Oktober 2024

Computeralgebra Rundbrief

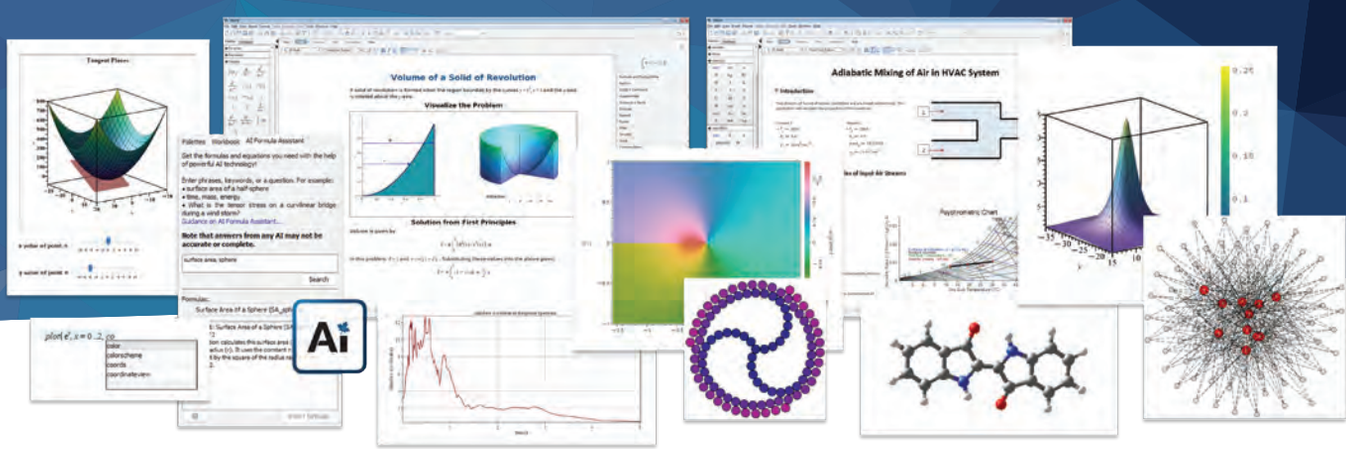
> Ausgabe 75

www.fachgruppe-computeralgebra.de

Maple™

Mehr leisten mit Maple 2024!

Lösen Sie mehr Probleme noch leichter mit Maple 2024



Neues Maple 2024 jetzt verfügbar!

Die leistungsstärkste und umfassendste Umgebung zum Erforschen, Visualisieren und Lösen selbst der schwierigsten mathematischen Probleme ist jetzt noch besser geworden!

Probieren Sie Maple kostenlos für 15 Tage ohne Verpflichtungen

www.maplesoft.com/CAR2024

Maplesoft
Mathématiques • Modélisation • Simulation
A Cybernet Group Company

www.maplesoft.com | info@maplesoft.com

Computeralgebra-Rundbrief

Nr. 75 Oktober 2024

Inhaltsverzeichnis

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)

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
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
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
https://www.gamm-ev.de

Mitteilungen der Sprecher

Liebe Mitglieder der Fachgruppe Computeralgebra,

diesmal dominiert das Thema Konferenzen gleich in mehrfacher Hinsicht die Mitteilungen der Sprecher. Zuerst möchten wir etwas Werbung in eigener Sache machen: die Computeralgebra-Tagung der Fachgruppe wird Anfang Juni 2025 in den Räumlichkeiten des MPI-MIN in Leipzig stattfinden; die Hauptvortragenden stehen bereits fest, die Vorbereitungen laufen und bald wird es auch Zeit für Einreichungen zu den Nachwuchsvorträgen. Daher meine Bitte an diejenigen, die im Hochschulumfeld tätig sind: Machen Sie den wissenschaftlichen Nachwuchs in unserem Gebiet auf die Konferenz aufmerksam! Zusätzlich zu den Fachvorträgen wird es noch einen Vortrag zum Forschungsdatenmanagement geben – angesichts der NFDI-Aktivitäten und insbesondere **MaRDI** *in der Mathematik ein brandaktuelles Thema. Wir freuen uns auf viele schöne Vorträge und hoffen auf die Qual der Wahl zum Preisträger des besten Nachwuchsvortrages.*

Von der ISSAC gibt es eine gute und zwei schlechte Nachrichten: Erfreulicherweise erhielt der Bid der Universität Oldenburg beim Business Meeting den Zuschlag für die Austragung der ISSAC 2026, was wir als Fachgruppe nach unseren Kräften unterstützen werden. Leider wird die Freude darüber aber getrübt von zwei unerfreulichen Nachrichten: Die ACM, traditionell auch der Publisher für die Proceedings der ISSAC, stellt derzeit sein Modell auf OpenAccess um, was direkt Publikationsgebühren für die Autoren zur Folge haben wird. An Institutionen, die keinen Rahmenvertrag mit ACM haben, kommen dann schnell 700,- bis 1200,- $ auf die Autoren zu. Ebenso unerfreulich sind die neuesten Entwicklungen bei der SIGSAM, einer SpecialInterestGroup in der ACM, die traditionell mit der ISSAC verknüpft ist. Bisher hatte diese als im Vergleich zur üblichen Größe sehr kleine SIG nur einen reduzierten Beitrag an die ACM abzuführen. Von dieser Sonderregelung ist die ACM nun aber abgerückt und verlangt den vollen Beitrag – angesichts der Mitgliederzahl und der geringen Erträge aus der ISSAC eine Existenzgefahr für die SIGSAM. In den Konferenzberichten schildert Gregor Kemper, der schon viele ISSACs besucht hat, und vor vielen Jahren auch Mitglied des Steering Committee der ISSAC war, seine Eindrücke von der Diskussion dieser Punkte beim Business Meeting.

Die Sprecherin der Fachgruppe Computeralgebra hat derzeit einen Sitz im Steering Committee der ISSAC inne. Dort wurde gemeinsam mit der Leitung der SIGSAM das Problem eingehend diskutiert und dann im Frühsommer beschlossen, die Community für ein Stimmungsbild zu befragen. Es standen drei Optionen zur Verfügung:

(1) SIGSAM bleibt selbständig und die Konferenzgebühren der ISSAC steigen drastisch an, um die Gebühren der ACM zu tragen.

(2) SIGSAM fusioniert mit einer anderen SIG, so dass der Betrag nur einmal statt zweimal anfällt und aus den Einnahmen von mehr als einer Konferenz getragen werden kann.

(3) SIGSAM hört auf, als SIG von ACM zu existieren, und ISSAC muss unabhängig von der ACM finanziell gemanaged werden.

In den ersten beiden Fällen wäre eine Publikation der Proceedings bei ACM verplichtend, im letzteren Fall wären auch andere Publisher mit ähnlichem Ansehen und niedrigeren Gebühren denkbar.
Die Umfrage ergab, dass sowohl (1) als auch (3) gegenüber (2) deutlich präferiert wurden und (3) wiederum etwas mehr Priorisierungen auf Platz 1 auf sich vereinen konnte als (1). Gegenwärtig überlegt das SIGSAM Board, welche Option dann unter Abwägung auch rein praktischer Randbedingungen verfolgt werden soll. Drücken wir die Daumen, dass ISSAC eine wichtige und erfolgreiche Konferenz bleibt und durch diese Querelen kein Verlust an Ansehen, Reichweite oder Praktikabilität entsteht.

Doch damit genug über Administratives. Kommen wir zum Inhalt des vorliegenden Rundbriefs, der nach einigen recht dicken Ausgaben in den letzten Semestern diesmal wieder recht dünn ausfällt: lediglich der Artikel von L. Panny zu Isogenien von abelschen Varietäten hat rechtzeitig den Weg in die Redaktion gefunden – aber weitere Artikel sind bereits für den Frühjahrsrundbrief versprochen. Andererseits ist die Rubrik Promotionen diesmal besonders gut gefüllt, da alle Einreichungen zum Dissertationspreis der Fachgruppe dort mit Abstract vorgestellt sind. Der diesjährige Preisträger ist Clemens Hofstadler mit seiner Promotion über nicht-kommutative Gröbner Basen und automatisierte Beweise von Operatoraussagen. Wir freuen uns auf seinen Hauptvortrag in Leipzig.

Wir wünschen Ihnen eine kurzweilige und anregende Lektüre.

Anne Frühbis-Krüger *Michael Cuntz*

Workshop-Förderung der Fachgruppe:

Sie veranstalten einen Workshop zu einem Thema aus dem Bereich der Computeralgebra und könnten mit einer kleinen finanziellen Unterstützung den Workshop deutlich interessanter oder effektiver gestalten? Die Fachgruppe Computeralgebra unterstützt Workshops mit bis zu 1000,– Euro.

Anträge können mit einer kurzen Beschreibung des Workshops (ca. 1 DIN A4 Seite; kurze Beschreibung des Gebiets, Thema des Workshops, Zielgruppe, Budget-Planung) und einer Darstellung, inwiefern diese Förderung einen deutlich erkennbaren Beitrag zum Gelingen des Workshops und zur Nachwuchsförderung liefert, an die Sprecherin der Fachgruppe gerichtet werden:

anne.fruehbis-krueger@uni-oldenburg.de,

bitte „**Workshop-Förderung**“ im Betreff angeben.

Fachgruppe Computeralgebra

GAP-Logo-Wettbewerb

Das GAP-Computeralgebrasystem unterstützt seit über 35 Jahren Forschung weltweit im Bereich der algorithmischen Gruppentheorie und verwandten Gebieten. GAP ist kostenlos und wird als „Open-Source-Software“ entwickelt.
Jetzt ist das GAP-Projekt auf der Suche nach einem neuen Logo. Dazu haben wir einen kleine Wettbewerb organisiert. Die Teilnahmebedingungen stehen auf unsere Webseite unter

https://www.gap-system.org/logo/

auf Englisch zur Verfügung. Wir würden uns über zahlreiche Teilnahme freuen.

Tagung der Fachgruppe Computeralgebra

Leipzig

02.06.–04.06.2025

https://fachgruppe-computeralgebra.de/leipzig-2025

Reclamhaus Leipzig, Foto: MPI-MIS.

Für die 11. Computeralgebra-Tagung der Fachgruppe ist diesmal das MPI-MIS in Leipzig unser Gastgeber. Nach den Unregelmäßigkeit der letzten Jahre wegen der Pandemie sind wir damit wieder im bewährten 2-jährigen Rhythmus. Die Tagung wird am Mittwochmittag beginnen und am Freitagmittag enden.

Ganz in der Tradition der früheren Tagungen werden auch diesmal mehrere Hauptvortragende Übersichtsvorträge über wichtige Themen aus Computeralgebra und über Computeralgebrasysteme halten, während in den anderen Vorträgen dem wissenschaftliche Nachwuchs Gelegenheit gegeben wird, seine Ergebnisse vorzustellen. Deutsch und Englisch sind dabei wie immer gleichberechtigte Konferenzsprachen. Für den besten Nachwuchsvortrag vergibt die Fachgruppe auch dieses Mal wieder einen mit 500,– Euro dotierten Preis.

> Hierzu sind Nachwuchswissenschaftler und -wissenschaftlerinnen **(Promovendi, Post-Docs)** aufgefordert, sich bis zum **15.04.2025** mit einem **Vortrag anzumelden**.

Als Hauptvortragende konnten wir folgende Wissenschaftlerinnen und Wissenschaftler gewinnen:

- **Clemens Hofstadler** (München)
- **Thomas Kahle** (Magdeburg)
- **Marta Panizzut** (Tromso)
- **Lorenz Panny** (München) (TBC)
- **Milena Wrobel** (Oldenburg)

In einem weiteren eingeladenen Vortrag wird uns Christiane Görgen einen Vortrag zu dem Thema 'Forschungsdatenmanagement' halten – ein aktuelles Thema für alle aktiven Forscher und Forscherinnen – und insbesondere für jüngere Teilnehmende sicher eine gute Gelegenheit sich zu informieren und ihre Fragen im Plenum oder individuell zu stellen.

Die Eckdaten zur Konferenz im Überblick:

Website: `https://fachgruppe-computeralgebra.de/leipzig-2025`

Termin und Ort: Die Tagung findet in der Zeit vom 02. – 04. Juni 2025 am MPI-MIS in Leipzig statt. Sie wird am 02. Juni 2025 um circa 13:00 Uhr eröffnet (Anreisetag) und endet am 04. Juni 2025 um circa 12:30 Uhr (Abreisetag).

Anmeldung: Die Anmeldung eines Vortrags ist bis 15. April 2025 möglich. Die Anmeldung ohne Vortrag ist bis 10. Mai 2025 möglich. Details zur Anmeldung finden Sie auf der Website der Tagung.

Konferenzgebühren: Jedes Nichtmitglied der Fachgruppe entrichtet vor Ort einen Unkostenbeitrag in Höhe von 20 € für die Kaffeepausen, alternativ kann man vor Ort zum Jahresbeitrag von 9 € Mitglied der Fachgruppe werden.

Nachwuchspreis: Die Fachgruppe Computeralgebra vergibt für den besten Vortrag von Promovendi/PostDocs wieder einen mit 500 € dotierten Nachwuchspreis. Verbunden mit dem Geldpreis ist die Einladung, auf der nächsten Tagung der Fachgruppe einen Hauptvortrag zu halten.

Foto der letzten Tagung 2023 in Hannover

Computing isogenies of abelian varieties: Dimension 1 and beyond

Lorenz Panny (Technische Universität München)

lorenz@yx7.cc

Isogenies in cryptography

Number theory and algebraic geometry are a near-infinite source of difficult computational problems, many of which are structured enough to build essential cryptographic systems such as public-key cryptography. As some traditional uses of elliptic curves and abelian varieties in cryptography are endangered by the looming threat of large-scale quantum computers, new constructions that are based on similar mathematical principles, but (conjecturally) post-quantum secure, have been proposed. Among the promising candidates for post-quantum cryptography is *isogeny-based cryptography*, which relies on the (presumed) hardness of computing an isogeny between two given abelian varieties over a finite field. The main advantage of this family of post-quantum cryptography is low communication cost (i.e., short public keys, ciphertexts, signatures, etc.); its main disadvantage is a high conceptual complexity and relatively slow performance. A short survey of isogeny-based cryptography was included in a previous *Rundbrief* article coauthored by the author [6], but a lot has happened in the ≈ 5 years that have passed since then. In this short article, I will sketch some of the exciting new developments in algorithms for isogenies of abelian varieties and their cryptographic applications.

Some preliminaries...

An isogeny between two abelian varieties A, B over the same base field is a surjective morphism $\varphi\colon A \to B$ with finite kernel which is also a group homomorphism. The degree of an isogeny is its degree as a rational map: In most cases (the technical condition is that the isogeny be separable), it equals the cardinality of the kernel subgroup. An important example of an isogeny is scalar multiplication: For elliptic curves, the multiplication-by-m map $[m]\colon E \to E$ has degree m^2; furthermore, if m is not divisible by the characteristic, then its kernel subgroup — the m-torsion subgroup $E[m]$ — is isomorphic to $\mathbb{Z}/m \times \mathbb{Z}/m$. Over finite fields, abelian varieties have more endomorphisms than just the scalar multiplications: For elliptic curves (i.e., abelian varieties of dimension 1), the (geometric) endomorphism ring has $\mathbb{Z}$-rank 2 or 4, corresponding to the curve being ordinary or supersingular. Endomorphisms feature a very strong connection to isogenies thanks to to the natural $\big(\mathrm{End}(E), \mathrm{End}(E')\big)$-bimodule structure of $\mathrm{Hom}(E, E')$; we'll discuss instances of this below.

The primary way to construct isogenies is to simply choose a finite subgroup: Every finite subgroup gives rise to an isogeny, and the isogeny is essentially unique (up to composition with purely inseparable isogenies). Note that for abelian varieties of dimension > 1, not all choices of subgroups are practically admissible due to restrictions in contemporary isogeny formulas.

Isogenies of elliptic curves always come in pairs: For every isogeny $\varphi\colon E \to E'$, there exists a unique dual isogeny $\widehat{\varphi}\colon E' \to E$ such that $\varphi \circ \widehat{\varphi}$ and $\widehat{\varphi} \circ \varphi$ both equal scalar multiplication by $\deg(\varphi)$. Here again, the situation is more complicated in dimension > 1.

Isogeny interpolation

Back in 2011, Jao and De Feo conjectured that the following *isogeny interpolation* problem might be hard, and suggested its use in cryptography to build a key exchange nowadays known as "SIDH".

Problem: The input are elliptic curves $E, E'/\mathbb{F}_q$, integers $d, N \in \mathbb{Z}_{\geq 1}$ such that q, d, N are pairwise coprime, and bases (P, Q) of $E[N]$ and (P', Q') of $E'[N]$. The goal is to find an isogeny $\varphi\colon E \to E'$ of degree d such that $\varphi(P) = P'$ and $\varphi(Q) = Q'$, assuming it exists.

Note that knowledge of $\varphi(P)$ and $\varphi(Q)$ implies knowledge of $\varphi|_{E[N]}$ since $E[N] = \langle P, Q\rangle$. Hence, the given information actually determines the action of the isogeny on N^2 points rather than just two: an amount of data that is exponential in its representation size. This interpretation also explains the "interpolation" terminology: The problem here is morally very similar to interpolating a polynomial from a list of input-output pairs, except that the representation of the input is much more compact, so that the straightforward Lagrange-style approach to interpolation is no longer necessarily optimal.

In theory, the isogeny φ is uniquely defined by its restriction to $E[N]$ as soon as $N^2 > 4d$. However, it is

a priori not at all obvious how to efficiently represent the output in general: That is the topic of the next section.

In a series of breakthrough papers in 2022, it was discovered that this problem is solvable in polynomial time[1] provided that N is smooth[2]. Since then, this new interpolation technique (based on higher-dimensional isogeny computations — see below) has been employed very effectively in new, more efficient algorithms for a vast family of computer-algebraic questions to do with abelian varieties. In this article, we survey some of those new techniques and their impact in cryptography.

We note that these new developments render parts of our earlier *Rundbrief* article [6] obsolete: This affects (only) the section titled "SIDH".

Representing isogenies

By definition, an isogeny is a tuple of polynomials defining the map as a morphism of varieties. Storing those polynomials is the most straightforward way of representing an isogeny; in this representation, the complexity of evaluating an isogeny is linear in the degree.

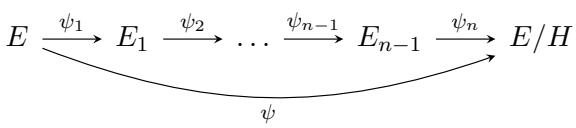
To discuss more efficient and flexible isogeny representations, we will first have to make sense of what "representing an isogeny" even means: The input is the domain of the isogeny together with some description of the kernel (e.g., a set of generators of the kernel subgroup, or an endomorphism-ring ideal defining that subgroup — see below), and the output is the codomain of the isogeny together with an efficient algorithm to evaluate the isogeny at any point lying in an extension of the base field of the isogeny.

In the following, we will mostly focus on the case of elliptic curves (abelian varieties of dimension 1) since it is the simplest and currently most complete. Note that almost all of the techniques readily generalize to abelian varieties of dimension > 1, but the algorithms have only been worked out practically in a few special cases. Lifting these restrictions is the subject of ongoing research.

Isogeny chains

The first observation is that isogenies can be decomposed into smaller isogenies whenever the degree is composite. This gives rise to our first efficient representation for large-degree isogenies: Long chains of small-degree isogeny steps. This representation applies to any isogeny of smooth degree.

In essence, the idea is to write the kernel subgroup $H \leq E$ as an ascending chain of prime-index subgroups $\{e\} \lneq H_1 \lneq H_2 \lneq \cdots \lneq H_n = H$ and construct a chain of isogenies



such that the kernels of each prime-degree isogeny step ψ_i are given by $\ker(\psi_1) = H_1$, $\ker(\psi_2) = \psi_1(H_2)$, $\ker(\psi_3) = \psi_2(\psi_1(H_2))$, and so on. Note that a chain of length n gives rise to an isogeny of degree $\Omega(\exp(n))$.

Interestingly, for isogenies with kernel isomorphic to $\mathbb{Z}/\ell^n$ for a fixed small prime ℓ, the optimal strategy of evaluating the chain can be implemented using only $O(n \log n)$ evaluations of scalar multiplication by ℓ and isogenies of degree ℓ, while the two "obvious" strategies take time $\Theta(n^2)$. This is a fun exercise for the reader.

Decomposing composite-degree isogenies like this reduces the problem of isogeny representations to the prime case. In this case, the classical approach are explicit formulas due to Vélu from 1971, which take time $\Theta(\ell)$ to compute and evaluate an ℓ-isogeny from its kernel. It was long suspected that this complexity might be optimal, until 2020, when the $\sqrt{\text{élu}}$ algorithm [1] with a complexity of $\widetilde{O}(\sqrt{\ell})$ finally broke through the perceived linear-time barrier established by Vélu.

In summary, decomposing an isogeny into prime steps which are then individually handled using $\sqrt{\text{élu}}$ remains the state of the art for constructing an isogeny chain from a generating set of its kernel subgroup. Note that this approach is therefore inherently limited to isogenies of *smooth* degree. At the moment, two main families of techniques are available to overcome this issue, which will be discussed in the following.

Isogenies as ideals

Another extremely fruitful approach to representing isogenies comes from identifying a given subgroup (i.e., an isogeny kernel) on the curve with a subset of their endomorphism rings.

Concretely, we associate to any nonzero (say, left) ideal I of the endomorphism ring $\mathrm{End}(E)$ the subgroup

$$E[I] := \bigcap_{\alpha \in I} \ker \alpha \,. \qquad (*)$$

This subgroup is necessarily finite: One easy way to see this is that $\mathrm{norm}(I) \in I$, hence $E[I] \subseteq E[\mathrm{norm}(I)]$. Conversely, a finite subgroup $H \leq E$ defines the ideal

$$I(H) := \left\{ \alpha \in \mathrm{End}(E) \;\middle|\; \ker(\alpha) \supseteq H \right\}.$$

It is a non-obvious fact (essentially due to Deuring [3] in the elliptic-curve case, later generalized to higher dimensions by Waterhouse [9]) that these two constructions are inverses of one another, hence there is a one-to-one correspondence between finite subgroups and (nonzero one-sided) endomorphism ideals.

One major advantage of this representation is that it allows one to easily write down even isogenies of large prime degrees, which would be exponentially larger using an explicit Vélu-style representation. Moreover, we have powerful tools for manipulating such ideals: The key point is that principal ideals correspond to endomorphisms, hence *ideals lie in the same class if and only if their associated isogenies lead to the same curve*.

[1] This is in the sense of complexity theory, i.e., the computational effort is polynomial in the *bit length* of the input! In other words, if $E[N]$ is defined over an extension of $\mathbb{F}_q$ of degree polynomial in $\log(q)$, then the overall runtime is polynomial in both $\log(q)$ and $\log(N)$.

[2] For $B \in \mathbb{N}$, an integer is B-*smooth* if none of its prime factors exceed B. Sometimes B is not specified explicitly.

Among other things, this observation gives rise to a well-known group action of $\mathrm{cl}(\mathcal{O})$ on the set of elliptic curves E with an embedding $\mathcal{O} \hookrightarrow \mathrm{End}(E)$, where $\mathcal{O}$ is some imaginary-quadratic order.

It also leads to the *Deuring correspondence*, a far-reaching equivalence of categories between supersingular elliptic curves with isogenies and invertible one-sided modules over the endomorphism ring with their homomorphisms. One particular implication is that the map from isomorphism classes of supersingular elliptic curves to isomorphism classes of their endomorphism rings is at most two-to-one (the fibers forming Galois orbits). By virtue of the explicit algorithms outlined above, combined with the seminal *KLPT* algorithm [5] for finding quaternion ideals of controlled norm in a given class, we may compute the reverse direction (constructing a supersingular elliptic curve with a given endomorphism ring) in polynomial time assuming GRH; see for instance [4]. This approach leads to a practically efficient algorithm for computing and evaluating any isogeny given by its associated ideal.

Higher dimensions

Another very efficient approach for computing and evaluating isogenies of non-smooth degree comes from abelian varieties of dimensions greater than one. Computing such isogenies is theoretically solved [7] assuming the isogeny is sufficiently respectful of a polarization on the involved varieties, but practical implementations remain restricted to special cases.

The current most promising approach to practically compute higher-dimensional isogenies relies on the theory of theta functions, a classical object in the study of abelian varieties. The theta coordinate system of level n for a g-dimensional variety consists of n^g coordinates; hence, as the dimension grows, it becomes more and more important to work with the lowest possible level.

For cryptographic applications, as it turns out, it is usually sufficient to use theta coordinates of level 2, despite the fact that they do not suffice to embed the given variety A, but rather just its Kummer variety $A/\{\pm 1\}$: Concretely, this means a given coordinate tuple represents an equivalence class of a point on the abelian variety modulo negation rather than a unique point. In reality, the sign ambiguity can usually be worked around.

Similar to the classical formulas of Vélu in dimension one, there exist algorithms to compute isogenies of principally polarized abelian varieties in time linear in the degree. However, note that the most common type of isogenies under consideration are of type $(\ell, \ell, ..., \ell)$, which means that the kernel subgroup is isomorphic to $(\mathbb{Z}/\ell)^g$ and maximally isotropic with respect to the Weil pairing coming from the polarization — hence the degree of such an isogeny is exponential in the dimension!

Kani's lemma

...is a now-legendary result concerning isogenies between *products* of abelian varieties. Its main application in computing isogenies lies in the very useful fact that isogenies between products between two (say) elliptic curves can *embed* lower-dimensional isogenies, even if those isogenies do not admit an efficient representation as a lower-dimensional isogeny a priori. The only thing that is required to explicitly compute and evaluate the higher-dimensional embedding isogeny is information on how the target lower-dimensional isogenies restrict to the N-torsion subgroup in which the kernel of the higher-dimensional isogeny lives. More concretely: Suppose given a commutative diagram of isogenies

$$\begin{array}{ccc} E_0 & \xrightarrow{\quad\varphi\quad} & E_1 \\ {\scriptstyle\psi}\downarrow & & \downarrow{\scriptstyle\psi'} \\ E_2 & \xrightarrow[\quad\varphi'\quad]{} & E_3 \end{array}$$

such that $\deg(\varphi) = \deg(\varphi')$ and $\deg(\psi) = \deg(\psi')$ and these degrees are coprime. Set $N := \deg(\varphi) + \deg(\psi)$. Then

$$\Phi = \begin{pmatrix} \varphi & \widehat{\psi'} \\ -\psi & \widehat{\varphi'} \end{pmatrix} : \; E_0 \times E_3 \longrightarrow E_1 \times E_2$$

is an isogeny of principally polarized abelian varieties. (The polarization is given by the product polarizations.) Its kernel is the (N, N)-subgroup

$$\ker \Phi = \left\{ \left(\widehat{\varphi}(T), \psi'(T)\right) \;\middle|\; T \in E_1[N] \right\}.$$

Note in particular that evaluating φ reduces to evaluating Φ by simply composing it with the embedding $E_0 \hookrightarrow E_0 \times E_3$ and the projection $E_1 \times E_2 \twoheadrightarrow E_1$.

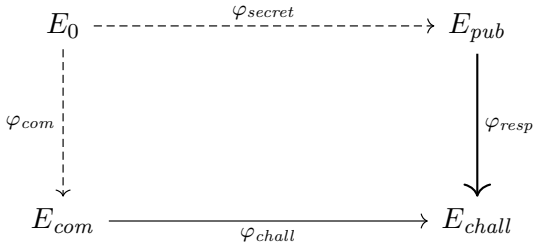
The key detail is that *in this case* efficient formulas to compute the isogeny chain are known provided that N is smooth, and in practice this is particularly convenient and fast when N equals a power of two: In this case, one may employ either the classical *Richelot isogenies* for Jacobians of genus-2 curves in Mumford representation, or the more recent formulas for $(2, 2)$-isogenies in theta coordinates [2] which are both faster and more amenable to generalization.

We mention in passing that embedding isogenies into higher-dimensional ones is a very general technique which has already led to asymptotic improvements in "classical" computational tasks associated to abelian varieties, such as computing endomorphism rings or zeta functions of ordinary elliptic curves over finite fields [8].

Digital signatures: *SQIsign*

In this section, we outline a recent cryptographic construction based on the techniques surveyed above. That primitive is a digital signature scheme: Essentially a cryptographic analogue of the age-old idea of signing one's name on paper to confirm the authenticity of a document. The key ingredient to a signature scheme is an *(interactive) identification scheme*, where a verifier asks questions to a prover who tries to convince the verifier that they know the private key associated to some pre-published information (the public key).

In SQIsign[3], the identification scheme in question is summarized in the following diagram:



The data flow is as follows: Ahead of time, the prover (whom we shall call Alice) chooses some random secret isogeny φ_{secret} from a fixed, publicly known starting elliptic curve E_0; the codomain curve E_{pub} is her public key. Later, whenever Alice wishes to identify herself, she samples another random secret isogeny φ_{comm} from E_0 and again publishes the codomain. The verifier[4] then samples a random isogeny φ_{chall} from E_{com} and publishes the isogeny (not just the codomain). Finally, the task that Alice has to perform in order to convince the verifier that she really knows φ_{secret} is to exhibit an isogeny φ_{resp} from E_{pub} to E_{chall}.

If Alice is actually herself, then this is fundamentally easy: She may simply compose the three isogenies

$$E_{pub} \xrightarrow{\widehat{\varphi_{secret}}} E_0 \xrightarrow{\varphi_{com}} E_{com} \xrightarrow{\varphi_{chall}} E_{chall}$$

to find such an isogeny. Publishing this isogeny, however, would be a fatal mistake: Since the isogeny chain contains the dual of the secret φ_{secret} as a prefix, it would be easy for any attacker to extract Alice's secret from this response isogeny, which would enable them to subsequently pretend to be Alice.

The way SQIsign resolves this issue is by essentially rewriting the "broken" response isogeny into another, random isogeny between the same pair of curves by means of the Deuring correspondence: A variant of the KLPT algorithm mentioned above can be used to randomize within the set $\mathrm{Hom}(E_{pub}, E_{chall})$ so long as the endomorphism ring of E_{pub} is known. This is a piece of information that is available to Alice since the starting curve E_0 is constructed in such a way that it comes with knowledge of its endomorphism ring, and Alice knows a connecting isogeny φ_{secret} from E_0 to E_{pub}, which allows her to deduce $\mathrm{End}(E_{pub})$ from $\mathrm{End}(E_0)$.

The original variant of SQIsign [10] then chooses a response isogeny of some convenient smooth degree, so that the ideal-to-isogeny translation for φ_{resp} can be done efficiently using "standard" isogeny chains. Newer variants of SQIsign (such as *SQIsignHD*, *SQIsign2D*, or *SQIPrime*) instead rely on the embedding technique using Kani's lemma to represent the response isogeny; this dramatically improves the performance (by a factor close to 10!) as well as the security (since the random sampling from $\mathrm{Hom}(E_{pub}, E_{chall})$ is less biased than if only smooth degrees are permitted).

Further improvements to SQIsign are expected (and indeed ongoing work). Among all post-quantum signature schemes currently under consideration, SQIsign variants boast the (by far) smallest public-key and signature sizes, comparable to some of today's popular quantum-insecure signature schemes.

For recent developments surrounding SQIsign, see `https://sqisign.org`.

I-sage-nies

All of the techniques surveyed in this article are fully algorithmic and have, to a large extent, been implemented. We highlight some recent improvements along these lines to the SageMath computer-algebra system by the author and others, which (sadly!) remain focused on the case of elliptic curves (i.e., dimension one). As of version 10.4, the following are available:

- Decomposing composite-degree isogenies given by kernel generators as isogeny chains.
- The $\sqrt{\text{élu}}$ algorithm to compute prime-degree isogenies in essentially square-root time.
- Symbolic sums of isogenies between the same pair of curves and conversion to isogeny chains.
- Computing the matrix of the restriction of an isogeny to an N-torsion subgroup.

Works in progress include:

- Left- and right-division of isogenies, whenever this makes sense.
- Computing endomorphism rings of ordinary and supersingular elliptic curves over finite fields.
- Evaluating the class-group action and computing the Deuring correspondence efficiently.
- Algorithms for higher-dimensional abelian varieties and their isogenies.

References

[1] Daniel J. Bernstein, Luca De Feo, Antonin Leroux, and Benjamin Smith: *Faster computation of isogenies of large prime degree*, ANTS XIV, 2020.

[2] Pierrick Dartois, Luciano Maino, Giacomo Pope, and Damien Robert: *An Algorithmic Approach to $(2,2)$-isogenies in the Theta Model and Applications to Isogeny-based Cryptography*, Preprint. `https://ia.cr/2023/1747`

[3] The name stands for "Short Quaternion and Isogeny Signature".

[4] More generally, the challenge isogeny can be sampled by anyone who can be trusted not to collude with Alice — this is a subtle but important detail that becomes relevant when transforming the interactive identification scheme to a (non-interactive) signature scheme, in which Alice will essentially generate the challenge by herself in a way that makes it impossible for her to force an advantageous result.

[3] Max Deuring: *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper* Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg 14 (1941), p. 197–272.

[4] Jonathan Komada Eriksen, Lorenz Panny, Jana Sotáková, and Mattia Veroni: *Deuring for the People: Supersingular Elliptic Curves with Prescribed Endomorphism Ring in General Characteristic*, LMFDB, Computation, and Number Theory (LuCaNT), 2023.

[5] David Kohel, Kristin E. Lauter, Christophe Petit, and Jean-Pierre Tignol: *On the quaternion ℓ-isogeny path problem*, LMS J. Comput. Math. 17 (2014), p. 418–432.

[6] Chloe Martindale and Lorenz Panny: *Isogeny-based Cryptography*, Computeralgebra-Rundbrief 65, Oktober 2019.

[7] Damien Robert: *Efficient algorithms for abelian varieties and their moduli spaces*, Habilitation à diriger les recherches, June 2021, Université Bordeaux.

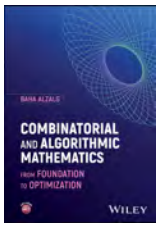
[8] Damien Robert: *Some applications of higher dimensional isogenies to elliptic curves (overview of results)*, Preprint. `https://ia.cr/2022/1704`

[9] William C. Waterhouse: *Abelian varieties over finite fields*, Annales scientifiques de l'É.N.S. 4^{e} série, tome 2, n° 4 (1969), p. 521–560.

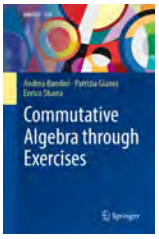
[10] Luca De Feo, David Kohel, Antonin Leroux, Christophe Petit, and Benjamin Wesolowski: *SQISign: Compact Post-quantum Signatures from Quaternions and Isogenies*, ASIACRYPT, Lecture Notes in Computer Science 12491 (2020), p. 64–93.

Publikationen über Computeralgebra

Neuerscheinungen:

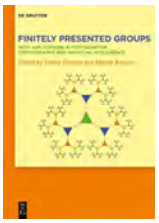


Baha Alzag,
Combinatorial and Algorithmic Mathematics,
John Wiley and Sons,
Juli 2024, 544 Seiten,
ISBN 978-1394235940

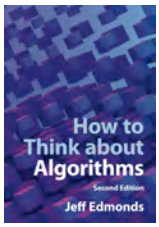


A. Bandini, P. Gianni, E. Sbarra,
Commutative Algebra through Exercises,
Springer Nature Switzerland,
Juli 2024, 403 Seiten
ISBN 978-3031569098

W. Decker et al. (Hrsg.),
The Computer Algebra System OSCAR: Algorithms and Examples,
Springer-Verlag,
Nov. 2024, 471 Seiten
ISBN 978-3031621260

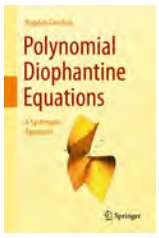


V. Diekert, M. Kreuzer (Hrsg.),
Finitely Presented Groups,
de Gruyter Verlag,
Okt. 2024, 252 Seiten,
ISBN 978-3111473376

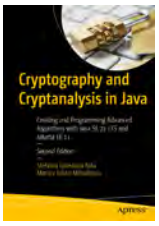


Jeff Edmonds,
How to Think about Algorithms,
Cambridge Univ. Press,
2. Auflage, März 2024,
616 Seiten,
ISBN 978-1009302135

J. Ellis-Monaghan, I. Moffatt (Hrsg.),
Handbook of the Tutte Polynomial and Related Topics,
CRC Press,
Aug. 2024, 804 Seiten,
ISBN 978-1032231938



Bogdan Grechuk,
Polynomial Diophantine Equations A Systematic Approach,
Springer-Verlag,
Sep. 2024, 829 Seiten,
ISBN 978-3031629488



S. L. Nita, M. I. Mihailescu,
Cryptography and Cryptanalysis in Java
Apress,
2. Auflage, Juli 2024,
315 Seiten,
ISBN 979-8868804403

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 Martin Kreuzer (`martin.kreuzer@uni-passau.de`) auf.

Andrea Bandini, Patrizia Gianni und Enrico Sbarra, Commutative Algebra through Exercises

Unitext 159, Springer Nature Switzerland, Cham 2024, 403 Seiten, ISBN 978-3031569098

Klassische Einführungen in die kommutative Algebra wie die Bücher von Atiyah-MacDonald [1], Kunz [2] oder Matsumura [3] sind meist sehr theoretisch und trocken. Modernere Werke wie die von Eisenbud [4] oder Kemper [5] schließen immerhin ein Kapitel über Gröbner-Basen und praktische, konstruktive Methoden ein. Das vorliegende Buch geht aber noch einen Schritt weiter. Der Schwerpunkt des Lernens wird auf die über 400 Übungsaufgaben verlagert. Selbst einfache Teile der Theorie werden so präsentiert, dass man angehalten ist, die Beweise eigenständig zu finden. Wann immer möglich, werden die manchmal recht abstrakten Begrifflichkeiten anhand von Beispielaufgaben mit Polynomringen und Moduln über Hauptidealbereichen illustriert und effektiv berechnet.

Das Buch ist in drei Teile gegliedert. Im ersten Teil werden die wichtigsten Definitionen und Sätze vorgestellt, so dass dieser Teil als knapp gefasstes Nachschlagewerk dienen kann. Hier sind nur die instruktivsten Beweise und die wichtigsten Methoden aufgeführt. Alle anderen Beweise stehen in einem separaten Kapitel am Ende des Buchs und können teilweise auch als Übungsaufgaben dienen.

Der zweite Teil des Buchs enthält die Übungsaufgaben, sortiert nach den Theoriekapiteln. Zusätzlich findet sich hier ein Abschnitt mit wahr/falsch Fragen, der sich hervorragend zur Lernkontrolle eignet. Schließlich haben die Autoren noch einen Abschnitt mit Wiederholungsaufgaben angefügt, so dass auch Anhänger wiederholender Lernmethoden wie der *Spaced Repetition* genug Material finden.

Im dritten Teil stehen schließlich die Beweise der theoretischen Resultate, die verschoben worden waren und die Lösungen der Übungsaufgaben. Allerdings eignet sich nur ein kleiner Teil dieser Aufgaben für eine Bearbeitung mithilfe eines Computeralgebrasystems.

Inhaltlich wird in sieben Kapiteln ein Großteil der grundlegenden kommutativen Algebra abgedeckt. Nach einem allgemeinen Kapitel über Ringe folgt sofort eines über Polynomringe, bei dem es hauptsächlich um Gröbner-Basen und effektive Methoden geht. Dann folgt ein Kapitel über affine algebraische Varietäten, das die Brücke zur algebraischen Geometrie herstellt, und anschließend geht es um Moduln, Tensorprodukte, Lokalisation sowie noethersche und artinsche Ringe plus die Primärzerlegung.

Der Theorieteil des Werks ist recht komprimiert und knapp geschrieben, was den Nachschlagecharakter betont. Dafür sind die Lösungen der Übungsaufgaben klar und ausführlich gestaltet, sodass sich der hier verfolgte aktive Lernansatz auch für ein Selbststudium eignet.

Das Buch basiert auf Vorlesungen und Übungen, die die Autoren über 10 Jahre lang an der Universität Pisa entwickelt und abgehalten haben. Es ist eine Übersetzung des Werks *Esercizi di algebra commutativa* derselben Autoren ins Englische. Leser, die des Italienischen mächtig sind und 2/3 des Preises sparen möchten, können sich also auch die italienische Version besorgen, die bei der Pisa University Press erschienen ist (vgl. [6]).

Insgesamt stellt das Buch einen frischen Ansatz für die Lehre in der kommutativen Algebra vor, der sich allem Anschein nach in Pisa bewährt hat und zum Ausprobieren einlädt. Die Tatsache, dass es jetzt in Englisch verfügbar ist, kommt der auch hierzulande um sich greifenden Internationalisierung der Studiengänge zugute. Sowohl für die universitäre Lehre im späten Bachelor- und im frühen Masterstudium als auch für das Selbststudium der kommutative Algebra stellt es einen ansprechenden neuen Beitrag dar.

Martin Kreuzer (Passau)

Referenzen

[1] M. F. Atiyah und I. G. Macdonald, Introduction to Commutative Algebra, Addison-Wesley, Reading 1969

[2] E. Kunz, Einführung in die kommutative Algebra und algebraische Geometrie, Vieweg, Braunschweig 1979

[3] H. Matsumura, Commutative Ring Theory, Cambridge University Press, Cambridge 1987

[4] D. Eisenbud, Commutative Algebra with a View Toward Algebraic Geometry, Springer-Verlag, New York 1995

[5] G. Kemper, A Course in Commutative Algebra, Springer-Verlag, Berlin 2011

[6] A. Bandini, P. Gianni und E. Sbarra, Esercizi die algebra commutativa (Manuali), Pisa University Press, Pisa 2023

Dissertationspreis der Fachgruppe Computeralgebra:

Die Fachgruppe Computeralgebra möchte herausragende Dissertationen im Themenbereich der Computeralgebra durch die Vergabe eines Dissertationspreises würdigen. Die Ausschreibung erfolgt zum ersten Mal im Jahr 2024 und danach jährlich, jeweils mit der Einreichungsfrist 1. April.

Eingereicht werden können deutsch- oder englischsprachige Dissertationen, die innerhalb von 12 Monaten vor der Einreichungsfrist verteidigt und veröffentlicht wurden. Zugelassen sind Dissertationen aus dem deutschsprachigen Raum, mit einem betreuenden Institut aus Deutschland, Österreich oder der Schweiz. Das Thema der Dissertation soll einen klaren Bezug zur Computeralgebra (Theorie, Algorithmen oder Implementierung) aufweisen.

Einreichungen können entweder als Eigenbewerbung oder als Nominierung durch die wissenschaftlichen Betreuerinnen und Betreuer per E-Mail an die Fachgruppe Computeralgebra

`ca-promotionspreis@mathematik.de`

erfolgen.

Einzureichen sind in elektronischer Form die Dissertation, eine Kurzfassung (max. 1/2 Seite), akademischer Werdegang mit Publikationsliste und optional ein Empfehlungsschreiben.

Der Dissertationspreis ist mit 500 Euro dotiert. Die Kurzfassungen aller eingereichten Dissertationen werden im Rundbrief der Fachgruppe Computeralgebra veröffentlicht.

Promotionen in der Computeralgebra

Um herausragende Dissertationen im Themenbereich der Computeralgebra zu würdigen vergibt die Fachgruppe Computeralgebra im Jahr 2024 zum ersten Mal einen Dissertationspreis. Die folgenden sechs Promotionen wurden im Jahre 2024 für den Dissertationspreis der Fachgruppe Computeralgebra nominiert. Der Preis wird bei der Computeralgebra-Tagung der Fachgruppe 02.-04.06.2025 in Leipzig verliehen.

Miroslav Stankovič: Moment-based loop analysis

TU Wien

February 2023

In this thesis, we explore automated analysis of loops of probabilistic programs (PPs). We look specifically at finding a quantitative loop invariant: a property of a given loop that describes its behaviour. Loop invariants are key for reasoning about program loops. In the context of probabilistic programs, variables represent distributions, and the invariant needs to capture the statistical properties of these distributions. In our work, we focus on computing so-called moment-based invariants (MBIs), invariant properties that describe the expected value and higher (and mixed) moments of program variables. While it is not feasible to compute all moments, which would fully characterize the underlying distribution, our methods are able to compute moments of arbitrary order, hence allowing us to capture the loop properties relatively precisely. As one of the main results in this thesis, we give a characterization of Prob-solvable loops, a class of PP loops, for which MBIs can be, in principle, always computed. We also describe a fully automated method of computing MBIs of arbitrary order for any program of this class. The method is implemented and evaluated on several challenging benchmarks from the literature. In the second part of the thesis, we study how moment-based analysis of Prob-solvable loops and MBIs can be applied to reasoning about various challenges in Bayesian networks (BNs). We extend the framework introduced earlier to accommodate encoding BNs as PPs and also provide a way to encode several tasks in BN analysis as computing MBIs in a corresponding PP - such as exact inference, expected number of samples, or sensitivity analysis. In the last part of the thesis, we briefly discuss extensions of this work. We fully characterize the class of programs for which MBIs can be computed (moment-computable programs) and investigate how to automatically estimate probability distributions from MBIs. We also consider programs that are not moment-computable, for which we look at combinations of variables and approximations.

Philipp Nuspl: Algorithms for linear recurrence sequences

Johannes Kepler Universität Linz

May 2023

In the past few decades, numerous tools for automatically discovering and pro- ving identities involving sequences and special functions were developed. These tools are often based on algorithms which manipulate sequences satisfying linear recurrences. If the recurrences have constant coefficients, these sequences are called C-finite and in the case of polynomial coefficients they are called D-finite. We study sequences satisfying recurrences with coefficients which are C- finite themselves and call them C2-finite. We investigate which properties and algorithms carry over from the classical C-finite and D-finite cases to this new setting. In particular, we show that most so-called closure-properties, which are known for the classical cases, also hold for C2-finite sequences, i.e., they are closed under termwise addition, termwise multiplication, interlacing and taking subsequences at arithmetic progressions. In many cases these operations are effective and we present algorithms for performing them. In general, however, these algorithms are closely related to and limited by certain decision procedures of C-finite sequences. Deciding whether every term of a sequence is positive or nonzero is not known to be decidable in theory. Nevertheless, we show that it is often easy to decide these properties in practice. Restricting the ring of C2-finite sequence to sequences which satisfy a mo- nic (i.e., having constant leading coefficient) linear recurrence with C-finite co- efficients, we obtain a subring where all closure properties can be performed effectively. On the other hand, we can allow more general sequences as coefficients. This way we obtain increasingly larger rings where the operations are more difficult to perform. Most of the theoretical results are also implemented in a package for the computer algebra system SageMath. The thesis contains a tutorial for this package. The tutorial shows how the examples given throughout the thesis can be per- formed automatically on the computer.

Johannes Schmitt: On $\mathbb{Q}$-factorial terminalizations of symplectic linear quotient singularities

Rheinland-Pfälzische Technische Universität Kaiserslautern-Landau

July 2023

Symplectic linear quotient singularities belong to the class of symplectic singularities introduced by Beauville in 2000. They are linear quotients by a group preserving a symplectic form on the vector space and are necessarily singular by a classical theorem of Chevalley–Serre–Shephard–Todd. We study Q-factorial terminalizations of such quo- tient singularities, that is, crepant partial resolutions that are allowed to have mild singularities. The only symplectic linear quotients that can possibly admit a smooth Q-factorial terminalization are by a theorem of Verbitsky those by symplectic reflection groups. A smooth Q-factorial terminalization is in this context referred to as a symplectic resolu- tion and over the past two decades, there is an ongoing effort to classify exactly which symplectic reflection groups give rise to quotients that admit symplectic resolutions. We reduce this classification to finitely many, precisely 45, open cases by proving that for almost all quotients by symplectically primitive symplectic reflection groups no such resolution exists. Concentrating on the groups themselves, we prove that a parabolic subgroup of a symplectic reflection group is generated by symplectic reflections as well. This is a direct analogue of a theorem of Steinberg for complex reflection groups. We further study divisor class groups of Q-factorial terminalizations of linear quotients by finite subgroups G of the special linear group and prove that such a class group is completely controlled by the symplectic reflections – or more generally junior elements – contained in G. We finally discuss our implementation of an algorithm by Yamagishi for the computa- tion of the Cox ring of a Q-factorial terminalization of a linear quotient in the computer algebra system OSCAR. We use this algorithm to construct a generating system of the Cox ring corresponding to the quotient by a dihedral group of order 2d with d odd acting by symplectic reflections. Although our argument follows the algorithm, the proof does not logically depend on computer calculations. We are able to derive the Q-factorial terminalization itself from the Cox ring in this case.

Katherine Kosaian: Formally verifying algorithms for real quantifier elimination

Carnegie Mellon University

August 2023

Statements in the first-order logic of real arithmetic ($\text{FOL}_{\mathbb{R}}$) that involve the "there exists" and "for all" quantifiers arise in various application domains, like the formal verification of cyber- physical systems and robot motion planning. These quantifiers are difficult for both humans and computers to handle, and the best way of analyzing these quantified formulas is to reduce them to logically equivalent quantifier-free formulas, through a process known as quantifier elimination (QE). QE makes formulas significantly simpler to analyze (as quantifier-free formulas can be easily evaluated by arithmetic in individual states, whereas quantified formulas cannot). Given the safety-critical nature of applications involving real quantifier elimination, having correct QE algorithms is crucial. For this, formally verifying QE algorithms—by implementing them in a theorem prover and developing associated proofs of correctness—is very desirable. These proofs of correctness are rigorous, as they rely only on the trusted core of the theorem prover, a (typically small) foundation of trusted code/logical axioms from which all other results are built. My thesis provides formally verified support for real QE with a two-pronged approach: First, develop support for efficient incomplete QE algorithms (which are specialized to a fragment of real arithmetic), with a focus on filling gaps in the existing body of related work. Next, develop support for a promising complete QE algorithm with the potential for eventual efficiency / good complexity. For the first goal, the thesis discusses a verification of linear and quadratic virtual substitution with a focus on experimentation and optimization; the experiments show that this verified VS implementation is competitive with unverified implementations of VS. For the second goal, the thesis discusses the verification of a complete QE algorithm that uses insights from the influential Ben-Or, Kozen, and Reif (BKR) algorithm; although this verified algorithm does not currently exploit all insights from BKR and does not yet realize practical efficiency, it lays groundwork for eventual verified complete QE algorithms with strong parallel complexity bounds. Both verifications are completed in the theorem prover Isabelle/HOL.

Clemens Hofstadler: Noncommutative Gröbner bases and automated proofs of operator statements

Johannes Kepler University Linz

September 2023

Linear operators play a fundamental role in various branches of mathematics and related disciplines. In linear algebra and geometry, for example, they appear in the form of matrices, representing linear transformations such as coordinate changes. In functional analysis, (bounded) operators on Hilbert spaces, or more generally, operators in operator algebras, serve as essential tools for understanding and manipulating function spaces. Their applications range from the study of integral and differential equations to tasks like filtering and transforming signals in the field of signal processing. In quantum mechanics, linear operators represent physical observables, and the Schrödinger equation involves these operators in describing the evolution of quantum systems. In the thesis, we develop an algebraic framework for automatically proving statements about linear operators by computations with noncommutative polynomials. More specifically, arbitrary first-order statements about identities of linear operators can be treated. We present a practical semi-decision procedure for validity of such formulas based on the verification of ideal member- ship in a free algebra. In contrast to classical approaches for automated theorem proving, these algebraic computations automatically incorporate linearity and they benefit from efficient ideal membership procedures. In particular, we exploit the theory of noncommutative Gröbner bases to verify ideal mem- bership in the free algebra. In order to enhance these computations, we generalise the concept of signature Gröbner bases, originally developed for commutative polynomials, to the free setting, and more generally, to mixed algebras, allowing a mixture of commutative and noncommuta- tive variables. We also provide SageMath implementations of the newly developed algorithms, which, as our experiments show, improve the state-of-the-art for noncommutative Gröbner basis computations. Based on Gröbner basis techniques, we also generalise existing and develop new algorithms for computing elements of specific forms in noncommutative polynomial ideals. These methods serve as one of the key steps in the aforementioned semi-decision procedure. Furthermore, we present novel methods for finding short proofs of operator statements, based on the ability to compute short certificates of ideal membership. All algorithms are implemented in various software packages for SageMath and Mathematica. We illustrate the capabilities of our framework and software through a case study on statements about the Moore-Penrose inverse, including classical facts and recent results. Furthermore, we showcase that our approach allows to discover new theorems, and we discuss how diagram chases in abelian categories can be automated using our framework.

Stefania Trentin: On the Rapoport-Zink space for GU(2,4) over a ramified prime

Universität Münster

November 2023

Shimura Varieties play a fundamental role in the framework of the Langlands Program and are defined as moduli spaces of Abelian varieties. One can reformulate the definition of a Shimura variety in terms of the associated Rapoport-Zink space, which is a moduli space of p-divisible groups over a ramified quadratic extension of the p-adic rationals $\mathbb{Q}_p$.

Whether the Rapoport-Zink space associated to a Shimura variety is flat has been an open question since their introduction in [RZ96]. In [Pap00] Pappas showed that this is the case for the Shimura variety associated to the group $\mathrm{GU}(1, n-1)$ and reduced the proof of flatness to proving that a certain polynomial ideal $J \subset \mathbb{F}_p[\underline{x}]$ is radical. The main difficulty in proving radicality of J, or equivalent flatness of the corresponding Rapoport-Zink space, is that this has to be done for any prime $p > 2$. There are several algorithms for computing the radical of an ideal, but they all require choosing a characteristic, see for example [Kem02]. On the other hand, computing Gröbner bases can be done almost independently on the characteristic. More precisely, it is shown in [Win88] that if G is a Gröbner bases for a lift of J to $\mathbb{Q}[\underline{x}]$, the image of G modulo p is a Gröbner bases for J over $\mathbb{F}_p$ for almost all primes p, and it is possible to compute the finite set of primes for which this is not the case. Based on this result we designed an algorithm testing radicality of the ideal J associated to $\mathrm{GU}(2, 4)$ only by means of Gröbner bases. The algorithm could than be performed over $\mathbb{Q}$ to deduce radicality over $\mathbb{F}_p$ for p not in a finite set of primes. The algorithm can be applied to any ideal if one has a good criterion for proving radicality of univariate polynomial ideals.

To conclude the study of our Rapoport-Zink space we analyzed its irreducible components and their intersections. In particular, they can be described in terms of some Deligne-Lusztig varieties for the orthogonal and symplectic groups of rank 3. The information on their intersection pattern and a further decomposition into finer strata is encoded into the associated admissible set, a finite set of an affine Weyl group whose combinatorial properties were studied using the computational algebra software SageMath [SD23].

References

[Kem02] G. Kemper, The calculation of radical ideals in positive characteristic, Journal of Symbolic Computation 34 (2002), no. 3, 229–238.

[Pap00] G. Pappas, On the arithmetic moduli schemes of PEL Shimura varieties, Journal of Algebraic Geometry 9 (2000), no. 3, 577–605.

[RZ96] M. Rapoport and Th. Zink, Period spaces for p-divisible groups (AM-141), Annals of Mathematics, Princeton University Press, 1996.

[SD23] The Sage Developers, Sagemath, the Sage Mathematics Software System (Version 9.8.6), 2023. https://www.sagemath.org.

[Win88] F. Winkler, A p-adic approach to the computation of Gröbner bases, Journal of Symbolic Computation 6 (1988), no. 2, 287–304.

Weitere neue Promotionen aus dem Bereich Computeralgebra:

Daniel Rademacher: Constructive recognition of finite classical groups with stingray elements

Betreuer: Alice Niemeyer (Aachen), Max Horn (Kaiserslautern)

Weitere Gutachter: Cheryl Praeger (Perth, Australien)

September 2024

Abstract: The *matrix group recognition project* aims to algorithmically answer fundamental questions about matrix groups over finite fields. One approach is to derive from a given set of group generators a data structure called *composition tree* which then is used as input for further algorithms. Using composition trees, computations of a large matrix group are decomposed into computations for smaller matrix groups until this process cannot be repeated anymore. The remaining leaf groups are the finite (quasi-)simple groups, which include the so-called *classical matrix groups* (such as $\mathrm{SL}_n(\mathbb{F}_q)$).

Efficient algorithms to deal with classical matrix groups are essential for the overall performance of creating the composition tree. The thesis presents a novel algorithm for constructively recognising classical groups within their natural representations, building upon preliminary concepts from Ákos Seress and Max Neunhöffer for special linear groups. The algorithm consists of three subalgorithms:

1. **GoingDown algorithm:** Recursively descends from the input group G (e.g. $\mathrm{SL}_n(\mathbb{F}_q)$) to a subgroup U isomorphic to a "base case group" (e.g. $\mathrm{SL}_2(\mathbb{F}_q)$) using stingray duos and reaching such a group in significantly fewer steps than traditional methods.
2. **BaseCase algorithm:** Utilises an efficient method for constructively recognising the base case group U forming a starting point for the computation of standard generators of G.
3. **GoingUp Algorithm:** Extends standard generators from the subgroup U to the original group G, employing an original approach to compute generators for intermediate subgroups.

The result shows significant improvements over the existing state-of-the-art algorithms, both in practical performance (comparing our implementation in GAP to the existing one in Magma) and in terms of theoretical complexity, although the latter is not yet fully proven.

Max Mayer: Advanced Algorithms For Induced Sequences And Residual Nilpotence In Polycyclic Groups

Betreuer: Max Horn (Kaiserslautern)

Weitere Gutachter: Bettina Eick (Braunschweig)

September 2024

Abstract: Polycyclic groups are class of finitely presented groups that are particular nice from a computational point of view. They are characterised by a normal series with cyclic factor groups. One can use this to represent elements of polycyclic groups by integer exponent vectors which allows explicit computations within these groups.

When working with infinite polycyclic groups one often faces the problem that fast computations are impeded by an exponential growth of the involved exponent vectors of intermediate results. Computing induced sequences of subgroups, which is an important core step for many algorithms, in particular is susceptible to this issue. This thesis develops novel efficient methods addressing this problem. For this we utilize the similarities between induced sequences and hermite normal forms for integer matrices, whose computation possess a broad theoretical foundation, which we transfer onto the polycyclic setting. The resulting GAP code outperforms the existing implementation substantially.

In the second part of this work we look at the question on how to decide whether a polycyclic group is residually nilpotent. A group G is called *residually nilpotent* if every non-trivial element has a non-trivial image in a nilpotent quotient of G. This property was already studied for many other classes of groups (e.g. free groups). It is known that all polycyclic groups possess a residually nilpotent normal subgroup of finite index. However, deciding whether the original group is residually nilpotent itself appears to be more challenging. We present and implement an effective algorithmic solution for the important subcase of polycyclic groups with an abelian normal subgroup N such that the quotient group G/N is nilpotent. These groups arise naturally as extensions of free abelian groups e.g. in number field theory.

Habilitationen in der Computeralgebra

Hery Randriamaro: Computer Algebra of Conditional Oriented Matroids
Betreuer: Wolfram Koepf (Kassel)
Weitere Gutachter: Jürgen Richter-Gebert (München), Volkmar Welker (Marburg)
Oktober 2024
Abstract:

In this habilitation thesis, first of all, the fundamental objects that led to conditional oriented matroids are reviewed. The starting point are matroids, introduced by Whitney (1935) as abstractions of the linear dependence of matrix columns. But matroids can also be defined in terms of their circuits and their basis. It is described how Folkman & Lawrence (1978) developed oriented matroids by inserting an orientation on matroids defined in terms of circuits, while Bland & Las Vergnas (1978) proceeded with a similar development but with cocircuits. The last description concerns lopsided sets, introduced by Lawrence (1983).

Afterwards, the first main objects of study, namely conditional oriented matroids, are described. Both important ones, oriented matroids and lopsided systems, are naturally specified. Deletion, contraction, and simplification of conditional oriented matroids are defined. Then, a generalization of the theorem of Mandel is provided. That theorem originally allows to determine the covector set of an oriented matroid from its set of topes using the composition condition. The generalization proves that the covector set of a conditional oriented matroid can also be determined by its set of topes, but by using the face symmetry condition.

The thesis continues with topoplane arrangements, introduced by Forge & Zaslavsky (2009). These are finite sets of topoplanes satisfying certain properties on intersections. From them the other main objects of study, namely transsective topoplane arrangements, can be derived. A conjecture of Forge & Zaslavsky (2009) on transsection, stating that the set of topological subspaces induced on a flat by a transsective topoplane arrangement is also a transsective topoplane arrangement, is proved. The property stating that the pair formed by a transsective topoplane arrangement and its face set corresponds to a conditional oriented matroid is afterwards established. Then, the open problem of Forge & Zaslavsky (2009) which asks if all transsective topoplane arrangements correspond to oriented matroids is answered for central transsective topoplane arrangements.

The main result of this thesis follows, namely a generalization of the topological representation theorem. It states that a sign set is the covector set of a simple conditional oriented matroid if and only if it is the sign set of a transsective topoplane arrangement. This allows to compute the Varchenko determinant for conditional oriented matroids. The referee of the article of Hochstättler & Welker (2019) suggested the computation of that determinant as a possible direction to generalize their works. This also permits to determine the dimension of the solution space of the Aguiar-Mahajan system for a conditional oriented matroid. A formula computing the unique solution is given for oriented matroids.

Finally, the implementation in SageMath of the functions on conditional oriented matroids in the thesis are provided. Primary ones allow to determine if a sign system is an oriented matroid or a lopsided system. More advanced ones give the simplification of a conditional oriented matroid or the conditional oriented matroid generated by its set of topes. And the last ones compute the Varchenko determinant of a conditional oriented matroid, and determine the solution of an Aguiar-Mahajan equation system of an oriented matroid.

Berichte von Konferenzen

ISSAC 2024

Raleigh, North Carolina, 16.07. – 19.07.2024

www.issac-conference.org/2024

Seit 2018 fand die ISSAC zum erstem Mal wieder auf dem amerikanischen Kontinent statt, in der mittelgroßen Stadt Raleigh, die die gigantische North Carolina State University beherbergt. Die Grunddaten sind schnell berichtet: Es gab 111 Teilnehmer und 49 akzeptierte Vorträge, die das Program Committee aus 84 Einreichungen ausgewählt hatte. Daneben gab es wie immer eingeladene Hauptvorträge, Tutorials, Poster und Software Demos. Letztere zwei Punkte führen direkt zu den durch die Fachgruppe gesponsorten Preisen für das beste Poster und für die beste Software-Präsentation, jeweils dotiert mit 250 Euro. Nach mittlerweile bestens etablierten Verfahren wurden die Preisträger von den jeweils zuständigen Komitees für Poster und Software ausgewählt, wofür wir uns herzlich bedanken. Das Ergebnis:

Poster-Preisträger: Daniel Profili, Hoon Hong und J. Rafael Sendra.
Titel: Conditions for eigenvalue configurations of two real symmetric matrices.

Software-Preisträger: Zoltán Kovács, Bernard Parisse, Tomas Recio, M. Pilar Velez and Jonathan H. Yu.
Titel: The ShowProof command in GeoGebra Discovery: Towards the automated ranking of elementary geometry theorems.

Herzlichen Glückwunsch!

Ein weiteres Mal war die ISSAC perfekt organisiert durch Martin Helmer als Local Arrangements Chair und Jonathan Hauenstein als General Chair.

Mehr zu berichten gibt es von dem Business Meeting. Wie immer wurde hier ein neues Mitglied des Steering Committee gewählt, wobei die Wahl aus drei Kandidatinnen und Kandidaten auf Wen-shin Lee (University of Stirling) fiel. Ein weiterer Standardpunkt war die Wahl des Austragungsortes für 2026. Hier gab es erfreulicherweise zwei Bewerbungen: eine vom Indian Institute of Technology in Chennai, und eine von der Universität Oldenburg. Letztere wurde von Florian Heß präsentiert. Die Wahl fiel auf Oldenburg. Auch hier: herzlichen Glückwunsch! Zuletzt war die ISSAC 2017 in Deutschland.

Der Elefant im Raum (um eine englische Redensweise zu übernehmen) auf dem Business Meeting war jedoch eine existenzielle Krise, in der sich unsere amerikanische Schwesterorganisation, die SIGSAM (= Special Interest Group in Symbolic and Algebraic Manipulation) befindet. Die ACM (= Association for Computing Machinery, amerikanisches Pendant zur GI, Muttergesellschaft der SIGSAM) verlangt seit einiger Zeit von ihren Special Interest Groups hohe jährliche Gebühren, die die SIGSAM als relative kleine Gruppe innerhalb weniger Jahre finanziell ruinieren würden. Ohne wesentliche neue Einkünfte würde die SIGSAM innerhalb weniger Jahre aufhören zu existieren. Was hat das mit der ISSAC zu tun? Dass unweigerlich die Blicke der SIGSAM auf die ISSAC als Geldquelle gefallen sind. So wurden mehrere Modelle vorgeschlagen, die den Fortbestand der SIGSAM ermöglichen könnten, wobei die ACM dann künftig bei jeder ISSAC Konferenz als Sponsor auftreten müsste, und zudem die Teilnahmegebühren erhöht würden, ganz grob gerechnet um mindestens 150$. Bisher war die ACM als Sponsor optional, so dass andere Träger, etwa gemeinnützige Universitäten in Europa, möglich waren. Es versteht sich, dass hierbei „Sponsoring“ ein Euphemismus für Gewinne abschöpfen ist. Unabhängig von der Situation der SIGSAM führt die ACM künftig ein Open Access Modell verpflichtend ein, so dass auf alle Veröffentlichungen bei der ISSAC Gebühren zwischen 700$ und 1500$ für Autoren oder deren Institutionen anfallen würden.

Dies ist der Hintergrund der recht kontroversen Diskussion, die beim Business Meeting auf die Abarbeitung der Standardpunkte folgte. Dabei wurden sehr verschiedene Argumente und Gesichtspunkte laut. Vor allem von Informatik-orientierten Teilnehmern wurde argumentiert, die ISSAC sei ohnehin viel zu billig, um ein hohes Prestige zu rechtfertigen, und die Veröffentlichung bei der ACM sei als Gütesiegel unverzichtbar. Andere Teilnehmer und Organisatoren berichteten von Erfahrungen, nach denen die ACM sowohl als Sponsor als auch als Verleger eher ein Hindernis als einen Mehrwert darstellten. Es wurde auch hinterfragt, wer eigentlich entscheidet. Müssten für ein verpflichtendes Sponsorship durch die ACM nicht die „Bylaws“ der ISSAC per Abstimmung (zwei Drittel Mehrheit unter den Teilnehmern der drei letzten Konferenzen) geändert werden? Wem „gehört“ die ISSAC eigentlich? Ab wann würde diese Regelung greifen? Eine gewisse Ironie mag es sein, dass der soeben ausgewählte Austragungsort Oldenburg kein Sponsoring durch die ACM beinhaltet.

Gregor Kemper (München)

International Congress on Mathematical Software (ICMS)

Durham, United Kingdom, 22.07. – 25.07.2024

https://maths.dur.ac.uk/icms2024

Nachdem pandemiebedingt die ICMS 2020 online stattfinden musste und die ICMS 2022 ausfiel, fand die ICMS 2024 vom 22. bis 25. Juli in Durham endlich wieder in Präsenz statt. Mit rund 140 Teilnehmern übertraf die ICMS 2024 die vorsichtigen Erwartungen. Aufgrund der Größe des Mathematikfachbereichs in Durham mit über 120 Fakultätsmitgliedern konnte die gesamte Konferenz dennoch in dem 2021 eröffneten Gebäude für Mathematik und Informatik abgehalten werden. Alle Teilnehmer übernachteten im nahgelegenen Collingwood College, benannt nach dem Mathematiker Sir Edward Foyle Collingwood.

Die ICMS 2024 umfasste 121 Teilnehmervorträge aufgeteilt in 12 Minisymposien und in bis zu vier parallelen Sessions. Es gab drei leicht verständliche Plenarvorträge, die sich mit verschiedenen mathematischen Systemen und Mathematikbereichen befassten:

(a) Matthias Köppe (UC Davis, USA): *The Reformation of Sage*

(b) Heather Macbeth (Fordham University, USA): *Algorithm and abstraction in formal mathematics*

(c) Mohab Safey El Din (Sorbonne University, France): *Polynomial system solving with the msolve library*

Hier sind ein paar entscheidende Einblicke in die Konferenz:

- Die Räume, in denen die parallelen Sessions stattfanden, waren nicht gleich groß und wurden den Sessions nach ihrer Anzahl an Sprechern zugeteilt. So kam es vor, dass einige Sessions mit wenigen Sprechern, aber großem Interesse die offizielle Kapazität ihres Raumes sprengten. Dank kooperativen und flexiblen Teilnehmern – und vielen Stühlen auf Rollen – war dies allerdings kein großes Problem.
- Wie in England zu erwarten war, war das bereitgestellte Essen polarisierend. Die meisten Teilnehmer hatten keine Probleme mit Sandwiches, Quiches, Samosas und Bhajis, die zum Mittagessen serviert wurden. Allerdings hatten einige Teilnehmer damit zu kämpfen, dass es keine warme Mahlzeit gab.
- Der nordostenglische Akzent ist für Nicht-Muttersprachler genauso schwer verständlich wie für Muttersprachler. Dies führte beim Einchecken an der College-Rezeption zu einigen amüsanten Szenen.
- Das Cateringteam hatte trotz wiederholter Warnungen deutlich unterschätzt, wie viel Kaffee der durchschnittliche Mathematiker am Tag konsumiert. Dieser Fehler wurde ab dem zweiten Tag behoben. Viele Teilnehmer fanden die Angewohnheit, Tee mit Milch zu trinken, ebenso befremdlich.
- James Davenport hielt – auf Bitten der Konferenzorganisatoren – während des Konferenzdinners ohne Vorwarnung und aus dem Stegreif eine meisterhafte Rede über die Mathematik und das Leben von Sir Edward Foyle Collingwood, der sein akademischer Onkel war.

Ich danke allen Organisatoren die an der Konferenz mitgewirkt haben: Oliver Daisey, Jeff Giansiracusa, Iolo Jones, David Lanners , Julio Quijas Aceves, Victoria Schleis, Arman Marti-Shahandeh, Yuvraj Singh, Daniele Turchetti.

Yue Ren (Durham)

Hinweise auf Konferenzen

GAMM - 95th Annual Meeting

Posen, Polen, 07.04. – 11.04.2025

jahrestagung.gamm-ev.de

The GAMM Annual Meeting 2025 will be hosted by Poznan University of Technology.

It will take place from April 7th to 11th, 2025, in Poznan, a city where the energies and inventiveness of Eastern and Western European people intertwine.

Submission of Abstracts will be open by 1st of October 2024.

SYMCOMP 2025

Lissabon, Portugal, 10.04. – 11.04.2025

symcomp2025.isel.pt

The ECCOMAS Thematic Conference on Numerical and Symbolic Computation: Developments and Applications, SYMCOMP2025 is the seventh conference in a series that started in 2013, and it aims bringing together academic and scientific communities that are involved with Numerical and Symbolic Computation in the most various scientific areas.

Exchanging experiences and knowledge about current and emerging research and development areas, is a major goal. The multidisciplinary character of this Conference promotes a privileged forum to establish and cross-fertilize new multidisciplinary and cross-sector collaborations.

CoCoA School 2025

Genua, Italien, 14.07. – 18.07.2025

sites.google.com/view/cocoaschool2025

Vom 14.7. bis 18.7.2025 findet an der Universität Genua (Italien) die nächste Ausgabe der internationalen Doktorandenschule *CoCoA School* statt. Wie immer gibt es zwei Kurse, nämlich *Multivariate Cryptography and Polynomial Systems*, gehalten von Alessio Caminata (Genua), und *Liaison Theory*, gehalten von Elisa Gorla (Neuchatel). Die zugehörigen Tutorien, bei denen das Computeralgebrasystem CoCoA zum Einsatz kommt, werden von Giulia Gaggero und Lisa Seccia (beide Neuchatel) durchgeführt.

Im Anschluss an die Schule folgt am 18.7. eine Minikonferenz zu Ehren des 80ten Geburtstags von Lorenzo Robbiano (Genua). Weitere Details, insbesondere die Anmeldemodalitäten, folgen demnächst auf der angegebenen Webseite der CoCoA School 2025.

ACA 2025

Heraklion (Kreta), Griechenland, 14.07. – 18.07.2025

aca2025.symbolic-computation.info

The Applications of Computer Algebra is scheduled on 14-18 July, 2025 and will be held at Heraklion (Crete), Greece.

The ACA conference series is devoted to promoting all kinds of computer algebra applications, and encouraging the interaction of developers of computer algebra systems and packages with researchers and users (including scientists, engineers, educators, and mathematicians).

ISSAC 2025

Guanajuato, Mexiko, 28.07. – 01.08.2025

www.issac-conference.org/2025

The International Symposium on Symbolic and Algebraic Computation (ISSAC) is the premier conference for research in symbolic computation and computer algebra. ISSAC 2025 will be the 50th meeting in the series, which started in 1966 and has been held annually since 1981. The conference presents a range of invited speakers, tutorials, short communications, software demonstrations and vendor exhibits with a center-piece of contributed research papers.

ISSAC 2025 will be held from July 28th to August 1st, 2025, at the Center for Research in Mathematics (CIMAT) in Guanajuato, Mexico.

ÖMG-DMV 2025

Linz, Österreich, 01.09. – 05.09.2025

www.jku.at/en/faculty-of-engineering-natural-sciences/organization/subject-areas/mathematics/oemg-dmv-2025

Organized by the Department of Mathematics at the Johannes Kepler University Linz (JKU), the annual joint meeting of the Österreichische Mathematische Gesellschaft (ÖMG), opens an external URL in a new window and the Deutsche Mathematiker-Vereinigung (DMV), opens an external URL in a new window will take place in Linz in 2025. The conference will consist of sections, mini-symposia, and several satellite events.

There will be a section on computer algebra organized by Christoph Koutschan (Linz) and Daniel Robertz (Aachen).

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`

Fachgruppe Computeralgebra

Fachgruppenleitung Computeralgebra 2023–2026

Sprecherin:
Prof. Dr. Anne Frühbis-Krüger
Carl-von Ossietzky Universität Oldenburg
Carl-von-Ossietzky-Straße 11, 26129 Oldenburg
0441 798-3233
anne.fruehbis-krueger@uni-oldenburg.de
https://uol.de/anne-fruehbis-krueger

Vertreterin der GI:
Prof. Dr. Erika Ábrahám
RWTH Aachen
Ahornstr. 55, 52056 Aachen
0241 80-21242, -22243 (Fax)
abraham@cs.rwth-aachen.de
https://ths.rwth-aachen.de/people/erika-abraham/

Fachreferent CA-Systeme und -Bibliotheken:
Prof. Dr. Claus Fieker
RPTU Kaiserslautern-Landau
Gottlieb-Daimler-Straße, 67663 Kaiserslautern
0631 205-2392, -4427 (Fax)
fieker@mathematik.uni-kl.de
https://www.mathematik.uni-kl.de/~fieker

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
https://uol.de/florian-hess

Fachexperte SFB-TRR 195:
Prof. Dr. Max Horn
RPTU Kaiserslautern-Landau
Gottlieb-Daimler-Straße, 67663 Kaiserslautern
0631 205-2730, -4427 (Fax)
mhorn@rptu.de
https://www.quendi.de/de/mathe

Fachreferent Publikationen:
Prof. Dr. Martin Kreuzer
Universität Passau
Innstr. 33, 94030 Passau
0851 509-3120, -3122 (Fax)
martin.kreuzer@uni-passau.de
https://staff.fim.uni-passau.de/kreuzer/

Vertreterin der GAMM:
Prof. Dr. Eva Zerz
RWTH Aachen
Pontdriesch 14/16, 52062 Aachen
0241 80-94544, -92108 (Fax)
eva.zerz@math.rwth-aachen.de
https://www.math.rwth-aachen.de/~Eva.Zerz/

Stellvertretender Sprecher:
Prof. Dr. Michael Cuntz
Leibniz Universität Hannover
Welfengarten 1, 30167 Hannover
0511 762-4252
cuntz@math.uni-hannover.de
https://www.iazd.uni-hannover.de/de/cuntz

Fachreferentin Industrie:
Xenia Bogomolec
Quant-X Security & Coding
Engelbosteler Damm 15, 30167 Hannover
0173 3031816
xb@quant-x-sec.com
https://quant-x-sec.com

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

Fachreferent CA-Systeme und -Bibliotheken:
Jun.-Prof. Dr. Tommy Hofmann
Universität Siegen
Walter-Flex-Straße 3, 57072 Siegen
0271-740-2868
tommy.hofmann@uni-siegen.de
https://www.thofma.com/

Fachreferent Themen und Anwendungen:
Prof. Dr. Gregor Kemper
Technische Universität München
Boltzmannstr. 3, 85748 Garching
089 289-17454, -17457 (Fax)
kemper@ma.tum.de
https://www.math.cit.tum.de/algebra/kemper

Fachreferent Redaktion Rundbrief:
Dr. Fabian Reimers
Technische Universität München
Boltzmannstr. 3, 85748 Garching
089 289-17474
reimers@ma.tum.de
https://www.math.cit.tum.de/algebra/reimers

www.fachgruppe-computeralgebra.de

GI DMV GAMM