März 2022

Computeralgebra Rundbrief

> Ausgabe 70

- Tagung der Fachgruppe 2022
- Verification of the strong Birch–Swinnerton-Dyer conjecture in dimension 2
- The mathematical research-data repository MathRepo
- Duale Zahlen und automatische Differentiation

www.fachgruppe-computeralgebra.de

Computeralgebra-Rundbrief

Nr. 70 März 2022

Fachgruppe Computeralgebra

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,

auch in diesen Mitteilungen kommen wir an dem Thema Corona einfach nicht vorbei. Pandemiebedingt hatten wir die Tagung der Fachgruppe ja um ein Jahr verschoben mit dem Ziel, dass sie nun in Präsenz stattfinden könnte. Das war schön gedacht und hätte auch gut funktionieren können, wenn nicht Omikron dazwischen gekommen wäre. Als klar wurde, dass die Tagung gerade in die Zeit der fünfeinhalbten Welle fallen würde, waren die Planungen schon zu weit fortgeschritten, um eine erneute Verschiebung sinnvoll erscheinen zu lassen. So fand die Tagung also, wie so viele andere in letzter Zeit, virtuell statt. Ein Erfolg war die Tagung dennoch: Sie war gut besucht, sehr abwechslungsreich und interessant (siehe Bericht auf Seite 6). Leid tat uns eben nur, dass das informelle Beisammenstehen, Reden und 'Netzwerken', wie man heute neudeutsch sagt, durch das Format wieder zu kurz kamen. Gerade deshalb, und als Ausgleich der Verschiebung wagen wir schon im kommenden Jahr den nächsten Anlauf: in der Pfingstwoche 2023 in Hannover – eine ausführliche Ankündigung dazu kommt im nächsten Heft.

In den letzten 2 Jahren hatten wir unser Programm zur Workshopförderung in Computeralgebra ausgesetzt, da es pandemiebedingt so gut wie keine Präsenzworkshops gab, bei denen wir durch einen Zuschuss zu den Kosten hätten helfen können, das Programm interessanter und runder zu machen. Der Hauptkostenfaktor von Workshops sind eben bekanntermaßen die Reisekosten. Nachdem nun allerdings die Entwicklung und vor allem die Saisonalität der Pandemie wieder auf Präsenzevents hoffen lässt, nehmen wir das Programm wieder auf und freuen uns auf Anträge zu interessanten Workshops. Details zur Workshopförderung finden Sie auf Seite 7.

Die laufende Wahlperiode neigt sich inzwischen schon wieder ihrem Ende zu: zum Jahresende stehen die nächsten Wahlen zur Fachgruppenleitung an. Nach dem erfolgreichen Versuch der Nutzung eines Online-Tools zur Wahl vor etwas über zwei Jahren wird die Wahl diesmal rein online stattfinden. Zeitgleich mit dem Rundbrief haben wir eine E-Mail mit allgemeinen Informationen zur kommenden Online-Wahl und zur Kandidatur versandt, so dass Sie am Erhalt dieser E-Mail überprüfen können, ob Sie von uns per E-Mail erreicht werden – wenn nicht, hilft `mitgliederservice@gi.de` *bei der Aktualisierung der E-Mail-Adresse. Wenn Sie sich vorstellen könnten, Verantwortung in der Fachgruppe zu übernehmen und für die Fachgruppenleitung zu kandidieren, dann scheuen Sie sich nicht, sich bei uns zu melden.*

Nun aber genug der Nachrichten in eigener Sache. Inhaltlich hat dieser Rundbrief wieder einiges zu bieten: Die Verifikation der Birch–Swinnerton-Dyer Vermutung in Dimension 2 steht im Mittelpunkt des forschungsbezogenen ersten Artikels ab Seite 8, während der eher infrastrukturell ausgelegte zweite Artikel MathRepo, ein Werkzeug der mathematischen Forschungsdatenverwaltung, ab Seite 16 vorstellt. Ein Artikel über automatische Differentiation in der Rubrik „Computeralgebra in der Schule“ und die informativen kleinen Rubriken zu Arbeitsgruppen, Publikationen und Konferenzen runden diese Ausgabe ab.

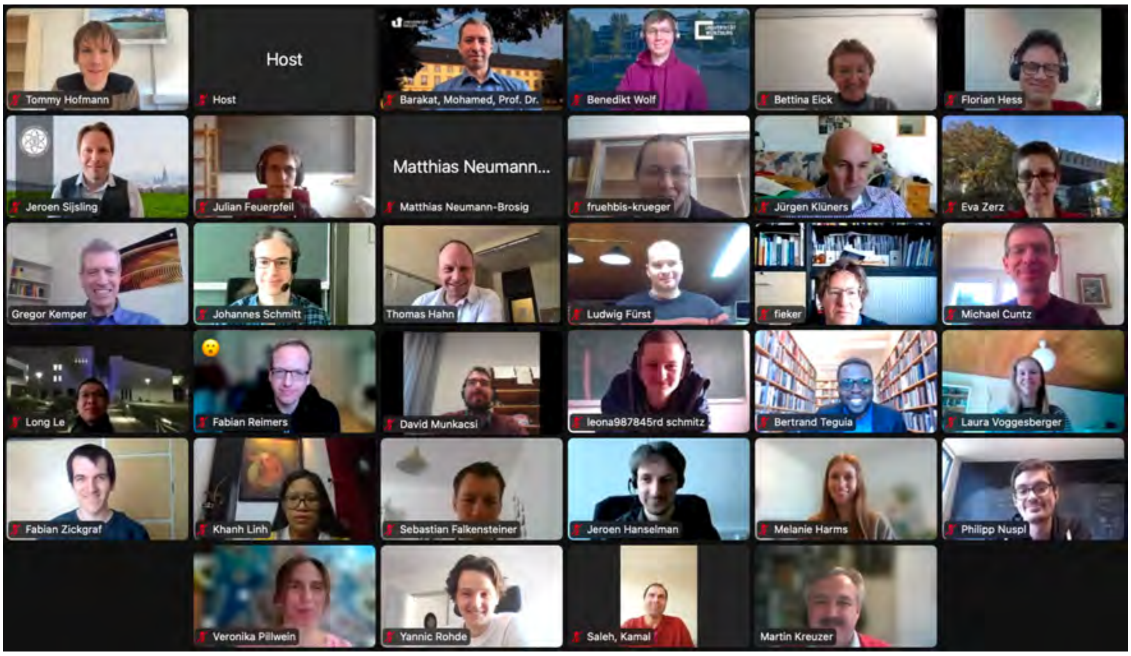
Wir wünschen Ihnen eine angenehme und anregende Lektüre.

Anne Frühbis-Krüger *Gregor Kemper*

Tagungen der Fachgruppe

Tagung der Fachgruppe Computeralgebra, München/Virtuell, 9.3. – 11.3.2022

https://fachgruppe-computeralgebra.de/muenchen-2022/



Tagung der Fachgruppe 2022 virtuell

Von 9. bis 11. März 2022 fand die neunte Computeralgebra-Tagung der Fachgruppe statt. Ursprünglich für 2021 geplant, war sie wegen der COVID-19-Pandemie nach 2022 verlegt worden. Leider hat Corona dann doch erneut zugeschlagen und statt einer Präsenzveranstaltung musste kurzfristig auf ein virtuelles Format gewechselt werden. Dank der hervorragenden Organisation durch Gregor Kemper und Thomas Hahn hat letztlich aber alles reibungslos funktioniert.

Das Ziel dieser Tagungsreihe ist es, einerseits Nachwuchswissenschaftlern zu ermöglichen ihre Ergebnisse vorzustellen, andererseits aber auch Hauptvortragende zu gewinnen, die Übersichtsvorträge über wichtige Gebiete der Computeralgebra und über Computeralgebra-Software geben. Für dieses Jahr konnten wir folgende Wissenschaftler als Hauptvortragende gewinnen:

- **Melanie Harms** (RWTH Aachen) *Invariant Varieties and Collision-Freeness for Polynomial Systems*
- **Tommy Hofmann** (Universität Siegen) *Lattice isomorphism and the integral matrix similarity problem*
- **Lukas Kühne** (MPI Leipzig) *Investigating Terao's freeness conjecture with computer algebra*
- **Veronika Pillwein** (RISC Linz) *Inequalities and computer algebra*
- **Timo de Wolff** (TU Braunschweig) *The SONC Cone: Primal and Dual Perspectives*

Die Tagung wurde am Mittwoch mit dem Hauptvortrag von Melanie Harms eröffnet, der Nachwuchs-Preisträgerin der Computeralgebra-Tagung 2019. Am Donnerstag und Freitag gab es je zwei weitere Hauptvorträge. Dazwischen wurden insgesamt 16 halbstündige Vorträge in zwei parallelen Sektionen gehalten. Das Programm wurde durch einen Beitrag von Thomas Richard über neue Features in Maple 2022 ergänzt sowie durch einen Bericht von Anne Frühbis-Krüger über Neuigkeiten aus der Fachgruppe.

Aufgrund des Onlineformats gab es in diesem Jahr leider keinen gemeinsamen Ausflug. Generell hatten wir uns eigentlich sehr auf den persönlichen Austausch mit anderen Teilnehmern in Präsenz gefreut. Im virtuellen Format gab es aber immerhin zwischen den Vorträgen die Möglichkeit zum Gespräch, welche auch immer wieder genutzt wurde, etwa zu interessanten Nachdiskussionen im Anschluss an einzelne Vorträge.

Am Donnerstagabend diskutierten die Mitglieder der Fachgruppenleitung schließlich die Nachwuchsbeiträge in Hinblick auf die für den letzten Tag vorgesehene Preisvergabe. Erfreulicherweise hat es wieder viele sehr gute Vorträge gegeben, sowohl was das fachliche Niveau anging, als auch die Verständlichkeit der Darstellung, die ja idealerweise auch einen Zugang für Nichtexperten ermöglichen sollten. Entsprechend schwer viel uns die Auswahl.

Schließlich konnte sich Timo Keller (Bayreuth) mit seinem Vortrag über „Exact verification of the strong Birch–Swinnerton-Dyer conjecture for some absolutely simple modular abelian surfaces“ durchsetzen. Er erhielt den mit 500 Euro dotierten Preis, der mit der Einladung verbunden ist, bei der nächsten Computeralgebra-Tagung einen Hauptvortrag zu halten.

Über viele Jahre wurde die Jahrestagung stets von Wolfram Koepf organisiert, der allerdings 2019 in den Ruhestand getreten ist. Unter seiner Leitung wurde ein hohes Niveau etabliert, an das es erst mal anzuknüpfen galt. Erfreulicherweise ist das voll und ganz gelungen, trotz der erschwerten Bedingungen bedingt durch die COVID-19-Pandemie. An dieser Stelle daher noch mal unser Dank an die Organisatoren, Gregor Kemper und Thomas Hahn, an alle Vortragenden sowie alle weiteren Unterstützer und Helfer.

Max Horn (Kaiserslautern)

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

Exact verification of the strong Birch–Swinnerton-Dyer conjecture for some absolutely simple modular abelian surfaces

Timo Keller, Michael Stoll
(Lehrstuhl Computeralgebra, Universität Bayreuth)

Timo.Keller@uni-bayreuth.de
Michael.Stoll@uni-bayreuth.de

Informal introduction

This article is on the *conjecture of Birch and Swinnerton-Dyer* (*BSD* for short) for abelian surfaces, originally formulated by Birch and Swinnerton-Dyer [1] in the 1960s for elliptic curves over $\mathbb{Q}$. Abelian surfaces are two-dimensional abelian varieties, and abelian varieties are higher-dimensional analogues of elliptic curves. An elliptic curve is an algebraic curve that carries a group structure. This means that we can add two points on the curve to get another point on the curve, and this addition has similar properties as the standard addition. Elliptic curves and abelian varieties are important in various contexts within mathematics, for example in the proof of Fermat's Last Theorem or in cryptography.

Using the numbers of points modulo each prime number on an abelian variety A that is defined over the rational numbers, one can construct a certain function, the L-function of A. The BSD conjecture for A proposes a surprising connection between the analytic behavior of the L-function of A and certain "global" invariants of A. These invariants include properties of the group of rational points on A on the one hand and the number of elements of the mysterious Shafarevich-Tate group $\text{Ш}(A)$ of A on the other hand. Since all other quantities that occur in the conjecture can be computed for given A, the conjecture can be expressed as "$\text{Ш}(A)$ is finite and has the expected number of elements".

Birch and Swinnerton-Dyer originally formulated their conjecture for elliptic curves. To prove this version is one of the seven "Millennium Problems" of the Clay Foundation.

For general elliptic curves and even more so for higher-dimensional abelian varieties, the conjecture is wide open. It is not even known that $\text{Ш}(A)$ is always finite. For so-called "modular" abelian varieties with additional properties, some parts of the conjecture are known, however, in particular the finiteness of $\text{Ш}(A)$. Every elliptic curve defined over the rational numbers is modular, and so it was possible to verify the BSD conjecture for many individual elliptic curves.

In this article, we report on our project with the goal to obtain the complete verification of the BSD conjecture also for many modular abelian surfaces. Except in cases that can be reduced to elliptic curves, this had not been done so far even for a single abelian surface. For the verification of the conjecture, we determined the size of $\text{Ш}(A)$. To this end, we used new ideas to generalize and improve the methods that have been successful for elliptic curves.

This work was supported by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) – Projektnummer STO 299/18-1, AOBJ: 667349.

State of the art

We now give more detailed and also more technical description of the objects involved. The BSD conjecture consists of two parts, which we will explain for the case of an abelian variety A of dimension g over $\mathbb{Q}$.

One attaches to A its L-function $L(A, s)$, which is defined by an Euler product over all prime numbers p. If A is the Jacobian variety of a curve X of genus g, the Euler factor at p for a prime p of good reduction is determined by the number of $\mathbb{F}_{p^n}$-points on the mod p reduction of X for $n \leq g$. It follows from the Weil conjectures for varieties over finite fields that the Euler product converges for $\operatorname{Re}(s) > \frac{3}{2}$ to a holomorphic function. A standard conjecture predicts that $L(A, s)$ extends to an entire function; this is known when A is *modular*, i.e., occurs as an isogeny factor of the Jacobian $J_0(N)$ of one of the modular curves $X_0(N)$. By the Modularity Theorem of Wiles and others [28, 22, 3], this is always the case when A is an elliptic curve over $\mathbb{Q}$ (this is now a special case of Serre's Modularity Conjecture [11]).

We now introduce the relevant global invariants of A. By the Mordell-Weil Theorem, the abelian group $A(\mathbb{Q})$ of rational points on A is finitely generated, so it splits as

$$A(\mathbb{Q}) \cong A(\mathbb{Q})_{\text{tors}} \oplus \mathbb{Z}^r,$$

where $A(\mathbb{Q})_{\text{tors}}$ is the finite *torsion subgroup* and r is a nonnegative integer, the *rank of* $A(\mathbb{Q})$. There is a natural positive definite quadratic form $\hat{h}$ on $A(\mathbb{Q}) \otimes_{\mathbb{Z}} \mathbb{R} \cong \mathbb{R}^r$, the *canonical height*, turning $A(\mathbb{Q})/A(\mathbb{Q})_{\text{tors}}$ into a lattice in a euclidean vector space. The squared covolume of this lattice (equivalently, the determinant of the Gram matrix of $\hat{h}$ with respect to a lattice basis) is the *regulator* Reg_A. The final global arithmetic invariant of A that

we need is the *Shafarevich-Tate group* $\text{Ш}(A)$. It can be defined as the localization kernel

$$\text{Ш}(A) = \ker\Big(\mathrm{H}^1(\mathbb{Q}, A) \to \bigoplus_v \mathrm{H}^1(\mathbb{Q}_v, A)\Big)$$

in Galois cohomology; here $\mathbb{Q}_v$ denotes the completion of $\mathbb{Q}$ with respect to a place v and the direct sum is over all places of $\mathbb{Q}$. Geometrically, $\text{Ш}(A)$ is the group of equivalence classes of everywhere locally trivial $A/\mathbb{Q}$-torsors. This group is conjectured to be finite, but this is completely open in general.

We also need some local invariants. To each prime p, one associates the *Tamagawa number* $c_p(A)$; this is the number of connected components of the special fiber at p of the Néron model $\mathcal{A}/\mathbb{Z}$ of A and equals 1 for all primes of good reduction. Let $(\omega_1, \ldots, \omega_g)$ be the pull-back to $\mathrm{H}^0(A, \Omega^1)$ of a basis of the free $\mathbb{Z}$-module $\mathrm{H}^0(\mathcal{A}, \Omega^1)$ of rank g. Then the *real period* of A is the volume of $A(\mathbb{R})$ measured using $|\omega_1 \wedge \cdots \wedge \omega_g|$:
$\Omega_A = \int_{A(\mathbb{R})} |\omega_1 \wedge \cdots \wedge \omega_g|$.

The *weak BSD* or *BSD rank conjecture* says that $L(A, s)$ has an analytic continuation to a neighborhood of $s = 1$ and

$$r_{\text{an}} := \operatorname{ord}_{s=1} L(A, s) = r\,.$$

The order of vanishing of $L(A, s)$ at $s = 1$ is also called the *analytic rank* of A.

The *strong BSD conjecture* says that in addition $\text{Ш}(A)$ is finite and

$$\begin{aligned} L^*(A, 1) &:= \lim_{s\to 1}(s-1)^{-r} L(A, s) \\ &= \frac{\Omega_A \prod_p c_p(A) \cdot \operatorname{Reg}_A \#\text{Ш}(A)}{\#A(\mathbb{Q})_{\text{tors}} \#A^\vee(\mathbb{Q})_{\text{tors}}}\,. \end{aligned}$$

Here $A^\vee$ is the dual abelian variety; it is isomorphic to A when A is a Jacobian, or, more generally, when A is principally polarized.

Since all the other invariants of A can (usually) be computed at least numerically, we define the *analytic order of Sha* to be

$$\#\text{Ш}(A)_{\text{an}} := \frac{L^*(A, 1)}{\Omega_A \operatorname{Reg}_A} \cdot \frac{\#A(\mathbb{Q})_{\text{tors}} \#A^\vee(\mathbb{Q})_{\text{tors}}}{\prod_p c_p(A)}\,.$$

Assuming the BSD rank conjecture, strong BSD can then be phrased as "$\text{Ш}(A)$ is finite and $\#\text{Ш}(A) = \#\text{Ш}(A)_{\text{an}}$."

Even the weak BSD conjecture for elliptic curves over $\mathbb{Q}$ is wide open in general (this is the Clay Millennium Problem mentioned above). However, the strong BSD conjecture has been verified for many "small" elliptic curves; see below. In our project we verified the strong BSD conjecture for the first time for a number of abelian surfaces A, in a situation where it cannot be reduced to BSD for some elliptic curves. Concretely, this means that A is absolutely simple.

Previously known results

Beside Serre's Modularity Conjecture, the two big theorems we use are the Gross–Zagier formula [9] and the Euler system of Heegner points of Kolyvagin–Logachev [12].

Assume that $A/\mathbb{Q}$ has real multiplication by an order $\mathcal{O}$ of a totally real number field of degree $g := \dim A$ over $\mathbb{Q}$, i.e. $\operatorname{End}_{\mathbb{Q}}(A) = \mathcal{O}$. By Serre's Modularity Conjecture and a result of Ribet [18], this is equivalent to the statement that A is an isogeny quotient of the Jacobian $J_0(N)$ of the modular curve $X_0(N)$ for some N (which we can take such that N^g equals the conductor of A), or that there is a newform $f \in S_2(\Gamma_0(N), \mathcal{O})$ with

$$L(A/\mathbb{Q}, s) = \prod_{\sigma:\mathcal{O}\hookrightarrow\mathbb{R}} L(f^\sigma, s);$$

in particular $L(A/\mathbb{Q}, s)$ is holomorphic on $\mathbb{C}$. In the following, let A, g, $\mathcal{O}$, f and N be as in this paragraph.

The *Gross–Zagier formula* relates the first derivative $L'(f/K, 1)$ of the L-function of f base changed to a certain imaginary quadratic field K, called Heegner field and defined below, to the height of a Heegner point $y_K \in J(K)$. This is a step towards the rank conjecture because it says that $r_{\text{an}}(f/K) = 1$ implies $r(A/K) \geq \dim A$.

The *Euler system of Kolyvagin–Logachev* proves that a GL_2-type abelian variety A over $\mathbb{Q}$ with $r_{\text{an}}(A/K) = \dim A$ even satisfies $r(A/K) = \dim A$, $r(A/\mathbb{Q}) = r_{\text{an}}(A/\mathbb{Q})$ and that $\text{Ш}(A/\mathbb{Q})$ is finite. However, as it depends crucially on explicit open image theorems only available for elliptic curves in general, in contrast to the case of $\dim A = 1$, it does not give an explicit finite support of $\text{Ш}(A/\mathbb{Q})$. These theorems are not available for $\dim A > 1$ because the moduli space of g-dimensional principally polarized abelian varieties has dimension $\frac{g(g+1)}{2} > 1$ for $g > 1$. In our work, we therefore prove such open image theorems algorithmically only for a given modular abelian surface, and using this, we work out an explicit version of Kolyvagin–Logachev.

Regarding rank > 1, there is no single elliptic curve of analytic rank > 1 known for which we know that its Shafarevich-Tate group is finite.

Exact verification for elliptic curves

In the case of elliptic curves, the various ingredients mentioned above have been worked out, made explicit and been improved to an extent that it was possible to verify the strong BSD conjecture for all elliptic curves E over $\mathbb{Q}$ of rank ≤ 1 and conductor $N < 5000$; see [8, 14, 15, 4, 13].

Exact verification for modular abelian surfaces

We now specialize to the case $g = 2$, i.e., modular abelian surfaces $A/\mathbb{Q}$. We assume that $A = J$ is a Jacobian, in particular principally polarized, and absolutely

simple. The latter is to exclude cases where one can reduce strong BSD to elliptic curves over number fields (potentially larger than $\mathbb{Q}$).

Strong BSD has been verified *numerically* and *up to squares* for some Jacobians by van Bommel [25].

Our overall strategy is:

1. Classify the *image of the residual Galois representations* $\rho_\mathfrak{p} := \rho_{f,\mathfrak{p}}$ for almost all $\mathfrak{p}$: Show explicitly that almost all of them are irreducible and have maximal image $\mathrm{GL}_2(\mathbb{F}_\mathfrak{p})^{\det \in \mathbb{F}_p}$.

2. For at least one Heegner field K, compute the Heegner point $y_K \in J(K)$ (or rather $2y_K \in J^K(\mathbb{Q})$ or $J(\mathbb{Q})$ if the L-rank is 0 or 1, respectively). This gives the *Heegner index* $I_K = \mathrm{Ann}_\mathcal{O}(J(K)/\mathcal{O}y_K)$ as an $\mathcal{O}$-ideal.

3. Compute a *finite support* of $\text{Ш}(A/\mathbb{Q})$ with our explicit version of the Heegner point Euler system from the previous two steps.

4. For the finitely many remaining primes do one of the following:

   (a) If $\mathrm{SL}_2(\mathbb{F}_p) \subseteq \operatorname{im}\rho_\mathfrak{p}$ and p is a prime of good or multiplicative bad reduction, we can use the GL_2 Iwasawa Main Conjecture [21, 20] to get the p-valuation of the order of the $\mathfrak{p}$-Selmer group by *computing the p-adic L-function* using overconvergent modular symbols.

   (b) Perform a $\mathfrak{p}$-*descent*; if $\rho_\mathfrak{p}$ is reducible, determine the characters constituting the semisimplification $\rho_\mathfrak{p}^{\mathrm{ss}}$ and perform an isogeny descent.

5. Compute the *analytic order of* Ш using modular symbols if $L(f,1) \neq 0$ or from $\#\text{Ш}(A^K/\mathbb{Q})_{\text{an}}$ and $\#\text{Ш}(A/K)_{\text{an}}$ if the L-rank is 1. To compute $\#\text{Ш}(A/K)_{\text{an}}$ exactly, we use the Gross–Zagier formula.

Our algorithms for 1 and 4 run very quickly. The most time-consuming part of 2 is the computation of the Mordell-Weil group. The last step 5 is very fast in the analytic rank 0 case and a bit slower for rank g. In general, the runtime is determined by the level N and the discriminant of the chosen Heegner field(s).

We now describe these substeps in more detail:

Classifying the images of the residual Galois representations

To prove $\text{Ш}(J/\mathbb{Q})[\mathfrak{p}] = 0$ for a prime ideal $\mathfrak{p}$ of $\mathcal{O}$ using the Euler system (see below), one assumption we need to know is that the residual Galois representation

$$\rho_\mathfrak{p} : \mathrm{Gal}(\overline{\mathbb{Q}}|\mathbb{Q}) \to \mathrm{Aut}_{\mathcal{O}/\mathfrak{p}}(J[\mathfrak{p}](\overline{\mathbb{Q}}))$$

is irreducible or even has *maximal image* $\mathrm{GL}_2(\mathbb{F}_\mathfrak{p})^{\det \in \mathbb{F}_p}$. The restriction $\det \in \mathbb{F}_p$ comes from the fact that the determinant of $\rho_\mathfrak{p}$ is the mod-p cyclotomic character

$$\chi_p : \mathrm{Gal}(\overline{\mathbb{Q}}|\mathbb{Q}) \to \mathbb{F}_p^\times$$

satisfying $\sigma(\zeta_p) = \zeta_p^{\chi_p(\sigma)}$ for a primitive p-th root of unity ζ_p. Another reason why we have to have information on $\rho_\mathfrak{p}$ is that we need to know the characters constituting its semisimplification if it is reducible when performing isogeny descents (see below).

We first determine a small finite set S of primes such that $\rho_\mathfrak{p}$ is irreducible for $\mathfrak{p} \notin S$: Assuming $\rho_\mathfrak{p}$ reducible, say

$$\rho_\mathfrak{p}^{\mathrm{ss}} \cong \varepsilon\chi_p \oplus \varepsilon^{-1}$$

with a character

$$\varepsilon : \mathrm{Gal}(\overline{\mathbb{Q}}|\mathbb{Q}) \to \mathbb{F}_\mathfrak{p}^\times,$$

we prove that the conductor d of ε satisfies $d^2 \mid N$ if $v_p(N) \leq 1$, with a more complicated condition if $p^2 \mid N$. This implies that $\varepsilon(\mathrm{Frob}_\ell)^{\mathrm{ord}_\mathfrak{p} \ell} = 1$ for $\ell \nmid pN$ with $\mathrm{ord}_\mathfrak{p} \ell$ the order of ℓ in $\mathbb{F}_\mathfrak{p}^\times$. Therefore p divides the gcd of the resultants

$$\mathrm{res}_{\mathbb{Z}[T]}\left(\det(T - \mathrm{Frob}_\ell \mid T_\mathfrak{p} J), T^{\mathrm{ord}_\mathfrak{p} \ell} - 1\right),$$

which is a non-zero integer which can be computed explicitly and very efficiently.

We can also exclude for all but finitely many p the possibility that the projectivized image is contained in $\mathbb{P}\mathrm{SL}_2(\mathbb{F}_p)$ if $\deg(\mathfrak{p}) = 2$.

Since $\rho_\mathfrak{p}$ always contains an element of order > 5 in its image if $p \geq 7$ (coming from the inertia subgroup at p), its projectivized image in $\mathrm{PSL}_2(\mathbb{F}_\mathfrak{p})$ is not exceptional, i.e., not contained in a subgroup isomorphic to A_4, S_4, or A_5.

By the classification of maximal subgroups of PSL_2 over a finite field, if $\rho_\mathfrak{p}$ for $p \geq 7$ is irreducible, not maximal and its projectivized image is not contained in $\mathbb{P}\mathrm{SL}_2(\mathbb{F}_p)$ if $\deg(\mathfrak{p}) = 2$, i.e., strictly contained in $\mathrm{GL}_2(\mathbb{F}_\mathfrak{p})^{\det \in \mathbb{F}_p}$, it is contained in the normalizer $N(C)$ of a Cartan subgroup C. One can show that the quadratic character given by modding out C from the image is unramified outside the level N. Using the Sturm bound and assuming that the newform f is non-CM, i.e., there is no imaginary quadratic field K with $a_p(f) = 0$ for all p inert in K, one can bound the p for which the image is contained in the normalizer of a Cartan. Hence we have established an explicit and small

finite set of primes outside of which $\rho_\mathfrak{p}$ is irreducible or even maximal.

To treat the finitely many remaining primes $\mathfrak{p}$, we compute $\Delta_\mathfrak{p}(\ell) = a_\ell(f)^2 - 4\ell \in \mathbb{F}_\mathfrak{p}$, the discriminant of the Euler factor at $\mathfrak{p}$ modulo $\mathfrak{p}$. If $\Delta_\mathfrak{p}(\ell) \neq 0$, $\rho_\mathfrak{p}(\mathrm{Frob}_\ell)$ has pairwise distinct eigenvalues, hence is contained in a unique Cartan subgroup. The latter is split iff $\Delta_\mathfrak{p}(\ell)$ is a square in $\mathbb{F}_\mathfrak{p}^\times$. If we can find an ℓ for a given $\mathfrak{p}$ such that $\rho_\mathfrak{p}(\mathrm{Frob}_\ell)$ is contained in a non-split Cartan subgroup, the image is reducible.

In practice and in all cases we considered, this procedure gives the set of reducible primes. To verify that $\rho_\mathfrak{p}$ is reducible, we compute $J[\mathfrak{p}](\overline{\mathbb{Q}})$ as a Galois module, see below.

Computing the Heegner point and Heegner index

Let K be an imaginary quadratic number fields in which all primes dividing the level N are split (in particular, unramified). This is called the *Heegner hypothesis*. It follows that there exists an ideal $\mathfrak{n}$ of the ring of integers $\mathcal{O}_K$ (this is *not* the endomorphism ring $\mathcal{O}$ of A!) of K with $\mathcal{O}_K/\mathfrak{n} \cong \mathbb{Z}/N$. Choose an ideal class $[\mathfrak{a}] \in \mathrm{Pic}(\mathcal{O}_K)$. Every such $\mathfrak{n}$ as above defines a CM point $(\mathcal{O}_K, \mathfrak{n}, [\mathfrak{a}]) \in Y_0(N)(K)$: It is the point in the moduli space $Y_0(N)$ of elliptic curves with a cyclic isogeny of degree N corresponding to the elliptic curve $\mathbb{C}/\mathfrak{a}$ (a priori defined over $\mathbb{C}$) and the isogeny $\mathbb{C}/\mathfrak{a} \to \mathbb{C}/\mathfrak{n}^{-1}\mathfrak{a}$ and is defined over the ring class field $H_{\mathcal{O}_K}$ of $\mathcal{O}_K$ (which always contains the Hilbert class field of K and is equal to it if the order $\mathcal{O}$ is maximal) by the theory of complex multiplication. Summing over all $[\mathfrak{a}] \in \mathrm{Pic}(\mathcal{O}_K)$, we get a cycle of degree $h_{\mathcal{O}_K}$, the class number of $\mathcal{O}_K$, on $Y_0(N)$. Subtracting $h_{\mathcal{O}_K}[\infty]$ with the cusp $\infty \in X_0(N)(\mathbb{Q}) \setminus Y_0(N)(\mathbb{Q})$, we get a 0-cycle on $X_0(N)$ defined over K. Its image in $J_0(N)(K)$ under the Abel-Jacobi morphism is called the *Heegner point* y_K. Mapping y_K to J under a modular parameterization $J_0(N) \to J$ gives the Heegner point on J. By abuse of notation, we denote it by y_K again.

The celebrated theorem of Gross–Zagier says that the height of $y_K \in J(K)$ is non-zero if and only if the order of vanishing of

$$L(f/K, s) = L(f, s)L(f \otimes \chi_K, s)$$

at $s = 1$ equals 1; here χ_K is the quadratic Dirichlet character attached to K. By a theorem of Waldspurger [26], for every newform f with $\mathrm{ord}_{s=1} L(f, s) \in \{0, 1\}$, there exist infinitely many K satisfying the Heegner hypothesis and the hypothesis on the order of vanishing of $L(f/K, s)$. Since a point is non-torsion if and only if its canonical height is non-zero, the Gross–Zagier formula establishes one inequality in the BSD rank conjecture: If $L(A/\mathbb{Q}, s)$ has order of vanishing $r_{\mathrm{an}} = g$, then $\mathrm{rk}\, A(\mathbb{Q}) \geq g$.

The Euler system of Kolyvagin (in the case of $g = 1$) and Kolyvagin-Logachev (for general real multiplication) not only proves the opposite inequality (and hence equality of the analytic and algebraic rank), but also the finiteness of the Shafarevich-Tate group:

Computing an explicit finite support of the Shafarevich-Tate group

This is a purely theoretical consideration, combining the results of the computation of $\mathcal{O}y_K \subseteq J(K)$ and the $\mathfrak{p} \subset \mathcal{O}$ with $\rho_\mathfrak{p}$ reducible.

It is crucial that the Heegner point

$$y_1 := y_K \in J(K[1])$$

with $K[1] = H_{\mathcal{O}_K}$ is the lowest level of a whole system $y_n \in J(K[n])$ with $K[n]$ the ring class field of the order $\mathcal{O}_{K,n} := \mathbb{Z} + n\mathcal{O}_K$. They satisfy a compatibility relation with respect to field norms in which the Euler factors of f occur; hence the name "Euler system".

Kolyvagin-Logachev define several constants $C_i(\mathfrak{p})$ for finitely many i, and show that they are equal to 0 for almost all $\mathfrak{p}$ and fixed i, such that $\mathfrak{p}^{\sum_i C_i(\mathfrak{p})}\,\mathrm{Sel}_{\mathfrak{p}^\infty}(J/\mathbb{Q}) = 0$. In particular, almost all $\mathrm{Sel}_\mathfrak{p}(J/\mathbb{Q})$ are 0 and all $\mathrm{Sel}_{\mathfrak{p}^\infty}(J/\mathbb{Q})$ are finite. The $C_i(\mathfrak{p})$ depend on the images of the Galois representations $\rho_{\mathfrak{p}^\infty} : \mathrm{Gal}(\overline{\mathbb{Q}}|\mathbb{Q}) \to \mathrm{Aut}(T_\mathfrak{p}J)$ and $\rho_\mathfrak{p}$, the annihilator I_K of $J(K)/\mathcal{O}y_K$ as an $\mathcal{O}$-module (the so-called *Heegner index*), and the Tamagawa product $c(J/K) = \prod_v c_v(J/K)$ of J (conjecturally, all primes dividing $c(J/K)$ also divide I_K, so the latter would be redundant). There are additional complications for $\mathfrak{p} \mid 2$ as one often considers the space of Galois modules A where complex conjugation acts as $+1$ or -1, and A does not decompose as $A^+ \oplus A^-$ in general if $2 \mid \#A$. This is not a problem for us, since one can efficiently compute $\mathrm{Sel}_2(J/\mathbb{Q})$.

By making the argument of Kolyvagin-Logachev explicit enough, we show that $\text{Ш}(J/\mathbb{Q})[\mathfrak{p}] = 0$ if $\mathfrak{p} \nmid 2I_K c(J/K)$ and $\rho_\mathfrak{p}$ is irreducible. On the way, we prove that if $\rho_\mathfrak{p}$ is irreducible, its image contains a non-trivial homothety and one has

$$\mathrm{H}^1(\mathbb{Q}(J[\mathfrak{p}])|\mathbb{Q}, J[\mathfrak{p}](\overline{\mathbb{Q}})) = 0$$

using the classification of subgroups of $\mathrm{PSL}_2(\mathbb{F}_\mathfrak{p})$.

One can define Euler systems more generally for p-adic Galois representations ρ. In our case, this Galois representation is $T_\mathfrak{p}J$. The existence of a non-trivial Euler system together with "large image" results on ρ implies the finiteness of the Selmer group of ρ, and under some hypotheses one can even bound the size of the Selmer group via the "index" of its first level, which is the Heegner index in case of the Heegner point Euler system of Kolyvagin-Logachev. However, only a few Euler systems have been constructed, for example the Euler system of Heegner points for modular abelian varieties, the Euler system of elliptic units for CM elliptic curves, and the Euler system of cyclotomic units for the class group of cyclotomic field. Using the latter, one can give a more elementary, albeit not necessarily easier proof of the Main Conjecture of Iwasawa theory for cyclotomic extensions of $\mathbb{Q}$ compared with the first proof of Mazur and Wiles, which used arithmetic geometry of modular curves.

Computing the p-adic L-function and using the GL_2 Iwasawa Main Conjecture

We wrote a Magma [2] implementation of locally analytic distributions and distribution valued modular symbols together with their Hecke action. Building upon this, we implemented Greenberg's improvement [7] of the Pollack–Stevens algorithm [17] computing the p-adic L-function of a newform f of level divisible exactly by p, i.e., bad multiplicative reduction, as the evaluation at the path $\{\infty \to 0\}$ of the unique overconvergent lift of the modular symbol attached to f. If p does not divide the level, we compute the p-stabilization of the modular symbol; this currently only works if $a_p(f) \in \mathcal{O}_{\mathfrak{p}}^{\times}$.

Comparing with Magma's implementation of the p-adic L-function of an elliptic curve, our algorithm outperforms Magma's even for small p and precision $O(p^n)$, because the Magma implementation uses the naive "Riemann sum" approach, which has complexity exponential in $\log p$. Our algorithm also runs faster than the one implemented in SageMath [24], which only works for primes of degree 1. We verified that our algorithm produces the same output as SageMath with the same choice of a generator of the principal units using primes of degree 1.

In the cases where we use this, the p-adic L-function has vanishing order 0 and constant term a p-adic unit, and $\mathrm{im}(\rho_{\mathfrak{p}^\infty})$ contains $\mathrm{SL}_2(\mathbb{Z}_p)$, so by the GL_2 Iwasawa Main Conjecture, $\mathrm{Sel}_{\mathfrak{p}}(J/\mathbb{Q}) = 0$ and hence $Ш(J/\mathbb{Q})[\mathfrak{p}] = 0$.

Performing isogeny descents

Let $\mathfrak{p} \mid p$ be an ideal of the endomorphism ring $\mathcal{O}$. We compute $J[\mathfrak{p}](\overline{\mathbb{Q}})$ as a $\mathrm{Gal}(\overline{\mathbb{Q}}|\mathbb{Q})$-module from a complex approximation on the analytic Jacobian $\mathbb{C}^g/\Lambda$, where $J[\pi](\mathbb{C}) = \frac{1}{\pi}\Lambda/\Lambda$ if $\mathfrak{p} = (\pi)$ is principal. (This is the case in all of our examples.) The computation is sped up significantly if we use Julia/Oscar [5]. If $\rho_{\mathfrak{p}}$ is also reducible, we can compute the (1-dimensional) characters constituting the semisimplification of $\rho_{\mathfrak{p}}$. We perform an isogeny descent on them, i.e., we compute an upper bound on the dimension of their Selmer groups $\mathrm{Sel}_\varphi(\mathbb{Q}, S)$ related to φ-eigenspaces of the unit group and the class group of $L = \mathbb{Q}(\varphi)$, the number field obtained by adjoining all values of φ. Here, S a finite set of primes v containing those dividing the level N such that $c_v(A/\mathbb{Q})$ is divisible by p. In all our examples with $\mathfrak{p} \nmid 2$, the sum of the dimensions of the Selmer group of φ and ψ is ≤ 1, hence $Ш(J/\mathbb{Q})[\mathfrak{p}] = 0$ since the existence of the perfect alternating Cassels-Tate pairing

$$Ш(J/\mathbb{Q}) \times Ш(J^\vee/\mathbb{Q}) \to \mathbb{Q}/\mathbb{Z}$$

(note that $Ш(J/\mathbb{Q})$ is known to be finite) implies that the dimension is even.

As the computation of the unit group and the class group is time-consuming even for moderately large values of $\#(\mathcal{O}/\mathfrak{p})$ and especially $[\mathbb{Q}(J[\mathfrak{p}]) : \mathbb{Q}]$, we use it only for small $\mathfrak{p}$ and reducible $\rho_{\mathfrak{p}}$.

Computing the analytic order of the Shafarevich-Tate group

Finally we have to compute $\#Ш(J/\mathbb{Q})_{\mathrm{an}}$. This is done by computing $\#Ш(J/K)_{\mathrm{an}}$ and $\#Ш(J^K/\mathbb{Q})_{\mathrm{an}}$ for a Heegner field K for $J/\mathbb{Q}$, where J^K is the quadratic twist of J by K. To compute $\#Ш(J/K)_{\mathrm{an}}$, we use the Gross–Zagier formula [9] for general abelian varieties of GL_2-type over $\mathbb{Q}$, using the Heegner point we computed above. To determine $\#Ш(J^K/\mathbb{Q})_{\mathrm{an}}$, we implemented a method that computes $L(J^K/\mathbb{Q}, 1)/\Omega_{J^K}$ with the twisted modular symbols of $J/\mathbb{Q}$, as directly computing $L(J^K/\mathbb{Q}, 1)/\Omega_{J^K}$ tends to be too slow, because the level of $J^K/\mathbb{Q}$ is ND_K^2 with D_K the discriminant of K, which can be fairly large; note that $J^K/\mathbb{Q}$ has analytic rank 0. With both analytic ranks at hand, we then use the equation $\#Ш(J/K)_{\mathrm{an}} = \#Ш(J/\mathbb{Q})_{\mathrm{an}} \cdot \#Ш(J^K/\mathbb{Q})_{\mathrm{an}}$ up to explicitly bounded powers of 2 and Dokchitser's code to compute the special L-value $L''(J/\mathbb{Q}, 1)$, van Bommel's code to compute the real period Ω_J and the Müller–Stoll code [16] to compute canonical heights on and the regulator $\mathrm{Reg}_{J/\mathbb{Q}}$ of a genus-2 Jacobian to compute the algebraic part $L''(J/\mathbb{Q}, 1)/(\Omega_J \,\mathrm{Reg}_{J/\mathbb{Q}})$ of the special L-value $L^*(J/\mathbb{Q}, 1)$. The remaining invariants needed to compute $Ш(J/\mathbb{Q})_{\mathrm{an}}$, namely the Tamagawa numbers and the torsion subgroup of $J(\mathbb{Q})$, can be obtained through existing Magma functions.

Verification of the conjecture for Atkin-Lehner quotients of modular curves

Using the above theory and algorithms, we managed to verify strong BSD exactly for all of the 28 genus-2 quotients $X_0(N)/W'(N)$ with $W'(N)$ a subgroup of the Atkin-Lehner operators such that the Jacobian is absolutely simple and of GL_2-type over $\mathbb{Q}$. We announced this result in [10] with the article giving full details to be published later.

Work in progress: more curves

There are curves of genus 2 whose Jacobians are isogeny factors of $J_0(N)$ for some N, but which are not (necessarily) Atkin-Lehner quotients of $X_0(N)$. We find such curves in the LMFDB [23] as curves of conductor N^2 whose Jacobians are absolutely simple and of GL_2-type over $\mathbb{Q}$. There are currently 97 such curves in the LMFDB (including some of the Atkin-Lehner quotients); these are curves with discriminant $\leq 10^6$ (which implies $N \leq 1000$). Recently, Andrew Sutherland has generated a much larger set of genus 2 curves that will eventually become part of the database; we will then apply our algorithms also to the curves from this set whose Jacobians are absolutely simple and of GL_2-type.

We plan to produce more curves of genus 2 whose Jacobians are isogeny factors of $J_0(N)$ for some $N \leq 1000$ (say) using the approach in [27] (which produces

numerical approximations to the curve up to a twist), enhanced by using the Sturm bound and point counting on the curve to determine the correct twist as sketched in [6]. To these curves, we will then apply our algorithms; we hope to be able to verify strong BSD for most of them. The LMFDB lists 1195 pairs of Galois conjugate newforms of level ≤ 1000, so that we can expect to find several hundred more examples in this way.

Our Magma code will be made available on `https://github.com/TimoKellerMath` as soon as we have finished our detailed article with more examples.

A challenge

The recent preprint [19] gives a recipe to construct absolutely simple modular abelian surfaces $A/\mathbb{Q}$ with odd primes p dividing $\#\text{Ш}(A/\mathbb{Q})$. In principle, our method can be used to verify strong BSD for them, but as the level of the quadratic twist A^D of A by the quadratic character with discriminant D equals ND^2, the computations quickly become infeasible. For example, all the 97 absolutely simple GL_2-type abelian surfaces listed in the LMFDB have analytic order of Ш approximately 1, 2 or 4. So we pose as a challenge to verify strong BSD for some $A/\mathbb{Q}$ with $\text{Ш}(A/\mathbb{Q})$ not a 2-group!

References

[1] B. J. Birch and H. P. F. Swinnerton-Dyer. Notes on elliptic curves. II. *J. Reine Angew. Math.*, 218:79–108, 1965.

[2] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3–4):235–265, 1997. Computational algebra and number theory (London, 1993).

[3] Christophe Breuil, Brian Conrad, Fred Diamond, and Richard Taylor. On the modularity of elliptic curves over **Q**: wild 3-adic exercises. *J. Amer. Math. Soc.*, 14(4):843–939, 2001.

[4] Brendan Creutz and Robert L. Miller. Second isogeny descents and the Birch and Swinnerton-Dyer conjectural formula. *J. Algebra*, 372:673–701, 2012.

[5] Claus Fieker, William Hart, Tommy Hofmann, and Fredrik Johansson. Nemo/Hecke: Computer Algebra and Number Theory Packages for the Julia Programming Language. In *Proceedings of the 2017 ACM on International Symposium on Symbolic and Algebraic Computation*, ISSAC '17, pages 157–164, New York, NY, USA, 2017. ACM.

[6] E. Victor Flynn, Franck Leprévost, Edward F. Schaefer, William A. Stein, Michael Stoll, and Joseph L. Wetherell. Empirical evidence for the Birch and Swinnerton-Dyer conjectures for modular Jacobians of genus 2 curves. *Math. Comp.*, 70(236):1675–1697, 2001.

[7] Matthew Greenberg. Lifting modular symbols of non-critical slope. *Israel J. Math.*, 161:141–155, 2007.

[8] Grigor Grigorov, Andrei Jorza, Stefan Patrikis, William A. Stein, and Corina Tarniţă. Computational verification of the Birch and Swinnerton-Dyer conjecture for individual elliptic curves. *Math. Comp.*, 78(268):2397–2425, 2009.

[9] Benedict H. Gross and Don B. Zagier. Heegner points and derivatives of L-series. *Invent. Math.*, 84(2):225–320, 1986.

[10] Timo Keller and Michael Stoll. Exact verification of the strong BSD conjecture for some absolutely simple abelian surfaces, 2021. Preprint, arXiv:2107.00325, to appear in Comptes Rendus Mathématique.

[11] Chandrashekhar Khare and Jean-Pierre Wintenberger. Serre's modularity conjecture. In *Proceedings of the International Congress of Mathematicians. Volume II*, page 280–293. Hindustan Book Agency, New Delhi, 2010.

[12] V. A. Kolyvagin and D. Yu. Logachëv. Finiteness of the Shafarevich-Tate group and the group of rational points for some modular abelian varieties. *Algebra i Analiz*, 1(5):171–196, 1989.

[13] Tyler Lawson and Christian Wuthrich. Vanishing of some Galois cohomology groups for elliptic curves. *Springer Proc. Math. Stat., vol. 188, Springer, Cham*, pages 373–399, 2016.

[14] Robert L. Miller. Proving the Birch and Swinnerton-Dyer conjecture for specific elliptic curves of analytic rank zero and one. *LMS J. Comput. Math.*, 14:327–350, 2011.

[15] Robert L. Miller and Michael Stoll. Explicit isogeny descent on elliptic curves. *Math. Comp.*, 82(281):513–529, 2013.

[16] Jan Steffen Müller and Michael Stoll. Canonical heights on genus-2 Jacobians. *Algebra Number Theory*, 10(10):2153–2234, 2016.

[17] Robert Pollack and Glenn Stevens. Overconvergent modular symbols and p-adic L-functions. *Ann. Sci. Éc. Norm. Supér. (4)*, 44(1):1–42, 2011.

[18] Kenneth A. Ribet. Abelian varieties over **Q** and modular forms. *Modular curves and abelian varieties*, 224:241–261, 2004.

[19] Ari Shnidman and Ariel Weiss. Elements of prime order in Tate-Shafarevich groups of abelian varieties over $\mathbb{Q}$, 2021. Preprint, arXiv:2106.14096.

[20] Christopher Skinner. Multiplicative reduction and the cyclotomic main conjecture for GL_2. *Pacific J. Math.*, 283(1):171–200, 2016.

[21] Christopher Skinner and Eric Urban. The Iwasawa main conjectures for GL_2. *Invent. Math.*, 195(1):1–277, 2014.

[22] Richard Taylor and Andrew Wiles. Ring-theoretic properties of certain Hecke algebras. *Ann. of Math. (2)*, 141(3):553–572, 1995.

[23] The LMFDB collaboration. L-functions and Modular Forms Database. `https://www.lmfdb.org/Genus2Curve/Q/`.

[24] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 9.4)*, 2022. `https://www.sagemath.org`.

[25] Raymond van Bommel. Numerical verification of the Birch and Swinnerton-Dyer conjecture for hyperelliptic curves of higher genus over $\mathbb{Q}$ up to squares. *Exp. Math.*, page 1–8, 2019.

[26] J.-L. Waldspurger. Sur les valeurs de certaines fonctions L automorphes en leur centre de symétrie. *Compositio Math.*, 54(2):173–242, 1985.

[27] Xiang Dong Wang. 2-dimensional simple factors of $J_0(N)$. *Manuscripta Math.*, 87(2):179–197, 1995.

[28] Andrew Wiles. Modular elliptic curves and Fermat's last theorem. *Ann. of Math. (2)*, 141(3):443–551, 1995.

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`

The mathematical research-data repository MathRepo

Claudia Fevola
(MPI for Mathematics in the Sciences, Leipzig)
Christiane Görgen
(Mathematisches Institut, Universität Leipzig)

fevola@mis.mpg.de
goergen@math.uni-leipzig.de

Research data in mathematics

MathRepo, located at https://mathrepo.mis.mpg.de, is an online repository for mathematical research data. Research data, broadly speaking, can be defined as „the recorded factual material commonly accepted in the scientific community as necessary to validate research findings“[1]. In mathematics, research data comes in many different flavours. For instance, in computer algebra it most often takes the form of mathematical documents, notebooks, research-software packages and libraries, computer algebra systems, algorithms, and collections of mathematical objects [GS21, e.g.]. MathRepo contains foremostly computer-algebra research data of three main types: computations performed for paper publications, additional lists of examples to theoretical results, and presentations of problems solved in workshops or lectures. It provides one central location for mathematicians to store and share any additional data they might want to make publicly available alongside their paper publications.

The repository was established in 2017 at the Max Planck Institute for Mathematics in the Sciences[2] (MPI MiS) in Leipzig, following the initiative of Bernd Sturmfels, Ronald Kriemann, and Yue Ren. It has had seven different maintainers over the past five years: Yue Ren and Mahsa Sayyary in 2017 and 2018, Lukas Kühne and Verena Morys from 2019, and the authors of this paper together with Carlos Améndola since 2021. There are of course a variety of other storage solutions across different scientific fields[3], some research data can be published as software packages [BEO02, e.g.], and some mathematical libraries have their own homepages[4]. However, an infrastructure which can both store and visually present a wide range of different data in a wiki- or blog-entry style was—and at the time of writing *is*—not yet broadly established. In particular, for smaller contributions to papers like proofs by computation in a particular programming language or lists of examples of objects with properties of interest, a centralised infrastructure was completely missing. MathRepo aimed to fill this gap.

At the time of writing, the repository has gathered a total of forty individual contributions. The contributor community is the nonlinear-algebra working group[5] at MPI MiS, though being a member is not necessary to gain access to the repository. Informally registering with MPI MiS's IT service is sufficient to obtain contributor rights. MathRepo is hosted on the servers of MPI MiS[6]. It is planned to last for at least the coming decade and is limited in size and capacities as is the underlying open-source software GitLab[7]. Just like with paper-storage options such as arXiv.org, also in MathRepo there is no hard quality control. Merge requests are accepted after a brief visual check of three basic requirements: that the content of a new page is mathematical research data, that it provides references to relevant literature, and that the authors are generally known in the nearby scientific community. In particular, there are no strict rules for the actual presentation of the mathematical content. Using MathRepo as a pure repository is just as possible as using it to provide an in-depth introduction to a topic of interest, as we will see in a number of examples below.

What makes a good repository?

In 2021 the Mathematical Research Data Initiative MaRDI[8] has set about developing and establishing infrastructure for research data in the German mathematics community. The declared purpose of the consortium is to establish the FAIR principles for these data: their long-term findability, accessibility, interoperability, and reusability shall be ensured [WDA+16, HWS21]. Currently, twenty-five partnering research organisations

[1] OMB Circular 110, https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A110/2cfr215-0.pdf

[2] https://www.mis.mpg.de

[3] See the list of research-data repositories at https://www.re3data.org, e.g.

[4] See the library „Small Phylogenetic Trees“ https://www.coloradocollege.edu/aapps/ldg/small-trees/small-trees_0.html or „The Markov Bases Database“ https://markov-bases.de, e.g.

[5] https://www.mis.mpg.de/nlalg/nlalg-people.html

[6] https://gitlab.mis.mpg.de

[7] https://docs.gitlab.com/ee/administration/instance_limits.html

[8] https://www.mardi4nfdi.de

within MaRDI are working towards this aim. These are universities and institutes from the Fraunhofer and Max Planck societies as well as the Leibniz Gemeinschaft, the professional societies DMV, GAMM, and GOR, the European Mathematical Society and partners from mathematically-inclined Clusters of Excellence within Germany. This network ensures a nationally consistent implementation and follows a bottom-up approach in setting up new standards. In MaRDI's computer-algebra task area, the `OSCAR`[9] group is a key player, for instance.

One way of implementing the FAIR principles in practice is via the usage of trustworthy storage solutions for research data. This article is a snapshot of the service that MathRepo provides to the computer-algebra and other mathematical communities in this context and at this precise point in time, in February 2022—after nearly five years of maintenance under different leads, with new programming languages and software solutions coming up, and MaRDI waiting in the wings.

All present and past maintainers of MathRepo have themselves contributed to the repository. In particular, the initiators had plenty hands-on experience in handling *not* FAIR research data: data which was promised in papers and stored on long-gone personal homepages, data blocked by pay walls, data which would run on one computer but not on another, and data which would just not provide the promised results. Their key strategy to address these issues with MathRepo was usability. They envisioned that if the repository was easy to access for authors that would offer a practical counterpart to other, decentralised, research-type specific or hard-to-maintain storage options. And if it was used by authors, it would become known to readers as well and thus self-establish in the community, replacing cumbersome past solutions. A low entry barrier was initially achieved by Yue Ren being the sole maintainer who uploaded and curated all of the contributions in 2017 and '18. It was later replaced by annual `GitLab`-training sessions with local contributors at the MPI MiS. Both strategies have had success and facilitated acceptance of the service in their local academic community, though MathRepo has never been aimed solely at that particular audience.

The key question for us is now: is the content of MathRepo FAIR in a MaRDI context? Or, more practically for you as the reader, is using MathRepo for your own research a solution for the future? We will discuss these questions over the coming sections, presenting the mathematics currently present on the repository and discussing what the FAIR principles mean for these in practice.

The mathematics in MathRepo

The common theme of all research data currently present on MathRepo is *nonlinear algebra*. This is a diverse and developing field of mathematics promoted by the recent expansion of nonlinear methods across applications [MS21, Stu22]. Of course, the theory, algorithms, and software from linear algebra and numerical linear algebra have a crucial function in the process of modelling problems arising in the natural sciences and engineering. But the natural occurrence of nonlinear equations in real-world applications together with an increasingly strong toolbox of new computational methods brought about a growing use of nonlinear approaches to mathematical modelling. These recent developments rely on techniques from algebraic geometry, topology, combinatorics, group theory, commutative algebra or representation theory. Vice versa, applications are also a central motor for driving new results in this field. Examples of this can be found in physics, polynomial optimization, partial differential equations, algebraic statistics, and algebraic vision [BÇD+21].

In practice, many of the applications of nonlinear algebra boil down to the problem of finding solutions to systems of polynomial equations. Broadly speaking, there are then two main computational approaches: symbolic and numerical. The former often relies on Gröbner bases' computations, the latter typically uses homotopy continuation. Several software and programming languages provide effective tools for these computations and MathRepo furnishes a valid collection of the most well known ones, including `GAP`, `Julia`, `Macaulay2`, `Magma`, `Maple`, `Mathematica`, `Matlab`, `Polymake`, `Sage`, and `Singular`.

Coding In many research projects in nonlinear algebra the symbolic and the numerical approach are both needed for solving different parts of the same problem, and turn out to be highly interlinked. As a result, scientists frequently use different software and programming languages even for a single research project. An example of this is shown on the MathRepo page `Landau Discriminants`, providing auxiliary material to [MT21]. This work applies methods from nonlinear algebra to the theory of scattering amplitudes in particle physics. In particular, these seemingly far-apart fields are practically and theoretically connected in the study of the so-called Landau equations. These are a set of polynomial equations determining allowed positions of singularities of Feynman integrals which arise in quantum field theory. The Landau discriminant parametrizes points for which the Landau equations have solutions. For each Feynman integral, the authors introduce the Landau discriminant as a projective variety whose points are potential singularities of the integral. Nonlinear algebraists can then foster the understanding of this physical setting by studying geometric properties of the discriminant, such as irreducibility, dimension, and degree.

Together with the theoretical findings, they provide an implementation of their work. Their `Julia` package `Landau.jl` numerically computes defining equations of the Landau discriminant for some Feynman in-

[9] `https://oscar.computeralgebra.de`

tegrals which were previously out of reach. A tutorial illustrating how to use the package is provided as a `Jupyter` notebook, linked to the MathRepo page. Further symbolic elimination methods are implemented in `Macaulay2` for computing Landau discriminants and are also presented and illustrated on the project page. These approaches complement and enrich each other: the symbolic method provides reliable outputs but cannot deal with examples involving a high number of variables while the numerical computations are not exact but can be used to compute the desired equations in an efficient way.

This project illustrates one big advantage of using MathRepo over different, say software-specific solutions: there is no constraint on choosing a particular programming language to work with, and the mathematician is free to do whatever their problem demands. Indeed, code fragments written in different languages can be easily combined and illustrated on the same web page, together with information about the respective software version and hardware setup provided at the bottom of the project page. An additional written explanation between these code snippets greatly facilitates interoperability between different systems and improves reusability for the reader.

Visualization Another key benefit of putting research-data on MathRepo is that important features of the various programming languages, such as interactive visualizations, can be presented. The page `Intersection Bodies of Polytopes`, illustrated in Fig. 1, makes use of this. In the corresponding article [BBMS22], the authors investigate the intersection body of a convex polytope combining tools from combinatorics and from real algebraic geometry. In particular, they implement an algorithm for computing its algebraic boundary in `Sage` and `OSCAR`. Visitors of this page can both download the `Jupyter` notebooks to run the computations independently and also directly look at the code together with an interactive gallery of the output.

Finally, a step-by-step explanation of how to compute the intersection body of the three-dimensional cube, and an interactive case study of translates of the 3-cube are provided. In contrast to a paper publication, the MathRepo storage solution gives access to three-dimensional visualizations of these objects. In this way curvature, convexity, and all pieces of the algebraic boundary can be investigated.

Teaching A third type of contribution to MathRepo are presentations of problems solved in workshops or lectures. Indeed, the repository is also a possible useful tool for teaching purposes or for learning how to code in the languages previously specified. For instance, `Invitation to Nonlinear Algebra` is a page where exercises, and examples dealing with polynomial rings, primary decomposition of ideals, tropical geometry, and tensors presented in the textbook [MS21] are solved and explained using `Macaulay2` and `Polymake`.

The web pages from MathRepo we illustrate here are just some examples of many very different contributions included in the repository and they emphasize some of its main features. An autonomous navigation of the web page is encouraged to get a more accurate idea of its possible types of use and to discover more interesting code presentations that are the building blocks of intuitions, examples, theorems, and their proofs.

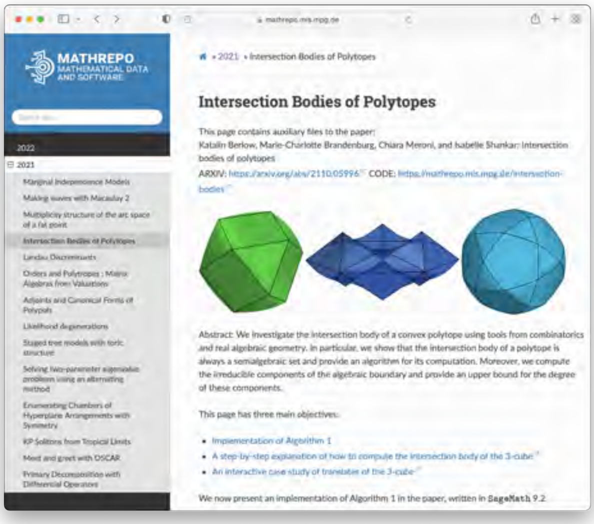


Figure 1: *A screenshot of the MathRepo subpage* `Intersection Bodies of Polytopes`*. The MathRepo logo is displayed in the top-left corner, below that is the list of all contributions sorted by year.*

A discussion of FAIRness

Nowadays there are general, not mathematics-specific guidelines for producing FAIR research data [JdMAJ+20, e.g.] and some of MaRDI's partnering research-data consortia in other disciplines are advanced in the process of implementing an apt infrastructure across their communities. Centrally, these implementations address *automated* search and usage of research data. Especially with respect to findability and accessibility, extensive metadata in some agreed-upon standard format is then essential. To implement interoperability, it need be possible to automatically combine different digital resources, and for reusability automated decisions of relevance and legal terms need to be made. These developments were not known to the MathRepo group until the kickoff of MaRDI in 2021 and are, at the time of writing, not yet established in the mathematics community. However, all four principles have throughout been implicitly addressed from a human-user standpoint as follows.

Findability Every subpage of MathRepo has a unique and persistent URL of the format `https://`

`mathrepo.mis.mpg.de/<project-name>` assigned by its respective authors. Project names are encouraged to be telling and related to the title of the corresponding publication, if existent. The MPI MiS's internal library service provides up-to-date references for the latter. Vice versa, the link to the MathRepo project page can be explicitly stated in a paper publication. The additional index on the repository's website which sorts entries by year and by programming language enables a direct as well as an associative findability on the web page itself. These measures facilitate findability for humans. The MPI MiS's front web page contains a link to the repository and it is known to the most widely-used search engines, thus also improving machine findability. Persistence of the repository and its links is guaranteed by the MPI MiS's directors' decision and is independent of the respective project and author location.

Accessibility All content available on MathRepo, both research data and their metadata, is freely accessible for all users from any location. The current project-page template features the following recommendations: provide author names, a citation of a relevant publication, possibly `arXiv` link, an abstract, and the system setup (programming language, version, hardware) for computations, as well as a corresponding author for the project page itself. These minimum requirements establish a local metadata standard while allowing for a lot of flexibility in actual content. The website is build on the `http` protocol, amenable to automated machine-search. The underlying `GitLab` is an open-source software. It provides an easy tracking tool, making historical changes and versions available for maintainers and contributors. These implementations make the website reasonably accessible without introducing a too technical setup.

Interoperability On a theoretical level, MathRepo facilitates interoperability of its content by providing an abstract for each page. This embeds the employed mathematical terms into context and thus allows readers to translate the content into their own mathematical language, making it interoperable for humans. On the computational side, the more recent pages on MathRepo provide information on how to reproduce their respective system setup, facilitating interoperability on a technical level.

Reusability Two implementations help readers to reproduce and reuse the MathRepo content. First, the abstract of each project page is often taken from a corresponding paper publication. It gives an indication as to which area of mathematics the research data belongs to and where to find additional background literature. Second, the pages created after 2018 each have a corresponding author named who can be contacted for direct information.

The combination of these measures makes the data present on MathRepo FAIRer than research material which is simply put on personal homepages. MathRepo retains the low entry barrier and the flexibility of such user-implemented solutions, as shown in examples in the previous section, while providing long-term storage and independence of the authors' current academic location. To the best of our knowledge, this is a standalone feature of the repository in the mathematics community. However, many of these solutions are practical in a local sense and are not yet embedded in a national or even global infrastructure for research data.

Current challenges

At the time of writing, the MathRepo project standards do not follow a recommended protocol for mathematical research-data presentation and metadata supply. They rather reflect the maintainers' experience with documentation needed for the usage and maintenance of computer-algebra software. This approach has initially allowed for a swift setup of the repository. However, it does come with certain limitations, many of which became visible only with the growth of the repository. Now, challenges are threefold: inconsistent layout across the individual project pages, out-of-date or broken content, and large variations in mathematical quality.

The reasons and implications of these issues are numerous and the MathRepo contributions of the past five years clearly show a process of how priorities changed over time. For instance, the template for authors has improved with every handover between different sets of maintainers, providing increasingly refined metadata and new guidelines for presentation. As a result however, the depth of detail of the individual contributions' metadata and the overall layout of the MathRepo project pages is not uniform. This is now a hurdle to both findability and automated accessibility, as well as a hurdle to reusability. For instance, metadata provided in different places across different pages encumbers findability for the human reader. Broken links to e.g. `binder` notebooks are an obstacle to accessibility and convey a general impression of content being out of date. Not sufficiently detailed references to employed programming languages hinder reproducibility on systems different from the authors'. Missing corresponding-author names in the early contributions impede reusability.

Even though training sessions at MPI MiS allow newcomers to learn to operate the `GitLab` setup, MathRepo's recommended project-page template is then often not followed in detail. This issue together with the great flexibility—to use MathRepo as a pure storage solution or, on the other extreme, as a platform for presenting teaching material—entail that contributions vary largely in quality. But then a combination of large variations both in quality and in presentation can confuse readers and, worse, make them wary to trust the content. This is challenging from a user perspective.

From a maintainers' perspective, non-compliance with locally established standards in the new contributions and an increasing number of breakage in the

past contributions hugely increase the workload that is needed to ensure some sort of consistency between the individual subpages of the repository. Additionally, the user community has recently grown in numbers and has spread in mathematical diversity, making it hard for the maintainers to understand and judge new content. For scientists for whom MathRepo is only one of many projects and time commitment is limited, this is manageable only while the repository is still reasonably small. This issue actually is part of a bigger problem in a publishing culture which values code and software less than research data that comes in the form of paper publications. But based on the past experiences and based on current research projects in the different working groups at MPI MiS, we predict more and more non-text research data and future growth of MathRepo. This snapshot marks a point at which it is still possible to tend to present issues before they become too large to manage.

Outlook

With increasing awareness of the importance of FAIR principles for sustainable research and with MaRDI launched, it is timely for us to address the above points of criticism. In particular, we plan to tackle three main issues: trustworthiness of the repository, barriers to reusability, and forward-compatibility of the standards for embedding into coming MaRDI infrastructure.

With respect to trustworthiness, we see two possible ways for improvement of the status quo: to implement a user check for executability of code and for mathematical correctness of the research data similar to a small-scale peer-review system, or to follow an established standard for research-data repositories and to apply for third-party certification, e.g. with CoreTrustSeal[10].

This latter idea immediately leads to our point on reusability. Many seals of quality require a clear statement of the terms of use of a repository. However, at the time of writing this is not present in MathRepo and the lack of a license statement does not imply that data is automatically open access [JdMAJ+20, cf.]. For future FAIRness of the repository, it is thus mandatory to choose an appropriate license. This can either be by maintainer's choice or each user could be required to choose their own from a list of standard open-access licenses.

We aim to address the above issues and also facilitate a future embedding into MaRDI infrastructure by setting up a new template with metadata standards. These shall beforehand be discussed within the current MaRDI community. Compliance with the new standards shall then be achieved by embedding a section on research-data management into coming MathRepo-training sessions, stressing the importance of making your research FAIR.

References

[BBMS22] Katalin Berlow, Marie-Charlotte Brandenburg, Chiara Meroni, and Isabelle Shankar. Intersection bodies of polytopes. *Beiträge zur Algebra und Geometrie/Contributions to Algebra and Geometry*, pages 1–21, 2022.

[BÇD+21] Paul Breiding, Türkü Özlüm Çelik, Timothy Duff, Alexander Heaton, Aida Maraj, Anna-Laura Sattelberger, Lorenzo Venturello, and Oğuzhan Yürük. Nonlinear algebra and applications. *Preprint available at* `arXiv:2103.16300`, 2021.

[BEO02] Hans Ulrich Besche, Bettina Eick, and E. A. O'Brien. A millennium project: constructing small groups. *Internat. J. Algebra Comput.*, 12(5):623–644, 2002.

[GS21] Christiane Görgen and Rainer Sinn. Mathematik in der Nationalen Forschungsdateninfrastruktur. *Mitteilungen der Deutschen Mathematiker-Vereinigung*, 29(3):122–123, 2021.

[HWS21] Nathalie Hartl, Elena Wössner, and York Sure-Vetter. Nationale Forschungsdateninfrastruktur (NFDI). *Inform. Spektrum*, 44(5):370–373, 2021.

[JdMAJ+20] Annika Jacobsen, Ricardo de Miranda Azevedo, Nick Juty, Dominique Batista, Simon Coles, Ronald Cornet, Mélanie Courtot, Mercè Crosas, Michel Dumontier, et al. Fair principles: Interpretations and implementation considerations. *Data Intelligence*, 2(1-2):10–29, 2020.

[MS21] Mateusz Michałek and Bernd Sturmfels. *Invitation to nonlinear algebra*, volume 211. American Mathematical Soc., 2021.

[MT21] Sebastian Mizera and Simon Telen. Landau discriminants. *Preprint available at* `arXiv:2109.08036`, 2021.

[Stu22] Bernd Sturmfels. Beyond linear algebra. In *Proceedings of the International Congress of Mathematicians, St. Petersburg*, 2022. Preprint available at `arXiv:2108.09494`.

[WDA+16] Mark Wilkinson, Michel Dumontier, IJsbrand Jan Aalbersberg, Gaby Appleton, et al. The FAIR guiding principles for scientific data management and stewardship. *Scientific Data*, 3(160018), 2016.

[10] `https://www.coretrustseal.org`

Über die Beziehung des Rings der dualen Zahlen zur automatischen Differentiation

Gerhard Heindl (Ebersberg)

mail@gerhardheindl.de

Der Ring $\mathbb{D}$ der dualen Zahlen

Der Ring der dualen Zahlen lässt sich analog zum Körper der komplexen Zahlen konstruieren. Bekanntlich ist die Menge $\mathbb{R} \times \mathbb{R}$ der reellen Zahlenpaare (x, y) bezüglich der Addition

$$(A) : (x_1, y_1) + (x_2, y_2) := (x_1 + x_2, y_1 + y_2)$$

und der Multiplikation

$$(M_C) : (x_1, y_1)*(x_2, y_2) := (x_1x_2 - y_1y_2, x_1y_2 + y_1x_2)$$

ein Körper, nämlich der Körper $\mathbb{C}$ der komplexen Zahlen. Die Schreibweise $x + iy$ für die komplexe Zahl (x, y) leitet sich aus der Gleichung

$$(S) : (x, y) = (x, 0) + (0, 1) * (y, 0)$$

ab, wenn man $i = (0, 1)$ setzt und für jedes $x \in \mathbb{R}$, $(x, 0)$ mit x identifiziert.

Bezüglich der Addition (A) und der Multiplikation

$$(M_D) : (x_1, y_1) * (x_2, y_2) := (x_1x_2, x_1y_2 + y_1x_2)$$

ist $\mathbb{R} \times \mathbb{R}$ nur ein kommutativer Ring, der sogenannte Ring $\mathbb{D}$ der dualen Zahlen. Es sind nur die Zahlenpaare (x, y) invertierbar, für die x von 0 verschieden ist. Für $x \neq 0$ hat man

$$(x, y)^{-1} = \left(\frac{1}{x}, -\frac{y}{x^2}\right),$$

und folglich für $x_2 \neq 0$:

$$\begin{aligned}(x_1, y_1)/(x_2, y_2) &:= (x_1, y_1) * (x_2, y_2)^{-1} \\ &= \left(\frac{x_1}{x_2}, \frac{x_2y_1 - y_2x_1}{x_2^2}\right).\end{aligned}$$

Offenbar erweitern die betrachteten arithmetischen Operationen die gleichnamigen Operationen für reelle Zahlen auf duale Zahlen, wenn man, was im Folgenden stets angenommen werde, $(x, 0) \in \mathbb{D}$ mit $x \in \mathbb{R}$ identifiziert.

Duale Zahlen wurden erstmals von E. Study in [4], S. 195-197, eingeführt und für kinematische und geometrische Anwendungen benutzt. Da die Darstellung (S) auch bei Ersetzung von (M_C) durch (M_D) gilt, wird für die duale Zahl (x, y) üblicherweise $x + \varepsilon y$ oder $x + y\varepsilon$ geschrieben, wobei jetzt $(0, 1)$ mit ε bezeichnet wird (siehe z. B. [4] S. 195 oder [2] § 30*). Während bei Zugrundelegung der Multiplikation (M_C) für komplexe Zahlen $i^2 = -1$ ist, gilt bei der Zugrundelegung der Multiplikation (M_D) für duale Zahlen $\varepsilon^2 = (0, 1) * (0, 1) = 0$. Im Folgenden soll jedoch für duale Zahlen die kürzere Schreibweise (x, y) beibehalten werden.

Die Erweiterung von differenzierbaren Funktionen

Für jede differenzierbare Funktion $h : \mathbb{R} \supset D_h \to \mathbb{R}$, D_h offen, führen wir die Erweiterung

$$h_d : D_h \times \mathbb{R} \ni (x, y) \mapsto (h(x), yh'(x)) \in \mathbb{D}$$

von h zu einer Funktion von der Teilmenge $D_h \times \mathbb{R}$ von $\mathbb{D}$ in $\mathbb{D}$ ein.

Sind f, g differenzierbare Funktionen, so folgert man aus $(A), (M_D)$, der Formel für die Division von dualen Zahlen, sowie den bekannten Rechenregeln für differenzierbare Funktionen:
Ist $D := D_f \cap D_g \neq \emptyset$, dann sind $f \pm g$ und $f * g$ definiert mit $D_{f\pm g} = D_{f*g} = D$ und es gilt für alle $(x, y) \in D \times \mathbb{R}$:

$$f_d(x, y) \pm g_d(x, y) = (f \pm g)_d(x, y),$$

$$f_d(x, y) * g_d(x, y) = (f * g)_d(x, y).$$

Ist $D' := D_f \cap \{x \in D_g : g(x) \neq 0\} \neq \emptyset$, so ist f/g definiert mit $D_{f/g} = D'$ und es gilt für alle $(x, y) \in D' \times \mathbb{R}$:

$$f_d(x, y)/g_d(x, y) = (f/g)_d(x, y).$$

Neben diesen algebraischen Regeln ist für die automatische Differentiation vor allem die folgende Regel von Bedeutung:

Die Funktionen h und g seien differenzierbar, und $g(D_g)$ sei eine Teilmenge von D_h. Dann gilt für alle $(x, y) \in D_g \times \mathbb{R}$:

$$h_d(g_d(x, y)) = (h \circ g)_d(x, y).$$

(Beweis: Für $(x, y) \in D_g \times \mathbb{R}$ ist $g_d(x, y) = (\xi, \eta)$ mit $\xi = g(x)$ und $\eta = yg'(x)$. Daher ist

$$h_d(g_d(x, y)) = h_d(\xi, \eta) = (h(\xi), \eta h'(\xi)) =$$

$$(h(g(x)), yg'(x)h'(g(x))) = (h \circ g)_d(x, y),$$

wobei die letzte Gleichung aus der Kettenregel folgt.)

Bemerkung zur Verknüpfung von differenzierbaren Funktionen mit konstanten Funktionen: Ist $c \in \mathbb{R}$, und f differenzierbar, so bezeichnet man die Funktion $D_f \ni x \mapsto f(x) \pm c$ üblicherweise mit $f \pm c$. Dabei wird also mit c auch die Funktion bezeichnet, die auf D_f den konstanten Wert c annimmt. Entsprechend sind Verknüpfungen wie $c \pm f, c * f, f * c, c/g$ und im Fall $c \neq 0$, g/c zu betrachten. Da immer klar ist, in welchem Kontext c auftritt, sind Verwechslungen nicht zu befürchten.

Automatische Differentiation

Eine, mit Hilfe der in einer Programmiersprache zur Verfügung stehenden algebraischen Operatoren $+, -, *, /$ und differenzierbaren Standardfunktionen zusammengesetzte Funktion q in einem in der Programmiersprache realisierbaren $x \in D_g$ automatisch zu differenzieren, bedeutet $q(x)$ und $q'(x)$ (bis auf Rundungsfehler) dadurch zu ermitteln, indem man

$$q_d(x, 1) = (q(x), q'(x))$$

berechnet. Es wird damit vermieden, dass man einen Funktionsausdruck für q' berechnen, und anschließend die Werte $q(x)$ und $q'(x)$ getrennt auswerten muss, um z. B. (im Fall $q'(x) \neq 0$) einen Newtonschritt

$$x - \frac{q(x)}{q'(x)}$$

durchzuführen. Selbst wenn man die Bestimmung eines Funktionsausdrucks für q' einem Computer-Algebra-Programm überlässt, so ist der Aufwand für eine anschließende getrennte Berechnung von $q(x)$ und $q'(x)$ wegen der dabei auftretenden Mehrfachberechnungen von Zwischenresultaten erheblich höher als der für die simultane Berechnung von $(q(x), q'(x))$ als $q_d(x, 1)$.

Ein einfaches, aber repräsentatives Beispiel:

Nehmen wir an, wir wollen für die für alle $x \in \mathbb{R}$ durch

$$q(x) := \frac{(\cos(x) - 1) * (\sin(x) + 3)}{\operatorname{asinh}(\cos(x) * \sin(x)) + 2}$$

definierte differenzierbare Funktion q sowohl $q(5)$ als auch $q'(5)$ bestimmen.

Man setzt dann also $w := (5, 1)$ und berechnet

$$\frac{(\cos_d(w) - 1) * (\sin_d(w) + 3)}{\operatorname{asinh}_d(\cos_d(w) * \sin_d(w)) + 2},$$

wobei die arithmetischen Operatoren die in $\mathbb{D}$ eingeführten sind. Aus den bereitgestellten Rechenregeln für erweiterte differenzierbare Funktionen folgt, dass das Ergebnis

$$q_d(w) = q_d(5, 1) = (q(5), q'(5))$$

ist. Entscheidend ist dabei, dass die arithmetischen Operatoren und für die Standardfunktionen $\cos, \sin, \operatorname{asinh}$ ihre Erweiterungen $\cos_d, \sin_d, \operatorname{asinh}_d$ programmierbar sind. Für alle $(x, y) \in \mathbb{R} \times \mathbb{R}$:

$$\begin{aligned} \cos_d(x, y) &= (\cos(x), -y\sin(x)),\ \sin_d(x, y) \\ &= (\sin(x), y\cos(x)), \\ \operatorname{asinh}_d(x, y) &= (\operatorname{asinh}(x), \frac{y}{\sqrt{1 + x^2}}). \end{aligned}$$

Das ist auch für die üblichen anderen differenzierbaren Standardfunktionen der Fall. Die Auswertung von $q_d(w)$ erfolgte mit einer Matlab-Funktion (für die nur die tatsächlich benötigten Operatoren und Funktionen programmiert wurden) mit dem Ergebnis

$$\begin{aligned} &(q(5), q'(5)) \\ &= (-0.844540587580294, 0.618202155258725). \end{aligned}$$

Eine umfassende Klasse von entsprechenden Operatoren und Funktionen wurde von C. Taylor [5] programmiert. Eine erste (eingeschränktere) Klasse dieser Art wurde, ohne Bezug auf duale Zahlen zu nehmen, von L.B. Rall in [3] entwickelt.

Die hier über die duale Arithmetik eingeführte Automatische Differentiation lässt sich in naheliegender Weise auf eine automatische Berechnung der Koeffizienten von Taylorpolynomem zu gegebenen Entwicklungspunkten verallgemeinern. Ferner existieren verschiedene Verfahren zur automatischen Berechnung von partiellen Ableitungen beliebiger Ordnung für entsprechend oft differenzierbare Funktionen von mehreren Veränderlichen (siehe z. B. [1]).

Literatur

[1] A. Griewank, A. Walther, *Evaluating Derivatives: Principles and Techniques of Algorithmic Differentiations*, SIAM, 2008

[2] B. Hornfeck, *Algebra*, Walter de Gruyter & Co, Berlin, 1969

[3] L.B. Rall, *The Artihmetic of Differentiation*, University of Wisconsin - Madison, Mathematics Research Center, Technical Summary Report 2688, 1984

[4] E. Study, *Geometrie der Dynamen, Die Zusammensetzung von Kräften und verwandte Gegenstände der Geometrie*, B.G. Teubner, 1903

[5] C. Taylor, *Matlab dual number class (for automatic differentiation)*, https://gist.github.com/chris-taylor/2005955

Theory and Constructive Methods in Representation Theory

I came to Kaiserslautern in summer 2019 from the University of Sydney in Australia and I work in representation theory. I am especially interested in the connections to Lie theory, algebraic geometry, category theory, and combinatorics. Moreover, I work on constructive methods in these fields and I am part of the DFG-Sonderforschungsbereich "Symbolic Tools in Mathematics and their Application" (`https://www.computeralgebra.de/sfb/`) that was recently extended by 4 more years after our successful application involving 21 project leaders from 6 German universities. My work group currently consists of 4 PhD students (Dario Mathiä, Liam Rogel, Johannes Schmitt, and Maria Walch) and 3 Master's students (Fabian Mäurer, Quang Lê Duc, and Erec Thorn). Some specific topics we are working on are the following:

1. Symplectic singularities. This field is very diverse and we are investigating questions ranging from the minimal model program in algebraic geometry to the representation theory of finite reductive groups. On the constructive side, I am developing a computer algebra package called CHAMP (`https://github.com/ulthiel/Champ`) to explicitly compute invariants in this context, gather data, and test conjectures.

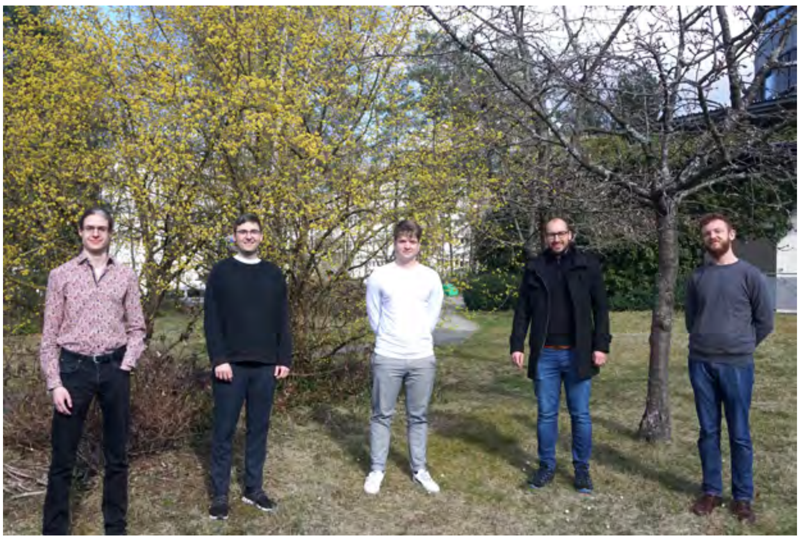
2. Soergel bimodules. The category of these modules and its diagrammatic description yields a combinatorial model of character sheaves on reductive groups. One of our goals is to make this (more) constructive in order to investigate some conjectures. To this end, we also attempt to develop a general framework to constructively work with tensor categories.

3. Cellularity. Cellular algebras have a rich combinatorial structure and arise frequently in representation theory but it is not so clear why cellularity is such a natural property. We are trying to provide an explanation from a categorical perspective.

4. JuLie. A core theme of our SFB is the development of the new computer algebra system OSCAR (`https://oscar.computeralgebra.de`) which is based on the programming language Julia. As a contribution to the OSCAR project—but also because the Julia language and its efficiency convinced me—I have begun to develop a package called JuLie (`https://github.com/ulthiel/JuLie.jl`) which I hope will be the basis for our future developments of constructive methods in representation theory.

5. Autoencoders. This is for us a rather new and interdisciplinary topic where we investigate the generalization capability of unsupervised deep neural networks, in particularly autoencoders, both directly with algebraic topology, as well as more abstractly from a categorical point of view.

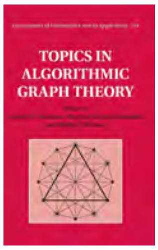
Ulrich Thiel (TU Kaiserslautern)



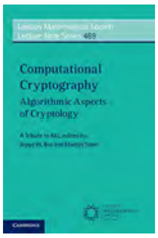
Publikationen über Computeralgebra

Neuerscheinungen:

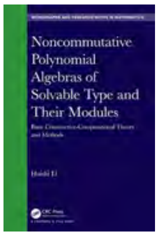
David Asche,
An Introduciton to Groups:
A Computer Illustrated Text,
CRC Press, Boca Raton 2021,
Kindle Edition, 89 Seiten,
ISBN 978-0852743775



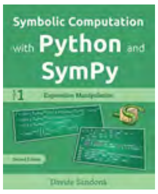
L. Beineke, M. Golumbik, R. Wilson,
Topics in Algorithmic Graph Theory,
Encycl. of Math. and Its Appl. 178,
Cambridge University Press 2021,
380 Seiten,
ISBN 978-1108492607



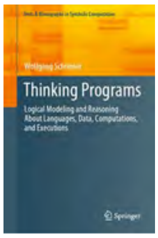
J. Bos, M. Stam (Ed.),
Computational Cryptography:
Algorithmic Aspects of Cryptology,
LMS Lecture Note Series 469,
Cambridge University Press 2021,
400 Seiten,
ISBN 978-1108795937



Huishi Li,
Noncommutative Polyn. Algebras
of Solvable Type and Their Modules:
Basic Constr.-Computational Theory,
CRC Press, Boca Raton 2021,
232 Seiten,
ISBN 978-1032079882



Davide Sandona,
Symbolic Computation
with Python and SymPy,
dsandona.space, 2021,
433 Seiten,
ISBN 979-8489815208



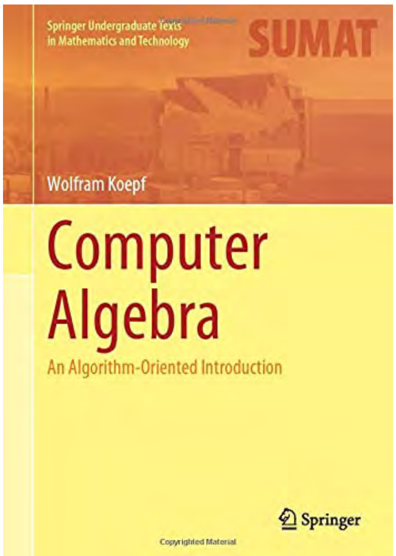
Wolfgang Schreiner,
Thinking Programs,
Texts and Monographs
in Symbolic Computation,
Springer, Cham 2021,
636 + xxxiii Seiten,
ISBN 978-3030805067

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`, `martin.kreuzer@uni-passau.de`) auf.

Besprechungen zu Büchern der Computeralgebra

Wolfram Koepf
Computer Algebra: An Algorithm-Oriented Introduction

Bei diesem Werk handelt es sich um die englische Übersetzung des Buchs [1], das bereits im Computeralgebra-Rundbrief 39 ausführlich besprochen wurde. Da sich diese Übersetzung inhaltlich nicht wesentlich von der deutschen Version unterscheidet, weisen wir hier hauptsächlich auf die Verbesserungen und Ergänzungen hin.



Die Computeralgebra-Sitzungen zum Buch können für drei Computeralgebra-Systeme heruntergeladen werden: Mathematica, Maple und Maxima. Da sich seit dem Erscheinen der deutschen Version 2006 Änderungen bei der Top-Level Sprachen und den eingebunden Funktionspaketen ergeben haben, wurden die expliziten Sitzungen dem jeweils aktuellen Stand der Systeme angepasst. Neben kleineren Korrekturen und Verbesserungen bleibt ein großer Unterschied: die Neuausgabe ist in englischer Sprache verfasst. Angesichts der fortschreitenden Internationalisierung insbesondere der Masterstudiengänge an den deutschen Universitäten ist dies in vielen Fällen sicherlich hilfreich.

Das Buch ist für den Erstkontakt der Studierenden mit der Computeralgebra sehr zu empfehlen, insbesondere wenn man neben der theoretischen Besprechung des Materials Wert auf explizite Computersitzungen und konkrete Beispielberechnungen legt.

Literatur:

[1] W. Koepf, Computeralgebra: Eine algorithmisch orientierte Einführung, Springer-Verlag, Berlin 2006, 528 Seiten.

Martin Kreuzer (Passau)

Promotionen in der Computeralgebra

Jayantha Suranimalee: Linear Algebra over Finitely Generated Fields and Rings
Betreuer: Claus Fieker (Kaiserslautern)
Weiterer Gutachter: Mohamed Barakat (Siegen)
Mai 2021

Abstract: In her thesis Suri generalised several linear algebra algorithms from the rational numbers to number fields and polynomials. In particular, many of those methods are deeply rooted in either the Euclidean structure of $\mathbf{Z}$ (and thus frequently in free modules). Others make use of completions and homomorphic images to avoid intermediate coefficient swell. In particular, Suri covers linear equations and determinants over number fields and over univariate polynomial rings. Key problems to overcome in number fields is that rational reconstruction is much more involved and that modules over the ring of integers are typically not free anymore.

Aslam Ali: Computations in Galois Cohomology
Betreuer: Claus Fieker (Kaiserslautern)
Weiterer Gutachter: Sebastian Pauli (Greensboro, SC)
Juli 2011

Abstract: A central object in class field theory is the second cohomology group with values in either the multiplicative group of the field (local case) or the idel-class group (global case). In either case this involves objects that are intrisically inexact and have to be approximates, which notoriously changes the cohomology. However, also in either case, the cohomology group itself has a well known precise answer: the group in question is always cyclic of the same size as the field degree. The thesis is concerned with constructing cohomologically trivial sub-objects such that the have a finite quotient. As an application Ali then covers computation of Galois groups of local fields.

Nikolaus-Konferenz 2021

Aachen, 10.12. – 11.12.2021

`https://www.math.rwth-aachen.de/Nikolaus2021`

Corona hat es einmal wieder spannend gemacht: Die Wochen und Tage vor der Nikolauskonferenz waren eine Zitterpartie, sicherlich vor allem für den Organisator, Frank Lübeck. Denn der Plan war, die Konferenz voll in Präsenz abzuhalten. Dies gelang auch, obwohl die Delta-Welle der Pandemie noch gut zehn Tage vor der Konferenz ihren Höhepunkt hatte. Zur Konferenzzeit war sie jedoch im Abklingen, und so war eine Präsenzveranstaltung tatsächlich sogar in recht entspannter Atmosphäre möglich, sozusagen im Hiatus zwischen Delta und Omikron. Die Konferenz wurde, um Corona-Jargon zu benutzen, im „2G+"-Modus abgehalten, also Zutritt für vollständig Geimpfte mit zusätzlichem aktuellen negativen Test.

Direkt vor der Nikolaus-Konferenz und ebenfalls in Aachen fanden die Darstellungstage statt, der Übergang zwischen beiden war fast fließend. Es kamen knapp 60 Teilnehmer aus ganz Europa, genauer aus der konvexen Hülle von Irland, Spanien, Polen und Griechenland. Die Nikolaus-Konferenz hatte 16 Vorträge, die von sehr unterschiedlichen Forschungsrichtungen innerhalb der Gruppen- und Darstellungstheorie handelten. Ähnlich wie die Tagung der Fachgruppe Computeralgebra hat auch die Nikolaus-Konferenz das Ziel, Nachwuchswissenschaftlerinnen und -wissenschaftler mit etablierteren zusammenzubringen. Gerade durch das Präsenzformat ist dies sehr gut gelungen. Viele Teilnehmer haben es genossen, endlich wieder auf einer „normalen" Konferenz sein zu dürfen. Ein weiteres Mal hat sich Frank Lübeck als perfekter Organisator erwiesen.

Gregor Kemper (München)

Dagstuhl Seminar 22072 on New Perspectives in Symbolic Computation and Satisfiability Checking

Dagstuhl, 13.02. – 18.02.2022

`www.dagstuhl.de/22072`

Symbolic Computation refers to algorithms for computers to perform symbolic mathematics, usually implemented in Computer Algebra systems. *Satisfiability Checking* refers to algorithms to efficiently check the satisfiability of a logical statement, developed originally for the Boolean domain and implemented in SAT solvers, but later extended to a wide variety of different theories in satisfiability modulo theories (SMT) solvers.

Traditionally, the two communities have been largely disjoint and unaware of the achievements of one another, despite there being strong reasons for them to discuss and collaborate, since they share many central interests. While progress in this direction has been made in recent years, many challenges still remain.

The goal of this Dagstuhl Seminar has been to give a new impulse to the cross-fertilization and collaboration activities that have been established in the last few years. It follows the work in Dagstuhl Seminar 15471, EU Horizon 2020 Grant 712689, and the SC^2 Workshop series it created. Unlike the workshop series, where existing work is presented, this seminar aimed at forging new working groups and collaborations to tackle problems and plan future research, and seeks to broaden the community of researchers working here. The organizers were Erika Abraham, James H. Davenport, Matthew England and Alberto Griggio.

It has been very interesting to see how the two communities get further connected, resulting in mutual influence and concrete collaborations, yielding elegant algorithms that extend the functionalities and improve the scalability of Computer Algebra systems on the one hand and SMT solvers on the other hand.

As Chris Brown observed in his talk *What SAT/SMT Has Taught Me*: "SAT/SMT solvers follow a very different paradigm than algorithms from the computer algebra community. In particular, there is an emphasis on bottom-up, conflict-driven approaches." With other words, SMT solvers typically make smart guesses and in case they detect that the guess was wrong, they exclude generalizations of these wrong guesses from further search. Making "'smart" guesses allows to avoid "uninteresting" parts of the search space, and the generalizations act as puzzle pieces to prove unsatisfiability. This highly effective methodology finds now its ways also into Computer Algebra systems.

(Dagstuhl Seminar 22072)

In the other direction, SMT solving has learned a lot from symbolic computation methods to offer support for checking the satisfiability of real-algebraic problems. For example, the SMT solvers CVC5, SMT-RAT, Yices2.0 and Z3 implement SMT-compliant adaptions of e.g. the virtual substitution, the subtropical satisfiability and the cylindrical algebraic decomposition methods.

The seminar took place in a hybrid mode, as due to the pandemic not all invitees were able to travel. With 16 physical and 23 online participants, the program needed to be fixed in advance, under consideration the different time zones of the online presenters. Whereas interaction with the online participants was naturally restricted, the physical participants enjoyed the wonderful Dagstuhl infrastructure to strengthen existing and initiate new collaborations.

Erika Abraham (Aachen)

Hinweise auf Konferenzen

Macaulay2 conference

Cleveland, Ohio, USA, 27.05. – 29.05.2022

`math.galetto.org/m2csu`

As a follow-up to the 2020 Macaulay2 @CSU virtual workshop, there will be a Macaulay2 conference at Cleveland State University in Cleveland, OH, from Friday, May 27, to Sunday, May 29, 2022 (conference activities expected to begin Friday afternoon and end late Sunday morning).

The main goal of the conference is to showcase state-of-the-art research in computational commutative algebra, algebraic geometry, and related areas, including (but not limited to) work resulting from the 2020 M2 @CSU workshop. In addition, we hope the conference will provide an ideal forum for the exchange of mathematical ideas in our community. To facilitate social interactions among colleagues, the primary focus will be on in-person participation.

Workshop on Differential Algebra

Leipzig, 06.06. – 08.06.2022

`www.mis.mpg.de/calendar/conferences/2022/difalg22.html`

This workshop is dedicated to interactions between nonlinear algebra and the study of differential equations, with a particular focus on computations and applications. Topics include linear PDE with constant coefficients, algebraic dynamical systems, D-modules, control theory, and the Ritt-Kolchin theory of differential polynomials.

Due to current Corona regulations, on-site participation is limited to 25 participants. The event will be streamed, too. As we have reached the maximum number of on-site participants, registration is possible for online attendance only.

75+80=155 years of commutative algebra

Osnabrück, 13.06. – 17.06.2022

`www.math-conf.uni-osnabrueck.de/8075155-years-of-commutative-algebra`

There will be a school and a conference dedicated to Winfried Bruns and Jürgen Herzog on the occasion of their 75th and 80th birthday in Osnabrück, June 13 -17, 2022.

Confirmed speakers of the school are Jan Draisma (Universität Bern), Alessandro De Stefani (Università di Genova), Martina Juhnke-Kubitzke (Universität Osnabrück), Thomas Kahle (OvGU Magdeburg).

Keynote lectures devoted to the birthdays of Winfried Bruns and Jürgen Herzog are given by Aldo Conca (Università di Genova) and Takayuki Hibi (Osaka University).

EACA 2022

Castellón de la Plana, Spanien, 20.06. – 22.06.2022

`fue.uji.es/en/conferences/EX210386`

The XVII EACA (Encuentro de Álgebra Computacional y Aplicaciones) will be held in Castellón de la Plana, Spain, in June 20–22.

EACA stands for "Encuentros de Álgebra Computacional y Aplicaciones" (Meetings on Computer Algebra and Applications). These meetings are organized by the Spanish "Red Temática de Cálculo Simbólico, Álgebra Computacional y Aplicaciones" (EACA Network on Symbolic Computation, Computer Algebra and Applications). Their purpose is twofold: first, to provide an appropriate meeting point both for researchers specialized in developing these areas and for those who use them in their own research activities; and second, to support and encourage participation by young researchers.

MEGA 2022

Krakau, Polen, 20.06. – 24.06.2022

`mega2022.up.krakow.pl`

The seventeenth MEGA conference 2022 will take place at the Pedagogical University of Cracow during the period June 20-24, 2022. MEGA 2022 is a satellite event of the International Congress of Mathematicians, to be held in St. Petersburg in 2022. At this time, we are working based on the assumption that the conference will take place in person.

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.

CCAAGS-22

Seattle, USA, 27.06. – 01.07.2022

`sites.google.com/view/ccaaggs-22/home`

CCAAGS-22 will bring together researchers working in the creative mixture of combinatorial and computational ideas in applied algebraic geometry.

We will also celebrate Bernd Sturmfels and his contributions to the field on the occasion of his 60th birthday.

ISSAC 2022

Lille, Frankreich, 04.07. – 07.07.2022

`www.issac-conference.org/2022`

The International Symposium on Symbolic and Algebraic Computation (ISSAC) is the premier conference for research in symbolic computation and computer algebra. ISSAC 2022 will be the 47th 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.

All areas of computer algebra and symbolic computation are of interest at ISSAC 2022.

ANTS-XV

Bristol, Vereinigtes Königreich, 08.08. – 12.08.2022

`people.maths.bris.ac.uk/∼jb12407/ANTS-XV`

The ANTS (Algorithmic Number Theory Symposium) meetings, held biannually since 1994, are the premier international forum for the presentation of new research in computational number theory and its applications. They are devoted to algorithmic aspects of number theory, including elementary number theory, algebraic number theory, analytic number theory, geometry of numbers, algebraic geometry, finite fields, and cryptography.

The 15th edition of ANTS will be held at the University of Bristol, from 8 to 12 August, 2022.

SC^2 Workshop 2022

Haifa, Israel, 12.08.2022

`www.sc-square.org/CSA/workshop7.html`

The 7th International Workshop on Satisfiability Checking and Symbolic Computation will be held on August 12, 2022, at Haifa, Israel. It will be a part of International Joint Conference on Automated Reasoning 2022, at FLOC 2022.

ACA 2022

Athen, Griechenland, 15.08. – 19.08.2022

`math.unm.edu/aca.html`

Traditionally, ACA (Applications of Computer Algebra) is organized in scientific sessions covering all foundational aspects and applications of computer algebra. Details about the planned special sessions will become available soon as these become accepted.

ACA2022 is part of SCALE (Symbolic Computation: Algorithms, Learning and Engineering), which takes place 8-26 August 2022, see https://scale.gtu.edu.tr/index.html.

GAMM - 92nd Annual Meeting

Aachen, 15.08. – 19.08.2022

`jahrestagung.gamm-ev.de`

The GAMM Annual Meeting 2022 will be hosted by RWTH Aachen University.

It will take place from 15th until 19th of August in the “Charlemagne”-city of Aachen, located right within the Euregio Rhein-Maas, the heart of Europe.

CASC 2022

Gebze, Türkei, 22.08. – 26.08.2022

`www.casc-conference.org`

The tools of Scientific Computing play an important role in the natural sciences and engineering. Computer Algebra Systems and the underlying algorithms for Symbolic Computation play an increasingly important role within Scientific Computation. The CASC workshop series has been running for over two decades to explore the interaction of these topics, their implementation, and their application.

DMV-Jahrestagung 2022

Berlin, 12.09. – 16.09.2022

`www.mi.fu-berlin.de/dmv2022`

The DMV Annual Meeting 2022 is hosted by the Berlin Mathematics Research Center MATH+ in cooperation with the Department of Mathematics and Computer Science of FU Berlin and will take place during September 12 - 16, 2022, on the Campus of FU Berlin (in presence).

Summer School on Computational Projective Algebraic Geometry

Kaiserslautern, 12.09. – 16.09.2022

`www.computeralgebra.de/summer-school-on-computational-projective-algebraic-geometry`

Anyone interested in the constructive side of algebraic geometry is welcome. The aim of this school is to learn about computational methods in projective algebraic geometry, both theoretical and practical. The lectures are accompanied by exercise sessions with the newly developed computer algebra system OSCAR.

SYNASC 2022

Linz, Österreich, 12.09. – 15.09.2022

`synasc.ro/2022`

SYNASC aims to stimulate the interaction among multiple communities focusing on defining, optimizing and executing complex algorithms in several application areas. The focus of the conference then ranges from symbolic and numeric computation to formal methods applied to programming, artificial intelligence, distributed computing and computing theory. The interplay between these areas, in fact, is essential in the current scenario where economy and society demand for the development of complex, data intensive, trustable and high performant computational systems.

*** Due to the COVID-19 pandemic, SYNASC 2022 will be organized as a hybrid event ***

*** Note that if the general health situation due to the COVID-19 pandemic does not allow for an in-presence event, the symposium will still be held in a remote mode ***

GI-Jahrestagung 2022

Hamburg, 26.09 – 30.09.2022

`informatik2022.gi.de`

Die #INFORMATIK2022 ist die offizielle Jahrestagung der Gesellschaft für Informatik e.V. (GI), der größten Vereinigung der Informatikerinnen und Informatiker im deutschsprachigen Raum und wird jährlich an wechselnden Orten veranstaltet. Die 52. Jahrestagung INFORMATIK 2022 findet vom 26. bis 30.09.2022 in Hamburg als Präsenzveranstaltung statt.

CoCoA - School and Conference on Computational Commutative Algebra

Hue, Vietnam, März 2023

`cocoa.dhsphue.edu.vn`

Die internationale Doktorandenschule und Tagung COCOA 2020 ist aufgrund der Pandemie nochmals verschoben wurden und findet jetzt im März 2023 in Hue (Vietnam) statt.

Computeralgebra-Tagung der Fachgruppe

Hannover, 31.05. – 02.06.2023

`www.fachgruppe-computeralgebra.de`

Über die Tagung der Fachgruppe Computeralgebra im März 2022 haben wir auf Seite 6 ausführlich berichtet. Bereits im kommenden Jahr soll die nächste Tagung aus dieser Reihe stattfinden. Diesmal in Präsenz und zwar in der Pfingstwoche 2023 in Hannover. Weitere Informationen dazu erhalten Sie in den nächsten beiden Ausgaben des Rundbriefs.

Fachgruppenleitung Computeralgebra 2020–2023

Sprecherin:
Prof. Dr. Anne Frühbis-Krüger
Carl-von Ossietzky Universität Oldenburg
Institut für Mathematik
Carl-von-Ossietzky-Straße 11, 26129 Oldenburg
0441 798-3233
`anne.fruehbis-krueger@uni-oldenburg.de`
https://uol.de/anne-fruehbis-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`
https://www.groups.ma.tum.de/algebra/kemper

Vertreterin der GI:
Prof. Dr. Erika Ábrahám
Fachgruppe Informatik
RWTH Aachen University
Ahornstr. 55, 52056 Aachen
0241 80-21242, -22243 (Fax)
`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`
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`
https://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`
https://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`
https://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`
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`
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`
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`
https://staff.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`
https://www.groups.ma.tum.de/algebra/reimers

Vertreterin der GAMM:
Prof. Dr. Eva Zerz
Lehrstuhl für Algebra und Zahlentheorie
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/