial functions“ werden einige der Präsentationen auch in den Proceedings der Konferenz vorgestellt. Diese sind aktuell noch in Arbeit und werden anschließend im Springer-Verlag erscheinen.

Stefan Toman (München)

#### 4. XIV. Mathematica-Tag

Berlin, 26. Februar 2013

[www.ordinate.de/mathematicaTag.htm](http://www.ordinate.de/mathematicaTag.htm)

Zum 14. Mal seit 1999 traf man sich am 26.02.2013 auf Einladung von WIAS (<http://www.wias-berlin.de>) und mathemas ordinate, Carsten Herrmann (<http://www.ordinate.de>) in Berlin-Mitte. Aufgelockert durch den traditionell von mathemas ordinate spendierten Imbiss gab es eine Reihe interessanter Vorträge. Interessierte können Skripte/Mathematica-Notebooks/CDFs der Vorträge erhalten (bitte eine Email senden an [carsten@ordinate.de](mailto:carsten@ordinate.de)). Herr Dr. Fuhrmann vom WIAS begrüßte die zahlreich Erschienenen und erläuterte die Aufgaben und Struktur des WIAS. Carsten Herrmann begrüßte die ca. 60 Teilnehmer mit einem kurzen Überblick über den Tagesablauf.

Im ersten Vortrag sprach Dr. Leonid Shifrin aus St. Petersburg zum Thema „RLink: linking Mathematica and R“. Herr Shifrin arbeitet als Consultant für Wolfram Research und ist der massgebliche Schöpfer des in Mathematica 9 neuen RLinks. R als mittlerweile weit verbreitete Programmiersprache und Entwicklungsumgebung für statistische Berechnungen und Grafik ist open source und für die wichtigen Rechnersysteme verfügbar. RLink ist als App Teil von Mathematica 9 und verbindet R und Mathematica; es erlaubt, Daten zwischen R und Mathematica auszutauschen, R-Code von Mathematica aus auszuführen, R-Funktionen mit Mathematica-Argumenten auszuführen, und das Ergebnis zu Mathematica zu übertragen. Herr Shifrin demonstrierte, dass sowohl R- als auch Mathematica-Anwender von RLink profitieren können.

Im zweiten Beitrag präsentierte Carsten Herrmann sein Notebook zum Thema: Survival und Reliability. Die Lebenszeitanalyse wird in zahlreichen Anwendungsbereichen, wie Medizin, Technik etc. verwendet. Mathematica bot bereits in der Vorversion (siehe vorige Mathematica-Tage) Ansätze zur Behandlung derartiger Probleme. In Version 9 wurde dies nun stark erweitert durch Funktionen wie SurvivalModelFit oder CoxModelFit, die sich gut zur Beurteilung der Survival-Schätzung und etwaiger Faktoren eignen. Mit 3 neuen Funktionen, die auch alle auf dem Konzept von Lifetime Analysis aufbauen, hat man dann auch im Bereich Reliability Techniken zur Beurteilung der Ausfallwahrscheinlichkeit von Systemen zur Verfügung.

Anschließend präsentierte Herr Dr. Rolf Mertig von der Fa. Gluon Vision einen kurzen Überblick über die technischen Unterschiede zwischen dem gratis CDF (Computable Document Format) und der CDF Enterprise 9.0, die so etwas wie standalone Mathematica-Anwendungen zu produzieren erlaubt. Er sprach auch die sich nun ergebenden „Business Opportunities“ an, erwähnte einige Beispiele, unter anderem auch die interessante Sammlung „Mathematica Scientific Demonstrations“ von Nasser M. Abbasis ([http://www.12000.org/my\\_notes/mma\\_demos/index.htm](http://www.12000.org/my_notes/mma_demos/index.htm)).

Nach der Mittagspause erläuterte Herr Prof. Dr. Rolf Sulanke in seinem Beitrag „Tensoralgebra mit Mathematica“ seinen Ansatz, den er in seinem Notebook dargestellt hat. Darin

wird ein neues Objekt „tensor“ implementiert, das im Unterschied zu den in MMA 9.0.1 angesprochenen Tensoren, die einfach nur Arrays sind, gestattet, kovariante, kontravariante und Tensoren gemischten Typs zu behandeln. Für dieses Objekt werden alle bekannten Tensoroperationen programmiert; die gesamte affine Tensoralgebra und die äußere Algebra über einem endlich-dimensionalen Vektorraum kann mit den neuen Funktionen bearbeitet werden. Die neuen Tensorfunktionen werden mit den in MMA built-in vorhandenen verglichen; Übergangsfunktionen beschreiben die Zusammenhänge. Herr Prof. Dr. Sulanke hat vor allem auch Mühe darauf verwendet, das Notebook in einem Stil zu verfassen, der zur Einarbeitung in MMA nützlich ist und es gleichzeitig für einschlägige Lehrveranstaltungen geeignet macht. Dieser mathematisch orientierte Vortrag fand recht reges Interesse. Das Notebook ist lesenswert!

Herr Dr. Markus von Almsick von der Fa. Wolfram Research bot dann „Eine Mathematica Version 9 Safari“ durch den „Dschungel“ der über 400 Neuerungen der im November 2012 erschienenen Version 9 von Mathematica. Anhand von Beispielen wurde die Tragweite der neuen Konzepte in der Statistik und Stochastik, der Bild- und Signalverarbeitung (3D-Volume-Rendering, DICOM Daten), dem User-Interface (Wolfram Predictive Interface) und bei Differentialgleichungen (Diskrete Ereignisse, stochastische Differentialgleichungen), Einheiten beleuchtet und diskutiert. Interessante Beispiele waren u.a.: Darstellung des Netzes der deutschen Bahn, Nutzung von Google-Maps etc.

Herr Dr. Jörg Polzehl vom WIAS Berlin demonstrierte die Möglichkeiten des „structural adaptive smoothing approach“, der am WIAS entwickelt wurde, und verglich es mit den in Mathematica zur Verfügung stehenden Tools. Ein kurzer Überblick über Anwendungen auf bildgebende Verfahren der Medizin rundete die Darstellung ab.

Abschliessend bot Patrick Scheibe vom Translationszentrum für regenerative Medizin der Universität Leipzig in seinem Beitrag „Verbesserung der Autocompletion in Mathematica“ eine „interessante Reise durch die Innereien“ von Mathematica. In Version 9 gibt es die automatische Autocompletion bei der Funktionseingabe. Die Art und Weise ist jedoch nicht unbedingt ideal. Patrick Scheibe erläuterte seine Methode, bei der CamelCase-Completion verwendet wird, bei der nicht nur die Vervollständigung von Präfixen (Integ zu IntegerDigits) sondern auch die Angabe nur der Grossbuchstaben – der Kamelhöcker- (also z. B. nach Eintippen von LLICP erscheint ListLineIntegralConvolutionPlot) zur Vervollständigung führt.

Abgerundet wurde der inhaltliche Tag mit einer technischen Fragen-und-Antworten-Runde (statt des Debugger in Mathematica sollte man die Eclipse-basierte Wolfram Workbench verwenden). Mit der üblichen nachmittäglichen Kaffeerunde klang der Mathematica-Tag aus. Der „Tag“ endete gegen 17h00. Der nächste, also Mathematica-Tag XV, soll dann Anfang Dezember 2013 wieder im WIAS stattfinden (Genauerer siehe <http://www.ordinate.de/mathematicaTag.htm>).

Carsten Herrmann





# XIV. Berliner Mathematica-Tag

Interdisziplinäres Kolloquium zur Anwendung von Mathematica in den Naturwissenschaften



**Weierstraß-Institut für  
Angewandte Analysis und Stochastik**  
Mohrenstr. 39  
10117 Berlin

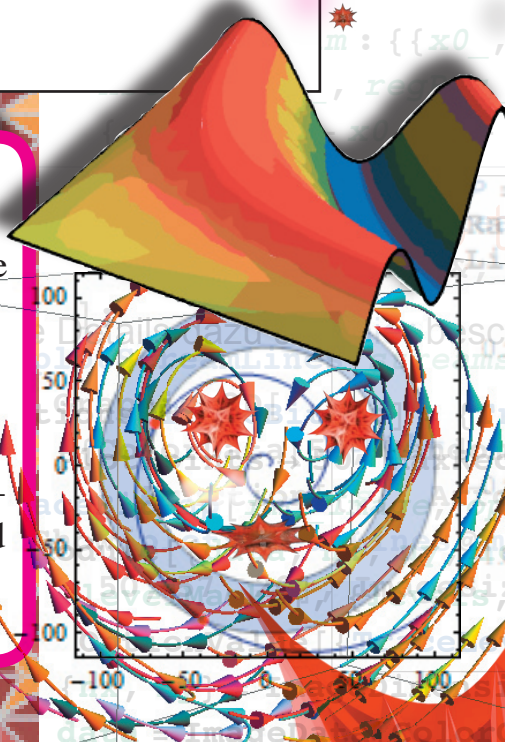
**26. Februar 2013**

## Neuigkeiten Mathematica 9

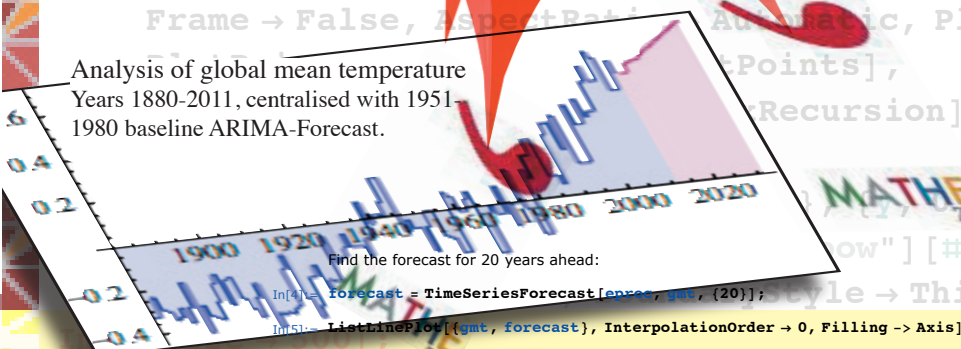
Prädiktive Schnittstelle...3D volumetrische Bildverarbeitung... symbolische Tensoralgebra...Hybrid und differentialalgebraische Gleichungen...Verbindung mit R...Einheiten (physikal. etc.)...Enterprise CDF...Zufallsprozesse...Markov-Ketten...Zuverlässigkeits- und Survival-Analyse...Zeitreihen und stochastische Differentialgleichungen...



**MATHEMATICA TAG**  
26. Februar 2013



Analysis of global mean temperature  
Years 1880-2011, centralised with 1951  
1980 baseline ARIMA-Forecast.



**Informationen/Anmeldung** <http://www.ordinate.de/mathematicaTag.html>

**mathemas | ordinate**



### 1. ECCAD – The East Coast Computer Algebra Day

Annapolis, Maryland, USA, 27.04.2013

<http://www.usna.edu/cs/eccad13/>

The East Coast Computer Algebra Day (ECCAD) is a one-day meeting for those interested in computer algebra and symbolic mathematical computation. It provides opportunities to learn and to share new results and current work in progress. The schedule includes prominent invited speakers along with contributed posters and software demonstrations. Plenty of time is allowed for unstructured interaction among the participants. Researchers, teachers, students, and users of computer algebra are all welcome!

Invited Speakers: Shafi Goldwasser (MIT), Manuel Kauers (RISC-Linz), Michael Monagan (Simon Fraser University).

This year's invited speakers represent the diverse interests of the community. Dr. Kauers' talk will focus on mathematics and algorithms in symbolic computations with differential equations. Dr. Monagan's will deal with issues involved in producing efficient software implementing algorithms for computing symbolically with polynomials. Dr. Goldwasser's talk will address security and cryptography, focusing on an interest her community shares with ours — computing with lattices. In fact, we encourage researchers in security and cryptography to attend ECCAD this year in order to foster collaboration and learning between our two communities on the many areas in which our interests overlap.

Organizing Committee: Dan Roche (US Naval Academy (chair)), Chris Brown (US Naval Academy), Dave Saunders (University of Delaware).

### 2. MEGA 2013 – Effective Methods in Algebraic Geometry

Frankfurt am Main, 3. – 7.06.2013

<http://math.uni-frankfurt.de/mega2013/>

MEGA is the acronym for Effective Methods in Algebraic Geometry (and its equivalent in Italian, French, Spanish, German, Russian, etc.). This series of biennial international conferences, with the tradition dating back to 1990, is devoted to computational and application aspects of Algebraic Geometry and related topics.

The conference will comprise invited talks, regular talks (based on a competitive submission process), software presentations, as well as a poster session.

Invited speakers are Lucia Caporaso (University Roma Tre), Felipe Cucker (City University of Hong Kong), Bas Edixhoven (University of Leiden), Benjamin Nill (Case Western Reserve University), Giorgio Ottaviani (University of Firenze), Frank-Olaf Schreyer (University of Saarbrücken), Markus Schweighofer (University of Konstanz), Seth Sullivant (North Carolina State University) and Rekha Thomas (University of Washington).

### 3. ACAT 2013 – 15th International Workshop on Advanced Computing and Analysis Techniques in Physics Research

Beijing, 16. – 21.5.2013

<http://acat2013.ihep.ac.cn/>

The ACAT workshop series, formerly AIHENP (Artificial Intelligence in High Energy and Nuclear Physics), was created back in 1990. Its main purpose is to gather researchers

related with computing in physics research together, from both physics and computer science sides, and bring them a chance to communicate with each other. It has established bridges between physics and computer science research, facilitating the advances in our understanding of the Universe at its smallest and largest scales. With the Large Hadron Collider and many astronomy and astrophysics experiments collecting larger and larger amounts of data, such bridges are needed now more than ever.

The 15th edition of ACAT aims to bring related researchers together, once more, to explore and confront the boundaries of computing, automatic data analysis and theoretical calculation technologies. It will create a forum for exchanging ideas among the fields and will explore and promote computing, data analysis and theoretical calculation technologies in fundamental physics research.

### 4. Workshop Questions, Algorithms, and Computations in Abstract Group Theory

Braunschweig, 21. – 24.5.2013

[http://www.icm.tu-bs.de/ag\\_algebra/ws-qac/index.php](http://www.icm.tu-bs.de/ag_algebra/ws-qac/index.php)

More than 100 years ago, Dehn proposed his famous problems on abstract groups: the word problem, the conjugacy problem and the isomorphism problem. It is long known that all three problems are undecidable in general. Nonetheless, they have inspired a rich theory of computations in abstract group theory.

There are various classes of groups, such as word hyperbolic, automatic and polycyclic groups, for which many natural decision problems are solvable. On the other hand, there are constructions of groups with unexpected properties such as the Tarski or Dehn monsters. Most problems are undecidable in these monsters. It remains open to understand both of these opposite ends and where the boundary between them lies.

Recently, the new research topic of cryptography based on abstract groups has been invented. This topic requires fundamental knowledge about the complexity and the efficiency of various algorithms on abstract groups. This has produced a new interest in computations with abstract groups.

Our aim is to combine researchers from the areas of abstract group theory, computer science and algebraic geometry to obtain new advances in algorithmic group theory.

### 5. Syzygies in Berlin

Berlin, 27. – 31.5.2013

<http://syzygies.math.fu-berlin.de/>

The workshop Syzygies in Berlin will bring together mathematicians ranging from graduate students to senior experts to study classical results and open problems surrounding syzygies, free resolutions and regularity. Syzygies in Berlin will take place at the Zuse-Institut.

The workshop's center of gravity is formed by four short courses (D. Eisenbud, R. Pandharipande, H. Schenk, F.-O. Schreyer). Interaction between early-stage and senior mathematicians will be facilitated by numerous working sessions, with computer algebra playing a supporting role. Three invited lectures will introduce participants to recent developments in the field.

## 6. CoCoA 2013 – International School on Computer Algebra

Osnabrück, 10. – 14.6.2013

<http://cocoa.dima.unige.it/conference/cocoa2013/>

Die CoCoA-Schule richtet sich an Diplomanden und Doktoranden aus der ganzen Welt, die an Themen aus der kommutativen Algebra oder algebraischen Geometrie arbeiten und das Computeralgebrasystem CoCoA einsetzen wollen. Es wird zwei Kurse mit zugehörigen Tutorien geben:

- (1) Lorenzo Robbiano, *Sets of Points and Mathematical Models* (Tutorien: Maria-Laura Torrente)
- (2) Winfried Bruns, *Algorithms for Toric Geometry* (Tutorien: t.b.a.)

Die CoCoA Schule findet bereits zum achten Mal statt und schließt sich an die erstmals in Deutschland stattfindende Konferenz MEGA 2013 an. Neben den Kursen und Tutorien wird es auch eine Poster-Session geben, in der die Teilnehmer ihre eigenen Arbeiten präsentieren sollen. Details zur Anmeldung und Durchführung sind auf der angegebenen Webseite abrufbar. Anmeldeschluss ist der 31.3.2013.

## 7. ISSAC 2013 – The 38th International Symposium on Symbolic and Algebraic Computation

Boston, USA, 26. – 29.06.2013

<http://www.issac-conference.org/2013/>

The International Symposium on Symbolic and Algebraic Computation (ISSAC) is the premier conference for research in symbolic computation and computer algebra. ISSAC 2013 is the 38th meeting in the series, started in 1966 and held annually since 1981, in North America, Europe and Asia. The conference presents a range of invited speakers, tutorials, poster sessions, software demonstrations and vendor exhibits with a centerpiece of contributed research papers.

Invited speakers are Henry Cohn (Microsoft Research, USA), Hendrik Lenstra (Universiteit Leiden, The Netherlands), Mohab Safey El Din (Paris 6, France). Invited software speaker is Stephen Wolfram (Wolfram Research Inc., USA).

## 8. CICM 2013 – Conference on Intelligent Computer Mathematics

Bath, UK, 8.– 12.07.2013

<http://www.cicm-conference.org/2013>

As computers and communications technology advance, greater opportunities arise for intelligent mathematical computation. While computer algebra, automated deduction, mathematical publishing and novel user interfaces individually have long and successful histories, we are now seeing increasing opportunities for synergy among these areas. The Conference on Intelligent Computer Mathematics offers a venue for discussing these areas and their synergy.

The conference will take place at the University of Bath ([www.bath.ac.uk](http://www.bath.ac.uk)), with James Davenport as the local organiser. It consists of four tracks: Calculemus (Chair: Wolfgang Windsteiger), Digital Mathematical Libraries (Chair: Petr Sojka), Mathematical Knowledge Management (Chair: David Aspinall) and Systems and Projects (Chair: Christoph Lange)

## 9. Fq11 – The 11th International Conference on Finite Fields and their Applications

Magdeburg, 22. – 26.07.2013

<http://www.math.uni-magdeburg.de/~fq11/>

The 11th International Conference on Finite Fields and their Applications will be held at Otto-von-Guericke University in Magdeburg, Germany. Invited speakers are Anne Canteaut (INRIA, France), Xiangdong Hou (University of South Florida, USA), Nicholas Katz (Princeton University, USA), Daniel Panario (Carleton University, Canada), Henning Stichtenoth (Sabanci University, Turkey), Christopher Umans (California Institute of Technology, USA) and Geertrui van de Voorde (Vrije Universiteit Brussel, Belgium).

## 10. Workshop on SymbolicData Design

Leipzig, 25. – 27.07.2013

<http://symbolicdata.org/wiki/Events.2013-07>

We invite for a second Workshop to discuss progress and prospects of the SymbolicData Project and resume the work done within the E-Science Benchmarking Project. The Workshop will take place in Leipzig at HTWK – Hochschule für Technik, Wirtschaft und Kultur Leipzig.

## 11. S<sup>2</sup>AM 2013 - Summer School in Algorithmic Mathematics

Hamburg, 2.9. – 6.9.2013

<http://www.computeralgebra.de/s2am-2013/>

Die „Summer School in Algorithmic Mathematics“ ist eine alljährliche Sommerschule, die sich an junge Wissenschaftler aus der algebraischen Geometrie, Gruppentheorie und Zahlentheorie richtet. Zusätzlich zu drei interessanten Vortragsreihen, bietet sie den Teilnehmern eine Plattform, sich und die eigene Arbeit in Form eines Vortrags oder eines Posters vorzustellen und sich mit anderen auszutauschen.

Die diesjährigen Vortragsreihen werden gehalten von: Claus Fieker (Kaiserslautern), Anne Frühbis-Krüger (Hannover), Alice Niemeyer (Aachen).

Die S<sup>2</sup>AM wird finanziert aus den Mitteln des DfG Schwerpunktprogramms 1489, und es stehen eine begrenzte Anzahl an kostenfreien Übernachtungsmöglichkeiten zur Verfügung.

## 12. CASC 2013 – 15th International Workshop on Computer Algebra in Scientific Computing

Berlin, 9. – 13.09.2013

<http://www14.in.tum.de/CASC2013/>

The methods of Scientific Computing play an important role in the natural sciences and engineering. Significance and impact of computer algebra methods and computer algebra systems for scientific computing has increased considerably over the last decade. Nowadays, computer algebra systems such as CoCoA, Macaulay, Magma, Maple, Mathematica, Maxima, Reduce, Singular and others enable their users to exploit their powerful facilities in symbolic manipulation, numerical computation, visualization. The ongoing development of computer algebra systems, including their integration and adaptation to modern software environments, puts



them to the forefront in scientific computing and enables the practical solution of many complex applied problems in the domains of natural sciences and engineering.

The topics addressed in the workshop cover all the basic areas of scientific computing as they benefit from the application of computer algebra methods and software.



### 13. Industrial Applications and Prospects of Computer Algebra 2013

Berlin, 16. – 17.09.2013

<http://www.computeralgebra.de/IndustrialApplications2013>

Am 16. und 17. September 2013 veranstaltet die Fachgruppe Computeralgebra in den Räumen des ZIB in Berlin einen Workshop zu Industrieanwendungen von Computeralgebra. Hauptaugenmerk liegt dabei auf der Schnittstelle zwischen mathematischen und praktischen Aspekten des Computeralgebraeinsatzes sowie auf Computeralgebra-Tools. Weitere Details finden Sie auf Seite 6.

### 14. 43. Jahrestagung der Gesellschaft für Informatik: Informatik 2013 – Informatik angepasst an Mensch, Organisation und Umwelt

Koblenz, 16. – 20.09.2013

<http://informatik2013.de/>

Die 43. Jahrestagung der Gesellschaft für Informatik findet in Koblenz statt. Vom 16. bis 20. September 2013 werden am Campus der Universität in Koblenz Workshops, Tutorien, wissenschaftliche und praxisnahe Sitzungen sowie sechs Partnerkonferenzen durchgeführt. Führende Personen aus Wissenschaft, Politik und Praxis geben einen Überblick über aktuelle Entwicklungen rund um das Leitthema der Tagung sowie über weitere aktuelle Ergebnisse aus Forschung und Entwicklung.

### 15. 18th ÖMG Congress and Annual DMV Meeting

Innsbruck, Österreich, 23. – 27.09.2013

<https://math-oemg-dmv-2013.uibk.ac.at/cms/index.php/home>

Plenary speakers are Ernst Hairer (Genf), Gitta Kutyniok (Berlin), Michael Lacey (Atlanta), Catharina Stroppel (Bonn), Michael Struwe (Zürich), Endre Szemerdi (New Jersey), Josef Teichmann (Zürich), Cedric Villani (Lyon and Paris), Umberto Zannier (Pisa) and Mathias Beiglböck (Wien). Public lecture will be given by Karl Sigmund (Wien).



## Aufnahmeantrag für Mitgliedschaft in der Fachgruppe Computeralgebra

(Im folgenden jeweils Zutreffendes bitte im entsprechenden Feld ☐ ankreuzen bzw. \_\_\_\_\_ ausfüllen.)

Titel/Name: _____		Vorname: _____	
<b>Privatadresse</b>			
Straße/Postfach: _____			
PLZ/Ort: _____		Telefon: _____	
E-mail: _____		Telefax: _____	
<b>Dienstanschrift</b>			
Firma/Institution: _____			
Straße/Postfach: _____			
PLZ/Ort: _____		Telefon: _____	
E-mail: _____		Telefax: _____	
Gewünschte Postanschrift: <input type="checkbox"/> Privatadresse <input type="checkbox"/> Dienstanschrift			

1. Hiermit beantrage ich zum 1. Januar 201\_\_\_\_ die Aufnahme als Mitglied in die Fachgruppe

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

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

- ☐ **€ 7,50** für Mitglieder einer der drei Trägergesellschaften
- |                               |                        |
|-------------------------------|------------------------|
| <input type="checkbox"/> GI   | Mitgliedsnummer: _____ |
| <input type="checkbox"/> DMV  | Mitgliedsnummer: _____ |
| <input type="checkbox"/> GAMM | Mitgliedsnummer: _____ |

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

- ☐ **€ 7,50.** Ich bin aber noch nicht Mitglied einer der drei Trägergesellschaften. Deshalb beantrage ich gleichzeitig die Mitgliedschaft in der

☐ GI ☐ DMV ☐ GAMM.

und bitte um Übersendung der entsprechenden Unterlagen.

- ☐ **€ 9,00** für Nichtmitglieder der drei Trägergesellschaften. ☐ Gleichzeitig bitte ich um Zusendung von Informationen über die Mitgliedschaft in folgenden Gesellschaften:

☐ GI ☐ DMV ☐ GAMM.

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

- |                          |  |
|--------------------------|--|
| <input type="checkbox"/> | a. Zusendungen aller Art mit Bezug zur Informatik, Mathematik bzw. Mechanik.                 |
| <input type="checkbox"/> | b. Zusendungen durch wiss. Institutionen mit Bezug zur Informatik, Mathematik bzw. Mechanik. |
| <input type="checkbox"/> | c. Nur Zusendungen interner Art von GI, DMV bzw. GAMM.                                       |

Ort, Datum: \_\_\_\_\_ Unterschrift: \_\_\_\_\_

Bitte senden Sie dieses Formular an:

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

---

## Fachgruppenleitung Computeralgebra 2011-2014

---

**Sprecher:**

Prof. Dr. Florian Heß  
Carl-von Ossietzky Universität Oldenburg  
Institut für Mathematik, 26111 Oldenburg  
0441-798-2906, -3004 (Fax)  
florian.hess@uni-oldenburg.de  
<http://www.staff.uni-oldenburg.de/florian.hess>

**Fachreferentin Publikationen und Promotionen:**

Prof. Dr. Anne Fröhbis-Krüger  
Institut für Algebraische Geometrie  
Welfengarten 1, 30167 Hannover  
0511-762-3592  
fruehbis-krueger@math.uni-hannover.de  
<http://www.iag.uni-hannover.de/~anne>

**Fachreferent Physik:**

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

**Fachexperte Industrie:**

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

**Fachreferentin Computational Engineering, Vertreterin der GAMM:**

Dr.-Ing. Sandra Klinge  
Lehrstuhl für Mechanik - Materialtheorie  
Ruhr-Universität Bochum  
Universitätsstr. 150, 44780 Bochum  
0234-32-26552, -14154 (Fax)  
sandra.klinge@rub.de  
[www.am.bi.ruhr-uni-bochum.de/Mitarbeiter/Ilic](http://www.am.bi.ruhr-uni-bochum.de/Mitarbeiter/Ilic)

**Vertreter der DMV:**

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

**Fachreferent CA an der Hochschule:**

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

**Fachexperte Schule:**

OStR Jan Hendrik Müller  
Rivius-Gymnasium der Stadt Attendorn  
Westwall 48, 57439 Attendorn  
02722-5953 (Sekretariat)  
jan.mueller@math.uni-dortmund.de  
[www.mathebeimueller.de](http://www.mathebeimueller.de)

**Redakteur Rundbrief:**

Dr. Michael Cuntz  
Fachbereich Mathematik  
Technische Universität Kaiserslautern  
Postfach 3049, 67653 Kaiserslautern  
0631-205-2515  
cuntz@mathematik.uni-kl.de  
<http://www.mathematik.uni-kl.de/~cuntz>

**Stellvertretende Sprecherin:**

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

**Fachexperte Lehre und Didaktik:**

Prof. Dr. Gilbert Greefrath  
Westfälische Wilhelms-Universität Münster  
Institut für Didaktik der Mathematik und der Informatik  
Fliednerstr. 21, 48149 Münster  
0251-8339396  
greefrath@uni-muenster.de  
<http://www.greefrath.de>

**Fachreferentin Fachhochschulen:**

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

**Fachreferent CA-Systeme und -Bibliotheken:**

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

**Fachreferent Schwerpunktprogramm 1489:**

Prof. Dr. Jürgen Klüners  
Mathematisches Institut der Universität Paderborn  
Warburger Str. 100, 33098 Paderborn  
05251-60-2646, -3516 (Fax)  
klueners@math.uni-paderborn.de  
<http://www2.math.uni-paderborn.de/people/juergen-klueners.html>

**Fachreferent Themen und Anwendungen:**

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

**Vertreter der GI:**

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

**Koordinator Internetauftritt:**

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

**Redakteurin Rundbrief:**

Dr. Gohar Kyureghyan  
Otto-von-Guericke Universität Magdeburg  
Institut für Algebra und Geometrie  
Universitätsplatz 2, 39106 Magdeburg  
0391-67-11650, -11213 (Fax)  
gohar.kyureghyan@ovgu.de  
<http://fma2.math.uni-magdeburg.de/~gkyureg>

## Werbeseite

## Werbeseite