

# Computeralgebra Rundbrief

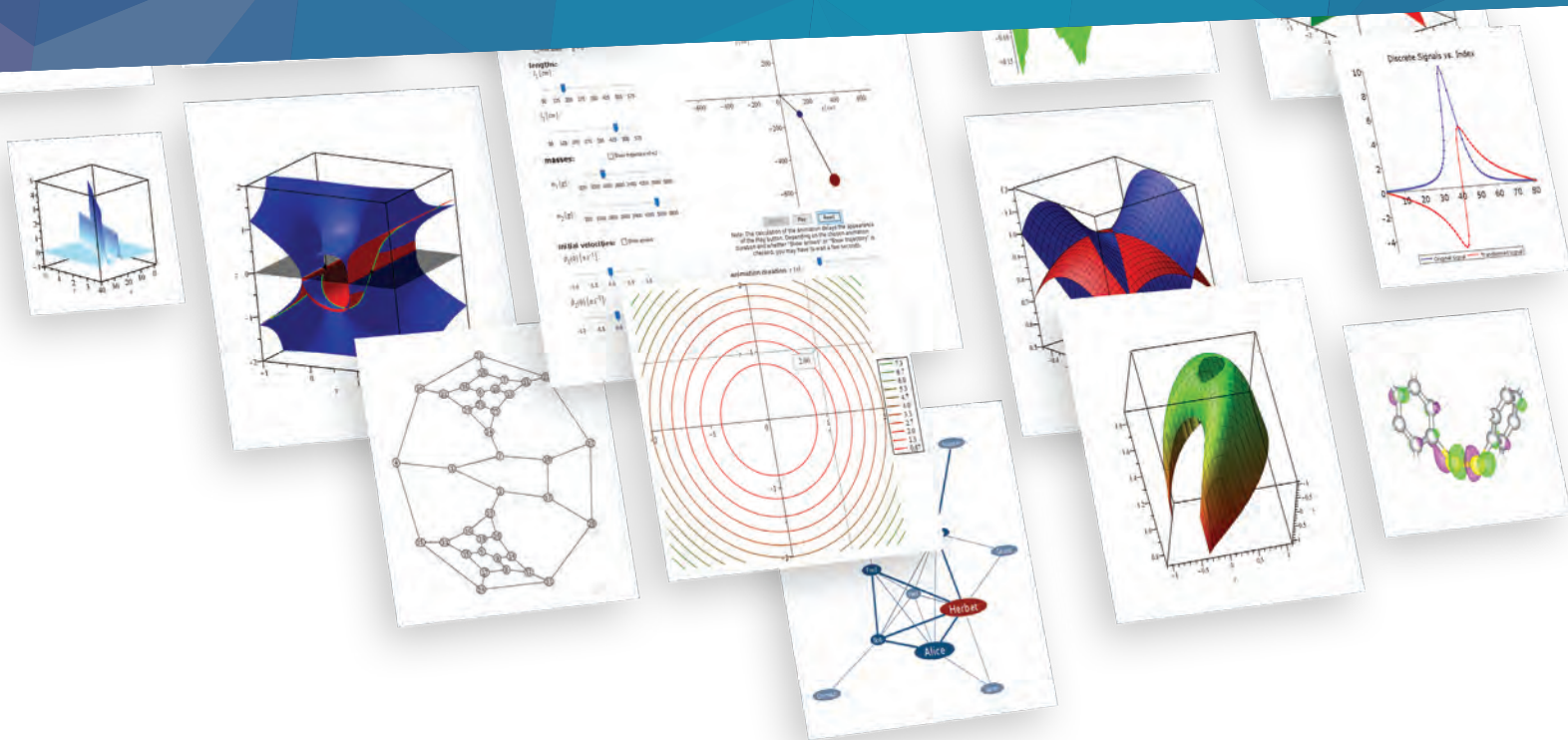
> Ausgabe 67

- ▶ Diskrete Logarithmen mit 30750 Bits
- ▶ Quantum Algebraic Attack
- ▶ GTPack
- ▶ Computeralgebra in der Lehre unter Corona
- ▶ Le compte est bon



# Sie nutzen Maple 2020 noch nicht?

Sehen Sie, was Sie bisher versäumt haben



## Neues Maple 2020 jetzt verfügbar!

Maple 2020 bietet eine umfangreiche Sammlung von Verbesserungen sowohl für langjährige Kunden als auch für diejenigen, die Maple zum ersten Mal verwenden.

Neben einer noch leistungstärkeren Mathematik-Engine bietet Maple 2020 auch neue und verbesserte Tools für interaktive Problemlösung, Anwendungsentwicklung, Lernfunktionen für Studenten, Dokumentenerstellung, Programmierung und mehr.

Probieren Sie Maple kostenlos für 15 Tage ohne Verpflichtungen  
[www.maplesoft.com/CAR2020](http://www.maplesoft.com/CAR2020)



## Inhaltsverzeichnis

<b>Inhalt</b> . . . . .	3
<b>Impressum</b> . . . . .	4
<b>Mitteilungen der Sprecher</b> . . . . .	5
<b>Tagungen der Fachgruppe</b> . . . . .	6
<b>Themen und Anwendungen</b> . . . . .	7
<i>Diskrete Logarithmen mit 30750 Bits</i> (J. Zumbrägel) . . . . .	7
<i>Quantum Algebraic Attack</i> (X. Bogomolec, P. Nonnenmann) . . . . .	10
<b>Neues über Systeme</b> . . . . .	12
<i>GTPack</i> (R. M. Geilhufe, W. Hergert) . . . . .	12
<b>Computeralgebra in der Hochschule</b> . . . . .	16
<i>Erfahrungsbericht aus Hannover über das Sommersemester 2020</i> (C. Pegel, M. Soriano, M. H. Vo Thi) . . . . .	16
<i>Feedback zur digitalen Lehre von Computeralgebra im Sommersemester 2020</i> (Y. Weber) . . . . .	18
<b>Computeralgebra in der Schule</b> . . . . .	19
<i>Le compte est bon</i> (M. Cuntz) . . . . .	19
<b>Publikationen über Computeralgebra</b> . . . . .	22
<b>Besprechungen zu Büchern der Computeralgebra</b> . . . . .	23
<i>Wolfram Hergert, R. Matthias Geilhufe: Group Theory in Solid State Physics and Photonics</i> (M. Kreuzer) . . . . .	23
<b>Promotionen in der Computeralgebra</b> . . . . .	24
<b>Berufungen</b> . . . . .	25
<b>Berichte von Konferenzen</b> . . . . .	26
<b>Hinweise auf Konferenzen</b> . . . . .	29
<b>Fachgruppenleitung Computeralgebra 2020–2023</b> . . . . .	31

## Impressum

Der Computeralgebra-Rundbrief wird herausgegeben von der Fachgruppe Computeralgebra der GI in Kooperation mit der DMV und der GAMM (verantwortlicher Redakteur: Dr. Fabian Reimers [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: <https://www.fachgruppe-computeralgebra.de>.

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

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



---

## Mitteilungen der Sprecher

---

*Liebe Mitglieder der Fachgruppe Computeralgebra,*

*zuerst einmal hoffen wir, dass Sie, Ihre Familien und auch Ihre Teams und Arbeitsgruppen bis jetzt gut durch die Unbilden der Corona-Pandemie gekommen sind, und wünschen Ihnen auch weiterhin vor allem Gesundheit, Anpassungsfähigkeit an die Situation und gute Nerven.*

*Wer hätte bei der Fertigstellung des letzten Rundbriefes Ende Februar gedacht, dass sich die Ereignisse so überschlagen würden? Damals starteten wir mit viel Elan in die neue 3-Jahresphase und planten gleich vier große Aktivitäten der Fachgruppe binnen 15 Monaten: die Industrietagung mit thematischem Fokus auf (Post-Quantum)-Kryptographie im September 2020, je ein Minisymposium auf der DMV-Jahrestagung und der Jahrestagung der GAMM sowie die Fachgruppen-Tagung im Frühjahr 2021. Schon Ende März hatte die Pandemie dann alle diese Pläne durcheinandergewirbelt. Ringsherum wichen Konferenzen auf Online-Formate aus oder verschoben um ein Jahr und auch wir mussten alle Pläne auf den Prüfstand stellen.*

*Bei der Industrietagung liegt ein wichtiger Fokus auf dem Herstellen von Kontakten zwischen Forschern, Industrie und Nachwuchs, so dass wir ein Online-Format hier für nicht wirklich zielführend halten, weswegen die Entscheidung für eine Verschiebung um ein Jahr nicht schwer fiel. Aus ähnlichen Gründen nahmen wir von dem Minisymposium mit acht Vorträgen bei der nun online stattfindenden DMV-Jahrestagung Abstand, denn unter den neuen Randbedingungen sahen wir den Networking-Effekt zumindest deutlich beeinträchtigt und konnten uns auch einer ausreichenden Resonanz nicht mehr sicher sein. Die GAMM nahm uns die Entscheidung über das dort geplante Minisymposium ab, indem die GAMM-Jahrestagung komplett um ein Jahr verschoben wurde. Für die Fachgruppentagung 2021, die nach langer Zeit erstmals nicht in Kassel hätte stattfinden sollen, sondern in München, folgen wir diesem Beispiel und verschieben ebenfalls um ein Jahr auf das Frühjahr 2022 in der Hoffnung, dass bis dahin auch eine mittelgroße Tagung wieder in irgendeiner Form in Präsenz stattfinden kann.*

*Als kleines Trostpflaster für unser ausgefallenes Minisymposium "Computeralgebra" bei der DMV-Jahrestagung und für das ebenfalls entfallene Minisymposium "Algebraic Methods in the Sciences" wird es jedoch einen kleinen Online-Workshop mit 4 Vorträgen am 27.11.2020 geben. Die Ankündigung dazu finden Sie auf der nächsten Seite.*

*Doch nicht nur die Pläne der Fachgruppe wurden durcheinander geworfen. Alle von uns, die in der (Hochschul-)Lehre tätig sind, mussten sich für die plötzlich erzwungene Online-Lehre mehr oder minder selbst neu erfinden. In der Rubrik „Computeralgebra in der Hochschule“ finden Sie in diesem Rundbrief zwei Erfahrungsberichte. Über weitere Kurzberichte, die noch andere Aspekte der Computeralgebra in Corona-Zeiten beleuchten oder vielleicht neuere Entwicklungen im 'hybriden' Wintersemester 20/21 zum Thema haben, würden wir uns freuen und könnten vielleicht noch zwei oder drei im nächsten Rundbrief abdrucken.*

*Auch die Computeralgebra selbst darf in diesem Heft natürlich nicht zu kurz kommen: Unter „Themen und Anwendungen“ findet sich ein Bericht über die Berechnung eines diskreten Logarithmus mit 30750 Bits – eine deutliche Verbesserung des vorigen Rekords. Das Paket GTPack für Anwendungen der Gruppentheorie auf Probleme aus dem Bereich der Physik ist Gegenstand des Beitrags in der Rubrik „Neues über Systeme“. Der Beitrag zur „Computeralgebra in der Schule“ beleuchtet dieses Mal einen Typ von Rechenaufgabe aus einer populären französischen Gameshow mit Hilfe von Kombinatorik und Computeralgebra.*

*Wir wünschen Ihnen eine angenehme und anregende Lektüre.*

Anne Frühbis-Krüger

Gregor Kemper

---

## Tagungen der Fachgruppe

---

Der Coronapandemie sind leider beide Minisymposia mit Themen der Computeralgebra auf der DMV-Jahrestagung zum Opfer gefallen: „Algebraic Methods for the Sciences“, organisiert von Ulrich Bauer, Paul Breiding und Rainer Sinn, sowie „Computeralgebra“ organisiert von Michael Cuntz, Anne Frühbis-Krüger, Max Horn und Gregor Kemper. Dass die Situation derzeit keine Veranstaltungen in der althergebrachten Form zulässt, steht für uns außer Frage. Doch viele größere Konferenzen und auch einige Oberseminare haben im letzten Semester und im Sommer gute Vorbilder für Onlineformate geliefert. Daher wird es einen kleinen Onlineworkshop als zumindest teilweisen Ersatz für die Minisymposia geben:

### Workshop Computational Algebra 2020

Virtueller Workshop, 27.11.2020

[www.fachgruppe-computeralgebra.de/ca2020](http://www.fachgruppe-computeralgebra.de/ca2020)

#### Veranstaltungsort & Registrierung

Der Workshop findet am 27. November 2020 von 13–17 Uhr (MEZ) statt und wird virtuell an der TU Kaiserslautern gehostet. Zur Teilnahme am Workshop ist eine Anmeldung im Vorfeld erforderlich, durch E-Mail an Frau Ingrid Dietz ([idietz@mathematik.uni-kl.de](mailto:idietz@mathematik.uni-kl.de)) mit dem Betreff „Workshop Computational Algebra 2020“ sowie unter Angabe ihres vollen Namens und ihrer Affiliation. Allen registrierten Teilnehmerinnen und Teilnehmer werden Teilnahmelink und Zugangscode per E-Mail zugesandt.

#### Vortragende

- Christian Eder (Kaiserslautern)
- Kathlen Kohn (Stockholm)
- Anna-Laura Sattelberger (Leipzig)
- Rainer Sinn (Berlin)

Titel und Abstracts der Vorträge werden in Kürze auf der Webseite der Veranstaltung veröffentlicht.

Bei weiteren Fragen erteilen die Organisatoren gerne Auskunft:

- Paul Breiding ([p.breiding@tu-berlin.de](mailto:p.breiding@tu-berlin.de))
- Michael Cuntz ([cuntz@math.uni-hannover.de](mailto:cuntz@math.uni-hannover.de))
- Max Horn ([horn@mathematik.uni-kl.de](mailto:horn@mathematik.uni-kl.de))



### Berechnung eines diskreten Logarithmus mit 30750 Bits

Jens Zumbärgel (Universität Passau)

jens.zumbraegel@uni-passau.de

Das diskrete Logarithmusproblem gehört neben dem Faktorisierungsproblem zu den wichtigsten Grundbausteinen der heutigen Public-Key-Kryptographie, doch deren Sicherheit könnte zukünftig auf etwas wackeligeren Beinen stehen. Zum Einen wird seit einigen Jahren über Fortschritte bei der Entwicklung von Quantencomputern berichtet, welche beide Probleme brechen können. Zum Anderen sind bestimmte diskrete Logarithmusprobleme in Körpern kleiner Charakteristik auch für klassische Computer wesentlich leichter als lange Zeit angenommen.

Nun wurde eine Rekordberechnung eines diskreten Logarithmus mit 30750 Bits aufgestellt, welche den bisherigen Rekord von 9234 Bits weit übertrifft. Die neue Berechnung ist die erste größere Demonstration, dass die theoretisch schnellsten Verfahren, die quasipolynomiellen Algorithmen, auch praktisch effizient sind.

---

#### Eine Rekordberechnung

Sei  $\mathbb{F}_2$  der Körper mit zwei Elementen, sei  $\mathbb{F}_{2^{30}} := \mathbb{F}_2[T]/(T^{30}+T+1)$  ein Erweiterungskörper vom Grad 30 sowie  $t := [T] \in \mathbb{F}_{2^{30}}$ , und sei

$$\mathbb{F}_{2^{30750}} := \mathbb{F}_{2^{30}}[X]/(X^{1025} + X + t^3)$$

ein Erweiterungskörper vom Grad 1025 sowie  $x := [X] \in \mathbb{F}_{2^{30750}}$ . Dann ist  $\alpha := x + t^9$  ein (vermuteter) Erzeuger der zyklischen Gruppe  $G := \mathbb{F}_{2^{30750}}^*$ . Um ein pseudozufälliges Element zu wählen, betrachtet man die Nachkommastellen der Konstante  $\pi$  und definiert

$$\beta := \sum_{i=0}^{30749} ([2^{i+1}\pi] \bmod 2) t^{29-(i \bmod 30)} x^{[i/30]} \in G.$$

Im Mai 2019 wurde der diskrete Logarithmus von  $\beta$  zur Basis  $\alpha$  berechnet, also eine Zahl  $\ell$  mit  $\beta = \alpha^\ell$ , welche 30750 Bits oder ca. 9300 Dezimalstellen groß ist. Für die Berechnung wurde ein High-Performance-Cluster am EPFL in Lausanne und eine Rechenzeit von ca. 2900 Core-Jahren verwendet. Um dieses Resultat einzuordnen, seien in Tabelle 1 einige Projekte der letzten Jahre von ähnlicher Größenordnung aufgelistet.

---

#### Bruch der $L(\frac{1}{3})$ -Barriere

Berechnungen von diskreten Logarithmen derartiger Größenordnung waren vor nicht einmal 10 Jahren noch undenkbar. Bis dahin war man davon ausgegangen, dass die schnellsten Index-Calculus-Verfahren für diskrete Logarithmen in einem endlichen Körper  $\mathbb{F}_Q$  mit  $Q$  Elementen die subexponentielle Laufzeit

$$L_Q(\frac{1}{3}) := \exp(O((\log Q)^{1/3}(\log \log Q)^{2/3}))$$

benötigen. Diese Verfahren sind vom Zahlkörpersieb abgeleitet, welches bis heute die Grundlage für den schnellsten Faktorisierungsalgorithmus bildet.

Im Jahre 2013 gab es jedoch spektakuläre Entwicklungen (siehe [11]), welche wesentliche Schritte des Indexkalküls polynomiell machten und insgesamt eine quasipolynomielle Laufzeit ergaben. Diese beruhen im Wesentlichen auf zwei Ideen, nämlich

1. eine spezielle, günstige Darstellung des endlichen Körpers, etwa als

$$\mathbb{F}_{q^k}[X]/(h_1 X^q - h_0)$$

mit Polynomen  $h_i$  vom Grad höchstens 2,

2. die Faktorisierung der „systematischen Gleichung“

$$X^q - X = \prod_{\mu \in \mathbb{F}_q} (X - \mu)$$

und deren Transformationen über  $\mathbb{F}_{q^k}$ .

Dass diese Algorithmen jedoch auch nachweislich effizient sind, sofern eine geeignete Körperdarstellung gegeben ist, wurde erst später in einer Arbeit [6] gezeigt, welche auch eine neue Variante des Algorithmus beinhaltet (dazu später mehr). Kürzlich ist es sogar gelungen, die Existenz einer Darstellung zu beweisen, welche zusammen mit einer Abwandlung des Algorithmus einen beweisbar quasipolynomiellen Algorithmus für alle Körper fester Charakteristik begründet [10].

Projekt	Jahr	Laufzeit
Faktorisierung einer 768-Bit RSA-Zahl	2009	1700 Cj.
Faktorisierungen von 1007-1199-Bits Mersenne-Zahlen	2015	7500 Cj.
Diskrete Logarithmen im 768-Bit Primkörper $\mathbb{F}_p$	2016	5300 Cj.
Faktorisierung einer 795-Bit RSA-Zahl	2019	900 Cj.
Diskrete Logarithmen im 795-Bit Primkörper $\mathbb{F}_p$	2019	3100 Cj.
Diskrete Logarithmen im binären Körper $\mathbb{F}_{2^{30750}}$	2019	2900 Cj.
Faktorisierung einer 829-Bit RSA-Zahl	2020	2700 Cj.

**Tabelle 1:** Einige Großprojekte der letzten Jahre zur Faktorisierung oder zum Berechnen diskreter Logarithmen mit der Laufzeit in Core-Jahren (Cj.), vgl. [7, 8, 9, 2, 4, 3].

## Die Methode der Zweierpotenzen

Was ist die grundlegende Idee des neuen Verfahrens, welches dieser Berechnung zugrunde liegt? In der ersten Phase der Index-Calculus-Methode werden die Logarithmen von allen Körperelementen der Form  $x + u$  für  $u \in \mathbb{F}_{2^{30}}$  berechnet. Dies ist aufgrund der systematischen Gleichung und Ausnutzung der Galoisgruppe durchaus machbar und benötigte etwa 35 Core-Jahre. Bei der zweiten Phase wird eine Darstellung des Ziellements als ein Produkt  $\beta = c \prod_u (x + u)^{e_u}$  mit Exponenten  $e_u \in \mathbb{Z}$  gesucht. Dies erfolgt mit der Methode des *Abstiegs*, bei der jeweils ein Element (in der Darstellung als Polynom in  $x$ ) durch Produkte von Elementen kleineren Grades ersetzt wird. Solche Ersetzungen zu suchen ist jedoch oft sehr schwierig und das Verfahren erzeugt mitunter extrem viele Nachkommen, so dass wiederum ein  $L_Q(\frac{1}{3})$ -Algorithmus resultiert.

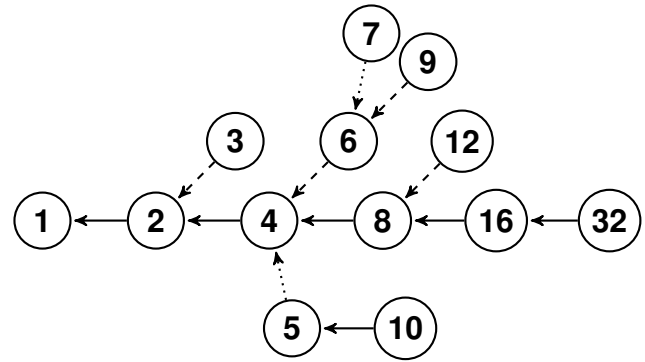
Die neue Idee besteht nun darin, ein Element  $f(x) \in \mathbb{F}_{2^{30750}}$  vom Grad  $2d$  auf einen Schlag durch Elemente  $g_i(x)$  vom Grad  $d$  zu ersetzen. Hierfür wird die ungemein nützliche Struktur der Körpererweiterungen von endlichen Körpern und deren Galois Theorie ausgenutzt. Und zwar betrachtet man das Polynom  $f$  statt über  $\mathbb{F}_{2^{30}} = \mathbb{F}_{q^k}$  über dem Erweiterungskörper  $\mathbb{F}_{q^{kd}}$ , wo es in quadratische Faktoren zerfällt. Weil man nun mit Hilfe der systematischen Gleichung diese quadratischen Faktoren über  $\mathbb{F}_{q^{kd}}$  in lineare Faktoren umschreiben kann, erhält man durch Anwenden einer Normabbildung die gewünschte Zerlegung über  $\mathbb{F}_{q^k}$ .

Wendet man dieses Prinzip rekursiv an, so lässt sich also ein Element vom Grad  $2^e$  nach nur  $e$  Schritten und in quasipolynomieller Zeit  $(\log Q)^{O(\log \log Q)}$  als Produkt von linearen Elementen schreiben, wofür wir die diskreten Logarithmen kennen. Und schließlich lässt sich jedes Körperelement – glücklicherweise – durch ein Polynom vom Grad eine Zweierpotenz repräsentieren.

## Vom Algorithmus zum Rekord

Dass der gerade skizzierte Algorithmus in allen Fällen funktioniert, ist nicht offensichtlich, und insbesondere der Beweis, dass die Grad-2-Eliminierung immer möglich ist, bildet das Kernstück des Artikels [6]. Ebenso hat man noch einige Arbeit, den Algorithmus geeignet in eine Rekordberechnung einzufügen und die jeweiligen Arbeitsschritte so zu optimieren, dass die Berechnung durchführbar wird. Erwähnt sei hier lediglich, dass

die Methode der Zweierpotenzen eine wichtige Komponente neben diversen anderen Algorithmen darstellt (vgl. Abbildung 1), und dass statt des Polynoms der systematischen Gleichung  $X^q - X$  Polynome der Form  $X^{q+1} + BX + X$ , welche von Blüher [1] untersucht wurden, einige Vorteile bringen.



**Abbildung 1:** Überblick über Abstiegsmethoden bei kleinen Graden. Die eingekreisten Zahlen entsprechen den Graden. Durchgezogene Pfeile beziehen sich auf zwei-nach-eins Abstiege, gestrichelte Pfeile stellen drei-nach-zwei Abstiege dar, und gepunktete Pfeile sind spezifische Methoden für ungerade Grade.

## Details der Berechnung

Die Berechnung des diskreten Logarithmus  $\log_\alpha \beta$  wurde in den Jahren 2016 bis 2019 an der Schweizer EPFL durchgeführt, zu den Details siehe Tabelle 2.

Phase	Zeitraum	Core-Std.
Relationenerzeugung	Feb 16	1
Lineare Algebra	Feb 16 - Apr 16	32 498
Startzerlegung	Sep 16	248 140
Klassischer Abstieg	Okt 16 - Jan 19	17 077 836
Abstieg kleiner Grade	Jan 19 - Mai 19	8 122 744
<b>Gesamtlaufzeit</b>		<b>25 481 219</b>

**Tabelle 2:** Die einzelnen Phasen und deren Laufzeit.

Mit  $q := 1024$  und  $k := 3$  haben wir eine Darstellung des Körpers  $\mathbb{F}_{2^{30750}}$  als  $\mathbb{F}_{q^k}[X]/(X^{q+1} + X + \gamma)$  mit  $\gamma := t^3$ , somit gilt für die Restklasse  $x$  die Gleichung

$$x^q = \frac{x + \gamma}{x}.$$

Die Schritte der Berechnung sind nun wie folgt.



1. *Relationenerzeugung.* Suche genügend viele  $a, b, c \in \mathbb{F}_{2^{30}} = \mathbb{F}_{326}$  derart, dass die Gleichung

$$(x^{33} + ax^{32} + bx + c)^{32} = \frac{1}{x}((b^{32}+1)x^{33} + \gamma x^{32} + (a^{32} + c^{32})x + a^{32}\gamma)$$

auf beiden Seiten in Linearfaktoren zerfällt. Unter Ausnutzung der Galoisgruppe über  $\mathbb{F}_q$  erhält man ein Gleichungssystem in 349 184 Variablen und Zeilengewicht 66.

2. *Lineare Algebra.* Löse dieses dünnbesetzte Gleichungssystem mit der Lanczos-Methode, um  $\log_\alpha(x+u)$  für alle  $u \in \mathbb{F}_{q^k}$  bestimmen.
3. *Startzerlegung.* Suche für das Zielelement  $\beta$  eine geeignete Darstellung

$$\alpha^i \beta = r(x)/s(x)$$

mit günstiger Faktorisierung für die Polynome  $r$  und  $s$ ; wir verwenden  $i := 47\,611\,005\,802$ .

4. *Klassischer Abstieg.* Um jeweils ein Element  $f(x)$  zu ersetzen, setze  $z := x^{2^{10-a}}$  und  $y := z^{2^a}$  für geeignete  $a \in \{2, 3, 4\}$  und suche Polynome  $u$  und  $v$ , so dass bei

$$u(z^{2^a})z + v(z^{2^a}) = u(y)\left(\frac{\gamma}{y+1}\right)^{2^{10-a}} + v(y)$$

eine Seite durch  $f$  teilbar ist und alle anderen Faktoren kleineren Grad haben.

5. *Abstieg für kleine Grade.* Diese Methode wird für die Grade in Abbildung 1 benutzt. Wie erwähnt beruht insbesondere der Abstieg von Grad  $2d$  nach Grad  $d$  auf eine Grad-2-Eliminierung im Erweiterungskörper  $\mathbb{F}_{q^{kd}}$ . Zu gegebenen  $f$  vom Grad 2 suchen wir  $a, b, c \in \mathbb{F}_{q^{kd}}$ , so dass bei

$$x^{q+1} + ax^q + bx + c = \frac{1}{x}((b+1)x^2 + (a+c+\gamma)x + a\gamma)$$

das Polynom der rechten Seite durch  $f$  teilbar ist und die linke Seite in Linearfaktoren zerfällt.

Man kann zeigen, dass letztere Bedingung genau dann eintritt, wenn

$$P_{kd}\left(\frac{(c-ab)^q}{(b-a^q)^{q+1}}\right) = 0$$

gilt, wobei die Polynome  $P_i$  rekursiv via  $P_1 := P_2 := 1$  und  $P_i := P_{i-1} - X^{q^{i-3}}P_{i-2}$  für  $i \geq 3$  definiert werden.

Um diese Grundideen robust und möglichst effizient zu machen, sind jedoch noch einige Kniffe vonnöten. Der interessierten Leserschaft sei hier auf die Details im Paper [5] verwiesen.

## Indiskrete Logarithmen?

Abgesehen von der bereits angedeuteten Gefahr durch Quantenalgorithmen bleibt die Frage, ob die neuartigen Algorithmen in kleiner Charakteristik sich auch auf andere Körper oder gar das Faktorisierungsproblem übertragen lassen. Bisher gelten diese Probleme noch als schwierig und somit die gängigen Kryptoverfahren als sicher, doch niemand kann weitere algorithmische Durchbrüche ausschließen, denn absolut beweisbare Sicherheitsgarantien gibt es derzeit nicht.

## Literatur

- [1] A. W. Blüher, “On  $x^{q+1} + ax + b$ ,” *Finite Fields Appl.* 10 (2014), no. 3, pp. 285–305.
- [2] F. Boudot, P. Gaudry, A. Guillevis, N. Heninger, E. Thomé, P. Zimmermann, “795-bit Factoring and Discrete Logarithms,” NMBRTHRY list, 02/12/2019.
- [3] F. Boudot, P. Gaudry, A. Guillevis, N. Heninger, E. Thomé, P. Zimmermann, “Factorization of RSA-250,” NMBRTHRY list, 28/02/2020.
- [4] R. Granger, T. Kleinjung, A. K. Lenstra, B. Wesolowski, J. Zumbrägel, “Discrete Logarithms in  $\text{GF}(2^{30750})$ ,” NMBRTHRY list, 10/07/2019.
- [5] R. Granger, T. Kleinjung, A. K. Lenstra, B. Wesolowski, J. Zumbrägel, “Computation of a 30750-Bit Binary Field Discrete Logarithm,” *Preprint* (2020), arXiv:2008.02717.
- [6] R. Granger, T. Kleinjung, J. Zumbrägel, “On the Discrete Logarithm Problem in Finite Fields of Fixed Characteristic,” *Trans. Amer. Math. Soc.* 370, no. 5 (2018), pp. 3129–3145.
- [7] T. Kleinjung, K. Aoki, J. Franke, A. K. Lenstra, E. Thomé, J. W. Bos, P. Gaudry, A. Kruppa, P. L. Montgomery, D. A. Osvik, H. te Riele, A. Timofeev, P. Zimmermann, “Factorization of a 768-Bit RSA Modulus,” *Advances in Cryptology—CRYPTO 2010*, pp. 333–350, Springer.
- [8] T. Kleinjung, J. W. Bos, A. K. Lenstra, “Mersenne Factorization Factory,” *Advances in Cryptology—ASIACRYPT 2014*, pp. 358–377, Springer.
- [9] T. Kleinjung, C. Diem, A. K. Lenstra, C. Priplata, C. Stahlke, “Computation of a 768-Bit Prime Field Discrete Logarithm,” *Advances in Cryptology—EUROCRYPT 2017*, pp. 185–201, Springer.
- [10] T. Kleinjung, B. Wesolowski, “Discrete Logarithms in Quasi-Polynomial Time in Finite Fields of Fixed Characteristic,” *Preprint* (2019), arXiv:1906.10668.
- [11] J. Zumbrägel, “Neue Algorithmen für das Diskreter-Logarithmus-Problem in kleiner Charakteristik,” *Computeralgebra-Rundbrief* 53, pp. 13–15 (2013).

# Quantum Algebraic Attack

(Game Changer Computeralgebra In the Context of Quantum Computing)

Xenia Bogomolec, Information Security  
Dr. Peter Nonnenmann, Quantum Theory  
(with scientific employment at DHBW Mannheim)

xb@quant-x-sec.com  
peter.nonnenmann@quant-x-sec.com



---

## Introduction

---

It has been widely accepted by industrial and governmental instances that currently used asymmetric cryptography relying on the hardness of integer factorization and discrete logarithm systems will no longer be valid with the advent of sufficiently potent quantum computers. Much less considered are quantum cryptanalyses on symmetric cryptography, amongst them

- 1) Chen and Gao's Quantum Algorithms for Boolean Equation Solving and Quantum Algebraic Attack on Cryptosystems, short **Quantum Algebraic Attack (QAA)** [1].
- 2) A fast quantum mechanical algorithm for database search, short **Grover's Search Algorithm** [2].

Grover's Search Algorithm was devised by *Lov Grover* in 1996. Many complexity analyses of Grover's Search on currently used cryptographic algorithms, such as AES, SHA-2 and SHA-3 have been published ever since [3, 4].

The Quantum Algebraic Attack, short QAA, published 2018, is far less understood but at the same time a strong potential game changer for basic design requirements of cryptographic algorithms. Computeralgebra plays an essential role within the innovative approach of solving the involved Boolean Multivariate Quadratic Equation System (BMQ) with a quantum computer.

---

## Mechanism of QAA

---

The Quantum Algebraic Attack applies to cryptosystems which can be reduced to a BMQ. A Boolean Quadratic Multivariate Equation System is a system of quadratic multivariate equations in which the values of the variables are the Boolean values *true* and *false*, or 1 and 0 respectively. Globally used cryptographic algorithms such as KECCAK (SHA-3), AES, TRIVIUM and MPQC (Multivariate Public Key Cryptosystem) can be reduced to a BMQ and are therefore affected by the

Quantum Algebraic Attack - if it is practical.

The key ingredients of the QAA are:

- 1) The HHL quantum algorithm [5], a Gaussian elimination solver for linear equation systems.
- 2) Computing a variety of the BMQ over  $\mathbb{C}$ .
- 3) Mapping the system to  $\mathcal{F}_2$ .

The QAA reduces the polynomial system in step 2) to a linear equation system in step 1) by encoding the polynomial system in step 2) into a specified Macaulay matrix. In the case of AES, the BMQ is in the ring  $\mathbb{C}[x]$  with 14 variables, and the Macaulay matrix of AES-256 is built from polynomials with 11904 variables (see [1], page 25, section before proposition 6.1).

---

## Feasibility of the QAA

---

The feasibility of the QAA depends on two factors:

- 1) The realization of adequately potent quantum computers.
- 2) The condition number  $\kappa$  of the Macaulay matrix derived from the BMQ of a specific affected cryptosystem.

An "Adequately potent quantum computer" in terms of number of stable qubits can only be determined for a cryptosystem if its  $\kappa$  is known.

Chen and Gao computed the runtime complexity of the QAA for the four previously mentioned cryptosystems. The complexity constant  $c$  of the *HHL algorithm* contributes to the runtime complexity linearly. The condition number  $\kappa$  is contained as a quadratic term.

Computing or estimating the values of the specific  $\kappa$  of a cryptosystem is the next step to identify whether it is prone to the QAA when sufficiently potent quantum computers are available.

Chen and Gao say: "*Condition numbers of equation systems are generally difficult to estimate, and estimating*

the condition numbers for these cryptosystems is an interesting future work” ([1], page 3).



Dr. Peter Nonnenmann is currently working on a solution to create the Macaulay matrix of the cryptosystem AES and compute its condition number  $\kappa$ . You can read more about the progress in our official paper on github [6](open source industrial-scientific project).

## Impact on Block Cipher Design

The very innovative design of the QAA has a considerable impact on how we might design cryptosystems in the future. E. g. in the case of a block cipher, we always have a symmetric key, from which sub keys are derived for the rounds of the block encryption. In classical settings and even wrt. Grover’s search, the complexity of the sub key derivation function adds to the runtime complexity of the whole encryption algorithm.

For the QAA, we have a different situation: The key derivation function has no impact on the runtime complexity, because:

- 1) The key and the expanded key are considered key variables in the BMQ.
- 2) The derived sub keys are considered state variables in the BMQ.

So for secure cryptography wrt. the QAA, we will need cryptosystems which cannot be reduced to a BMQ or

cryptosystems which can be reduced to a BMQ but have a specified Macaulay matrix with a large condition number  $\kappa$ .

We have received the friendly support from industry (Mathworks) and scientists (Prof. Dr. Siegfried Rump, Head of the Institute for Reliable Computing, TU Harburg amongst others).

Interested contributors are welcome to join us!

## References

- [1] Y. A. Chen, X. S. Gao, Quantum Algorithms for Boolean Equation Solving and Quantum Algebraic Attack on Cryptosystems, <https://arxiv.org/pdf/1712.06239v3.pdf>, 2018.
- [2] L. K. Grover, A fast quantum mechanical algorithm for database search, Gary L. Miller, editor, *Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing (STOC 1996)*, pages 212–219 ACM, 1996.
- [3] M. Grassl, B. Langenberg, M. Roetteler, R. Steinwandt, Applying Grover’s algorithm to AES: quantum resource estimates, <https://arxiv.org/abs/1712.06239>, 2018.
- [4] M. Amy, O. Di Matteo, V. Gheorghiu, M. Mosca, A. Parent, J. Schanck, Estimating the cost of generic quantum pre-image attacks on SHA-2 and SHA-3s, <https://eprint.iacr.org/2016/992.pdf> QCrypt, 2016.
- [5] A.W. Harrow, A. Hassidim, S. Lloyd, Quantum algorithm for linear systems equations, *Physical Review Letters*, 103(15): 150502, 2009.
- [6] Open source industrial-scientific project initiated by Quant-X Security & Coding GmbH P. Nonnenmann, X. Bogomolec, and various temporary contributors Feasibility of the Quantum Algebraic Attack on AES, [https://github.com/XeniaGabriela/QAA\\_Condition\\_Nr/blob/master/official\\_paper/QAA\\_on\\_AES\\_paper.pdf](https://github.com/XeniaGabriela/QAA_Condition_Nr/blob/master/official_paper/QAA_on_AES_paper.pdf): 2020.

### GTPack

**R. Matthias Geilhufe (Stockholm University)**

**Wolfram Hergert (Universität Halle)**

matthias.geilhufe@su.se

wolfram.hergert@physik.uni-halle.de



---

### Introduction

The application of group theoretical methods in physics has had a long tradition. However, recently we witness an increasing interest in group theory, initiated by various novel research directions, such as: i) great interest in topological matter and underlying symmetry principles [1]; ii) competition, interaction, and intertwining of coexisting orders in complex quantum materials [2]; iii) the availability of effective computer algebra tools allowing for analyzing super complex algebraic problems [3, 4]. To accommodate the lack of efficient tools in the community we have initiated the Mathematica group theory package GTPack, offering more than 200 modules ranging from basic abstract group and representation theory to more applied tools for electronic, photonic, or phononic structure theory as well as Landau theory of transitions [5]. With the goal of opening up an interdisciplinary discussion within the computer algebra community we are aiming to present a brief overview of the package and its application to research and education in this communication.

GTPack is build as a compilation of 17 subpackages shown in Figure 1. These packages can roughly be grouped under the headlines “Basic functionality”, “Structure”, and “Application”. Under “Basic functionality” we collect subpackages covering basic group and representation theory (calculate multiplication tables, classes, cosets, character tables, representation matrices, projection operators, Clebsch-Gordan coefficients, etc.) as well as information of the point and space groups relevant in physics applications. “Structure” consists of various packages containing modules to store, manipulate and generate structures of crystals and molecules as well as for import (export) to (from) standard formats such as cif, POSCAR, etc. “Applications” concerns: the construction of effective electronic Hamiltonians based on tight-binding, plane-wave, and crystal field theory; the construction of the master equation for photonic crystals; the calculation of phonons based on the harmonic approximation; the symmetry analysis of electronic, photonic, phononic states; etc.

---

### Download, documentation, and tutorials

The first version of GTPack was released in July 2018. The current version is GTPack 1.2, released in June 2020. The package can be downloaded at <http://gtpack.org>. We provide a full Mathematica style documentation of all available modules as well as a few introductory tutorials. The documentation and tutorials are also available online:

Download:

<http://gtpack.org/download/>

Documentation:

<http://gtpack.org/documentation/>

Tutorials:

<http://gtpack.org/tutorials/>

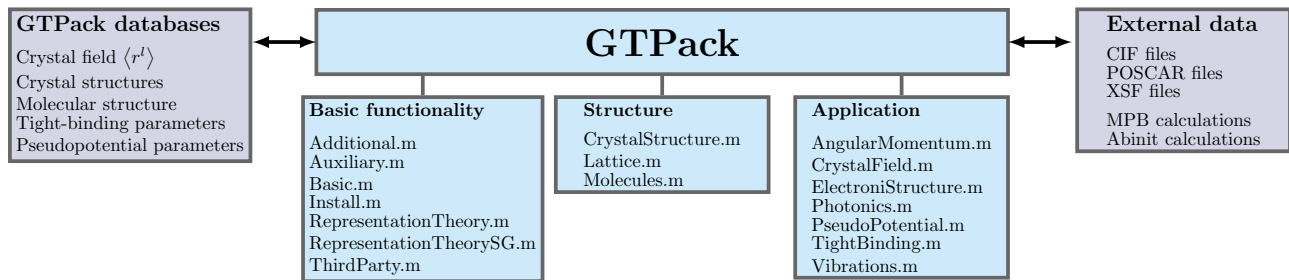
A full concise introduction into the application of group theory in solid state physics and photonics is given in our book [6]. As of August 2020, the total amount of registered GTPack users is 776.

---

### Research applications

GTPack has been applied in various research projects, covering a wide range of topics, such as photonic crystals, surface science, magnetism, topological and quantum materials, and quantum chemistry. Prior versions of GTPack were developed on the example of photonic crystals, i.e., materials with periodically modulated dielectric constant, where the transmission of light strongly depends on the frequency and wave vector. Such materials have been discussed as potential light-based alternatives to electronic devices. The application of group theory and GTPack allows to assign the corresponding irreducible representations of photonic modes to which has been used, e.g., to determine uncoupled modes in transmission experiments [7, 8]. Topological materials and topological photonic crystals exhibit non-trivial edge states with the potential for coherent transport of light and quantum information at macroscopic





**Figure 1:** *Structure of GTPack.*

scales. Using the information of irreducible representations at high symmetry points of photonic band structures GTPack was applied to determine topological photonic crystals in the formalism of the topological quantum chemistry [9]. Furthermore, in a more recent study, GTPack was applied to find higher order topological photonic crystals exhibiting robust corner modes in a 2-dimensional photonic crystal with hexagonal symmetry [10].

Topological phases of matter were also described in organic, i.e., carbon based materials, where point and line nodes in electronic band structures were identified using data mining on the organic materials database - OMDb [11]. In the post processing, GTPack was applied to understand the protection of these nodes, where two cases of nodes were distinguished [12, 13]: i) nodes protected by crystalline symmetry, i.e., nodes where bands are associated to higher dimensional irreducible representations; ii) nodes protected by band topology, i.e., nodes formed from crossings of bands with different band characteristics, also referred to as accidental crossings. Furthermore, GTPack was applied to describe the so-called Hund-nodal line semimetal phase which is predicted to occur in the twisted magnetic phases of double perovskite materials, where the magnetic order is induced by the double exchange mechanism [14]. The nonlinear interplay of magnetic order and magnetism was recently discussed using group theoretical models and ab initio investigations for  $\text{MnBi}_2\text{Te}_4$  [15] and  $\text{CrI}_3$  [16].

Besides the classification of topological phases of matter, the symmetry classification of the superconducting state has attracted a lot of attention. This process was initiated historically with the discovery of the heavy fermion superconductors in the late 1970s and 1980s. However, even today novel forms of unconventional superconductors are explored. GTPack was applied to investigate the symmetry of multipole-fluctuation-mediated superconductivity which might arise in materials like  $\text{SrTiO}_3$ ,  $\text{PrTi}_2\text{Al}_{20}$ ,  $\text{Li}_2(\text{Pd}, \text{Pt})_3\text{B}$  [17]. Furthermore, GTPack was applied to classify superconducting pairing functions which are odd in Matsubara frequency or relative time permutation, giving rise to the so-called odd-frequency or Berezinskii superconductivity [18]. Such a superconducting transition would represent an example of intrinsically dynamic quantum matter.

## Teaching applications

Lectures on group theoretical methods in physics or quantum chemistry are delivered world-wide. In these more applied lectures the focus lies on the influence of symmetry to physics or chemistry problems. Unfortunately, many relevant examples can become tedious for larger symmetry groups if performed with pen and paper. Hence, students are either confronted with exercises containing simple groups which are not necessarily the most relevant ones in applications or they are referred to huge collections of tables which can easily become tiring. GTPack provides a simple computational framework where students can perform calculations on their own after having learned the underlying principles. This way the lecture can concentrate on the discussion and interpretation of the results. Furthermore, examples based on GTPack are more flexible when it comes to questions, e.g., with respect to modifications of the underlying symmetry of an example. Additionally, the usage of GTPack can be taught as a separate computational course which could be based on the examples explained in our book [6].

Furthermore, GTPack modules on tight-binding or plane wave approaches can nicely be incorporated into examples within lectures on solid state theory or condensed matter theory. Again, this perspective opens the path towards a more interactive way of teaching where students can easily modify examples to discuss variations in physical properties like the electronic band structure or density of states. Also, standard courses on solid state and condensed matter theory usually contain lectures on point and space group symmetries which can be complemented using GTPack.

## Example: generalized Ginzburg-Landau theory

We show the construction of fourth order terms for a generalized Ginzburg-Landau theory. For details of the method we refer to Ref. [19]. The theory describes the phase transition from the normal state in a metal into a superconducting state, associated to a superconducting gap function  $\Delta(\vec{k})$ . Such a state involves a pairing of two electrons, hence, considering spin-orbit interaction and half-integer total angular momentum of an electron, the pairing wave function will have an integer

angular momentum. Therefore, the symmetry can be described in terms of ordinary point groups instead of double groups. The total symmetry group of the system is given by

$$\mathcal{G} = \mathcal{G}_0 \otimes \mathcal{G}_{\mathcal{K}} \otimes U(1), \quad (1)$$

with  $\mathcal{G}_0$  denoting the point group of the lattice (we consider symmorphic space groups),  $\mathcal{G}_K$  denoting the group generated by time-reversal symmetry, and  $U(1)$  the group of complex phases  $e^{i\phi}$ . While the transition into the superconducting state might break any of the present symmetries, the normal state is fully symmetric under  $\mathcal{G}$  and so a Ginzburg-Landau expansion has to be invariant under all these terms. We pick the simplest non-trivial example of the cubic point group  $\mathcal{G}_0 = O_h$ , and a general gap function transforming as the two dimensional irreducible representation  $E_g$ ,

$$\Delta = \mu\Delta_\mu + \nu\Delta_\nu. \quad (2)$$

For a spin-singlet state, the gap function can be expressed as  $\Delta(\vec{k}) = i\sigma_y \Psi(\vec{k})$ , with  $\sigma_y$  being the respective Pauli matrix and  $\Psi$  a scalar function. The two basis functions corresponding to  $E_g$  are found to transform as  $\Delta_\mu \sim (x^2 + y^2 - 2z^2)$  and  $\Delta_\nu \sim x^2 - y^2$ . While the second order term has the simple isotropic form  $a \left( \frac{T}{T_c} - 1 \right) (|\mu|^2 + |\nu|^2)$ , we construct the fourth order terms from the direct product  $\bar{E}_g \otimes E_g \otimes \bar{E}_g \otimes E_g$  (here  $\bar{\phantom{x}}$  denotes complex conjugation; term involves complex conjugation for the sake of U(1) gauge invariance), and projecting out the subspace transforming as the totally symmetric representation  $A_{1g}$ . We obtain two linearly independent terms given by

$$f = \beta_1 \left( |\mu|^4 + |\nu|^4 \right) + \beta_2 |\mu|^2 |\nu|^2. \quad (3)$$

The corresponding Mathematica code involving GT-Pack is given in Fig. 2.

## Summary and outlook

GTPack is versatile tool for group theory applications in physics. In the first two years, it has been used successfully for various applications in research and teaching. In an ongoing effort GTPack is planned to be extended, e.g., with respect to electronic structure calculations, space groups, angular momentum, and crystal field applications. We see great potential for interdisciplinary collaborations in the development of efficient computer algebra algorithms for physics applications. Such tools could be a promising path for a future classification of the quantum phases of matter in functional materials, where a manual inspection becomes impossible due to the large, but finite combinatorical space, when it comes to realizable symmetries in materials.

We install the group  $O_h$  (GTInstallGroup) and calculate the corresponding character table and representation matrices (GTGetIreps).

```

In[ ] := grp = GTInstallGroup[0h];

{ct, ir} = {{classes, chars, names}, {grp, ireps}} =
  GTGetIreps[grp, GOIrepNotation -> "Mulliken"];

```

Character Table:

	Ee	3 C <sub>2z</sub>	3 IC <sub>2x</sub>	6 C <sub>2f</sub>	6 IC <sub>4x</sub>	6 IC <sub>2a</sub>	6 C <sub>4z</sub>	8 IC <sub>36</sub>	8 C <sub>3p</sub>	IEe
A <sub>1g</sub>	1	1	1	1	1	1	1	1	1	1
A <sub>2u</sub>	1	1	-1	-1	1	1	-1	-1	1	-1
A <sub>2g</sub>	1	1	1	-1	-1	-1	-1	1	1	1
A <sub>1u</sub>	1	1	-1	1	-1	-1	1	-1	1	-1
E <sub>u</sub>	2	2	-2	0	0	0	0	1	-1	-2
E <sub>g</sub>	2	2	2	0	0	0	0	-1	-1	2
T <sub>1u</sub>	3	-1	1	-1	-1	1	1	0	0	-3
T <sub>1g</sub>	3	-1	-1	-1	1	-1	1	0	0	3
T <sub>2u</sub>	3	-1	1	1	1	-1	-1	0	0	-3
T <sub>2g</sub>	3	-1	-1	1	-1	1	-1	0	0	3

We calculate the transformation behavior of basis functions corresponding to  $E_g$  (GTSymmetryBasisFunctions).

```
ln[5]:= GTSymmetryBasisFunction[ct, {x^2+y^2, x^2-y^2}]
```

	$A_{1g}$	$A_{2u}$	$A_{2g}$	$A_{1u}$	$E_u$	$E_g$	$T_{1u}$	$T_{1g}$	$T_{2u}$	$T_{2g}$
$x^2 + y^2$	$\frac{2}{3}(x^2 + y^2 + z^2)$	0	0	0	0	$\frac{1}{3}(x^2 + y^2 - 2z^2)$	0	0	0	0
$x^2 - y^2$	0	0	0	0	0	$x^2 - y^2$	0	0	0	0

We decompose  $\bar{E}_g \otimes E_g \otimes \bar{E}_g \otimes E_g$  (GTrep). Note that the characters of  $E_g$  are real

```
In[*]:= GTIrep[chars[[6]] ^ 4, ct];
```

$$3 A_{1g} \oplus 3 A_{2g} \oplus 5 E_g$$

We generate the representation  $\Gamma = \bar{E}_g \otimes E_g$  (GTDirectProductRep) and calculate Clebsch-Gordan-Coefficients for the direct product  $\Gamma \otimes \Gamma$  and basis functions transforming as  $A_{1g}$ .

```

In[ ]:= dp = GTDirectProductRegConjugate[i reps[[6]]], i reps[[6]], GOfast → True] //
FullSimplify;
cgc = Flatten[GTClebschGordanCoefficient{dp, dp, i reps[[1]],
GOfast → True], 1]

```

$$\text{Out}[ ] := \left\{ \left\{ \frac{1}{\sqrt{2}}, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, \frac{1}{\sqrt{2}} \right\}, \right. \\ \left\{ 0, 0, 0, \frac{1}{\sqrt{2}}, 0, 0, 0, 0, 0, 0, 0, 0, \frac{1}{\sqrt{2}}, 0, 0, 0 \right\}, \\ \left. \left\{ 0, 0, 0, 0, 0, 0, \frac{1}{\sqrt{2}}, 0, 0, \frac{1}{\sqrt{2}}, 0, 0, 0, 0, 0, 0 \right\} \right\}$$

We rewrite the output in terms of the generalized Ginzburg-Landau terms  $\mu, \nu, \bar{\mu}, \bar{\nu}$

```

[m × n] := norm = {μ, v}; conj = {μ̄, v̄};
basis = Flatten[KroneckerProduct[Flatten[KroneckerProduct[conj, norm]],
    Flatten[KroneckerProduct[conj, norm]]]];

```

```
Inf := basis.# &/@ cgc // Union
```

$$Out[*] = \left\{ \sqrt{2} \mu v \bar{\mu} \bar{v}, \frac{\mu^2 \bar{\mu}^2}{\sqrt{2}} + \frac{v^2 \bar{v}^2}{\sqrt{2}} \right\}$$

**Figure 2:** *GTPack workflow to construct fourth order terms in a generalized Ginzburg-Landau theory.*

## References

- [1] Ching-Kai Chiu, Jeffrey CY Teo, Andreas P Schnyder, and Shinsei Ryu. Classification of topological quantum matter with symmetries. *Rev. Mod. Phys.*, 88(3):035005, 2016.
- [2] Eduardo Fradkin, Steven A. Kivelson, and John M. Tranquada. Colloquium: Theory of intertwined orders in high temperature superconductors. *Rev. Mod. Phys.*, 87:457–482, May 2015.
- [3] Kasper Peeters. Cadabra2: computer algebra for field theory revisited. *J. Open Source Softw.*, 3(32):1118, 2018.
- [4] Malcolm AH MacCallum. Computer algebra in gravity research. *Living Rev. Relativ.*, 21(1):6, 2018.

- [5] R. M. Geilhufe and Wolfram Hergert. GTPack: A Mathematica Group Theory Package for Application in Solid-State Physics and Photonics. *Front. Phys.*, 6:86, 2018.
- [6] Wolfram Hergert and R. M. Geilhufe. *Group Theory in Solid State Physics and Photonics: Problem Solving with Mathematica*. Wiley-VCH, 2018. ISBN: 978-3-527-41133-7.
- [7] W Hergert and Markus Däne. Group theoretical investigations of photonic band structures. *physica status solidi (a)*, 197(3):620–634, 2003.
- [8] W Hergert, M Däne, and D Ködderitzsch. 6. symmetry properties of electronic and photonic band structures. In *Computational Materials Science*, pages 103–125. Springer, 2004.
- [9] María Blanco de Paz, Maia G. Vergniory, Dario Bercioux, Aitzol García-Etxarri, and Barry Bradlyn. Engineering fragile topology in photonic crystals: Topological quantum chemistry of light. *Phys. Rev. Research*, 1:032005, Oct 2019.
- [10] Matthew Proctor, Paloma Arroyo Huidobro, Barry Bradlyn, Maria Blanco de Paz, Maia G Vergniory, Dario Bercioux, and Aitzol Garcia-Etxarri. On the robustness of topological corner modes in photonic crystals. *arXiv:2007.10624*, 2020.
- [11] Stanislav S Borysov, R Matthias Geilhufe, and Alexander V Balatsky. Organic materials database: An open-access online database for data mining. *PloS one*, 12(2):e0171501, 2017.
- [12] R. Matthias Geilhufe, Adrien Bouhon, Stanislav S. Borysov, and Alexander V. Balatsky. Three-dimensional organic dirac-line materials due to nonsymmorphic symmetry: A data mining approach. *Phys. Rev. B*, 95:041103, Jan 2017.
- [13] R Matthias Geilhufe, Stanislav S Borysov, Adrien Bouhon, and Alexander V Balatsky. Data mining for three-dimensional organic dirac materials: focus on space group 19. *Scientific reports*, 7(1):1–7, 2017.
- [14] R Matthias Geilhufe, Francisco Guinea, and Vladimir Juričić. Hund nodal line semimetals: The case of a twisted magnetic phase in the double-exchange model. *Physical Review B*, 99(2):020404, 2019.
- [15] M Rodriguez-Vega, Ze-Xun Lin, A Leonardo, A Ernst, G Chaudhary, MG Vergniory, and Gregory A Fiete. Phonon-mediated dimensional crossover in bilayer  $\text{CrI}_3$ . *arXiv:2003.11158*, 2020.
- [16] Martin Rodriguez-Vega, A Leonardo, and Gregory A Fiete. Group theory study of the vibrational modes and magnetic order in the topological antiferromagnet  $\text{MnBi}_2\text{Te}_4$ . *arXiv:2007.01794*, 2020.
- [17] Shuntaro Sumita and Youichi Yanase. Superconductivity induced by fluctuations of momentum-based multipoles. *arXiv preprint arXiv:2004.08086*, 2020.
- [18] R Matthias Geilhufe and Alexander V Balatsky. Symmetry analysis of odd-and even-frequency superconducting gap symmetries for time-reversal symmetric interactions. *Physical Review B*, 97(2):024507, 2018.
- [19] Manfred Sgrist and Kazuo Ueda. Phenomenological theory of unconventional superconductivity. *Reviews of Modern physics*, 63(2):239, 1991.

## Erfahrungsbericht aus Hannover über das Sommersemester 2020

Christoph Pegel, Marcos Soriano, My Hanh Vo Thi (Hannover)

pegel@math.uni-hannover.de  
soriano@math.uni-hannover.de  
vothi@idmp.uni-hannover.de

---

### Einleitung: Ausgangslage

Wir wollen über unsere Konzepte und Erfahrungen beim Einsatz von Computeralgebra in der Lehre während des Online-Sommersemesters 2020 berichten. In den vergangenen drei Jahren haben wir Kenntnisse sowie Material für das Fach Lineare Algebra gesammelt und seit über einem Jahr arbeiten wir projektgefördert am systematischen Aufbau eines digitalen Fragenpools für die Grundveranstaltungen Analysis und Lineare Algebra. Mit Hilfe dieser Vorarbeiten konnten im Online-Semester zwei Kurse zur Linearen Algebra verstärkt durch Computeralgebra-basiertes Übungsmaterial unterstützt werden. Der eine Kurs gehört zum Studiengang Mathematik (circa 150 Teilnehmende). Der andere war Teil des Service-Bereiches und ist vorwiegend an Informatik-Studierende gerichtet (über 400 Teilnehmende). In beiden Kursen fand die Lehre überwiegend asynchron statt. Alle Materialien wurden über die von unserer Universität unterstützte Lernplattform ILIAS angeboten, die unter anderem über ein STACK Plug-in verfügt, welches auf dem Computeralgebrasystem MAXIMA basiert.

---

### Lernaktivitäten

Für das erfolgreiche Absolvieren eines Moduls sehen unsere Prüfungsordnungen neben einer abschließenden *Prüfungsleistung* (für beide Kurse in Form einer Klausur) auch semesterbegleitende Aktivitäten (*Studienleistung*) vor, die von den jeweiligen Dozierenden sehr flexibel gestaltet werden dürfen. Unser Grundgedanke war, mit Hilfe digitaler Übungsaufgaben die studentischen Lernaktivitäten zu diversifizieren. In aller Kürze aufgezählt: schriftliche Hausaufgaben, Online-Quizzes und Online-Tests.

Zur Erfassung der Studienleistung haben wir ein simples Belohnungssystem mit Sternen als Wertungspunkte eingeführt: Jede erfolgreich absolvierte Lernaktivität konnte eine im Vorfeld festgelegte maximale Anzahl von Sternen einbringen. Pro Hausaufgabenblatt waren das – je nach Umfang – zwei oder drei Sterne, pro Online-Quiz ein Stern und pro Online-Test zwei Sterne. Eine Mindestanzahl an Sternen für das Erreichen der Studienleistung des jeweiligen Kurses wurde gefordert,

doch *wann* und *wie* die Lernaktivitäten eingebracht wurden, konnten flexibel, selbstständig und individuell von den Teilnehmenden entschieden werden.

### Hausaufgaben

Ein gewisser Anteil schriftlicher Hausaufgaben wurde in beiden Kursen beibehalten: Es gab jeweils sechs Aufgabenblätter, die im zweiwöchentlichen Rhythmus bearbeitet wurden. Moderate Gruppenarbeit (Abgaben in Paaren) wurde ausdrücklich begrüßt. Durch den parallelen Einsatz digitaler Übungsaufgaben konnte man bei dieser Lernaktivität den Fokus auf das Verfassen mathematischer Argumentationen und Beweise legen.

Die Abgabe studentischer Lösungen sowie deren Korrektur, Bewertung und spezifische Rückmeldungen wurden komfortabel durch das Hausaufgabentool von ILIAS koordiniert. Dies hatte den positiven Nebeneffekt einer viel engeren Monitorierung dieser Aktivität als sie bei Kursen mit diesen Teilnehmerzahlen in der Regel üblich und möglich ist.

### Online-Quizzes

Die Kursinhalte wurden wöchentlich in der Form von Vorlesungsvideos und Skriptabschnitten bereitgestellt. Um die Auseinandersetzung mit diesem Material und die Reflexion über den Inhalt zu fördern, haben wir dieses (gegenüber früheren Kursinstanzen innovative) Element mit klar umrissener Zielsetzung eingeführt: „Lese das Skript, schaue Dir die passenden Videos an und prüfe anschließend Dein Wissen und Verständnis mit diesem Quiz“. Zum Bestehen des wöchentlichen Quizzes wurde ein moderater Mindestprozentsatz an richtigen Antworten verlangt. Ein Quiz konnte bis zu drei Mal durchgeführt werden.

Jedes Quiz hatte einen Umfang von zehn bis zwölf Fragen und war unmittelbar an die Vorlesungsinhalte der jeweiligen Woche gekoppelt. Die Fragen zielten im Wesentlichen auf sprachliche Aspekte sowie das Verständnis grundlegender Definitionen und Sätze ab. Die Bearbeitung sollte keine aufwändigen Rechnungen umfassen. Fragenformate vom Typ Mehrfachauswahl, Zuordnungsfragen sowie Lückentexte wurden daher bevorzugt. Es wurde viel Wert auf eine möglichst differenzierte und ausführliche Rückmeldung gelegt.



Alle drei bis vier Wochen wurde ein umfangreicher Online-Test zum gerade abgeschlossenen Thema freigeschaltet. Um einen gewissen Eindruck über die Inhalte zu vermitteln seien hier einige der abgedeckten Themen aufgelistet: Determinanten, Eigenwerttheorie, Euklidische und Unitäre Vektorräume, Projektive Geometrie sowie Multilineare Algebra. Eine ausgefeilte Taxonomie zur Kategorisierung der Inhalte und anderer Aspekte sorgte für die gebotene Übersicht und soll die langfristige Pflege und den vielfältigen Einsatz der entwickelten Aufgabenpools gewährleisten. In der Regel hatten die Studierenden um die drei Wochen Zeit zur Bearbeitung (mit beliebigen Unterbrechungen) und durften auch hier bis zu drei Mal den Test durchführen. Der beste Versuch ging in die Wertung ein, wobei die erzielte Punktzahl passend in Sterne umgewandelt wurde.

Der Schwerpunkt der Online-Tests lag deutlich bei algorithmischen Fragestellungen und Rechenaufgaben; an dieser Stelle war der Einsatz von Computeralgebra unabdingbar. Um die Attraktivität solcher Aufgaben zu erhöhen, haben uns frühere Erfahrungen und ein umfassender systematischer Austausch mit Endanwendern in der Form von Fragebogenevaluationen und Interviews überzeugend gezeigt, dass diese mindestens zwei Kriterien erfüllen müssen: Zum einen sollten die behandelten Beispiele eine „aufgabentypische“ Mindestkomplexität aufweisen, wobei zum anderen die erforderlichen Rechnungen „im Rahmen“ bleiben und problemlos von Hand durchführbar sein müssen.

Die ausgewogene Berücksichtigung beider Kriterien stellt zweifellos eine gewisse Herausforderung dar, führt aber auf der anderen Seite eine sehr interessante Facette der Entwicklung und Implementation solcher Aufgaben vor. Wir haben uns dabei grundsätzlich auf die Entwicklung und Umsetzung von Algorithmen zur zufallsgesteuerten Erzeugung „unter Nebenbedingungen“ der erforderlichen mathematischen Objekte gestützt (es seien beispielhaft unimodulare Matrizen mit beschränkten Einträgen erwähnt) und diese möglichst breit in unterschiedlichen Kontexten eingesetzt. Dabei haben wir zwei verschiedene Strategien verfolgt, die beide von ILIAS/STACK unterstützt werden: Wann immer es möglich ist, sollte eine sorgfältige Gestaltung dazu führen, dass in Echtzeit eine randomisierte Aufgabeninstanz durch das System produziert wird. Ansonsten haben wir im Vorfeld eine ausreichende Anzahl an Instanzen zufällig generiert und manuell die ungünstigen darunter aussortiert. Diese Möglichkeit ist weniger systembelastend und bei eingeschränkten Ressourcen vorzuziehen.

Abschließend möchten wir noch erwähnen, dass sämtliche Quizzes und Tests als zusätzliche Lernunterstützung während der mehrwöchigen Vorbereitungsphase auf die Prüfung uneingeschränkt und mit der Option der sofortigen Rückmeldung freigeschaltet wurden. Gerade im Hinblick auf diese Möglichkeit ist es wichtig, mittels Randomisierung für eine praktisch unbe-

schränkte Auswahl an Übungsaufgaben zu sorgen.

---

## Rückmeldungen und Ergebnisse

---

Auf unterschiedlichem Wege – unter anderem durch eine im kleineren der beiden Kurse durchgeführte detaillierte Umfrage – haben uns überwiegend sehr positive Rückmeldungen seitens der Teilnehmenden erreicht. Die Breite und Vielfalt des Angebots an Übungsmaterial sowie die großzügigen Möglichkeiten zur Steuerung des eigenen Lernprozesses wurden besonders hervorgehoben. Im Vergleich zu anderen Veranstaltungen scheint gerade diese Flexibilität für eine spürbare Entlastung und Minderung des empfundenen Leistungsdruckes in diesem schwierigen Semester gesorgt zu haben.

Aus Dozierendensicht können wir positiv anmerken, dass beide Kurse mit recht erfreulichen Prüfungsergebnissen abgeschlossen wurden. Bereits eine oberflächliche Analyse der Ergebnisse und der Vergleich zu früheren Kursinstanzen (mit nahezu identischen Inhalten) sowie zu anderen Kursen derselben Kohorte im selbigen Online-Semester deuten für uns als Lehrende auf eine deutliche Verbesserung des Lernerfolgs hin – gerade im unteren und mittleren Leistungsbereich.

---

## Fazit und Ausblick

---

Das durch äußere Umstände erzwungene vollständige Ausweichen auf digitale Formate im Sommer bewerten wir rückblickend als eine insgesamt positive und für künftige Semester sehr lehrreiche Erfahrung. Die meisten Teilnehmenden der beiden Kurse wünschen sich für die Zukunft als weiteres, ergänzendes Element für die Lehre den Einsatz digitaler Übungsaufgaben. Dieser sollte nach Möglichkeit auch auf andere Veranstaltungen erweitert werden. Aus unserer Sicht ist damit eine erhebliche Ausdifferenzierung und Erweiterung des traditionellen Übungsangebots möglich.

Natürlich wurden viele Elemente der Präsenzlehre schmerzlich vermisst; so ist es uns zum Beispiel nicht gelungen, einen adäquaten virtuellen Ersatz für wöchentliche Übungsgruppen zu finden. Nichtsdestotrotz wurden wir von zahlreichen Studierenden ermahnt und gebeten, die meisten der eingeführten und als positiv empfundenen Maßnahmen und Instrumente für die ersetzte Zeit nach Corona unbedingt zu übernehmen und in die Präsenzlehre zu integrieren.

Erwähnt werden muss allerdings, dass die Bereitstellung des hier beschriebenen Angebots mit einem nicht unerheblichen Aufwand verbunden war, der durch die aktuellen Fassungen einzelner Lehrverpflichtungsverordnungen unzureichend abgebildet wird und nur durch die Perspektive eines längerfristigen Einsatzes etwas kompensiert wurde. Doch dafür müssen in der Regel umfassendere, übergreifende Strukturen geschaffen werden, die die Beiträge der Dozierenden einzelner Veranstaltungen koordinieren und bündeln.

# Feedback zur digitalen Lehre von Computeralgebra im Sommersemester 2020

Yvonne Weber (Kaiserslautern)

yweber@rhrk.uni-kl.de

---

## Computeralgebra digital: Algebra nun mal wirklich rein auf dem Computer

---

Man sollte meinen, Computeralgebra ist angesichts seiner intrinsischen Natur eines der vergleichsweise am besten geeigneten Fächer für digitale Lehre. Tatsächlich hat sich bei der Betreuung von dritt- und viert-Semester Bachelorstudierenden zur Vorlesung *Symbolisches Rechnen* an der TU Kaiserslautern in diesem Sommersemester gezeigt, dass sich Computeralgebra in digitalem Format auf sein Wesentliches reduziert und konzentriert: Algebraische Berechnungen mit dem Computer.

Symbolisches Rechnen bedeutet Rechnen mit Variablen. Im Gegensatz zu numerischen Methoden wird mit exakten Objekten gerechnet. Die Vorlesung von Prof. Dr. Claus Fieker fand als eine Telekonferenz live online statt und orientierte sich an einem kompakten Skript, Abschnitte dessen den Studierenden zur Vorbereitung auf jeden Telekonferenz-Termin aufgetragen wurden. Neben einer reinen Theorie-Übung, in der es hauptsächlich um Beweise ging, gab es eine Praktische Programmier-Übung, deren Ziel die Implementierung einiger Algorithmen aus der Vorlesungen in der Programmiersprache JULIA mithilfe von Zahlentheorie-Paketen war. Über Letztere möchte ich im Folgenden meine Erfahrungen kund tun, zudem der Ablauf diesmal stark von dem uns bis dato vertrauten Konzept abwich.

Die Programmier-Übung fand als eine Telekonferenz mit Screen-Sharings statt. Der Fokus lag auf dem interaktiven Testen von Beispielen direkt in der Konsole, was live von allen mitverfolgt und diskutiert werden konnte. Laufzeitvergleiche, ein noch größeres Augen-

merk auf den Programmier- und Testcode, die eigentliche Implementierung der Algorithmen sowie Hinweise auf nützliche Programmierhacks haben deutlich an Priorität gewonnen. Dies wiederum steigerte - so mein Eindruck - die Motivation und das Interesse der Studierenden. Theoretische Hintergründe wurden mündlich kürzer besprochen. Aus technischer Sicht ist das Screen-Sharing im Vergleich zu einem Beamer mit Kabeln im Computerraum um einiges weniger aufwändig. Auch das Wechseln zwischen Vortragenden verlief einwandfrei nahtlos.

Leicht problematisch war, dass es beim Vorführen aufeinanderfolgender Befehle eine Verzögerung gab zwischen der Übertragung des Tons und der bildlichen Übertragung der Ausgabe in der Konsole, was teilweise zu Verwirrung führte. Deshalb ist empfehlenswert, dabei ganz bewusst auf Langsamkeit zu achten.

Der große Nachteil ist, dass die Betreuung beim Programmieren sowie der Support bei Installationsproblemen der Software viel schwieriger waren. Nichts ersetzt das direkte Gespräch zu zweit vor einem Bildschirm beim Beheben eines Fehlers. Da Hilfe in erster Linie am Anfang des Semesters, wenn die Studierenden eine ihnen unbekannte Sprache und Syntax neu lernen, von Nöten ist, wäre ratsam, eine Art Vorkurs zur Einführung in die Programmiersprache anzubieten.

Als persönliches Feedback für den abgegebenen Code erhielt jede Gruppe ein kleines JULIA-Programm mit den erreichten Punkten und einer Textausgabe zu den Details der Bewertung.

Trotz der Herausforderungen bei der Betreuung ist Computeralgebra im Kern als solche digital bestens vermittelbar.



## „Le compte est bon“ lösen mit Computeralgebra

Michael Cuntz (Hannover)

cuntz@math.uni-hannover.de

---

### Einleitung

Welche Möglichkeiten gibt es, die Zahl 438 aus den Zahlen 2, 3, 7, 10, 100 zu berechnen, indem man nur die Operationen  $+$ ,  $-$ ,  $\cdot$  und  $/$  verwendet? Jede der Ausgangszahlen darf hierbei höchstens einmal verwendet werden. Also z. B.

$$438 = (7 - 3) \cdot (10 + 100) - 2$$

oder

$$438 = (3 + 7/7) \cdot (10 + 100) - 2.$$

Oder wie sieht es aus, wenn man die Zahl 652 aus den Zahlen 3, 3, 5, 6, 9, 10 erhalten will? In diesem Fall ist es unmöglich, nur wie kann man das entscheiden? Immerhin kann man mit diesen Zahlen die Zahl 651 erreichen,

$$651 = ((10 + 3 \cdot 6 \cdot 9) - 5) \cdot 3,$$

aber „näher“ kommt man nicht.

Das Fernsehspiel „Des chiffres et des lettres“, das ich aus meiner Kindheit noch kenne und in Frankreich auch in der Schule gespielt wird, wird schon seit etwa 50 Jahren im französischen Fernsehen ausgestrahlt. In dem Spiel müssen die Kandidaten in zwei Disziplinen antreten: Einerseits sollen sie aus gegebenen Buchstaben ein möglichst langes Wort kombinieren („Le mot le plus long“), andererseits einer gegebenen Zahl durch elementare Operationen wie in den obigen Beispielen möglichst nahe kommen („Le compte est bon“). Natürlich werden mittlerweile in der Sendung Computer benutzt, um optimale Lösungen zu berechnen. Wir wollen hier kurz besprechen, wie „Le compte est bon“ mit Computeralgebra gelöst werden kann.

---

### Kombinatorik

#### Spielregeln

Zunächst müssen wir präzisieren, wie das Spiel definiert ist. Im Spiel werden eine Zahl  $N \in \{101, \dots, 999\}$  und sechs Zahlen  $a_1, \dots, a_6 \in \{1, \dots, 10, 25, 50, 75, 100\}$

vorgegeben. Hierbei dürfen die Zahlen  $1, \dots, 10$  eventuell doppelt vorkommen. Das Ziel des Spiels ist es, die Zahl  $N$  ausgehend von  $a_1, \dots, a_6$  durch die elementaren Operationen  $+$ ,  $-$ ,  $\cdot$  und  $/$  zu berechnen.

Nicht ganz klar aus den Regeln ersichtlich ist, dass die Zwischenergebnisse immer ganze Zahlen bleiben müssen. Will man etwa die Zahl 15 aus 1, 5, 6, 7 berechnen, muss man zwischendurch rationale Zahlen verwenden. Eine Lösung wäre  $15 = 6/(7/5 - 1)$ ; diese ist aber nicht regelkonform.

Außerdem sind meines Wissens negative Zwischenergebnisse nicht erlaubt. Da ich diese Regel aber nicht explizit gefunden habe, gehen wir hier davon aus, dass negative Zahlen erlaubt sind, dass aber der Operator  $-$  nicht unär verwendet werden darf.

#### Catalan-Zahlen

Es gibt eine Menge Symmetrien, die in der Lösung des Spiels verwendet werden können. Zuerst müssen wir uns aber klar machen, wie die Ausdrücke am Ende geklammert werden können. Will man z. B. drei Elemente  $a, b, c$  mit einer Operation  $\circ$  (z. B.  $-$ ) verknüpfen, gibt es bei fester Reihenfolge der Elemente die beiden Möglichkeiten  $(a \circ b) \circ c$  und  $a \circ (b \circ c)$ . Bei vier Elementen  $a, b, c, d$  sind es die fünf Ausdrücke

$$\begin{aligned} ((a \circ b) \circ c) \circ d, & \quad (a \circ (b \circ c)) \circ d, & \quad (a \circ b) \circ (c \circ d), \\ & & \quad a \circ ((b \circ c) \circ d), & \quad a \circ (b \circ (c \circ d)). \end{aligned}$$

Es sei  $C_n$  die Anzahl der Ausdrücke, in denen die Operation  $n$ -mal vorkommt. Da wegen der Klammerung die Operation an einer eindeutigen Stelle zuletzt durchgeführt wird, sieht man die Rekursion

$$C_n = \sum_{k=1}^n C_{k-1} C_{n-k}.$$

Zum Beispiel mithilfe von erzeugenden Funktionen kann man  $C_n = \frac{1}{n+1} \binom{2n}{n}$  folgern (siehe etwa [Aig04]). Die Anzahl der Ausdrücke, die man bei einer (nicht assoziativen) Operation also betrachten muss, ist die berühmte *Catalan-Zahl*.

Ohne Symmetrien zu verwenden, können wir nun also zunächst abschätzen, dass wir  $C_n$  mögliche Klammern betrachten müssen, wenn wir  $n+1$  Elemente einsetzen. Für jede Operation haben wir vier Möglichkeiten, und die  $n+1$  Elemente werden aus den  $a_1, \dots, a_6$  auf  $\binom{6}{n+1}$  Weisen ausgewählt und können in  $(n+1)!$  verschiedenen Möglichkeiten eingesetzt werden. Wir erhalten also (höchstens)

$$\sum_{n=0}^5 4^n \binom{6}{n+1} (n+1)! C_n = 33665406$$

Ausdrücke, die wir auswerten müssen, um das Spiel komplett zu lösen. Das ist für einen modernen Computer nicht viel; einen einfachen Algorithmus geben wir weiter unten an.

### Symmetrien

Aber eigentlich würden wir mit diesen Ausdrücken viel zu viele Rechnungen probieren:

**Assoziativität:** Es gilt etwa  $(a+b)+c = a+(b+c)$  oder  $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ .

**Kommutativität:** Außerdem haben wir  $a+b = b+a$  und  $a \cdot b = b \cdot a$ .

**Distributivität:** Wenn die Zahlen  $a, b, c$  gegeben sind, ist zudem  $a \cdot (b+c) = a \cdot b + a \cdot c$ . Wenn es nur darum geht, irgendeine Lösung zu finden, könnte man sich also hier einen Fall sparen.

**Multiplizitäten:** Gilt  $a_1 = a_2$ , so wird der Vorfaktor  $(k+1)!$  in der Formel kleiner. Dasselbe gilt in komplizierterer Form allgemeiner, wenn die Zahlen  $a_1, \dots, a_6$  nicht verschieden sind.

Statt einer Catalan-Kombinatorik dürfen wir eigentlich ein allgemeineres kombinatorisches Modell verwenden. Solche Modelle sind in der Kombinatorik bekannt und basieren auf gewissen Pfaden mit Labels in einem Gitter (oder Bäumen mit Labels).

### Algorithmus

Folgenden Algorithmus kann man verwenden, um alle Lösungen zu finden, die exakt  $N$  ergeben:

`LeCompteEstBon(A, N, F, (i0, j0), s)`

Alle Lösungen des Spiels „Le compte est bon“

**Eingabe:** Zahlen  $A = [a_1, \dots, a_n]$  und  $N$ , Flags  $F = [f_1, \dots, f_n]$ , ein Paar von Indizes  $(i_0, j_0)$ , ein Ausgabestring  $s$ .

**Ausgabe:** alle Ausdrücke in  $A$ , die  $N$  ergeben.

Für alle Paare  $(i, j) \in \{1, \dots, n\}$  mit  $i < j$ ,  $(i, j) >_{lex} (i_0, j_0)$  und  $f_i = f_j = 0$ :

- Setze  $F' := [f'_1, \dots, f'_n, 0]$ , mit  $f'_k = f_k$  für  $k \neq i, j$  und  $f'_i = f'_j = 1$ .
- Bilde einen neuen Ausgabestring  $s'$  aus  $s$  und der Rechnung  $a_i + a_j = (a_i + a_j)$ .
- Falls  $a_i + a_j = N$ , gib  $s'$  aus.
- `LeCompteEstBon(A + [ai + aj], N, F', (i, j), s')`.
- [...die drei letzten Zeilen für alle anderen Operationen nochmal ...]

Die Funktion `LeCompteEstBon` ruft man nun mit der Liste  $A = [a_1, \dots, a_n]$  der gegebenen Zahlen und

der Zielzahl  $N$  auf, sowie mit  $f_i = 0$  für  $1 \leq i \leq n$ ,  $i_0 = j_0 = 0$  und  $s$  dem leeren String.

Dieser Vorschlag berücksichtigt bereits einen Teil der oben aufgelisteten Symmetrien. Die Tatsache, dass das neue Paar  $(i, j)$  lexikographisch größer als das letzte sein soll, erspart eine Menge überflüssiger Rechnungen, da gemeinsame Teile von Ausdrücken nicht mehrfach ausgewertet werden.

Eine Implementierung löst je nach Programmiersprache das Problem in mehr oder weniger einer Sekunde. Das obige Beispiel  $A = [2, 3, 7, 7, 10, 100]$  und  $N = 438$  hat laut `LeCompteEstBon` 15 Lösungen.

## Computeralgebra

### Rationale Funktionen

Es gibt jedoch eine einfache Methode, um alle Symmetrien auf einmal zu berücksichtigen ohne die Kombinatorik genauer zu verstehen. Jeder Ausdruck, den wir oben betrachten, kann „symbolisch“ als eine rationale Funktion in den Einträgen  $x_1, \dots, x_6$  angesehen werden. Wir können also mit einem Computeralgebrasystem ein für alle Mal alle diese rationalen Funktionen ausrechnen und abspeichern.

Für Ausdrücke mit 1, 2, 3, 4, 5 bzw. 6 Zahlen erhalten wir so 1, 4, 24, 176, 1440 bzw. 12608 verschiedene rationale Funktionen; das sind übrigens auch genau die Zahlen, die bei der genaueren Analyse der Kombinatorik herauskommen (vergleiche [CHN16]).

Bei jeder dieser Funktionen können noch die Variablen permutiert werden. Wir erhalten stattdessen 1, 6, 68, 1170, 27142 bzw. 793002 verschiedene Funktionen (man beachte, dass hier wieder automatisch Symmetrien eingehen).

Nun müssen jedoch noch für jede Funktion auf  $n$  Variablen die  $\binom{6}{n}$  Teilmengen von  $\{a_1, \dots, a_6\}$  eingesetzt werden. Damit erhalten wir

$$6 + 90 + 1360 + 17550 + 162852 + 793002 = 974860$$

rationale Funktionen in sechs Variablen. Insgesamt genügt es demnach 974860 Ausdrücke bei  $a_1, \dots, a_6$  auszuwerten. Der naive Ansatz ohne Symmetrien müsste mehr als 34-mal so viele Ausdrücke ausprobieren.

### Feinheiten

Den Ansatz mit Computeralgebra kann man noch auf viele Arten verbessern. Zum Beispiel haben die 974860 rationalen Funktionen deutlich weniger verschiedene Zähler; man könnte also die Zähler sammeln und mehrfaches Einsetzen vermeiden. Es gibt allerdings auch mehrere kleine Probleme:

Ein Problem ist, dass wir durch die rationalen Funktionen nicht mehr die Vorgabe einhalten, dass alle Zwischenergebnisse ganzzahlig bleiben. So müssen wir also nach Auswertung nochmal prüfen, ob der Ausdruck regelkonform ist.

Ein zweites Problem ist, dass es nicht offensichtlich ist, wie man aus der rationalen Funktion einen passenden Ausdruck rekonstruiert, z. B. ist

$$(x \cdot u + y \cdot u) / (z \cdot w + u \cdot v \cdot w) = (x+y) / (w \cdot (z/u + v)).$$

Das Problem kann man umgehen, indem man sich zu jeder Funktion a priori einen Ausdruck merkt.

Schließlich spart Algorithmus `LeCompteEstBon` von oben durch die Rekursion mehrfaches Auswerten von Teilen von Ausdrücken, was bei den rationalen Funktionen nicht so einfach zu realisieren ist.

Tatsächlich verhält es sich hier so wie bei vielen Problemen: Mit Computeralgebra läßt sich ein Problem oft in wenigen Zeilen Code lösen, die allerdings nicht unbedingt eine optimale Laufzeit haben. Trotz der obigen Anmerkungen benötigen wir am Ende etwas weniger Auswertungen als im ersten Ansatz, dieser Vorsprung geht aber leider komplett dadurch verloren, dass

die meisten Computeralgebra-Systeme den Code interpretieren.

## Literatur

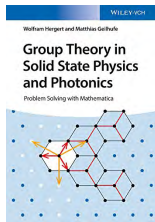
- [Aig04] M. Aigner, *Diskrete Mathematik*, fifth ed., Vieweg Studium: Aufbaukurs Mathematik. Friedr. Vieweg & Sohn, Wiesbaden, 2004.
- [CHN16] Frédéric Chapoton, Florent Hivert, and Jean-Christophe Novelli, *A set-operad of formal fractions and dendriform-like sub-operads*, *Journal of Algebra* **465** (2016), 322 – 355.

---

## Publikationen über Computeralgebra

---

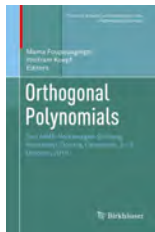
### Neuerscheinungen:



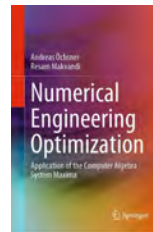
Wolfram Hergert, Matthias Geilhufe,  
*Group Theory in Solid State Physics  
and Photonics: Problem Solving with  
Mathematica*,  
Wiley-VCH Verlag, Weinheim 2018,  
377 Seiten,  
ISBN 978-3-527-41133-7



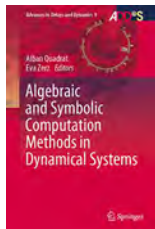
Andreas Weber,  
*Computer Algebra  
in Scientific Computing*,  
MDPI Publishing Services,  
Basel 2019, 160 Seiten,  
ISBN 978-3-039-21730-4



Mama Foupouagnigni,  
Wolfram Koepf (Hrsg.),  
*Orthogonal Polynomials*,  
Birkhäuser, Basel 2020,  
693 Seiten,  
ISBN 978-3-030-36743-5



Andreas Öchsner, Resam Makvandi,  
*Numerical Engineering Optimiza-  
tion: Application of the Computer  
Algebra System Maxima*,  
Springer Int. Publishing, Cham 2020,  
236 Seiten,  
ISBN 973-3-030-43387-1



Alban Quadrat, Eva Zerz (Hrsg.),  
*Algebraic and Symbolic Computa-  
tion Methods in Dynamical Systems*,  
Springer Int. Publishing, Cham 2020,  
311+XV Seiten,  
ISBN 978-3-030-38355-8

Die Rubrik Publikationen ist nicht allein auf eine Liste von Neuerscheinungen und Neuauflagen beschränkt. Sie lebt vor allem von fundierten Rezensionen von Fachgruppenmitgliedern für Fachgruppenmitglieder, die wir an dieser Stelle gerne abdrucken. Sollte eines der oben genannten Bücher, insbesondere eine der Neuerscheinungen, Ihr Interesse geweckt haben, und Sie möchten dieses für den Computeralgebra-Rundbrief besprechen, nehmen Sie bitte Kontakt zu Jürgen Klüners oder Martin Kreuzer ([klueners@math.uni-paderborn.de](mailto:klueners@math.uni-paderborn.de), [martin.kreuzer@uni-passau.de](mailto:martin.kreuzer@uni-passau.de)) auf.

### Wolfram Hergert und R. Matthias Geilhufe Group Theory in Solid State Physics and Photonics

Das Thema dieses Buchs sind moderne Anwendungen symbolischer Berechnungen in der Festkörperphysik, der Photonik und weiteren Teilgebieten der Physik. Die Grundstrukturen in diesen Bereichen folgen häufig Symmetrieprinzipien, woraus sich in natürlicher Weise eine Verbindung zur algorithmischen Gruppentheorie ergibt. Die Autoren verfolgen mit ihrer Darstellung dabei mehrere Ziele:

(1) Die gruppentheoretischen Grundlagen werden unter intensiver Zuhilfenahme des selbstentwickelten Mathematica-Pakets GTPack in lebhafter und anschaulicher Weise erläutert. Für längere technische Beweisführungen wird dabei auf die einschlägige Literatur verwiesen.

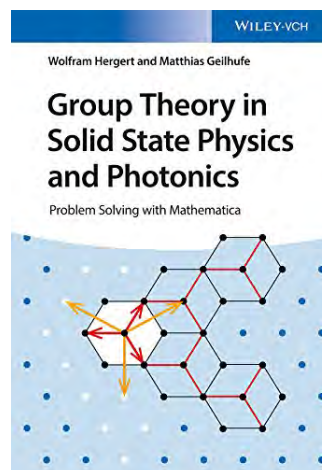
(2) Durch intuitive Befehlsnamen und -syntax soll dem Leser die Anwendung erleichtert und die Einbindung in eigenständige Forschungen ermöglicht werden.

(3) Auf die detaillierte Ausarbeitung der Algorithmen wird zugunsten der Untersuchung und Lösung realer physikalischer Probleme verzichtet. Für die tatsächlich implementierten Algorithmen werden wieder passende Referenzen bereitgestellt.

Die untersuchten Teilgebiete der Physik beruhen unter anderem auf dem Standardmodell der Elementarteilchen, auf Symmetriebetrachtungen und auf konkreten gruppentheoretischen Berechnungen. Spannende Entdeckungen wie Fullerene, Kohlenstoff-Nanotuben oder Quasikristalle wären ohne diese Hilfsmittel nicht möglich gewesen, so dass das vorliegende Werk einen wichtigen Beitrag zu aktuellen Entwicklungen leisten kann. Die Autoren gehen dabei in vier Teilabschnitten wie folgt vor:

(1) Zuerst werden grundlegende Aspekte der Gruppentheorie und insbesondere der Symmetriegruppen erläutert, wobei neben den klassischen diskreten Symmetriegruppen auch fortgeschrittene Themen wie nicht-kristallographische Gruppen, Darstellungstheorie oder Brillouin-Zonen zur Sprache kommen.

(2) Der zweite Teil behandelt die Anwendungen der Gruppentheorie in der elektronischen Strukturtheorie, also der Bewegung von Elektronen in den elektromagnetischen Feldern von Festkörpern. Die hierfür notwendigen Berechnungen erfordern die Lösung der Schrödinger-Gleichung und gelten als einige der schwierigsten und härtesten Aufgaben der Physik. Die Symmetrien der unterliegenden Systeme liefern dazu starke Restriktionen, die mittels gruppentheoretischer Methoden ausgenutzt werden können.



(3) Im dritten Teil werden Anwendungen im Gebiet der Photonik erklärt, wobei hier die Maxwellschen Gleichungen im Zentrum der Aufmerksamkeit stehen.

(4) Der vierte und letzte Teil betrifft schließlich weitere Anwendungen auf Schwingungsprobleme für Moleküle und Phasenübergänge gemäß der Landau-Theorie.

Trotz der Fülle des Materials ist das Buch stets übersichtlich und klar geschrieben und gestaltet. Die verwendeten Notationen sind mathematisch sauber, und an keiner Stelle greifen die Autoren auf physik-typische Kurznotationen, schludrige Begriffsbildungen oder archaische Bezeichnungen zurück, die vergleichbare Werke für eine mathematische Leserschaft oft schwer verständlich machen.

Das Buch ist allen algorithmisch orientierten Forschern, die sich für Anwendungen der Computeralgebra in der Festkörperphysik interessieren, sehr zu empfehlen. Als einzige kleine Einschränkung ist allerdings anzumerken, dass für die Berechnungen mit GTPack eine Mathematica-Lizenz erforderlich ist. In Instituten der theoretischen Physik sollte diese problemlos verfügbar sein, doch unter Mathematikern wird oftmals auch auf Open Source Programme (wie GAP mit dem Erweiterungspaket Cryst) oder Systeme mit weithin vorhandenen Campuslizenzen (wie Maple) vertraut. In diesem Fall ist der potentielle Leser gut beraten, die Verfügbarkeit oder Finanzierung einer geeigneten Mathematica-Lizenz im Voraus zu klären. Dann steht einer kurzweiligen und profitablen Einführung in die modernen Anwendungen der algorithmischen Gruppentheorie auf die Festkörperphysik nichts mehr im Wege.

Martin Kreuzer (Passau)



### **Bertrand Teguia Tabuguia: Power Series Representations of Hypergeometric Type and Non-Holonomic Functions in Computer Algebra**

**Betreuer: Wolfram Koepf (Kassel)**

**Zweitgutachter: Werner Seiler (Kassel)**

**Mai 2020**

**Abstract:** A Laurent-Puiseux series

$$\sum_{n=n_0}^{\infty} a_n (z - z_0)^{n/k} \quad (a_n \in \mathbb{K}, k \in \mathbb{N}, n_0 \in \mathbb{Z}) \quad (4)$$

where  $k$  denotes the corresponding Puiseux number and  $\mathbb{K}$  an infinite computable field, is mainly characterized by the general coefficient  $a_n$ . We consider the case where  $a_n$  is a term of an  $m$ -fold hypergeometric sequence. That is  $a_{n+m} = r(n)a_n$ , for all sufficiently large integers  $n$ ,  $r(n)$  is a rational function over  $\mathbb{K}$ , and  $m$  is a positive integer. A Laurent-Puiseux series with an  $m$ -fold hypergeometric sequence as general coefficient is said to be of hypergeometric type, with type  $m$ . We call hypergeometric type function any expression (mostly meromorphic) that can be written as a hypergeometric type series.

To find the general coefficient in (4) of a given hypergeometric type function, three key steps are to be considered [1]. Given an expression  $f$ ,

1. find a holonomic differential equation (DE) satisfied by  $f$ ;
2. deduce a holonomic recurrence equation (RE) satisfied by the Taylor coefficients of  $f$ ;
3. find all  $m$ -fold hypergeometric term solutions of the obtained RE.

Last but not least, the series representation is handled by determining the linear combination of all the resulting hypergeometric type series provided some initial values using Taylor approximation of suitable order.

The understanding of these three steps is essential for our work. In [1], Koepf described the first two steps for getting holonomic recurrence equations of any given hypergeometric type function. But the third step was not complete as he considered three sub-families of hypergeometric type functions: *exp-like* functions, *rational* functions, and the functions whose recurrence equation obtained in step 2 is a *two-term* recurrence relation. In this thesis, we clearly solve the third step and develop a complete algorithm to compute power series of linear combinations of hypergeometric type functions by using a new algorithm which finds all  $m$ -fold hypergeometric term solutions of holonomic recurrence equations. Also, we investigate an algorithm to represent power series of non-holonomic and non-hypergeometric type functions like  $\tan(z)$ ,  $\frac{1+\tan(z)}{1-\tan(z)}$ ,  $\frac{z}{\exp(z)-1}$ ,  $\frac{\arctan(z)}{1+z}$ ,  $\exp(z^2 + z)$  etc.

In addition, we confirm the asymptotically fast behavior of an algorithm based on holonomic recurrence equations to compute Taylor expansions of holonomic functions (see [2, Chapter 10]), and present some interesting results for the automatic proof of certain identities that are generally difficult to prove (see [2, Chapter 9]) like

$$\frac{1 + \tan(z)}{1 - \tan(z)} = \exp \left( 2 \operatorname{arctanh} \left( \frac{\sin(2z)}{1 + \cos(2z)} \right) \right)$$

by characterizing non-holonomic functions with non-linear recurrence equations and some initial values.

Our implementations are done in the computer algebra system Maxima 5.37.2, and regrouped in our package FPS. The CAS Maple is also used for comparison in order to show the improvements given by our algorithms and their implementations.

### **References**

- [1] Koepf, W.: Power series in computer algebra. *Journal of Symbolic Computation* **13**, 1992, 581–603
- [2] Koepf, W.: *Computeralgebra. Eine algorithmisch orientierte Einführung*. Springer, Berlin-Heidelberg, 2006, ISBN 3-540-29894-0

---

### **Sergio Siccha: Normalizers of primitive groups with non-regular socles in polynomial time**

**Betreuerin: Alice Niemeyer (Aachen)**

**Zweitgutachter: Mohamed Barakat (Siegen)**

**Juli 2020**

**Abstract:** For two groups  $G$  and  $H$ , which are contained in a common overgroup  $K$ , we call the *normalizer of  $G$  in  $H$*  the subgroup of  $H$  consisting of those elements that leave  $G$  invariant under conjugation, and denote it by  $N_H(G)$ . We say that a problem for permutation groups can be solved in *polynomial time*, if there exists an algorithm that, given permutation groups of degree  $n$ , can solve the problem in time bounded polynomially in  $n$  and in the sizes of the given generating sets. The main result of this thesis is that for a primitive group  $G \leq \operatorname{Sym} \Omega$  with non-regular socle the normalizer  $N_{\operatorname{Sym} \Omega}(G)$  can be computed in polynomial time.

An essential tool is the, in this thesis newly developed, concept of permutation morphisms. These generalize permutation isomorphisms and enable us to define a category of permutation groups. In this category we can elegantly describe direct products of permutation groups and actions induced on block systems.

Our main result is obtained by the following steps. We define weak canonical forms of primitive groups: essentially a group is in weak canonical form if its socle admits a nice action. By using the theory of permutation morphisms we show that we can compute weak canonical forms for all primitive groups efficiently. For a primitive group in weak canonical form we show that we can compute the normalizer of the socle in polynomial time. We then use the normalizer of the socle, a logarithmic reduction, and simply exponential time algorithms for the normalizer and the group intersection problem to design a polynomial time algorithm to compute  $N_{\operatorname{Sym} \Omega}(G)$  in polynomial time.

We also discuss further possible applications of weak canonical forms in testing conjugacy of permutation groups and finding small permutation representations of primitive groups.



**Prof. Dr. Max Horn** hat zum 1.4.2020 eine Professur für Algorithmische Geometrie und Algebra an der TU Kaiserslautern angetreten.



### Antrag auf Mitgliedschaft in der Fachgruppe Computeralgebra

Die Fachgruppe Computeralgebra sieht es als ihre Aufgabe an, Lehre, Forschung, Entwicklung, Anwendungen, Informationsaustausch und Zusammenarbeit auf dem Gebiet der Computeralgebra in Deutschland zu fördern.

Eine Mitgliedschaft in der Fachgruppe Computeralgebra gibt es bereits ab 7,50 € pro Jahr (für Mitglieder von DMV, GI oder GAMM; ansonsten 9 €).

#### Vorteile einer Mitgliedschaft:

- Sie fördern durch Ihren Beitrag die Workshops, Seminare, Tagungen und andere Aktivitäten auf dem Gebiet der Computeralgebra, die die Fachgruppe organisiert und unterstützt.
- Sie erhalten zweimal im Jahr den Computeralgebra-Rundbrief mit vielen interessanten Informationen rund um die Computeralgebra frei Haus.
- Sie verleihen unserer Stimme an Gewicht, die wir aktiv in Diskussionen um die Stellung der Computeralgebra in der Ausbildung in Schule und Hochschule einbringen.

Wir würden uns sehr über Ihre Unterstützung freuen. Die Mitgliedschaft in der Fachgruppe steht allen offen. Weiter Informationen zur Mitgliedschaft und einen Aufnahmeantrag finden Sie auf unserer Webseite unter folgender Adresse, oder scannen Sie einfach den QR-Code.

<https://fachgruppe-computeralgebra.de/aufnahmeantrag>



### GAP-Days Frühjahr 2020

Virtueller Workshop, 23.03. – 27.03.2020

[www.gapdays.de/gapdays2020-spring](http://www.gapdays.de/gapdays2020-spring)

Ursprünglich sollten diese GAP-Days in St Andrews, Schottland stattfinden. Kurzfristig wurden sie aus aktuellem Anlass dann aber doch per Jitsi und Slack ausgetragen. Das Hauptthema dieser 11. GAP-Days war diesmal recht unmathematisch: Etwa ein dutzend meist junger Mathematiker:innen lernten in mehreren Vorträgen Aspekte der Infrastruktur des GAP-Computeralgebra-Systems kennen, insbesondere den Aufbau der Webseite und das Releasemanagement. Das ist zwar mathematisch völlig uninteressant, aber gleichzeitig essentiell für jeden, der auch in Zukunft neue Versionen von GAP erhalten möchte. Dankenswerterweise fanden sich unter den Teilnehmern eine große Zahl begeisterter Helfer, die das gelernte Wissen sofort tatkräftig in die Praxis umsetzten, um die Webseite auf eine komplett neue Infrastruktur umzusetzen, und damit aktiv die zukünftige Entwicklung von GAP unterstützt haben. Vielen Dank nochmal an dieser Stelle an alle, die mitgemacht haben!

Max Horn (TU Kaiserslautern)

### ANTS-XIV (Fourteenth Algorithmic Number Theory Symposium)

Auckland, Neuseeland, 29.06. – 04.07.2020

[www.math.auckland.ac.nz/~sgal018/ANTS/](http://www.math.auckland.ac.nz/~sgal018/ANTS/)

Die diesjährige Tagung litt, wie viele andere auch, unter der Corona Pandemie. Um trotzdem das Beste daraus zu machen, war das Modell der Tagung im Vorfeld aufgezeichnete Vorträge (contributed talks), live (via Zoom) Hauptvorträge und dann Diskussionen (ca. 10 min pro Vortrag) zu festen Zeitpunkten. Die Tagung wurde thematisch und nach Zeitzeonen aufgeteilt, so dass es für alle Zeitzeonen akzeptable Sessions gab. Parallel zu dem Zoom Meeting wurden Chats via Zulip organisiert - einige dieser Chats waren noch für mehrere Wochen aktiv. Insgesamt hat dieses Modell sehr gut funktioniert, neben sehr interessanten Vorträgen gab es lebhafte Diskussionen.

Thematisch waren die Hauptvorträge mit Andrew Booker (Bristol, UK), David Harvey (UNSW, Australia), Isabel Vogt (Stanford, USA), David Jao (Waterloo, Canada), Felipe Voloch (Canterbury, New Zealand), und Rachel Pries (Colorado State University, USA) gut verteilt und hoch aktuell. Wie bei ANTS üblich waren die anderen Vorträge von klassischer algorithmischer Zahlentheorie über arithmetische Geometrie und Gitter bis zu Kryptographie ebenfalls weit gestreut. Ein Posterpräsentation rundete das Programm ab.

Der Selfridge Preis für den besten eingereichten Artikel ging dieses Jahr an Jonathan Love und Dan Boneh für „Supersingular curves with small non-integer endomorphisms“.

Auf der Vollversammlung wurde diskutiert ANTS auch in Zukunft zumindest auch online anzubieten, speziell wurde herausgestellt, dass dieses Format viel einfacher und familienfreundlicher ist, als eine Reise nach Neuseeland.

Claus Fieker (TU Kaiserslautern)

### ICMS 2020

Braunschweig, 13.07. – 16.07.2020

[www.icms-conference.org/2020](http://www.icms-conference.org/2020)

Der diesjährige International Congress on Mathematical Software (ICMS) hätte vom 13. bis 16. Juli an der TU Braunschweig stattfinden sollen. Wegen der durch das Sars-Cov-2-Virus ausgelösten Pandemie wurde daraus eine virtuelle Tagung.

Höhepunkt waren die drei Hauptvorträge von Erika Ábrahám (Solving Real-Algebraic Formulas with SMT-RAT), Alan Edelman (Julia — The Power of Language) und Victor Shoup (NTL: a Library for Doing Number Theory). Zudem gab es 14 thematisch organisierte Sektionen mit insgesamt mehr als 120 Vorträgen von etwa 200 Teilnehmern. Die Proceedings erschienen bei Springer als Band 12097 der Serie Lecture Notes in Computer Science. Sie enthalten 48 Arbeiten, die vom Programmkomitee in einem Begutachtungsprozess ausgewählt wurden.

Geleitet wurde die Tagung von Anna Maria Bigatti und Jacques Carette (PC Co-chairs), James H. Davenport (Chair of Advisory Board), Timo de Wolff (Local Chair) und mir (General Chair).

Michael Joswig (TU Berlin & MPI-MiS, Leipzig)

### ISSAC 2020

Virtuelle Konferenz, 20.07. – 22.07.2020

[www.issac-conference.org/2020](http://www.issac-conference.org/2020)

Auch die ISSAC musste in diesem Jahr unter Pandemie-Bedingungen stattfinden. Eigentlich sollte sie im griechischen Kalamata (für mathematisch interessierte Leser problemlos auch im Original *Καλαμάτα* lesbar) stattfinden, wurde dann aber komplett und konsequent als virtuelle Konferenz abgehalten, was durch das starke Engagement der lokalen Organisatoren ermöglicht wurde. Neben den offensichtlichen Einbußen brachte dies immerhin den Vorteil, dass die Organisatoren darauf verzichteten, eine Tagungsgebühr zu erheben.

Das Akronym ISSAC steht *International Symposium on Symbolic and Algebraic Computation*, und damit für eine der bedeutendsten internationalen Konferenzen im Bereich Computeralgebra. Zwar hat die Fachgruppe Computeralgebra derzeit keinen Sitz im Steering Committee der ISSAC, ist jedoch weiter eng mit der ISSAC verbunden unter anderem durch die von uns vergebenen Preise. Mehr hierzu später.

Den General Chair haben in diesem Jahr Ioannis Z. Emiris und Lihong Zhi übernommen. Das Programmkomitee wurde von Anton Leykin geleitet und wählte aus 118 eingereichten Vorträgen 58 aus, die auf der ISSAC präsentiert wurden. Beide diese Zahlen sind rekordverdächtig. All diese Vorträge wurden als vorab von den Vortragenden aufgezeichnete Präsentationen zur Verfügung gestellt. Um auch die für jede Konferenz essentiellen Publikumsfragen zu ermöglichen, richteten die Organisatoren Zoom-Sitzungen ein, die jeweils am (europäischen) frühen Nachmittag stattfanden und für jeden Vortrag fünf Minuten für Fragen und Antworten der Autoren bereitstellten. Dies war mit einem erheblichen technischen und organisatorischen Aufwand verbunden. Für jede Sitzung wurde ein Team von drei „Chairs“ eingesetzt, die neben der üblichen Ansage der Vorträge und

dem Zeitmanagement die Zoom-Verwaltung und das Verlesen der über den Chat einlaufenden Fragen übernehmen mussten. Dass dies reibungslos verlief, ist bemerkenswert, und dem engagierten und ausgesprochen kompetenten Einsatz der lokalen Organisatoren zu verdanken. Diese hatten viele Entscheidungen zu treffen und Eventualitäten zu bedenken. Dass alle synchronen Veranstaltungen am frühen Nachmittag stattfanden, war beispielsweise aufgrund der internationalen Teilnehmerschaft von Fernost und Australien bis zur amerikanischen Westküste geradezu zwingend. Die Organisatoren stellten für die Teilnehmer eine sechsseitige “Gebrauchsanleitung“ mit unverzichtbaren Informationen zur Verfügung.

Neben den eingereichten Vorträgen gab es drei eingeladene Hauptvorträge, die synchron über Zoom abgehalten wurden. Auf die sonst üblichen Tutorials wurde diesmal verzichtet. Außerdem wurden 10 Poster und sechs Software-Demos präsentiert, die auch einen Auswahlprozess durchlaufen hatten. Für weitere Details, Titel und Autoren sei auf die wie immer gut organisierte Homepage der Konferenz verwiesen.

Zwei dieser Details sollen allerdings in diesem Bericht erwähnt und sogar hervorgehoben werden, nämlich die bereits oben erwähnten von der Fachgruppe Computeralgebra gesponsorten Preise. Es handelt sich um den Distinguished Poster Award und den Distinguished Software Demonstration Award, die wir auch in diesem Jahr und auch im Kontext der virtuellen Konferenz vergeben haben. Erneut wurden für die Preisträger durch die ohnehin bestehenden Poster- und Software-Komitees ermittelt, wofür wir uns sehr bedanken. Der Preis für das **beste Poster** ging an:

**Autoren:** Apostolos Chalkis, Vissarion Fisikopoulos, Panagiotis Repouskos und Elias Tsigaridas.

**Titel:** Sampling the feasible sets of SDPs and volume approximation.

Als **beste Software-Demo** wurde ausgezeichnet:

**Autoren:** Colin Crowley, Jose Israel Rodriguez, Jacob Weiker und Jacob Zoromski.

**Titel:** MultiRegeneration for polynomial system solving.

Auch das ISSAC Business Meeting wurde, einschließlich der anstehenden Abstimmungen, online abgehalten und verlief pannenfrei. Einer der Punkte war die Wahl eines neuen Mitglieds des Steering Committees. Hierfür traten vier Kandidatinnen und Kandidaten an, von denen Veronika Pillwein (RISC, Linz) gewählt wurde. Außerdem stand wie immer die Auswahl des Austragungsorts in zwei Jahren an. Erfreulicherweise gab es drei Bewerbungen: aus Havanna (Kuba), Lille (Frankreich) und Notre Dame (Indiana, USA). Von diesen setzte sich in der Wahl Lille durch, relativ knapp vor Havanna.

Als Austragungsort für den nächsten Sommer ist Sankt Petersburg geplant. Trotz des reibungslosen Ablaufes der diesjährigen virtuellen Konferenz ist zu hoffen, dass sich bis dahin die Welt aus dem Würgegriff der Pandemie befreien kann und ein echtes Zusammenkommen wieder möglich ist.

Gregor Kemper (München)

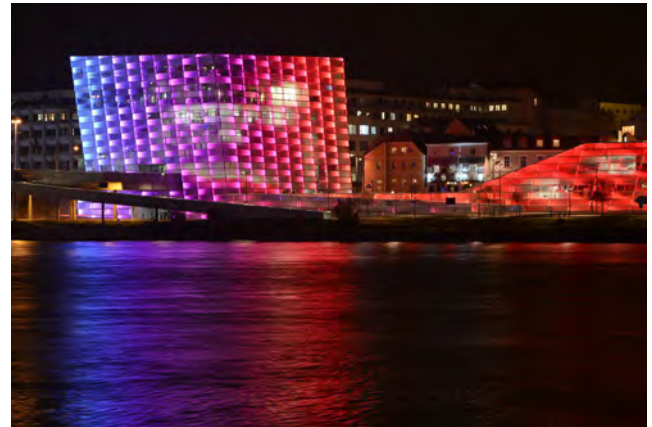
## CASC 2020

Linz, Österreich, 14.09. – 18.09.2020

[www.casc-conference.org](http://www.casc-conference.org)

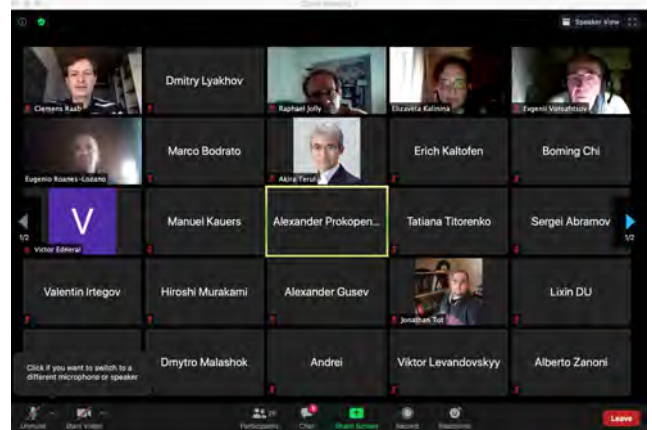
This year, the 22th CASC (Computer Algebra in Scientific Computing) conference was held at Johannes Kepler University in Linz, the capital city of Upper Austria. For the first time it took place virtually and the local organizing committee headed by Manuel Kauers did a wonderful job in doing all of the Zoom arrangements.

As in previous years, not only papers published in the conference proceedings were presented (34 talks), but also ones based on reviewed extended abstracts (13 talks). The presentations were presented in a single track, all being given using the videotelephony and online chat service Zoom.



(Ars Electronica Linz)

The tradition of having invited talks was upheld by having a 45 minute presentation of Werner Seiler on “singularities of algebraic differential equations” on Tuesday morning and Ovidiu Radulescu presenting “tropical geometry of biological systems” on Thursday morning.



(Some Participants of CASC 2020)

Within the business meeting on Tuesday evening, the location of the upcoming CASC 2021 conference was discussed which will be held in Sochi, Russia. The virtual excursion on Wednesday evening led the participants to the beautiful views of Ars Electronica Linz, which is the one of the places of deep space.

The program of the CASC 2020, as well as a link to the online version of the Proceedings (LNCS 12291) may be found at the web site.

<http://www.casc-conference.org/2020/>

Dmitry Lyakhov

#### 4. Jahrestagung des SFB/TRR 195

Kaiserslautern/Online, 22.09. – 24.09.2020

[www.computeralgebra.de/sfb/our-news/fourth-annual-conference-of-the-sfb-trr-195/](http://www.computeralgebra.de/sfb/our-news/fourth-annual-conference-of-the-sfb-trr-195/)

In der vorletzten Septemberwoche war eigentlich die Jahrestagung des SFB/TRR 195 mit interessanten Vortragenden aus dem In- und Ausland und natürlich mit Teilnehmern von innerhalb und außerhalb des SFB als krönender Abschluss der ersten Phase in Kaiserslautern geplant. Doch die Corona-Pandemie zwang schon früh zum Umplanen, so dass die Tagung schließlich als reine Online-Konferenz stattfinden musste.

Dieser neuen Situation wurde bewusst durch eine Verkürzung der Vorträge auf jeweils 20 Minuten Rechnung getragen, so dass das Programm sich auf drei Nachmittage straffte. Thematisch breit gefächert, aber stets angesiedelt im Spannungsfeld zwischen mathematischer (und vor allem algebraischer) Forschung mit experimentellem Bezug, Algorithmik und Software, gaben die 17 kurzen Vorträge

Einblicke in aktuelle Entwicklungen und boten Anlaß zur Diskussion, auch wenn das sich bei einer Online-Tagung etwas ungewohnt oder bisweilen sogar schwierig anfühlte. Gerade der informelle Austausch zwischen Kollegen verschiedener Spezialgebiete, wie er sich in Konferenzpausen ungezwungen ergibt, läßt sich eben doch nicht vollständig online emulieren.



Insgesamt war es eine interessante und anregende Tagung, bei der die Hauptlast der gelungenen Organisation in den Händen von Ulrich Thiel lag.

Anne Frühbis-Krüger (Oldenburg)

### Maple Conference

Virtuelle Konferenz, 02.11. – 06.11.2020

[www.maplesoft.com/mapleconference](http://www.maplesoft.com/mapleconference)

This conference is dedicated to exploring different aspects of the math software Maple, including Maple's impact on education, new symbolic computation algorithms and techniques, and the wide range of Maple applications. Attendees will have the opportunity to learn about the latest research, share experiences, and interact with Maple developers.

The conference will take place online, and will include live presentations and discussions as well as recordings and chatrooms, in order to accommodate time zones. Maplesoft staff will also offer Maple training sessions on a variety of topics during the conference.

### Gemeinsame Tagung IMU und DMV

Jerusalem, Israel, 08.03. – 10.03.2021

<http://u.math.biu.ac.il/~vishne/Conferences/IMU-DMV-2021>

Vom 8.3. bis 10.3.2021 wird in Jerusalem eine gemeinsame Tagung der Israelischen Mathematikervereinigung (IMU) und der DMV stattfinden. Weitere Informationen finden Sie auf der Website der Tagung.

### GAMM-Jahrestagung 2021

Kassel, 15.03. – 19.03.2021

[jahrestagung.gamm-ev.de](http://jahrestagung.gamm-ev.de)

Wegen der Corona-Krise musste die für Mitte März 2020 geplante GAMM-Jahrestagung in Kassel leider abgesagt werden. Dafür wird nun die GAMM-Jahrestagung 2021 in Kassel abgehalten. Auch das geplante Minisymposium zur Computeralgebra wurde auf 2021 verschoben. Die nachfolgenden GAMM-Jahrestagungen sollen in Aachen (2022), Dresden (2023) und Magdeburg (2024) stattfinden.

### MEGA 2021

Tromsø, Norwegen, 07.06. – 11.06.2021

[puremath.no/mega2021](http://puremath.no/mega2021)

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, over any characteristics.

The 16th edition of MEGA will take place at UiT (The Arctic University of Norway) including 10 invited talks as well as contributed talks. Information on submission and deadlines will be available on the Web-Site.

### ISSAC 2021

St. Petersburg, Russland, 18.07. – 22.07.2021

[www.issac-conference.org/2021](http://www.issac-conference.org/2021)

The International Symposium on Symbolic and Algebraic Computation (ISSAC) is the premier conference for research in symbolic computation and computer algebra. ISSAC 2021 will be the 46th meeting in the series, which started in 1966 and has been held annually since 1981. The conference presents a range of invited speakers, tutorials, poster sessions, software demonstrations and vendor exhibits with a center-piece of contributed research papers.

### Rings and Polynomials

Graz, Österreich, 19.07. – 24.07.2021

[integer-valued.org/rings2020](http://integer-valued.org/rings2020)

There will be a conference on "Rings and Polynomials" at Technische Universität Graz (TU Graz) in Graz, Austria, July 19-24, 2021.

Topics include: integer-valued polynomials, polynomial functions, multiplicative ideal theory, topological methods in ring theory, Zariski-Riemann spaces of valuation domains, factorization theory in rings and semigroups, Prüfer and Krull domains and generalizations.

The conference at the Institute of Analysis and Number Theory of Technische Universität Graz (TU Graz) continues the series of biennial ring-theory conferences held alternately at the two math departments in Graz since 2012 - at TU in 2012, at KFU in 2014, at TU in 2016, and at KFU in 2018. We hope to see the participants of the previous events again in Graz 2021, as well as many new participants.

### CoCoA 2020 - International School and Workshop on Computer Algebra

Universität Hue (Vietnam), 23.08. – 27.08.2021

[cocoa.dhsphue.edu.vn](http://cocoa.dhsphue.edu.vn)

The COCOA 2020 has been postponed because of coronavirus precautions and will be moved from its originally scheduled March dates to August 23-27, 2021.

CoCoA is a computer algebra system, which specializes in handling ideals and modules over rings of multivariate polynomials. The techniques used are mainly based on the theory of Gröbner bases.

The aim of this workshop is to offer researchers an exposition to contemporary research topics in Computer Algebra and Computational Commutative Algebra and to give an opportunity for young researchers to learn recent developments in these research areas and to discuss their topics with other researchers and well-known professors. COCOA 2020 follows the previous very successful format with two carefully selected intensive courses plus tutorials (using the computer algebra system CoCoA) and expert talks conducted by eminent researchers in the field. There will be a poster session for showcasing contemporary and ongoing research by young researchers. The workshop is devoted to the 75th anniversary of Professor Lorenzo Robbiano.

## **INFOS 2021: GI-Fachtagung Informatik und Schule – Lehrerbildung**

Wuppertal, 08.09 – 10.09.2021

[www.infos2021.de](http://www.infos2021.de)

Die 19. GI-Fachtagung Informatik und Schule (INFOS) des Fachausschusses »Informatische Bildung in Schulen« findet in der Bergischen Universität Wuppertal statt. Die Tagung steht unter dem Motto »Lehrerbildung«.

Im allgemeinbildenden Kontext stellt sich die Frage der informatischen Qualifikation aller Lehrkräfte. Dies adressiert bildungswissenschaftliche, fachbezogene und explizit informatische Bildungsaspekte. Informatik entfaltet darüber hinaus für alle Fächer attraktive Gestaltungsoptionen. Zur Strukturierung und Organisation stellen sich in allen drei Phasen der Bildung von Lehrkräften – nicht nur aus informatikdidaktischer Perspektive – Fragen in der hochschulbezogenen, ersten Phase der Bildung von Lehrkräften, der studienseminarbezogenen, zweiten Phase der Ausbildung von Lehrkräften sowie der dritten Phase der Fort- und Weiterbildung von Lehrkräften. Die Tagung widmet sich der wissenschaftlichen Diskussion der informatischen Bildung aller Lehrkräfte und aller Schülerinnen und Schüler.

## **DMV-ÖMG-Jahrestagung 2021**

Passau, 27.09. – 01.10.2021

[www.mathematik.de/dmv/jahrestagungen](http://www.mathematik.de/dmv/jahrestagungen)

Die DMV-Jahrestagung 2021 wird vom 27.9.-1.10. in Passau stattfinden. Geplant ist dort eine Sektion Computeralgebra. Weitere Informationen folgen.

## **CCAAGS-22**

Seattle, USA, 27.06. – 01.07.2022

[sites.google.com/view/ccaaggs-22/home](https://sites.google.com/view/ccaaggs-22/home)

CCAAGS-22 aims to bring together researchers working in the creative mixture of combinatorial and computational ideas in applied algebraic geometry. As part of the event we will celebrate Bernd Sturmfels and his contributions to the field.

Details of the conference will be posted at the website as they become available.



---

## Fachgruppenleitung Computeralgebra 2020–2023

---

**Sprecherin:**

Prof. Dr. Anne Fruehbs-Krueger  
Carl-von Ossietzky Universität Oldenburg  
Institut für Mathematik  
Carl-von-Ossietzky-Straße 11, 26129 Oldenburg  
0441 798-3233  
[anne.fruehbs-krueger@uni-oldenburg.de](mailto:anne.fruehbs-krueger@uni-oldenburg.de)  
<https://uol.de/anne-fruehbs-krueger>

**Stellvertretender Sprecher:**

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

**Vertreterin der GI:**

Prof. Dr. Erika Abraham  
Fachgruppe Informatik  
RWTH Aachen University  
Ahornstr. 55, 52056 Aachen  
0241 80-21242, -22243 (Fax)  
[abraham@cs.rwth-aachen.de](mailto:abraham@cs.rwth-aachen.de)  
<https://ths.rwth-aachen.de/people/erika-abraham/>

**Fachreferentin Industrie:**

Xenia Bogomolec  
Coding Services Hannover  
Engelbosteler Damm 15, 30167 Hannover  
0173 3031816  
[indigomind@protonmail.ch](mailto:indigomind@protonmail.ch)  
<https://quant-x-sec.com>

**Fachreferent CA an der Hochschule:**

Prof. Dr. Michael Cuntz  
Leibniz Universität Hannover  
Institut für Algebra, Zahlentheorie und Diskrete Math.  
Welfengarten 1, 30167 Hannover  
0511 762-4252  
[cuntz@math.uni-hannover.de](mailto:cuntz@math.uni-hannover.de)  
<http://www.iazd.uni-hannover.de/~cuntz>

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

Prof. Dr. Claus Fieker  
Fachbereich Mathematik  
Technische Universität Kaiserslautern  
Gottlieb-Daimler-Straße, 67663 Kaiserslautern  
0631 205-2392, -4427 (Fax)  
[fieker@mathematik.uni-kl.de](mailto:fieker@mathematik.uni-kl.de)  
<http://www.mathematik.uni-kl.de/~fieker>

**Fachexperte Physik:**

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

**Vertreter der DMV:**

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

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

Prof. Dr. Max Horn  
Fachbereich Mathematik  
Technische Universität Kaiserslautern  
Gottlieb-Daimler-Straße, 67663 Kaiserslautern  
0631 205-2730, -4427 (Fax)  
[horn@mathematik.uni-kl.de](mailto:horn@mathematik.uni-kl.de)  
<https://www.quendi.de/de/mathe>

**Fachreferent Themen, Anwendungen und Publikationen:**

Prof. Dr. Jürgen Klüners  
Mathematisches Institut der Universität Paderborn  
Warburger Str. 100, 33098 Paderborn  
05251 60-2646, -3516 (Fax)  
[klueners@math.uni-paderborn.de](mailto:klueners@math.uni-paderborn.de)  
<https://math.uni-paderborn.de/ag/klueners/>

**Fachreferent Themen, Anwendungen und Publikationen:**

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](mailto:martin.kreuzer@uni-passau.de)  
<http://www.fim.uni-passau.de/~kreuzer>

**Fachreferent Redaktion Rundbrief:**

Dr. Fabian Reimers  
Zentrum Mathematik – M11  
Technische Universität München  
Boltzmannstr. 3, 85748 Garching  
089 289-17474  
[reimers@ma.tum.de](mailto:reimers@ma.tum.de)  
<http://www.groups.ma.tum.de/algebra/reimers>

**Vertreterin der GAMM:**

Prof. Dr. Eva Zerz  
Lehrstuhl D für Mathematik  
RWTH Aachen  
Pontdriesch 14/16, 52062 Aachen  
0241 80-94544, -92108 (Fax)  
[eva.zerz@math.rwth-aachen.de](mailto:eva.zerz@math.rwth-aachen.de)  
<http://www.math.rwth-aachen.de/~Eva.Zerz/>

# BEGEISTERT FÜR MINT IN 10 MINUTEN.

Mit den praxisorientierten Lektionen „TI Codes“  
wecken Sie sofort das Interesse Ihrer Schülerinnen  
und Schüler an Informatik und Robotik.

Verwenden Sie zur Programmierung in Python  
einfach die vorhandenen TI-Nspire™ CX II-T CAS  
Rechner oder Software. **Für eine Übung  
benötigen Sie nicht mehr als 10 Minuten.**



Hier gehts los:

**[education.ti.com/de/activities/  
ti-codes-overview](https://education.ti.com/de/activities/ti-codes-overview)**

