März 2024

Computeralgebra Rundbrief

> Ausgabe 74

www.fachgruppe-computeralgebra.de

Computeralgebra-Rundbrief

Nr. 74 März 2024

Inhaltsverzeichnis

Impressum

Der Computeralgebra-Rundbrief wird herausgegeben von der Fachgruppe Computeralgebra der GI in Kooperation mit der DMV und der GAMM (verantwortlicher Redakteur: Dr. Fabian Reimers car@mathematik.de)

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

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

GI (Gesellschaft für Informatik e.V.)
Wissenschaftszentrum
Ahrstr. 45
53175 Bonn
Telefon 0228-302-145
Telefax 0228-302-167
bonn@gi.de
https://gi.de

DMV (Deutsche Mathematiker-Vereinigung e.V.)
Mohrenstraße 39
10117 Berlin
Telefon 030-20377-306
Telefax 030-20377-307
dmv@wias-berlin.de
https://www.mathematik.de

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

Mitteilungen der Sprecher

Liebe Mitglieder der Fachgruppe Computeralgebra,

der 1. April, die Einreichungsfrist zum Dissertationspreis der Fachgruppe Computeralgebra rückt näher! Wie schon in den Mitteilungen der Sprecher im letzten Rundbrief berichtet, vergibt die Fachgruppe Computeralgebra dieses Jahr erstmals einen Preis für eine herausragene Dissertation im Themenbereich der Computeralgebra. Die Ausschreibung befindet sich auf Seite 32 in diesem Rundbrief. Es sind sowohl Selbstbewerbungen als auch Einreichungen durch Betreuende/Gutachtende möglich. Wir freuen uns auf viele interessante Einreichungen!

Auch die Computeralgebra-Tagung 2025 wirft schon ihre Schatten voraus. Diesmal werden wir in Leipzig zu Gast sein und zwar vom 2. bis 4. Juni 2025. Nähere Informationen, wie Webseite, Hauptvortragende und Anmeldeinformationen folgen in der Herbstausgabe des Rundbriefs. Heute möchten wir nur sagen: 'save the date' und 'bitte weitersagen' an den wissenschaftlichen Nachwuchs in Ihrem Umfeld.

Nach diesen kurzen Informationen in eigener Sache, kommen wir auch schon zum Inhalt des Rundbriefs. Diesmal haben wir gleich drei Artikel in der Rubrik "Themen und Anwendungen": Im ersten erfordert eine Fragestellung aus der arithmetischen Geometrie die Entscheidung, ob ein bestimmtes Ideal radikal ist in beliebiger Charakteristik $p > 2$. Der nachfolgende Artikel beschäftigt sich dann mit automatisiertem Beweisen von Aussagen über Identitäten linearer Operatoren mittels Computeralgebra, ehe uns der dritte schließlich in den Themenbereich des Machine Learning (in mathematischem Kontext) mitnimmt. Abgerundet wird diese Ausgabe dann durch einen Artikel in der Rubrik "Neues über Systeme", der sich mit Coinvarianten eine Klasse von Gruppen in Oscar befasst.

Wir wünschen Ihnen eine kurzweilige und anregende Lektüre.

Anne Frühbis-Krüger *Michael Cuntz*

Pappas' Ideal and Radicality Testing over Positive Characteristic

Stefania Trentin (University of Münster)

stefania.trentin96@gmail.com

Introduction

Motivation and definition of Pappas' Ideal

In arithmetic geometry, a field of mathematics at the intersection of algebra, geometry and number theory, special families of algebraic varieties, called Shimura varieties play a central role. One can think of a Shimura variety as a generalization of a modular curve, *i.e.* a moduli space of elliptic curves, in the following sense. It is a classical result, see [10], that elliptic curves over the complex numbers are in bijection with the set of lattices in the complex plane of the form $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$, for $\omega_{1,2} \in \mathbb{C}^\times$. If we consider an isomorphism between two elliptic curves, this translates into a homothety of the corresponding lattices, *i.e.* a transformation $\Lambda \mapsto c\Lambda$ for some $c \in \mathbb{C}^\times$. This means that when we consider elliptic curves up to isomorphism, we can restrict to lattices of the form $\Lambda = \mathbb{Z} \oplus \mathbb{Z}z$, for $z \in \mathbb{C}^\times$ and by swapping $\omega_{1,2}$ if necessary, we can always assume that $\mathrm{Im}(z) > 0$, so that z lies in the complex upper half-plane $\mathbb{H}$. Observe now that the linear algebraic group $\mathrm{PSL}_2(\mathbb{R})$ acts transitively on $\mathbb{H}$ by the Möbius transformation $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) z = \frac{az+b}{cz+d}$ and that the stabilizer of $i \in \mathbb{H}$ with respect to this action is the subgroup $\mathrm{SO}_2(\mathbb{R})$. It follows that the set of complex elliptic curves up to isomorphism, or equivalently the upper half plane $\mathbb{H}$, is in bijection with the quotient $\mathrm{PSL}_2(\mathbb{R})/\mathrm{SO}_2(\mathbb{R})$. The next step in the generalization of this construction would be for example to increase the dimension of the upper half space, or to allow different algebraic groups to act on it. Roughly speaking, these kinds of modifications lead to the definition of a Shimura variety, as a moduli space of isomorphism classes of Abelian varieties (which are a generalization of elliptic curves) equipped with extra structure (as a generalization of the Möbius transform).

The role of Shimura varieties in arithmetic geometry, in particular in the framework of the Langlands program, is a central one. This ambitious web of conjectures aims to find an underlying unifying structure between algebraic geometry, number theory and (harmonic) analysis. The expectation is that representation theory, and in particular representation of cohomology groups of Shimura varieties will serve as a unifying object on which all three disciplines can act, thus providing a common ground. For a nice introduction to Shimura varieties and the Langlands programm see [13].

An interesting family of Shimura varieties are those associated with the action of unitary groups on a Hermitian space $\mathbb{H}_n$, this time over $\mathbb{F}_p$. To each of these Shimura varieties one can associate another moduli space, called Rapoport-Zink space, see [8], which allows a more explicit description and a better understanding of its geometry. However, even some basic properties, such as smoothness or flatness of a given Rapoport-Zink space, still remain open questions in many cases. We focus here on the proof of flatness of the Rapoport-Zink space for the Shimura variety associated to the unitary group of signature $\mathrm{GU}(2,4)$ defined over an algebraically closed field of odd positive characteristic $\overline{\mathbb{F}}_p$. A fundamental result in this direction is due to Pappas [7], who proved that the flatness of our Rapoport-Zink space is equivalent to the following polynomial ideal being radical.

Theorem 1 [7, Sec. 4.16] Let X denote the 6-dimensional generic symmetric matrix with entries in $\mathbb{F}_p[x_{ij}, 1 \leq i \leq j \leq 6]$ with $p > 2$, that is

$$X = \begin{pmatrix} x_{11} & \cdots & x_{11} \\ \vdots & \ddots & \vdots \\ x_{16} & \cdots & x_{66} \end{pmatrix}.$$

Then the Rapoport-Zink space associated to the Shimura variety for $\mathrm{GU}(2,4)$ over $\overline{\mathbb{F}}_p$ is flat if and only if Pappas' ideal

$$J = \langle X^2, \bigwedge^3 X, \mathrm{trace}(X) \rangle,$$

is radical. Here, the right-hand side denotes the ideal of $\mathbb{F}_p[x_{ij}, 1 \leq i \leq j \leq 6]$ generated by the polynomials given by the entries of X^2, the rank-3 minors of X and by its trace.

It is beyond the scope of this article to present the proof of this theorem, so we only refer to the original paper [7, Sec. 4.16]. Roughly speaking, we have seen that Shimura varieties arise from linear algebraic groups, so the appearance of a matrix ideal should not surprise too much. The question whether Pappas' ideal is radical, or equivalently whether the corresponding Rapoport-Zink space is flat, has been open since then and is still unsolved in dimension higher than 6. To overcome this problem, some variants of the Rapoport-Zink space were also introduced in the literature, which ensure flatness.

It is interesting to remark that a similar ideal was already defined and conjectured to be radical by De Concini and Procesi [2] in the context of invariant theory. Consider the GL_n-orbit under conjugation of an $n \times n$ matrix A with $A^2 = 0, \bigwedge^3 A = 0$ and $\bigwedge^2 A \neq 0$ and let $\mathcal{I}$ be the ideal of polynomials which vanish on this orbit. Then $\mathcal{I}$ is by definition radical and the closure of the orbit of A consists of matrices X with $X^2 = 0$ and $\bigwedge^3 X = 0$. In [2] it is conjectured that the ideal $\mathcal{I}$ coincides with the ideal $\mathcal{J}$ generated by the entries of X^2, the rank-3 minors of X and the non-leading coefficients of the characteristic polynomial of X. Since we have $\mathcal{J} \subseteq \mathcal{I} \subseteq \sqrt{\mathcal{J}}$ this is equivalent to $\mathcal{J}$ being radical. It is clear that Pappas' ideal J is just the restriction of $\mathcal{J}$ to the subvariety of symmetric matrices, as the coefficients of the characteristic polynomial of X in degree $\leq n-3$ are generated by the rank-3 minors, and for the coefficient σ_2 of degree $n-2$ the usual identity $\mathrm{tr}(X^2) = \mathrm{tr}(X)^2 - 2\sigma_2(X)$ holds.

Radicality and characteristic: computational algebra meets model theory

Our goal is now to show that Pappas' ideal is radical. This is not a problem if we fix the characteristic p, as there are well-established algorithms [4] to compute the radical of an ideal, and then to compare it with the original ideal. However, our goal is to prove radicality for any choice of $p > 2$. Our first approach was to look at Matsumoto's and Kemper's algorithms see [6], respectively [4], for computing the radical of an ideal in positive characteristic p and try to perform it *symbolically*, that is in some way for all primes at once. However, as both algorithms require considering p-powers of an additional variable in order to compute a basis of the radical, this approach was not suitable to design a proof of radicality independent of p. On the other hand, computing the radical of J would be sufficient to answer our question, but in principle not necessary. In other words, we would content ourselves with developing a radicality testing algorithm just telling us whether J is radical, without necessarily computing the radical, provided that such algorithm is able to work independently on the characteristic, *i.e.* to prove radicality for (almost) all primes p at once.

This may seem quite ambitious, as we know that radicality (or primality) of an ideal usually depends on the characteristic. Consider for example the ideal in $\mathbb{F}_p[x, y]$ generated by the polynomial $x^2 + y^2$. This ideal is radical if and only if $p \neq 2$ (and it is even prime if -1 is not a square modulo p, that is for all $p \not\equiv 1 \mod 4$). We also remark that the same ideal over $\mathbb{C}$ is radical, but not prime. In other words, we have an ideal that is radical over $\mathbb{F}_p$ for almost all primes p as well as over $\mathbb{C}$, and it is not prime for infinitely many primes and in characteristic zero. This is not just a coincidence, but it is actually an easy example of a powerful result from model theory.

Recall that in model theory a *language* consists of all sentences that can be formulated using a given set of symbols. In particular, the language of rings consists of all the statements that can be expressed just using the symbols $+, \cdot, 0, 1$ (see [5] for a detailed explanation). The *compactness theorem*, see [5, Cor. 2.2.10], states that any sentence in the language of rings is true over an algebraically closed field of characteristic zero if and only if it is true over an algebraically closed field of characteristic p for every p *large enough*. We would like to apply this result to the statement "the ideal $J \subset R$ is radical", which is equivalent to the statement "for every $f \in R$, if $f^n \in J$ then $f \in J$". This sentence does not seem to belong to the language of rings, as it requires using the quantifier $\forall$, the full set of natural numbers (for the exponent and the degree of f) and the quantifier $\exists$ as $f \in I$ means "$\exists$ a linear combination of the generators of I that is equal to f". However, the exponent n in the statement above can be bounded by the so-called Noether exponent, which depends on the degree of the generators of J. The degree of f can be bounded in a similar way, so that we do not need the full set of natural numbers. Furthermore, if R is a polynomial ideal, the statement "J is radical" can actually be formulated in an equivalent way without quantifiers, we refer to [1, Sec. 5.1] for a detailed explanation of these results. It follows that for a polynomial ring, the statement can be formulated in the language of rings. The following theorem is then a direct consequence of the compactness theorem.

Theorem 2 [1] An ideal $J \subset \mathbb{C}[x_1, \ldots, x_m]$ is radical if and only if its image modulo p is radical in $\bar{\mathbb{F}}_p[x_1, \ldots, x_m]$ for every p *large enough*.

Equivalently, since finite fields and fields of characteristic zero are perfect, our ideal J is radical over $\mathbb{Q}$ if and only if it is radical over $\mathbb{F}_p$ for large enough p. The theorem above still holds if we substitute radical with prime, see [1]. In our example above we have verified Theorem 2 and its version for prime ideals in the particular case of the ideal $(x^2 + y^2)$.

Theorem 2 gives us some inspiration for designing our radicality testing algorithm. In principle, we can lift J to characteristic zero, simply by considering the same generators as polynomials in $\mathbb{Q}[x_{ij}, 1 \leq i \leq j \leq 6]$, and after testing for radicality over $\mathbb{Q}$ (which can be done by any computer algebra system by computing the radical and comparing it with J) we are reassured that for p large enough Pappas' ideal J is radical. However, the compactness theorem from model theory is highly non-constructive and gives no hint on how to

find a prime P_0 such that for $p > P_0$ radicality in characteristic zero is equivalent to radicality in characteristic p. As our goal is to prove radicality over any $p > 2$, this answer is not completely satisfying as long as we do not have a way to compute P_0. Once we know P_0 we can check in the usual way if J is radical for the remaining (finitely many) primes $p \leq P_0$.

The algorithm

Gröbner bases and dependence on the characteristic

As announced in the previous section, the core idea underlying our algorithm is to find a way to perform all computations in characteristic zero and then move back to positive characteristic, keeping track of the finitely many primes for which this may not hold and which we have to check separately. If model theory gives the theoretical fundament but it is still highly non-constructive, computer algebra provides the concrete tools to completely answer our question. In particular, the key ingredient is the following result on Gröbner bases by Winkler.

Theorem 3 [12, Thm. 1] Let $F = (f_1, \ldots, f_m)^t$ be a finite sequence of polynomials in $\mathbb{Q}[x_1, \ldots, x_n]$ and $G = (g_1, \ldots, g_r)^t$ the normalized reduced Gröbner basis for F in $\mathbb{Q}[x_1, \ldots, x_n]$. Then, for almost all primes p the images $\overline{F} = F \bmod p$ and $\overline{G} = G \bmod p$ exist and $\overline{G}$ is the normalized reduced Gröbner basis for $\overline{F}$ in $\mathbb{F}_p[x_1, \ldots, x_n]$. Moreover, the primes for which $\overline{G}$ is not a Gröbner basis, called *unlucky primes*, are the divisors of the denominators of the coefficients of F and G and of the coefficients of the entries of the polynomial matrices Z and Y such that $G = Z.F$ and $Y.G$, together with R, the Syzygy matrix of G.

Roughly speaking, Winkler's result on the independence of the characteristic of Gröbner basis could be seen as a sort of computational algebra analogon of the compactness theorem, at least for the direction from characteristic zero to characteristic p.

So far we have seen that proving radicality in characteristic zero implies radicality in characteristic p, provided p is large enough. However, we do not have a concrete way to describe what *large enough* actually means. On the other hand, we have a way to compute Gröbner bases of an ideal in $\mathbb{F}_p[x_1, \ldots, x_n]$ simultaneously for almost all primes p, by doing so over $\mathbb{Q}$, and at the same time to produce the (finite) set of primes for which this is not the case. The next step is then to combine these two results by designing an algorithm that checks radicality only using Gröbner bases. If we are able to do so, then we can perform all computations over $\mathbb{Q}$, updating after any Gröbner basis calculation the set U of unlucky primes and finally deduce radicality for all $p \notin U$. Last, we only have to check radicality for the finitely many primes in U.

We need to make precise what we mean by an algorithm checking radicality *only using Gröbner bases*. Indeed, Matsumoto's and Kemper's algorithms for computing the radical of an ideal also rely on Gröbner bases computations only. However, the bases one needs to compute strongly depend on the characteristic p of the coefficient field, as they contain the preimage of the Frobenius map. This is not suitable for our purpose, as we are rather trying to perform all operations *symbolically* by carrying them out over $\mathbb{Q}$. Writing an algorithm that tests radicality of an ideal by using only Gröbner bases is quite a hard task in full generality, nevertheless we can give an *ad-hoc* algorithm for our ideal J. Our strategy is inspired to the primality testing algorithm by Gianni, Trager and Zacharias [3].

In the following proposition we recall some relevant results about the operations that can be performed via Gröbner bases computations, proofs can be found for example in [3, Sec. 3]. These operations will then be allowed for constructing our algorithm.

Lemma 4 Let I be an ideal in $R[x_1, \ldots, x_m]$ and G a Gröbner basis for I with respect to the lexicographic order given by $x_1 > x_2 > \cdots > x_m$.

1. $G \cap R[x_i, \ldots, x_m]$ is a Gröbner basis for the elimination ideal $I \cap R[x_i, \ldots, x_m]$.
2. Consider the quotient map $\pi : R[x_1, \ldots, x_m] \to (R/R \cap I)[x_1, \ldots, x_m]$. Then $\pi(G \setminus G \cap R)$ is a Gröbner basis for $\pi(I)$.
3. Let S be a multiplicatively closed subset of R. Then G is a Gröbner basis for $S^{-1}I$ in the localization $S^{-1}R[x_1, \ldots, x_m]$.
4. For a Gröbner basis G of the ideal $\langle tI, ts - s\rangle \subset R[t, x_1, \ldots, x_n]$ with respect to a monomial order such that $t > x_i$ the set $(G \cap R[x_1, \ldots, x_m])/s$ is a Gröbner basis for the division ideal $(I : s)$.

Our first step for proving that J is radical is to reduce ourselves to solving the same problem for a sequence of polynomial ideals in one variable. This will turn out to be much easier as the resulting univariate ideals will be generated by polynomials of degree at most two. Our strategy is based on the following observation.

Lemma 5 Let I be an ideal in $R[x]$, where R is any commutative ring with unit. Then I is radical if and only if the image of I in $(R/R \cap I)[x]$ is radical. Moreover, if I is radical, then so is the ideal $R \cap I$ in R.

It follows that in order to prove that $J \subset \mathbb{F}_p[x_{11}, \ldots x_{66}]$ is radical we can start for example by inspecting its intersection $J_{12} = J \cap \mathbb{F}_p[x_{12}, x_{13}, \ldots, x_{66}]$. Since computing elimination ideals can be performed via Gröbner bases, we can do this over $\mathbb{Q}$ and then move back to positive characteristic while keeping track of the unlucky primes. If J_{12} is not radical, then by the previous lemma J is not radical either, and we have to stop. Otherwise, to prove that J is radical is equivalent to prove that the image $\overline{J}$ of J in $R_{12}[x_{11}]$ is radical, where $R_{12} = \mathbb{F}_p[x_{12}, \ldots, x_{66}]/J_{12}$. Again, computing the image of an ideal under a quotient map is an operation that can be done via Gröbner bases, hence is allowed in our algorithm. If J_{12} is radical, then the algebra R_{12} is reduced, hence we are confronted with the easier problem

of proving radicality for an ideal in a univariate polynomial ring with reduced coefficient ring. We can apply this reasoning recursively to each variable x_{ij}, so that we obtain the following chain of ideals

$$J_{66} = J \cap \mathbb{F}_p[x_{66}] \subset J_{56} = J \cap \mathbb{F}_p[x_{56}, x_{66}] \subset \cdots \cdots \subset J_{12} = J \cap \mathbb{F}_p[x_{12}, x_{13}, \ldots, x_{66}] \subset J.$$

Our strategy then consists of proving radicality twenty-one times, one for each variable x_{ij}, as follows.

- We start with proving that J_{66} is radical.
- At step ij we know that the previous ideal J_{ij+1} (or J_{i+1i+1} if $j = 6$) is radical, and we prove that the image $\overline{J_{ij}}$ in $R_{ij+1}[x_{ij}]$ is radical, which by Lemma 5 implies that J_{ij} is radical as well. Here again $R_{ij+1} = \mathbb{F}_p[x_{ij+1}, \ldots, x_{66}]/J_{ij+1}$.

So far the algorithm is quite general and can be applied to any polynomial ideal. The challenge is now to prove that the intermediate ideals $\overline{J_{ij}}$ in $R_{ij+1}[x_{ij}]$ are radical, just by using *allowed* Gröbner bases computations. As we are going to see this is not a problem in our case, as the resulting ideals $\overline{J_{ij}}$ will be reduced to principal ideals generated by polynomials of degree at most two.

We start by computing a Gröbner basis for J with respect to the lexicographic order given by $x_{11} > x_{12} > \cdots > x_{66}$. By Theorem 3 we know we can do so by computing a basis for the ideal in $\mathbb{Q}[x_{11}, \ldots, x_{66}]$ obtained by lifting the generators of J. The set of unlucky primes turns out to be $U = \{2, 3\}$. Computations were done using the Mathematical Software SageMath [9] and a complete list of the Gröbner basis elements together with a script for the calculation of the unlucky primes can be found in [11]. Now consider the chain of elimination ideals above. Lemma 4 gives an efficient way to compute a Gröbner basis for each intermediate ideal $\overline{J_{ij}}$, for $p \notin U$. This is given by the image of G_{ij} in $R_{ij+1}[x_{ij}]$, where

$$G_{ij} = (G \cap \mathbb{F}_p[x_{ij}, \ldots, x_{66}]) \setminus (G \cap \mathbb{F}_p[x_{ij+1}, \ldots, x_{66}]).$$

Here by x_{ij+1} we mean again the variable directly after x_{ij} in the lexicographic order. Observe that this set-theoretical intersection does not require computing any basis, hence the set of unlucky primes remains $U = \{2, 3\}$ and the operations above can be done again symbolically for all other primes simultaneously.

For $p \notin U = \{2, 3\}$, we can now inspect the subsets G_{ij}. We observe that these satisfy one of the following.

1. G_{ij} is empty. This is the case for the eight variables $\{x_{35}, x_{45}, x_{55}, x_{26}, x_{36}, x_{46}, x_{56}, x_{66}\}$.
2. G_{ij} contains a linear polynomial in x_{ij}. For $j \leq 4$ one possible linear polynomial is the 3×3 minor of X corresponding to the rows $i, 5, 6$ and the columns $j, 5, 6$, which has leading coefficient $x_{55}x_{66} - x_{56}^2$. The subset G_{15} contains a linear polynomial in x_{15} as well, with leading coefficient x_{16}. This polynomial is given by the entry $(5, 6)$ of X^2.
3. The remaining subsets G_{16} and G_{25} consist of only one polynomial of degree 2.

As we have already announced above, this quite simplifies our quest, as it is an easier problem to prove that a principal ideal or an ideal containing a linear polynomial is radical. We give now the proof for each of the three cases separately.

Proof of the empty case. If G_{ij} is empty this means that the image of J_{ij} in the quotient ring $R_{ij+1}[x_{ij}]$ is zero, or in other words that $J_{ij} = J_{ij+1}$. Since we know that the ideal J_{ij+1} preceding J_{ij} in the chain above is radical, there is nothing to prove.

Proof of the linear case. Consider G_{ij} for $j \leq 4$, together with G_{15}. In these cases G_{ij}, and therefore $\overline{J_{ij}}$ contains a linear polynomial in x_{ij}. However, $\overline{J_{ij}}$ is far from being principal. Our goal is now to reduce to the case of a principal ideal generated by a monic linear polynomial, which is then clearly radical. To do so we can localize at the leading coefficient of the fixed linear polynomial of G_{ij}. Localization does not preserve radicality in general, unless we localize by a non-zero divisor modulo $\overline{J_{ij}}$, compare [11, Lem. 2.15].

To test if an element s is a zero-divisor modulo J one can compare the division ideal $(J : s) = \{f \in \mathbb{F}_p[x_{11}, \ldots, x_{66}] \mid fs \in J\}$ with J. If these ideals coincide then s is not a zero-divisor modulo J. As we have recalled in Lemma 4 it is possible to compute a division ideal via Gröbner bases. Hence, we can again perform computations *symbolically* over $\mathbb{Q}$ and obtain that the leading coefficients of the chosen linear polynomials in the subsets G_{ij} are not zero-divisors modulo $\overline{J_{ij}}$. It follows that radicality is preserved after localizing at these elements, and that the image of $\overline{J_{ij}}$ in the localization contains a linear monic polynomial in x_{ij}. Therefore, it is clearly radical. The set of unlucky primes remains $U = \{2, 3\}$.

Proof of the quadratic case. It remains to discuss the two steps corresponding to the elimination ideals $\overline{J_{25}}$ and $\overline{J_{16}}$. As we have already mentioned, these ideals are principal and generated by a polynomial of degree two. It suffices then to show that the leading coefficients and discriminants of these quadratic polynomials are non-zero divisors modulo J. This implies computing four other Gröbner bases and the corresponding sets of unlucky primes, according to Proposition 3. The set U of unlucky primes becomes quite large in this case and contains forty-two primes ≤ 809. It remains to check radicality for these primes separately, then we obtain that for $p \neq 2$ Pappas' ideal J is radical.

Remarks

As we have seen, the first part of our algorithm is quite generic and can be applied to any polynomial ideal. In order to complete the radicality testing in full generality one needs a *good criterion* for proving radicality of univariate polynomial ideals, which only uses (the same) Gröbner bases for any characteristic. It would be interesting to investigate the existence of such criteria in order to complete the generalization of our algorithm.

As we have already mentioned, the analogon of Theorem 2 holds for prime ideals, too. Observe that

we can give a proof of the "only if" direction just by means of computational algebra. Indeed, the primality testing algorithm by Gianni, Trager and Zacharias [3] only uses Gröbner bases computations which do not depend on the characteristic. By Winkler's theorem, in a similar way as in our algorithm above, we can then perform computations over $\mathbb{Q}$ and deduce primality in positive characteristic for all p outside the finite set U of unlucky primes, that is for all primes $\geq P_0 = \max(U)$. The advantage of this proof is that it gives a concrete way to compute P_0.

Acknowledgments

This article is based on the work in [11, Cpt. 2] which was supported by the ERC Consolidator Grant 770936: *NewtonStrat*.

References

[1] Madeline G. Barnicle, *Uniform Properties of Ideals in Rings of Restricted Power Series*, Bulletin of Symbolic Logic, **28**(2022), no.2.

[2] Corrado de Concini and Claudio Procesi, *Symmetric functions, conjugacy classes and the flag variety*, Inventiones mathematicae **64** (1981) no. 2, pp. 203-219.

[3] Patrizia Gianni, Barry Trager and Gail Zacharias, *Gröbner bases and primary decomposition of polynomial ideals*, Journal of Symbolic Computation, **6** (1988), no.2, pp. 149-167.

[4] Gregor Kemper, *The calculation of radical ideals in positive characteristic*, Journal of Symbolic Computation, **34** (2022), no. 3, pp. 229-238.

[5] David Marker, *Model theory: An introduction*, Springer New York, 2010.

[6] Ryutaro Matsumoto, *Computing the radical of an ideal in positive characteristic*, Journal of Symbolic Computation **32** (2001), pp. 263-271.

[7] George Pappas, *On the arithmetic moduli schemes of PEL Shimura varieties*, Journal of Algebraic Geometry, **9** (2000) no. 3, pp.577-605.

[8] Michael Rapoport and Thomas Zink, *Period Spaces for p-divisible Groups*, Annals of Mathematics, 1996

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

[10] Joseph H. Silverman, *The Arithmetic of Elliptic Curves*, Springer New York, 2009.

[11] Stefania Trentin, *On the Rapoport-Zink space for GU(2,4) over a ramified prime*, Westfälische Wilhelms-Universität Münster (2023)

[12] Franz Winkler, *A p-adic approach to the computation of Gröbner bases*, Journal of Symbolic Computation, **6** (1988), no.2, pp. 287-304.

[13] Alex Youlcis, (2015/09/17) *Shimura Varieties: Motivation*, Hard Arithmetic, `https://ayoucis.wordpress.com/2015/09/17/shimura-varieties-motivation`.

Proving Operator Identities with Computer Algebra

Clemens Hofstadler (University of Kassel)

clemens.hofstadler@mathematik.uni-kassel.de

Introduction

Linear operators play a fundamental role in various branches of mathematics and related disciplines. In linear algebra and geometry, for example, they appear in the form of matrices, representing linear transformations such as coordinate changes. In functional analysis, (bounded) operators on Hilbert spaces, or more generally, operators in operator algebras, serve as essential tools for understanding and manipulating function spaces. Their applications range from the study of integral and differential equations to tasks like filtering and transforming signals in the field of signal processing. In quantum mechanics, linear operators represent physical observables, and the Schrödinger equation involves these operators in describing the evolution of quantum systems.

In this article, we illustrate a framework for automatically proving first-order statements about identities of linear operators with the help of computer algebra methods. In this framework, proving the correctness of operator statements is translated into computations with noncommutative polynomials, which can be automated using dedicated computer algebra software. To this end, we also discuss our SAGEMATH package `operator_gb`[1], which provides precisely this functionality. This article is based on the joint works [13, 3]. We also refer to [11] for further details.

From operator identities to noncommutative polynomials

We illustrate on a classical result about the Moore-Penrose inverse how identities of linear operators can be translated into noncommutative polynomials and how new identities can be derived from computations with these polynomials. We also show how our SAGEMATH package `operator_gb` can be used to automate these polynomial computations.

The Moore-Penrose inverse

The *Moore-Penrose inverse*, originally described by E. H. Moore [17] and later rediscovered by Roger Penrose [19], generalises the notion of the matrix inverse from nonsingular square matrices to all, including rectangular, matrices. The Moore-Penrose inverse of a complex matrix A is the unique matrix B satisfying the four *Penrose identities*

$$\begin{aligned} ABA &= A, & BAB &= B, \\ (AB)^* &= AB, & (BA)^* &= BA. \end{aligned} \tag{1}$$

Here, A^* denotes the Hermitian adjoint of a complex matrix A. Recall that the Hermitian adjoint is a linear map that satisfies

$$(AB)^* = B^*A^*, \qquad (A^*)^* = A, \tag{2}$$

for all complex matrices A and B.

The following is a classical fact about the Moore-Penrose inverse.

Lemma 1 For an invertible matrix A, the Moore-Penrose inverse coincides with A^{-1}.

Proof If B is the Moore-Penrose inverse of A, then

$$B = A^{-1}AB = A^{-1}ABAA^{-1} = A^{-1}AA^{-1} = A^{-1}. \tag{3}$$

At the end of the last century, people realised that matrix identities, or more generally, identities of linear operators, can be modelled by noncommutative polynomials, and that computations like (3) can be automated using algebraic computations involving such polynomials [9, 8, 7], see also [21, 20] for recent work.

Noncommutative Polynomials

In our setting, noncommutative polynomials are elements in a free (associative) algebra $\mathbb{Z}\langle X\rangle$ with integer coefficients and noncommutative indeterminates in a finite set X. More precisely, for a set $X = \{x_1, \ldots, x_k\}$, the free monoid over X is the set $\langle X\rangle$ of all finite words over the alphabet X, including the empty word 1, together with concatenation of words as the monoid operation. The *free algebra* $\mathbb{Z}\langle X\rangle$ over the ring of integers $\mathbb{Z}$ is the set of finite formal sums

$$\mathbb{Z}\langle X\rangle = \left\{ \sum_{w\in\langle X\rangle} c_w w \;\middle|\; c_w \in \mathbb{Z}, c_w = 0 \text{ for almost all } w \right\}$$

[1] available at `https://github.com/ClemensHofstadler/operator_gb`

together with the addition and multiplication

$$\sum_{w\in\langle X\rangle} c_w w + \sum_{w\in\langle X\rangle} d_w w = \sum_{w\in\langle X\rangle} (c_w + d_w)w$$

$$\left(\sum_{u\in\langle X\rangle} c_u u\right)\cdot\left(\sum_{v\in\langle X\rangle} d_v v\right) = \sum_{w\in\langle X\rangle}\sum_{uv=w} (c_u d_v)w.$$

Remark 2 If $X = \{x\}$ is a singleton, then $\langle X\rangle = \{x^n \mid n \in \mathbb{N}\}$ and $\mathbb{Z}\langle X\rangle = \mathbb{Z}[x]$ is simply the ring of univariate (commutative) polynomials. If $|X| > 1$, then $\mathbb{Z}\langle X\rangle$ is a noncommutative ring.

More generally, the free algebra $R\langle X\rangle$ could be defined over any commutative coefficient ring R with unity. For our application, we focus on $R = \mathbb{Z}$.

We consider the elements in $\mathbb{Z}\langle X\rangle$ as *noncommutative polynomials* with coefficients in $\mathbb{Z}$ and monomials in $\langle X\rangle$. Note that indeterminates in $\mathbb{Z}\langle X\rangle$ still commute with coefficients, but not with each other.

Example 3 For $f_1 = xy + x$, $f_2 = x - 2 \in \mathbb{Z}\langle x, y\rangle$, we have $f_1 + f_2 = xy + 2x - 2$ and

$$f_1 f_2 = (xy + x)(x - 2) = xyx - 2xy + xx - 2x,$$
$$f_2 f_1 = (x - 2)(xy + x) = xxy - 2xy + xx - 2x.$$

Note that $f_1 f_2 \neq f_2 f_1$.

For a set of polynomials $F \subseteq \mathbb{Z}\langle X\rangle$, we denote by (F) the *(two-sided) ideal* generated by F, that is,

$$(F) = \left\{ \sum_{i=1}^{d} a_i f_i b_i \;\middle|\; f_i \in F, a_i, b_i \in \mathbb{Z}\langle X\rangle, d \in \mathbb{N} \right\}.$$

A central problem when working with (non)commutative polynomials is the *ideal membership problem*. Given (non)commutative polynomials $f, f_1, \ldots, f_r$, the ideal membership problem asks if f belongs to the ideal generated by $f_1, \ldots, f_r$. In the setting of commutative polynomials, the theory of Gröbner bases [2] allows to decide this problem, using, for example, Buchberger's algorithm [1].

A Gröbner bases theory also exists for noncommutative polynomials in the free algebra. A noncommutative version of Buchberger's algorithm in the free algebra was first developed over coefficient fields [18], and later generalised to other coefficient domains, most notably to $\mathbb{Z}\langle X\rangle$ [16, 14]. In contrast to the commutative case, however, ideal membership of noncommutative polynomials is only semi-decidable. In particular, ideals in the free algebra need not admit a finite Gröbner basis and the noncommutative Buchberger algorithm is, in fact, only an enumeration procedure. This is a consequence of the undecidability of the word problem for semigroups [6, Thm. 4.5], which can be reduced to the ideal membership problem in $\mathbb{Z}\langle X\rangle$, see, for example, [22, Rem. 2.2.12].

More precisely, *verifying* membership of a polynomial in a finitely generated ideal in the free algebra is always possible. For example, the noncommutative analogue of Buchberger's algorithm and the concept of polynomial reduction can be used as such a semi-decision procedure. Such methods to verify noncommutative ideal membership are implemented in different computer algebra systems (see, for example, [15] and references therein) and also in our software package `operator_gb`. However, *disproving* ideal membership in the free algebra is not possible in general.

Translating operator identities into polynomials

If A, B are matrices or operators, then the identity $A = B$ can be identified with the polynomial $a - b \in \mathbb{Z}\langle a, b\rangle$. More generally, identities of composite operators can be translated into noncommutative polynomials by introducing a noncommutative indeterminate for each basic nonzero operator, and by uniformly replacing each operator by the respective indeterminate in the difference of the left- and right-hand side of each identity. Potentially present zero operators are simply replaced by the zero in $\mathbb{Z}\langle X\rangle$.

For example, by introducing indeterminates a, b, a^*, b^* representing the matrices A, B, A^*, B^*, the Penrose identities (1) can be translated into the following polynomials in $\mathbb{Z}\langle a, b, a^*, b^*\rangle$:

$$aba - a, \quad bab - b, \quad b^*a^* - ab, \quad a^*b^* - ba. \tag{4}$$

Note that, here, we used the properties (2) of the Hermitian adjoint to simplify the Penrose identities before translating them into polynomials.

Similarly, the fact that a matrix A is invertible can be encoded via the two noncommutative polynomials

$$aa^{-1} - 1, \qquad a^{-1}a - 1. \tag{5}$$

Remark 4 Here, we have translated the identity matrix into the multiplicative identity 1 in the free algebra. We note that this translation is not always sound! It can happen that, by using this naive translation, wrong statements can be inferred. However, for the example that we consider, one can show that the naive translation is indeed sound. We refer to Remark 6 for a justification and further information.

Proving new identities

With the translation described above, a computation like (3) corresponds to the polynomial statement

$$\begin{aligned} b - a^{-1} = {} & -b(aa^{-1} - 1) - (a^{-1}a - 1)baa^{-1} \\ & + a^{-1}(aba - a)a^{-1} + (a^{-1}a - 1)a^{-1}. \end{aligned} \tag{6}$$

Algebraically, the relation (6) means that the polynomial $b - a^{-1}$ lies in the ideal generated by the polynomials (4) and (5) encoding the assumptions of Lemma 1.

The following result shows that such an ideal membership is equivalent to the correctness of the corresponding statement about linear operators. It follows from the more general Theorem 16. Below, we identify

each identity of operators $S = T$ with the noncommutative polynomial $s - t$ using the translation described previously.

Corollary 5 An identity $P = Q$ of linear operators follows from other identities $S_1 = T_1, \ldots, S_n = T_n$ if and only if the noncommutative polynomial $p - q$ lies in the ideal $(s_1 - t_1, \ldots, s_n - t_n) \subseteq \mathbb{Z}\langle X \rangle$.

Thus, the representation given in (6) immediately yields a proof of Lemma 1. (In fact, essentially the same one that is given below Lemma 1.) Moreover, since the polynomial computation is independent of the concrete operator context, this representation also proves a corresponding statement in every setting where it can be formulated. For example, we immediately obtain an analogous result for elements in arbitrary rings with involution or for bounded linear operators on Hilbert spaces.

Remark 6 In Remark 4, we mentioned that identity matrices (and more generally, identity operators) cannot always be naively translated into 1. In particular, translating different identity operators into the same constant 1 can be problematic, as this leads to a loss of information.

Therefore, identity operators generally have to be treated like any other basic operator, which means introducing a new indeterminate for every identity operator and explicitly representing their algebraic identities in terms of polynomials. In some cases, however, a naive translation of identity operators is possible, as was shown in [5]. For example, when 1 is not contained in the ideal $(s_1 - t_1, \ldots, s_n - t_n)$ generated by the translated assumptions. One can verify that this is the case in our example, justifying our translation in (5).

Automated proof using `operator_gb`

Corollary 5 provides a way to automate proving statements about linear operators by using computer algebra software to verify ideal membership of noncommutative polynomials. Our SAGEMATH package `operator_gb` allows to do this, using a command called `certify`. In particular, the package allows to compute a representation of an ideal element as a linear combination of the generators. This representation serves as a verifiable certificate for the ideal membership and can be considered as a proof of the corresponding operator statement. The package also provides several useful auxiliary functions. For example, to generate the polynomials encoding the Penrose identities, it provides the command `pinv`.

Remark 7 Thus far, our software package only supports computations in the free algebra $\mathbb{Q}\langle X \rangle$. To ensure that the computations are also valid over $\mathbb{Z}\langle X \rangle$, as required by Corollary 5, one has to check whether all coefficients that appear in the computed representation are in fact integers. The `certify` method checks this automatically and issues a warning if necessary. We note that, in all our applications thus far, this has never happened.

```
# load the package
sage: from operator_gb import *

# create free algebra - ai = a^{-1}
sage: R.<a, b, a_adj, b_adj, ai>
....: = FreeAlgebra(QQ)

# generate assumptions
sage: F = pinv(a, b, a_adj, b_adj)
....: + [a*ai - 1, ai*a - 1]

# verify ideal membership of claim
sage: proof = certify(F, b-ai)

Done! Ideal membership of all claims
could be verified!

# print found representation
sage: pretty_print_proof(proof, F)
 b - ai =
 -b*(a*ai - 1) - (ai*a - 1)*b*a*ai
 + ai*(a*b*a - a)*ai + (ai*a - 1)*ai
```

Treating existential statements

The method described in the previous section allows to verify that an operator identity follows from other identities by checking ideal membership of noncommutative polynomials. Despite being useful for proving various nontrivial statements, this technique still has its limitations. Specifically, it does not cover existential statements that arise, for example, when solving operator equations. This type of statement requires an extended approach.

In the following, we discuss how to treat existential statements. As an illustrative example, we consider the following sufficient condition for the existence of the Moore-Penrose inverse of a bounded linear operator on a Hilbert space. Note that the Moore-Penrose inverse in this setting is defined analogously to the matrix case via the Penrose identities (1). Below, A^* denotes the adjoint operator of A.

Lemma 8 Let A be a bounded linear operator on a Hilbert space satisfying $A = A^*$ and $CA^2 = A$ for some operator C. Then, A has a Moore-Penrose inverse.

In the polynomial framework, the only possibility to prove such an existential statement is to derive an explicit expression for the existentially quantified operator. Once such an explicit expression is obtained, the statement can be reformulated as a basic statement concerning identities and treated like in the previous section.

For our example, this means finding an expression for the Moore-Penrose inverse B in terms of A, C and their adjoints such that the Penrose identities (1) hold

modulo the assumptions $A = A^*$ and $CA^2 = A$. Algebraically, this corresponds to finding a polynomial $b = b(a, c, a^*, c^*)$ such that the elements (4), representing the Penrose identities, lie in the ideal generated by

$$a - a^*, \qquad caa - a, \qquad a^*a^*c^* - a^* \tag{7}$$

encoding the assumptions.

Note that we have translated the single identity $CA^2 = A$ into two polynomials. This is because, whenever an identity $S = T$ holds, then so does the adjoint identity $S^* = T^*$.

Using properties of Gröbner bases, it is possible to employ a number of heuristics for finding elements of a certain form in noncommutative polynomial ideals. One such approach involves introducing a dummy variable x for the desired expression b. With this dummy variable, we consider the ideal I generated by the assumptions (in our example given by (7)) and by the identities that b shall satisfy, but with b replaced by x (in our example these are the Penrose identities (4) for x). Every polynomial of the form $x - b'$ in I corresponds to a candidate expression b' for b, and by applying the elimination property of Gröbner bases [4], we can systematically search for such candidate expressions. Our software package offers a user-friendly interface that simplifies the process of searching for expressions of this nature.

```
sage: R.<a,c,a_adj,c_adj,x,x_adj>
....: = FreeAlgebra(QQ)
sage: F = [a-a_adj, c*a*a-a,
....: a_adj*a_adj*c_adj-a_adj]
sage: P = pinv(a, x, a_adj, x_adj)
sage: I = NCIdeal(F + P)
sage: I.find_equivalent_expression(x)

        [...,x - a*c_adj^2,...]
```

Several of the candidate expressions for b found by the heuristic still contain the dummy variable x or its adjoint, and are thus useless. We have omitted them above. However, the polynomial $x - ac^*c^*$ shows that $b = ac^*c^*$ is a desired representation. We use our software to show that b satisfies the Penrose identities under the assumptions (7).

```
sage: MP = a * c_adj * c_adj
sage: MP_adj = c * c * a_adj
sage: claims = pinv(a, MP, a_adj,
....: MP_adj)
sage: proof = certify(F, claims)

Done! Ideal membership of all
claims could be verified!
```

We note that, here, `claims` is a list consisting of four polynomials, one for each of the four Penrose identities. In such cases, `certify` verifies the ideal membership of each element in the list and returns a list, here assigned to `proof`, providing a representation of each polynomial in `claims`.

Based on Corollary 5, this computation proves Lemma 8. The crucial step of this proof was that we could explicitly construct an expression for the existentially quantified operator. We note that it is not a coincidence that we could do this. *Herbrand's theorem* [10], a fundamental result in mathematical logic, states that such an explicit expression always exists and that it can be constructed as a polynomial expression in terms of the basic operators appearing in the statement, provided that the operator statement is indeed true. Thus, by enumerating all such polynomial expressions, we are guaranteed to find an appropriate expression if the considered statement is correct.

Of course, naively enumerating all possible polynomial expressions quickly becomes infeasible. Therefore, it is important to have good heuristics that allow to systematically search for suitable candidate expressions. Our software package implements, apart from the heuristic described above, several such techniques for finding polynomials of special form in noncommutative ideals. We refer to [12] for explanations of these methods and to [3, App. A] for the corresponding commands of the software.

Theoretical foundation

In the following, we describe the theory justifying the computations done in the previous sections. While, in general, our framework allows to treat arbitrary first-order statements about identities of operators, we focus here, for a simpler presentation, on $\forall\exists$*-quasi-identities* (Definition 15). We note that, in practice, most statements can be effectively cast into this specific format. For a presentation of our framework in full generality, see [13].

Modelling operator statements

To formally model statements about linear operators, we consider a subset of many-sorted first-order logic. More precisely, we fix a denumerable set of *object symbols* $\mathbf{Ob} = \{v_1, v_2, \dots\}$ and call a pair $(u, v) \in \mathbf{Ob} \times \mathbf{Ob}$ a *sort*. We also fix a denumerable set of variables $\{x_1, x_2, \dots\}$ as well as, for each sort (u, v), a *zero constant* $0_{u,v}$. Furthermore, we fix a *sort function* σ mapping each variable x to a sort $\sigma(x) \in \mathbf{Ob} \times \mathbf{Ob}$ and each zero constant $0_{u,v}$ to $\sigma(0_{u,v}) = (u, v)$.

Intuitively, variables correspond to basic operators and the zero constants model distinguished zero operators. The images of these symbols under the sort function σ represent their domains and codomains.

Using these basic symbols, we can construct terms and, building upon that, operator statements. Note that the following definition also extends the sort function from variables and constants to terms.

Definition 9 A *term* is any expression that can be built up inductively using the following rules:

1. each variable x is a term of sort $\sigma(x)$;

2. each zero constant $0_{u,v}$ is a term of sort (u, v);

3. if t is a term, then $-t$ is a term of sort $\sigma(-t) \coloneqq \sigma(t)$;

4. if s, t are terms of sort $\sigma(s) = \sigma(t)$, then $s + t$ is a term of sort $\sigma(s + t) \coloneqq \sigma(s)$;

5. if s, t are terms of sort $\sigma(s) = (v, w)$, $\sigma(t) = (u, v)$, then st is a term of sort $\sigma(st) \coloneqq (u, w)$;

Terms are simply all noncommutative polynomial expressions that can be formed from the variables and the zero constants under the restrictions imposed by the sort function. They correspond to all operators that can be formed from the basic operators with the arithmetic operations of addition, negation, and composition.

Definition 10 An *operator statement* is a first-order formula that can be built up inductively using the following rules:

1. if s, t are terms of sort $\sigma(s) = \sigma(t)$, then $s \approx t$ is an operator statement;

2. if φ is an operator statement, then so is $\neg\varphi$;

3. if φ, ψ are operator statements, then so is $\varphi * \psi$ for $* \in \{\vee, \wedge, \to\}$;

4. if φ is an operator statement, then so is $Qx : \varphi$ for any variable x and $Q \in \{\exists, \forall\}$;

We abbreviate a block of consecutive equally quantified variables $Qx_1Qx_2 \dots Qx_k$, with $Q \in \{\exists, \forall\}$, by $Q\boldsymbol{x}$. If a term t or an operator statement φ depends on variables $\boldsymbol{x} = x_1, \dots, x_k$, we also write $t(\boldsymbol{x})$ or $\varphi(\boldsymbol{x})$ respectively to emphasise this dependency.

To assign a meaning to operator statements, we have to specify what we formally mean by a *linear operator*. As it turns out, the setting of *morphisms* in *preadditive semicategories* provides a very natural and general setting for this.

Preadditive semicategories

Linear operators appear in various forms (ring elements, matrices, homomorphisms, etc.). To treat all these different contexts uniformly, we require an algebraic structure that generalises across these settings. To this end, we use concepts from category theory, in particular, that of preadditive semicategories. Preadditive semicategories provide a natural and very general environment for studying linear operators, prescribing only linearity as a structural constraint.

Definition 11 A *semicategory* $\mathcal{S}$ consists of

- a class $\mathrm{Ob}(\mathcal{S})$ of *objects*;

- for every two objects $U, V \in \mathrm{Ob}(\mathcal{S})$, a set $\mathrm{Mor}(U, V)$ of *morphisms* from U to V;

- for every three objects $U, V, W \in \mathrm{Ob}(\mathcal{S})$, a binary operation $\circ\colon \mathrm{Mor}(V, W) \times \mathrm{Mor}(U, V) \to \mathrm{Mor}(U, W)$ called *composition of morphisms*, which is associative;

A semicategory $\mathcal{S}$ is called *preadditive* if every set $\mathrm{Mor}(U, V)$ is equipped with a binary operation $+$, turning it into an abelian group, such that composition of morphisms is bilinear, i.e., $A \circ (B + C) = (A \circ B) + (A \circ C)$ and $(A + B) \circ C = (A \circ C) + (B \circ C)$. The neutral element of the abelian group $\mathrm{Mor}(U, V)$ is called the *zero morphism* from U to V, denoted by $0_{U,V}$.

Remark 12 A (preadditive) semicategory is a (preadditive) category without identity morphisms.

A semicategory can be thought of as a collection of objects, linked by arrows (the morphisms) that can be composed associatively. While the words *object* and *morphism* do not imply anything about the nature of these things, one can intuitively think of objects as sets and of morphisms as maps between these sets. Preadditive semicategories have the additional property that morphisms with the same start and end can be added, yielding an abelian group structure that is compatible with the composition of morphisms.

Statements about linear operators in different settings can be handled uniformly by considering them as statements about morphisms in preadditive semicategories. We provide several examples of common settings that fall within this approach.

Example 13 In the following, R denotes an arbitrary ring (not necessarily with 1).

1. The ring R can be identified as a preadditive semicategory that consists of a single object, say $\mathcal{R}$ for some (arbitrary) symbol $\mathcal{R}$, and morphism set $\mathrm{Mor}(\mathcal{R}, \mathcal{R}) = R$. The abelian group operation on $\mathrm{Mor}(\mathcal{R}, \mathcal{R})$ is given by the addition in R and the composition of morphisms by the multiplication in R. Thus, in this setting, the morphisms are precisely the ring elements.

2. The set $\mathbf{Mat}(R)$ of matrices with entries in R can be considered as a preadditive semicategory by taking as objects the natural numbers $\mathbb{N}$ and letting $\mathrm{Mor}(n, m) = R^{m \times n}$ for all $n, m \in \mathbb{N}$, equipped with matrix addition as the abelian group operation. Composition is given by matrix multiplication. Here, morphisms correspond to matrices with entries in R.

3. The category R-**Mod** of left modules over R is a preadditive semicategory. Here, objects are left R-modules and morphisms are module homomorphisms between left R-modules. As a special case, also K-**Vect**, the category of vector spaces over a field K with K-linear maps as morphisms, is a preadditive semicategory. Note that the objects in these categories form proper classes and not sets.

4. For $K \in \{\mathbb{R}, \mathbb{C}\}$, the category $\mathbf{Hilb}_K$, whose objects are Hilbert spaces over K and whose morphisms are the bounded K-linear maps between these Hilbert spaces, is a preadditive semicategory.

Universal truth of operator statements

An *interpretation* $\mathcal{I}$ allows to interpret an operator statement φ as a statement about morphisms in a preadditive semicategory $\mathcal{S}$. It assigns to each object symbol $u \in \mathbf{Ob}$ an object $\mathcal{I}(u) \in \mathrm{Ob}(\mathcal{S})$ and to each variable x of sort $\sigma(x) = (u, v)$ a morphism $\mathcal{I}(x)\colon \mathcal{I}(u) \to \mathcal{I}(v)$. Each zero constant $0_{u,v}$ is mapped to the zero morphism in the abelian group $\mathrm{Mor}(\mathcal{I}(u), \mathcal{I}(v))$. This ensures that the terms in φ are translated into well-formed morphisms in $\mathcal{S}$. Then, φ can be evaluated to a truth value by interpreting the boolean connectives and the quantifiers like in classical first-order logic, interpreting $\approx$ as the identity in $\mathcal{S}$.

Definition 14 An operator statement φ is *universally true* if φ evaluates to true under all possible interpretations in every preadditive semicategory $\mathcal{S}$.

Note that an interpretation of φ depends implicitly on the sort function σ, and thus, so does the semantic evaluation of φ. An operator statement may be universally true with respect to one sort function but not with respect to another. For instance, statements that hold for square matrices may not hold for rectangular matrices. Therefore, we should only refer to universal truth with respect to a specific sort function. For the sake of brevity, we assume a fixed sort function σ and disregard this dependency in the following.

Definition 15 A $\forall\exists$*-quasi-identity* is an operator statement of the form

$$\forall \boldsymbol{x} \exists \boldsymbol{y} : \bigwedge_{i=1}^{n} s_i(\boldsymbol{x}) \approx t_i(\boldsymbol{x}) \to \bigwedge_{j=1}^{n'} p_j(\boldsymbol{x}, \boldsymbol{y}) \approx q_j(\boldsymbol{x}, \boldsymbol{y}).$$

In the definition of $\forall\exists$-quasi-identities, we also allow degenerate cases without universally or existentially quantified variables, that is, where $\boldsymbol{x} = \emptyset$ or $\boldsymbol{y} = \emptyset$. However, we note that a $\forall\exists$-quasi-identity has to be a sentence, meaning that all variables that appear have to be quantified by a quantifier.

The following theorem characterises the universal truth of $\forall\exists$-quasi-identities by ideal membership of noncommutative polynomials. In the following, we translate each identity $s(\boldsymbol{x}) \approx t(\boldsymbol{x})$ into the noncommutative polynomial $s(\boldsymbol{x}) - t(\boldsymbol{x}) \in \mathbb{Z}\langle \boldsymbol{x} \rangle$ using the translation described in the first section.

Theorem 16 A $\forall\exists$-quasi-identity

$$\forall \boldsymbol{x} \exists \boldsymbol{y} : \bigwedge_{i=1}^{n} s_i(\boldsymbol{x}) \approx t_i(\boldsymbol{x}) \to \bigwedge_{j=1}^{n'} p_j(\boldsymbol{x}, \boldsymbol{y}) \approx q_j(\boldsymbol{x}, \boldsymbol{y}),$$

where $\boldsymbol{y} = y_1, \ldots, y_m$, is universally true if and only if there exist terms $\boldsymbol{z} = z_1(\boldsymbol{x}), \ldots, z_m(\boldsymbol{x})$ depending only on $\boldsymbol{x}$ such that $\sigma(z_k) = \sigma(y_k)$, for all $k = 1, \ldots, m$, and such that the ideal membership

$$p_j(\boldsymbol{x}, \boldsymbol{z}) - q_j(\boldsymbol{x}, \boldsymbol{z}) \in \big(s_1(\boldsymbol{x}) - t_1(\boldsymbol{x}), \ldots, s_n(\boldsymbol{x}) - t_n(\boldsymbol{x})\big)$$

holds in the free algebra $\mathbb{Z}\langle \boldsymbol{x} \rangle$ for all $j = 1, \ldots, n'$.

If a $\forall\exists$-quasi-identity φ contains no existentially quantified variables and $n' = 1$, then Theorem 16 reduces to Corollary 5.

If φ contains existentially quantified variables, we can proceed as follows: To find suitable terms $\boldsymbol{z} = z_1(\boldsymbol{x}), \ldots, z_m(\boldsymbol{x})$ as required by the theorem, we first search for elements of the form $p_j(\boldsymbol{x}, \boldsymbol{z}) - q_j(\boldsymbol{x}, \boldsymbol{z})$ with arbitrary $\boldsymbol{z}$ in the ideal $(s_1(\boldsymbol{x}) - t_1(\boldsymbol{x}), \ldots, s_n(\boldsymbol{x}) - t_n(\boldsymbol{x}))$ and then check *a posteriori* if there is a $\boldsymbol{z}$ among them such that $p_j(\boldsymbol{x}, \boldsymbol{z}) \approx q_j(\boldsymbol{x}, \boldsymbol{z})$ is a well-formed formula for all $j = 1, \ldots, n'$ and such that $\boldsymbol{z}$ is as required by the theorem. We note that this is also the technique we have employed in the second section.

In full generality, the theory developed in [13] allows to treat arbitrary operator statements, leading to a semi-decision procedure for verifying universal truth.

Theorem 17 There is a semi-decision procedure for universal truth of arbitrary first-order operator statements based on verification of ideal memberships in free algebras.

We have used this semi-decision procedure in combination with our software package `operator_gb` to automate the proofs of a variety of statements regrading the Moore-Penrose inverse as part of a case study [3]. Furthermore, our approach has allowed us to generalise different results in operator theory and to discover new theorems, see [11, Sec. 7] for further information.

References

[1] B. Buchberger, *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal*, PhD thesis, University of Innsbruck, Austria, 1965.

[2] T. Becker and V. Weispfenning, *Gröbner bases*, Graduate Texts in Mathematics, Springer, 1993.

[3] K. Bernauer, C. Hofstadler, and G. Regensburger, *How to Automatise Proofs of Operator Statements: Moore-Penrose Inverse; A Case Study*, In Computer Algebra in Scientific Computing, pp. 39–68, 2023.

[4] M. A. Borges and M. Borges, *Gröbner Bases Property on Elimination Ideal in the Noncommutative Case*, In Gröbner Bases and Applications, Cambridge University Press, pp. 323–337, 1998.

[5] C. Chenavier, C. Hofstadler, C. G. Raab, and G. Regensburger, *Compatible rewriting of noncommutative polynomials for proving operator identities*, In Proceedings of ISSAC 2020, pp. 83–90, 2020.

[6] M. Davis, *Computability and Unsolvability*, McGraw-Hill Book Co., Inc., 1958.

[7] J. W. Helton and M. Stankus, *Computer Assistance for "Discovering" Formulas in System Engineering and Operator Theory*, Journal of Functional Analysis, 161:289–363, 1999.

[8] J. W. Helton, M. Stankus, and J. J. Wavrik, *Computer simplification of formulas in linear systems theory*, IEEE Transactions on Automatic Control, 43(3):302–314, 1998.

[9] J. W. Helton and J. J. Wavrik, *Rules for computer simplification of the formulas in operator model theory and linear systems*. In Nonselfadjoint operators and related topics, pp. 325–354. Springer, 1994.

[10] J. Herbrand, *Recherches sur la théorie de la démonstration*, PhD thesis, University of Paris, France, 1930.

[11] C. Hofstadler, *Noncommutative Gröbner bases and automated proofs of operator statements*, PhD thesis, Johannes Kepler University Linz, Austria, 2023.

[12] C. Hofstadler, C. G. Raab, and G. Regensburger, *Computing elements of certain form in ideals to prove properties of operators*, Mathematics in Computer Science, 16(2):1–19, 2022.

[13] C. Hofstadler, C. G. Raab, and G. Regensburger, Universal truth of operator statements via ideal membership, arXiv preprint, arXiv:2212.11662, 2022.

[14] V. Levandovskyy, T. Metzlaff, and K. Abou Zeid, *Computation of free non-commutative Gröbner bases over $\mathbb{Z}$ with* SINGULAR:LETTERPLACE, In Proceedings of ISSAC 2020, pp. 312–319, 2020.

[15] V. Levandovskyy, H. Schönemann, and K. Abou Zeid, LETTERPLACE – *a Subsystem of* SINGULAR *for Computations with Free Algebras via Letterplace Embedding*, In Proceedings of ISSAC 2020, pp. 305–311, 2020.

[16] A. A. Mikhalev and A. A. Zolotykh, *Standard Gröbner-Shirshov Bases of Free Algebras Over Rings, I: Free Associative Algebras*, International Journal of Algebra and Computation, 8(06):689–726, 1998.

[17] E. H. Moore, *On the reciprocal of the general algebraic matrix*, Bulletin of the American Mathematical Society, 26:294–295, 1920.

[18] F. Mora, *Gröbner bases for non-commutative polynomial rings*, In International Conference on Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes, pp. 353–362, 1985.

[19] R. Penrose, *A generalized inverse for matrices*, Mathematical Proceedings of the Cambridge Philosophical Society, 51:406–413, 1955.

[20] C. G. Raab, G. Regensburger, and J. Hossein Poor, *Formal proofs of operator identities by a single formal computation*, Journal of Pure and Applied Algebra, 225(5):106564, 2021.

[21] L. Schmitz and V. Levandovskyy, *Formally Verifying Proofs for Algebraic Identities of Matrices*, In Intelligent Computer Mathematics, pp. 222–236, 2020.

[22] X. Xiu, *Non-commutative Gröbner bases and applications*, PhD thesis, University of Passau, Germany, 2012.

The ML4Maths Pipeline

Sara Veneziale, Imperial College London

s.veneziale21@imperial.ac.uk

Introduction

Pattern recognition has been at the core of mathematical discovery for centuries, perhaps most famously the conjecture of the Prime Number Theorem by Gauss. Increases in computational efficiency have lead mathematicians to enlist the help of computers in performing experiments which drive conjecture formulation, for example the Birch and Swinnerton-Dyer Conjecture in the 1960s [6]. These computer assisted experiments have led to a growth in interest and availability of big datasets of mathematical objects; see [9, 2, 29, 13].

The increase in development and use of computational tools in pure mathematics is complemented by a new emerging methodology that studies mathematical objects using tools from data analysis and machine learning (ML) [17, 39]. Such methods have been widely applied in the natural sciences, but have been rather underutilised in pure mathematics.

In this note, we will explore two ways in which machine learning tools can be useful to mathematicians. Firstly, being able to build high-accuracy machine learning models can lead to the formulation of conjectures, which can be subsequently proven employing specialist domain knowledge. This approach can be thought of as accelerating the usual pattern recognition that has always driven pure mathematics research, since machine learning algorithms can process tens of thousands more examples than humans in a fraction of the time. Secondly, machine learning models can supercharge data-driven and computational processes. As things stand, many steps in computational pipelines are 100% accurate but impossibly slow. Machine learning methods can be orders of magnitude faster and retain very high accuracy, making computationally expensive questions accessible and guiding the discovery of new results.

We outline the main steps involved in this process: ensuring a mathematical question is amenable to these methods, gathering the correct data, and building the machine learning model. These steps could be described as the *ML4Maths pipeline*. We note that this pipeline has the potential of being widely applicable to a variety of areas of mathematics, and we demonstrate its power by means of a concrete example in algebraic geometry on detecting terminal singularities for toric Fano varieties; see [16]. Whilst we concentrate on how machine learning methods can unlock conjecture generation and bypass expensive computational routines, we remark that there are other promising applications that we will not touch upon. For example machine learning can be used for constructing examples of certain objects [5], exhibiting counterexamples to conjectures [38], or accelerating exact computational routines [22, 35]. Finally, all aforementioned approaches are complementary to the idea of using Large Language Models (LLMs), (possibly) in conjunction with formal proof assistant to generate new proofs [41, 24, 36]. This is a fertile new research area, that we will not focus on in this note, since we are more interested in how the working mathematician, who might not have access to big GPU clusters, can benefit from machine learning in their research. In fact, the example we touch upon and the ones we reference often employ classical machine learning architectures, which are relatively low in computational cost compared to LLMs.

ML4Maths pipeline

The main steps of this so-called *ML4Maths pipeline* described above are outlined in Figure 1.

The first step is formulating an appropriate mathematical question, such as whether machine learning can detect a certain property or whether it is able to figure out a relationship between various mathematical invariants. The core of using a machine learning approach to answer such a question is *data*. This workflow is particularly effective for those problems for which one is able to generate many distinct examples, where we lack a general understanding: there are many such questions, but it is important to note that not all problems will have this feature. Data could be already available (as remarked in the Introduction, there are already many big mathematical datasets), or it might be necessary to create it from scratch. Here, there is the potential for the question to change, since in order to create a large amount of correct samples, the user might need to impose extra conditions. One must bear in mind that this process can introduce bias. For example, it is important to consider whether the class of objects appearing in the data will be representative of a more general class or whether the way the data is being sampled will influence the analysis results. For these reasons, the data generation step is actually one of the most important steps of this workflow.

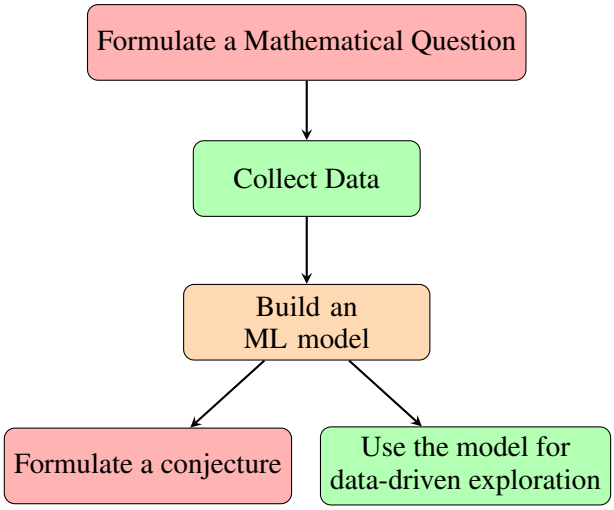


Figure 1: *The steps in the ML4Maths pipeline. Red are mathematical steps, green are computational steps, and yellow is a machine learning step.*

After generating data (or choosing an available dataset), the next step is to train a machine learning model. There are many frameworks to choose from, both within traditional machine learning and deep learning methods. This has become accessible thanks to many well-documented machine learning libraries, such as [33, 34, 1]. In this note, we treat an example where a neural network classifier is used to detect a certain property of algebraic varieties, but this is not the only architecture that has been explored. There are instances of using more traditional machine learning methods like support vector machines, random forest classifiers [14, 12]; reinforcement learning [40, 20, 4]; genetic algorithms [5]; or even data analysis tools that do not require machine learning [21, 30].

Once a model has been successfully trained, there are different directions that can be explored. The model could be used as inspiration to conjecture a new result, which can then be proven using traditional mathematical methods. There have been examples of using *saliency analysis* to understand the importance of the different features in the predictions made by the model [17, 14, 23]. Saliency analysis is a tool to aid in understanding neural networks, which measures which inputs of the network influence the output the most. Moreover, an accurate machine learning model might be useful to accelerate the exploration of large mathematical datasets, taking the place of an expensive computational routine – this will be the focus of our example in the remainder of this note.

The Question and the Data

The mathematical context of the example brought forward is the classification of Fano varieties, the basic building blocks of algebraic geometry [10, 28]. Their classification, which has been an open question since the 1980s, can be thought as building a Periodic Table for geometry [18, 31, 32]. These basic pieces can be hard to study because they are not necessarily smooth and well-behaved. The correct restriction is allowing them to admit mild – but unavoidable – singularities. Namely, such varieties are $\mathbb{Q}$-*factorial* and admit at worst *terminal singularities*, and they are called $\mathbb{Q}$-Fano. Therefore, the mathematical question form [16] (joint work of Tom Coates, Alexander Kasprzyk, and the author) is, **can machine learning track when a Fano variety is $\mathbb{Q}$-Fano?**

To approach any mathematical question with machine learning we need to be able to generate a large amount of data. Generating a correctly labelled dataset to answer this question for *any* Fano variety might be too hard. Hence we restrict to a 'nice' class of varieties, *toric varieties*, which are highly symmetrical and whose geometry is tightly controlled by combinatorics. For toric Fano varieties, checking $\mathbb{Q}$-factoriality is easy, while checking whether they have at worst terminal singularities is an algorithmic but computationally expensive process. To each n-dimensonal toric variety X we can associate a combinatorial object Σ, its *fan*, which is a collection of convex cones in $\mathbb{R}^n$. For X having at worst terminal singularities is equivalent to the cones of Σ containing no lattice points on or under a certain hyperplane. Whilst this criterion is easy to state, it quickly becomes very computationally inefficient when the dimension of the toric variety increases. To put this into perspective, generating the 10 million samples in our dataset of interest took around 30 CPU years using this method. Therefore, we would like to find a criterion that is able to detect whether a toric Fano variety has at worst terminal singularities without constructing the fan and performing lattice point calculations. Our question therefore becomes more specific: **can machine learning track when a $\mathbb{Q}$-factorial toric Fano variety has at worst terminal singularities from its GIT data?**

What do we mean by GIT data? In the case of weighted projective spaces $\mathbb{P}(a_0, \ldots, a_n)$ (which are toric Fano varieties of Picard rank one), the GIT data consists of the weights $(a_0, \ldots, a_n)$ of the action of $\mathbb{C}^\times$ on $\mathbb{C}^{n+1}$,

$$\lambda \cdot (z_0, \ldots, z_n) = (\lambda^{a_0} z_0, \ldots, \lambda^{a_n} z_n)$$

whose geometric quotient $(\mathbb{C}^{n+1} \setminus \{0\})/\mathbb{C}^\times$ is the weighted projective space $\mathbb{P}(a_0, \ldots, a_n)$.

For a general toric Fano of Picard rank r and dimension $N-r$, the GIT data is the integer-valued matrix describing an action $(\mathbb{C}^\times)^r$ on $\mathbb{C}^N$, whose geometric quotient is the variety. In our context, we will concentrate on toric Fano varieties of Picard rank two and dimension eight. The GIT data of these varieties is a 2×10 integer-valued matrix

$$\begin{bmatrix} a_1 & a_2 & \cdots & a_{10} \\ b_1 & b_2 & \cdots & b_{10} \end{bmatrix} \tag{8}$$

which describes the action $(\mathbb{C}^\times)^2$ on $\mathbb{C}^{10}$

$$(\lambda, \mu) \cdot (z_1, \ldots, z_{10}) = (\lambda^{a_1} \mu^{b_1} z_1, \ldots, \lambda^{a_{10}} \mu^{b_{10}} z_{10})$$

Our aim is to detect whether a toric Fano variety has at worst terminal singularities directly from its GIT data,

without constructing the fan and performing the traditional cone-by-cone analysis. To explore this question, we built a balanced dataset of 10 million examples (5 million have at worst terminal singularities and 5 million do not) of $\mathbb{Q}$-factorial toric Fano varieties in dimension eight and Picard rank two [15]. The steps in the sample generation are outlined in Algorithm 1, and they were carried out using MAGMA [7]. The choice of dimension and Picard rank is justified as follows.

- For the Picard rank one case (which in our case of interest is just weighted projective spaces), there already exists an efficient combinatorial criterion that depends only on the GIT data of the weighted projective spaces; see [27].
- In low dimension detecting terminal singularities is easier (e.g. in dimension two it is equivalent to smoothness), however there is not enough data to effectively probe this question with machine learning methods (e.g. in dimension three and Picard rank two there are only 34 examples of interest; see [26]).

Algorithm 1 Generation and insertion of a data sample.

```
status:=Random(True, False).
while No Insertion do
    W:=Random(Weight Matrix in Standard Form).
    Σ:=Fan(W).
    if W is Q-factorial then
        if IsTerminal(Σ) eq status then
            if W is not in dataset then
                Insert W.
            end if
        end if
    end if
end while
```

There are two group actions that change the GIT data but leave the corresponding geometric quotient, i.e. the toric variety, unchanged. Namely, for Picard rank two dimension eight toric varieties, there is an S_{10}-action permuting the columns of (8), and a $\mathrm{GL}_2(\mathbb{Z})$ action reparametrising the torus $(\mathbb{C}^\times)^2$, acting by left multiplication. This is important to consider. In fact, ideally our machine learning terminality criterion will be invariant under these actions. There are many ways of approaching group-invariant and group-equivariant problems in machine learning; see [43, 42, 11, 3]. In this example, instead of choosing a model architecture that is invariant under these group actions, we perform a preprocessing step that transforms each weight matrix into a specific representative of its group orbit. Such representatives are of the form

$$\begin{bmatrix} a_1 & a_2 & \cdots & a_{10} \\ 0 & b_2 & \cdots & b_{10} \end{bmatrix}$$

where the columns are cyclically ordered, $a_i, b_i \in \mathbb{Z}_{\geq 0}$, and $a_{10} < b_{10}$. There are two such representatives for each group orbit, and one preferred one can be chosen by consistently.

Many representations of mathematical objects come equipped with a group action or an equivalence relation on them. Therefore, when applying machine learning tools to mathematical questions it is important to consider whether one should take these symmetries into consideration, either by employing machine learning invariant or equivariant architectures, or applying a suitable preprocessing step.

The Model and the Consequences

Having built a labelled dataset, we are now in a position to train a machine learning model. In this example, we train a multi-layer perceptron (MLP) – a type of neural network – with three hidden layers, taking the flattened weight matrices as input (i.e. an input vector of 20 entries) and outputting a probability (between 0 and 1) of the input having at worst terminal singularities. For a survey on neural networks see [19, 37]. For the purpose of this section, the reader should think of the neural network as a function approximator, whose design depends on many parameters (which are chosen by the user).

The MLP is trained on 5 million samples and predicts terminality with an accuracy of 95% accuracy on the remaining 5 million unseen samples, which are used for testing. It is implemented using PyTorch [33]. This was very surprising. Since it is unlikely that the neural network is able to rebuild the fan structure and perform lattice point counts, this hints that a simpler criterion that detects terminal singularities directly from the GIT data must exist. In fact, floating point arithmetic and data normalisation destroy the integer relations needed to perform lattice point counts.

Having this machine learning model had two direct consequences. First, it inspired a new mathematical result: a new algorithm that detects terminal singularities for a Picard rank two variety given its GIT data (hence without performing any computation using the fan). This algorithm is up to 15 times faster than the original cone-by-cone analysis.

Second, the machine learning model is itself an incredibly efficient (albeit not 100% accurate) method to test terminality. In fact, it is approximately 450 times faster than the original algorithm when tested on a single example. However, it also greatly benefits from batching, so it can be up to 30 000 times faster when testing 10 000 samples at once (we summarise the timing comparisons in Table 1). Therefore, we can use the machine learning model to generate large quantities of data, where the terminality check is performed using the model instead of the traditional method. The result will only be *probable* $\mathbb{Q}$-Fano varieties, but the high accuracy of the model makes this a valuable dataset to visualise the landscape of these objects for preliminary analysis and pattern recognition. In [16], we generated 100 million samples using the machine learning model in order to visualise the approximate picture of the landscape of these objects. This took 120 CPU hours, which is massive gain compared to the original algorithm, with

which it would have taken 300 CPU *years*. While exploring the landscape, we discovered a dependence between the asymptotics of the quantum period and another geometric invariant called the *Fano index*, and we expect this approach to bring even more insight on the Fano classification problem in the future.

This methodology has the potential of being broadly applicable to more general classes of algebraic varieties. In fact, all known smooth Fano varieties are either toric varieties, toric complete intersections, or quiver flag zero loci [25]. It is expected that this might hold in the non-smooth setting as well. The last two classes share with toric varieties the nice property of their structure being highly controlled by combinatorics, which makes them amenable to computer-assisted exploration methods. A promising future research direction is to apply similar methods to detecting singularities for these classes of varieties, which will bring more insight into the structure of these objects, and eventually aid in producing complete sketches of the landscape of Fano varieties.

# Samples	Alg 1	Alg 2	ML
1	1×	15×	450×
10 000	1×	15×	30 000×
100M	300 CPU yrs	20 CPU yrs	120 CPU hrs

Table 1: *Timings comparison for the original algorithm (Alg 1), the new algorithm (Alg 2), and the machine learning model (ML).*

Future Directions

In this note we have explored just one way in which the workflow of integrating mathematical, computational, and machine learning techniques in pure mathematics research can be highly effective. Other areas stand to gain from similar approaches, this being especially true in the context of computer algebra and computational geometry, which are subjects that already have a strong exchange of ideas between pure and computational approaches.

References

[1] M. Abadi, et al. TensorFlow: Large-scale machine learning on heterogeneous systems. Online, 2015. `http://www.tensorflow.org`.

[2] J. Adams, A. Paul, R. Cui, S. Salamanca-Riba, P. Trapa, M. van Leeuwen, and D. Vogan. Atlas of Lie groups and representations. Online, 2016. `http://www.liegroups.org`.

[3] B. Aslan, D. Platt, and D. Sheard. Group invariant machine learning by fundamental domain projections. In *NeurIPS Workshop on Symmetry and Geometry in Neural Representations*, pages 181–218. PMLR, 2023.

[4] G. Bérczi, H. Fan, and M. Zeng. An ML approach to resolution of singularities. In *Topological, Algebraic and Geometric Learning Workshops 2023*, pages 469–487. PMLR, 2023.

[5] P. Berglund, Y.-H. He, E. Heyes, E. Hirst, V. Jejjala, and A. Lukas. New Calabi–Yau manifolds from genetic algorithms. *Physics Letters B*, page 138504, 2024.

[6] B. J. Birch and H. P. F. Swinnerton-Dyer. *Notes on elliptic curves. II.* Walter de Gruyter, Berlin/New York Berlin, New York, 1965.

[7] W. Bosma, J. Cannon, and C. 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).

[8] G. Brown, A. Corti, and F. Zucconi. Birational geometry of 3-fold Mori fibre spaces. In *The Fano Conference*, pages 235–275. Univ. Torino, Turin, 2004.

[9] G. Brown and A. M. Kasprzyk. The graded ring database. Online, 2007–present. `http://www.grdb.co.uk`.

[10] P. Cascini. New directions in the minimal model program. *Boll. Unione Mat. Ital.*, 14(1):179–190, 2021.

[11] S. Chen, E. Dobriban, and J. H. Lee. A group-theoretic framework for data augmentation. *The Journal of Machine Learning Research*, 21(1):9885–9955, 2020.

[12] T. Coates, J. Hofscheier, and A. M. Kasprzyk. Machine learning: The dimension of a polytope. In *Machine Learning in Pure Mathematics and Theoretical Physics*, pages 85–104. World Scientific, 2023.

[13] T. Coates and A. M. Kasprzyk. Databases of quantum periods for Fano manifolds. *Scientific Data*, 9(1):163, 2022.

[14] T. Coates, A. M. Kasprzyk, and S. Veneziale. Machine learning the dimension of a Fano variety. *Nature Communications*, 14(5526), 2023.

[15] T. Coates, A. M. Kasprzyk, and S. Veneziale. A dataset of 8-dimensional $\mathbb{Q}$-factorial Fano toric varieties of Picard rank 2, 2023. doi:10.5281/zenodo.10046893.

[16] T. Coates, A. M. Kasprzyk, and S. Veneziale. Machine learning detects terminal singularities. *Advances in Neural Information Processing Systems*, 36, 2024.

[17] A. Davies, et al. Advancing mathematics by guiding human intuition with AI. *Nature*, 600:70–74, 2021.

[18] P. Del Pezzo. Sulle superficie dell'n^{mo} ordine immerse nello spazio ad n dimensioni. *Rend. del Circolo Mat. di Palermo*, 1:241–255, 1887.

[19] I. Goodfellow, Y. Bengio, and A. Courville. *Deep Learning*. MIT Press, 2016. `http://www.deeplearningbook.org`.

[20] S. Gukov, J. Halverson, C. Manolescu, and F. Ruehle. Searching for ribbons with machine learning. arXiv:2304.09304 [math.GT], 2023.

[21] Y.-H. He, K.-H. Lee, T. Oliver, and A. Pozdnyakov. Murmurations of elliptic curves. arXiv:2204.10140 [math.NT], 2022.

[22] K. Heal, A. Kulkarni, and E. C. Sertöz. Deep learning Gauss–Manin connections. *Advances in Applied Clifford Algebras*, 32(2):24, 2022.

[23] H. Jenne, H. Chau, D. Brown, J. Warley, T. Doster, and H. Kvinge. Can we count on deep learning: Exploring and characterizing combinatorial structures using machine learning. In *The 3rd Workshop on Mathematical Reasoning and AI at NeurIPS'23*, 2023.

[24] A. Q. Jiang, S. Welleck, J. P. Zhou, T. Lacroix, J. Liu, W. Li, M. Jamnik, G. Lample, and Y. Wu. Draft, sketch, and prove: Guiding formal theorem provers with informal proofs. In *The Eleventh International Conference on Learning Representations*, 2023.

[25] E. Kalashnikov. Four-dimensional Fano quiver flag zero loci. *Proc. Royal Society A.*, 475(2225):20180791, 23, 2019.

[26] A. M. Kasprzyk. Toric Fano three-folds with terminal singularities. *Tohoku Math. J. (2)*, 58(1):101–121, 2006.

[27] A. M. Kasprzyk. Classifying terminal weighted projective space. arXiv:1304.3029 [math.AG], 2013.

[28] J. Kollár and S. Mori. *Birational geometry of algebraic varieties*, volume 134 of *Cambridge Tracts in Mathematics*. Cambridge University Press, Cambridge, 1998.

[29] M. Kreuzer and H. Skarke. Complete classification of reflexive polyhedra in four dimensions. *Adv. Theor. Math. Phys.*, 4(6):1209–1230, 2000.

[30] K.-H. Lee. Data-scientific study of Kronecker coefficients. arXiv:2310.17906 [math.RT], 2023.

[31] S. Mori and S. Mukai. Classification of Fano 3-folds with $B_2 \geq 2$. *Manuscripta Math.*, 36(2):147–162, 1981/82.

[32] S. Mori and S. Mukai. Erratum: "Classification of Fano 3-folds with $B_2 \geq 2$". *Manuscripta Math.*, 110(3):407, 2003.

[33] A. Paszke, S. Gross, F. Massa, A. Lerer, J. Bradbury, G. Chanan, T. Killeen, Z. Lin, N. Gimelshein, L. Antiga, et al. Pytorch: An imperative style, high-performance deep learning library, 2019.

[34] F. Pedregosa, et al. Scikit-learn: Machine learning in Python. *Journal of Machine Learning Research*, 12:2825–2830, 2011.

[35] D. Peifer, M. Stillman, and D. Halpern-Leistner. Learning selection strategies in Buchberger's algorithm. In *International Conference on Machine Learning*, pages 7575–7585. PMLR, 2020.

[36] B. Romera-Paredes, et al. Mathematical discoveries from program search with large language models. *Nature*, 625(7995):468–475, 2024.

[37] F. Ruehle. Data science applications to string theory. *Physics Reports*, 839:1–117, 2020.

[38] A. Z. Wagner. Constructions in combinatorics via neural networks. arXiv:2104.14516 [math.CO], 2021.

[39] G. Williamson. Is deep learning a useful tool for the pure mathematician? *Bull. Amer. Math. Soc.*

[40] Y. Wu and J. A. De Loera. Turning mathematics problems into games: Reinforcement learning and Gröbner bases together solve integer feasibility problems. arXiv:2208.12191 [cs.LG], 2022.

[41] K. Yang, A. Swope, A. Gu, R. Chalamala, P. Song, S. Yu, S. Godil, R. J. Prenger, and A. Anandkumar. Leandojo: Theorem proving with retrieval-augmented language models. *Advances in Neural Information Processing Systems*, 36, 2024.

[42] D. Yarotsky. Universal approximations of invariant maps by neural networks. *Constructive Approximation*, 55(1):407–474, 2022.

[43] M. Zaheer, S. Kottur, S. Ravanbakhsh, B. Poczos, R. R. Salakhutdinov, and A. J. Smola. Deep sets. *Advances in Neural Information Processing Systems*, 30, 2017.

Coinvariants of Pseudo-reflection Groups

Johannes Schmitt (Universität Siegen)

johannes2.schmitt@uni-siegen.de

Introduction

Pseudo-reflection groups exhibit many intriguing and often surprising properties, a few of which we want to present here. We focus on the invariant theory – and in particular the coinvariants – of these groups and start out with classical results. We then discuss more recent progress in this area that originated in the context of symplectic singularities. To illustrate these results, we compute examples using the computer algebra system OSCAR.

Pseudo-reflection groups

Throughout this article, let K be a field and V be a K-vector space of finite dimension $n \coloneqq \dim_K(V)$. We assume that $\mathrm{char}(K) = 0$, if not denoted otherwise. In dimension 2 or 3, it is intuitively clear what a 'reflection' on V is supposed to be: it should be a transformation of V that reflects the elements along a given (hyper)plane. Formalizing this idea, we call a matrix $g \in \mathrm{GL}(V)$ a *reflection*, if the fixed space of g is an $(n-1)$-dimensional subspace and if $g^2 = \mathrm{id}_V$. A finite group $G \leq \mathrm{GL}(V)$ is called a *reflection group*, if it is generated by reflections. For example, the dihedral group D_8 of order 8 is the group of symmetries of a square in the plane. As such, it is a reflection group generated by the four reflection symmetries along a vertical, a horizontal and two diagonal lines through the square.

Generalizing the idea of a reflection, we relax the requirement on the order and call an element $g \in \mathrm{GL}(V)$ of finite order a *pseudo-reflection*, if the fixed space of g is an $(n-1)$-dimensional subspace of V. A finite group $G \leq \mathrm{GL}(V)$ is called a *pseudo-reflection group*, if it is generated by pseudo-reflections.

Invariant theory

Invariant theory is a discipline that dates back more than 150 years and lies at the intersection of group theory, representation theory and algebraic geometry. One studies the action of a group $G \leq \mathrm{GL}(V)$ on the ring $K[V]$ of polynomial functions on V which extends the given action of G on V. That is, for $f \in K[V]$ and $g \in G$, we put $(g.f)(v) \coloneqq f(g^{-1}.v)$ for all $v \in V$. Note that after a choice of basis for V and its dual space, the ring $K[V]$ is isomorphic to a polynomial ring $K[x_1, \ldots, x_n]$ and an element $g \in \mathrm{GL}(V) \cong \mathrm{GL}_n(K)$ acts via a linear change of variables. The polynomials left invariant under this action are the *invariants* of G and these invariants form the *invariant ring* $K[V]^G \leq K[V]$. The polynomial ring $K[V]$ is naturally graded by the standard degree of polynomials. As the action of the group G on $K[V]$ is linear, the invariant ring inherits this grading. The ring of *coinvariants* of G is the ring $K[V]^{\mathrm{co}\,G} \coloneqq K[V]/I$ where $I \trianglelefteq K[V]$ is the ideal generated by the invariants of positive degree.

Classical invariant theory was considered finished with two articles by Hilbert in 1890 and 1893 in which he published several foundational theorems in modern algebra – among them the basis theorem and the famous Nullstellensatz. Nevertheless, invariant theory continued to live on and we discuss some of the remarkable discoveries (the last one in preprint from 2024!) in this article.

OSCAR

To conduct our experiments with invariants and coinvariants we use the computer algebra system OSCAR [5]. An introduction to this fairly new system can be found in an earlier issue of this Rundbrief, see [11]. The online documentation

docs.oscar-system.org

gives a detailed overview of the implemented functionality for invariant theory in OSCAR. For more in-depth information on the algorithms and computational invariant theory in general, see the textbook [6]. OSCAR is written in the programming language Julia [1] and the code snippets in the text were copied directly from the Julia (or OSCAR) command line (with some minor formatting to fit the width of the page).

Invariants

Let us enter the dihedral group D_8 mentioned above into OSCAR. This group acts on the plane by reflections, so $V = K^2$. In theory, we would put $K = \mathbb{R}$, but for computational purposes we prefer a field in which precise computations are possible. Indeed, $K = \mathbb{Q}$ suffices in this case and we can construct D_8 via two generating reflections.

```
julia> s1 = QQ[0 1; 1 0]
[0   1]
[1   0]

julia> s2 = QQ[-1 0; 0 1]
[-1   0]
[ 0   1]

julia> D8 = matrix_group(s1, s2)
Matrix group of degree 2
  over rational field
```

The two elements s_1 and s_2 defined above correspond to a reflection of a square centred in the origin of V along a diagonal and a vertical line, respectively. We expect two more reflections in D_8 corresponding to the other two reflection symmetries of the square and indeed:

```
julia> filter(is_pseudo_reflection,
                collect(D8))
4-element Vector{
  MatrixGroupElem{QQFieldElem, QQMatrix}}:
 [0 -1; -1 0]
 [-1 0; 0 1]
 [0 1; 1 0]
 [1 0; 0 -1]
```

The remaining four elements of D_8 correspond to rotational symmetries of the square.

A presentation of the invariant ring

Next, we compute invariants of D_8 in the following sense. The invariant ring $K[V]^G$ of a finite group $G \leq \mathrm{GL}(V)$ is an *affine algebra* by a theorem of Hilbert and Noether. This means that there is an isomorphism of rings $K[V]^G \cong K[y_1, \ldots, y_k]/I$ where $K[y_1, \ldots, y_k]$ is a polynomial ring in k variables and $I \trianglelefteq K[y_1, \ldots, y_k]$ an ideal.

Let us compute such a presentation of the invariant ring of D_8. In OSCAR, we first have to set up the invariant ring as a 'container' or 'context object':

```
julia> RD8 = invariant_ring(D8)
Invariant ring
  of matrix group of degree 2 over QQ
```

No serious computations are done so far, but here comes the promised presentation of $\mathbb{Q}[V]^{D_8}$:

```
julia> A, AtoR = affine_algebra(RD8)
(Quotient of multivariate polynomial ring
  by ideal (0),
 Hom: A -> graded multivariate
  polynomial ring)
```

This returns an affine algebra A with $A \cong \mathbb{Q}[V]^{D_8}$ and an injective morphism $A \to \mathbb{Q}[V]$ with image $\mathbb{Q}[V]^{D_8}$. We examine A in detail:

```
julia> A
Quotient
  of multivariate polynomial ring
  in 2 variables over QQ graded by
    y1 -> [2]
    y2 -> [4]
  by ideal (0)
```

We see that $A = \mathbb{Q}[y_1, y_2]$ is a polynomial ring in two variables and the ideal I is trivial in this case. We come back to the information regarding the grading in a moment.

That I is trivial is not a coincidence, but one of the remarkable properties of pseudo-reflection groups in characteristic 0. Namely, under the assumption $\mathrm{char}(K) = 0$, a finite group $G \leq \mathrm{GL}(V)$ is a pseudo-reflection group if and only if the invariant ring $K[V]^G$ is a polynomial ring, by a theorem of Chevalley, Shephard and Todd [3, 14].

This theorem holds verbatim for fields with $\mathrm{char}(K) = p > 0$, if $p \nmid |G|$, by Serre [13]. However, if $p \mid |G|$, only one implication holds, namely if $K[V]^G$ is a polynomial ring, then G is a pseudo-reflection group. A complete classification of pseudo-reflection groups which do not have a polynomial ring of invariants is given by Kemper and Malle [12].

Degrees

As mentioned in the beginning, the invariant ring $K[V]^G$ is graded by the standard degree since the action of G is linear. We can hence find a generating set of $K[V]^G$ as a K-algebra consisting of homogeneous polynomials. Furthermore, the number and the degrees of the homogeneous polynomials in a generating system of minimal cardinality are unique by a graded version of Nakayama's lemma. Such a generating system is called a system of *fundamental invariants*. The cardinality of a system of fundamental invariants must be at least $n = \dim_K(V)$. This follows from the fact that $K[V]^G \leq K[V]$ is an integral extension and hence $\dim(K[V]^G) = \dim(K[V])$, where $\dim$ denotes the Krull dimension.

Let G be a pseudo-reflection group. Then $K[V]^G$ is a polynomial ring and hence the number of fundamental invariants is exactly $n = \dim_K(V)$. We now want to consider not only the number, but also the the degrees of a system of fundamental invariants. As an example, we consider the symmetric group S_n acting on an n-dimensional vector space V by permuting the variables. The transpositions act as reflections, so S_n is a reflection group in this representation. The reader might already

guess that fundamental invariants of S_n are the elementary symmetric polynomials. This is also what we get in OSCAR when we compute a system of fundamental invariants for $n = 4$ and with coefficients in $K = \mathbb{Q}$.

```
julia> S4 = symmetric_group(4)
Sym(4)

julia> RS4 = invariant_ring(QQ, S4)
Invariant ring
  of Sym(4)

julia> fundamental_invariants(RS4)
4-element Vector{MPolyDecRingElem{...}}:
 x[1] + x[2] + x[3] + x[4]
 x[1]*x[2] + x[1]*x[3] + x[2]*x[3]
  + x[1]*x[4] + x[2]*x[4] + x[3]*x[4]
 x[1]*x[2]*x[3] + x[1]*x[2]*x[4]
  + x[1]*x[3]*x[4] + x[2]*x[3]*x[4]
 x[1]*x[2]*x[3]*x[4]
```

The fundamental invariants are of degrees $d_1 = 1$, $d_2 = 2$, $d_3 = 3$ and $d_4 = 4$. These (unique) numbers are also called the *degrees* of the reflection group. We notice that the product of the degrees coincides with the group order: $1 \cdot 2 \cdot 3 \cdot 4 = 4! = |S_4|$. Further, if we count the reflections, that is, transpositions in S_4, we arrive at $\sum_{i=1}^{3}(4-i)$ and this coincides with the sum $\sum_{i=1}^{4}(d_i - 1)$ in the example.

These identities can be generalized to a theorem about the degrees of a pseudo-reflection group (in characteristic 0, as usual). Namely by [14], for such a group G with degrees $d_1, \ldots, d_n$, we have $d_1 \cdots d_n = |G|$ and $\sum_i (d_i - 1)$ is the number of pseudo-reflections in G.

We already saw this for the dihedral group D_8. We computed that a presentation of $\mathbb{Q}[V]^{D_8}$ is given by:

```
julia> A
Quotient
  of multivariate polynomial ring
  in 2 variables over QQ graded by
    y1 -> [2]
    y2 -> [4]
  by ideal (0)
```

The printed information regarding the grading of A tells us that OSCAR computed fundamental invariants f_1 and f_2 of degree 2 and 4, respectively. Then, $A = \mathbb{Q}[y_1, y_2]$ was endowed with the corresponding grading that makes the morphism $A \to \mathbb{Q}[V]$ given by $y_i \to f_i$ a graded morphism. Coming back to the degrees of D_8, we have $d_1 = 2$ and $d_2 = 4$. With the above formulas, we see that, indeed, $d_1 \cdot d_2 = 8 = |D_8|$ and $(d_1 - 1) + (d_2 - 1) = 4$ is the number of reflections in D_8.

Coinvariants

We now turn to coinvariants of pseudo-reflection groups. Let $f_1, \ldots, f_n \in K[V]^G$ be a system of fundamental invariants for a pseudo-reflection group G. Then the ring of coinvariants of G is the quotient

$$K[V]^{\mathrm{co}\,G} := K[V]/\langle f_1, \ldots, f_n \rangle \ .$$

One sees that $K[V]^{\mathrm{co}\,G}$ is of Krull dimension 0 and hence a finite-dimensional K-vector space.

The regular representation

We start out with computing the dimension of $K[V]^{\mathrm{co}\,G}$ as a vector space for the two groups we had before.

```
julia> coRS4, _ = quo(polynomial_ring(RS4),
       ideal(fundamental_invariants(RS4)))
(Quotient of multivariate polynomial ring
 by ideal with 4 generators, Map: graded
 multivariate polynomial ring -> coRS4)

julia> vector_space_dimension(coRS4)
24

julia> coRD8, _ = quo(polynomial_ring(RD8),
       ideal(fundamental_invariants(RD8)));

julia> vector_space_dimension(coRD8)
8
```

The dimension of $K[V]^{\mathrm{co}\,G}$ coincides with the group order in both cases. This fact, which holds in general for pseudo-reflection groups in characteristic 0, is a first hint of a deeper theorem regarding the structure of $K[V]^{\mathrm{co}\,G}$.

The ring $K[V]^{\mathrm{co}\,G}$ is a non-trivial G-module as the elements of $K[V]^{\mathrm{co}\,G}$ are explicitly not invariant under the action of G. We investigate this further and compute the character of this module for $G = D_8$. To do so, we have to write the action of generators of D_8 as matrices in a fixed vector space basis of $\mathbb{Q}[V]^{\mathrm{co}\,D_8}$. There is no direct way to do this in OSCAR, but all the non-trivial pieces are there, so that we can manage this in a few lines of code.

```
julia> coRD8, RtocoRD8 = quo(
       polynomial_ring(RD8),
       ideal(fundamental_invariants(RD8)));

julia> V, VtocoRD8 =
         vector_space(QQ, coRD8);

julia> reps = dense_matrix_type(QQ)[];

julia> for g in gens(D8)
         M = zero_matrix(QQ, dim(V), dim(V))
         for i in 1:dim(V)
           v = VtocoRD8\(RtocoRD8(
                (RtocoRD8\VtocoRD8(V[i]))^g
               ))
           for j in 1:dim(V)
             M[i, j] = v[j]
           end
         end
         push!(reps, M)
       end
```

Now we build the character χ corresponding to $\mathbb{Q}[V]^{\mathrm{co}\,D_8}$ by taking the traces of these matrices.

```
julia> chi = character(gmodule(D8, reps))
class_function(character table of D8,
  QQAbElem{...}[8, 0, 0, 0, 0])
```

As the reader might already recognize from the values of χ, this is the *regular character* of D_8.

```
julia> chi == regular_character(D8)
true
```

This means that $\mathbb{Q}[V]^{\mathrm{co}\,D_8}$ as a $\mathbb{Q}D_8$-module is the *regular representation* of D_8, that is, $\mathbb{Q}D_8$ as a $\mathbb{Q}D_8$-module. This holds in general due to a theorem by Chevalley [3]: the ring of coinvariants of a pseudo-reflection group G in characteristic 0 gives the regular representation of G. The theorem of Chevalley extends again directly to the case of positive characteristic p, if $p \nmid |G|$.

Doubling up

For the remainder of this article, we assume that $K \leq \mathbb{C}$. In this case, a pseudo-reflection group G is also called a *complex reflection group*. If $K \leq \mathbb{R}$, the group G is a reflection group and also called a *real reflection group* or *Coxeter group*. As we have seen above, we understand the coinvariants of G – they give the regular representation. We now 'double' the action of G and study the coinvariants of this action.

We can embed G into $\mathrm{GL}(V^*)$, where V^* is the dual space of V, and together with the given embedding $G \leq \mathrm{GL}(V)$, we obtain an embedding of G into $\mathrm{GL}(V \oplus V^*)$. We denote the image of this embedding by $G^{\circledast} \leq \mathrm{GL}(V \oplus V^*)$. Notice that G and $G^{\circledast}$ are isomorphic as (abstract) groups. However, in terms of invariant theory, we always work with pairs of a group and a fixed representation, so that the transition from V to $V \oplus V^*$ is far from trivial. These 'doubled-up' actions of a complex reflection group give rise to examples of *symplectic singularities* and research in this context lead to intriguing new results in invariant theory, a few of which we present in the following. For an introduction to symplectic singularities (with a computational focus) see an earlier issue of this Rundbrief [15].

In the beginning, we introduced 'being a pseudo-reflection group' as a property of the group itself. More precisely, this should be seen as a property of a pair (G, V) consisting of a group and a representation. We see that if $G \leq \mathrm{GL}(V)$ is a pseudo-reflection group, then $G^{\circledast} \leq \mathrm{GL}(V \oplus V^*)$ is not. In case $V = K^n$, by definition of the dual representation, an element $g \in G \subseteq \mathrm{GL}_n(K)$ gives rise to the element $\left(\begin{smallmatrix} g & 0 \\ 0 & (g^{-1})^\top \end{smallmatrix}\right) \in G^{\circledast}$. For example, the generating reflections of D_8 from the beginning give rise to elements with fixed space of codimension 2.

```
julia> t1 = diagonal_matrix(s1,
                transpose(inv(s1)))
[0   1   0   0]
[1   0   0   0]
[0   0   0   1]
[0   0   1   0]

julia> t2 = diagonal_matrix(s2,
                transpose(inv(s2)))
[-1   0    0   0]
[ 0   1    0   0]
[ 0   0   -1   0]
[ 0   0    0   1]
```

As a consequence, the invariant ring $K[V \oplus V^*]^{G^{\circledast}}$ is not a polynomial ring and little is known about the structure of $K[V \oplus V^*]^{G^{\circledast}}$ in general. Still, we can say something about the coinvariants.

Haiman's conjecture

We construct the group $D_8^{\circledast}$ and the corresponding ring of coinvariants.

```
julia> D8d = matrix_group(t1, t2);

julia> RD8d = invariant_ring(D8d);

julia> A, _ = quo(polynomial_ring(RD8d),
      ideal(fundamental_invariants(RD8d)));

julia> vector_space_dimension(A)
25
```

Recall that the number of pseudo-reflections in D_8 is $N = 4$, so we have $(N+1)^2 = \dim_{\mathbb{Q}}(\mathbb{Q}[V \oplus V^*]^{\mathrm{co}\,D_8^{\circledast}})$. Presumably, observations like this led Haiman to the following conjecture.

Let G be a Coxeter group, so all pseudo-reflections are of order 2. The *Coxeter number* is defined to be $h := 2N/n$ where N is the number of reflections in G and n the rank of G. Haiman [10] conjectured that

$$\dim_K \left(K[V \oplus V^*]^{\mathrm{co}\,G^{\circledast}}\right) \geq (h+1)^n \qquad (*)$$

and proved this for the symmetric groups. Some years later, Gordon [7] could prove this conjecture for all Coxeter groups using deep arguments involving rational Cherednik algebras.

We just saw that we have an equality in the formula for the dihedral group D_8. However, 'usually', as Gordon puts it, $(h+1)^n$ is only a lower bound for the dimension. The family of dihedral groups can be seen as a subfamily of the complex reflection groups of type $G(m, p, n)$ in the classification by Shephard and Todd [14]. These groups are normal divisors of wreath products $C_m \wr S_n$ where $C_m = \langle \zeta_m \rangle \leq \mathbb{C}^\times$ is the cyclic group of order m generated by a primitive m-th root of unity ζ_m and S_n the symmetric group on n letters. As an example where $(h+1)^n$ is only a lower bound on the dimension of the coinvariants, we consider the group $G = G(2, 2, 4)$. This is a normal subgroup of $C_2 \wr S_4$ of index 2 which can be realized over $K = \mathbb{Q}$ (it is a Coxeter group). Generating reflections are given as follows.

```
julia> r1 = QQ[-1 0 0 0; 0 1 0 0;
               1 0 1 0; 0 0 0 1];

julia> r2 = QQ[1 0 0 0; 0 -1 0 0;
               0 1 1 0; 0 0 0 1];

julia> r3 = QQ[1 0 1 0; 0 1 1 0;
               0 0 -1 0; 0 0 1 1];

julia> r4 = QQ[1 0 0 0; 0 1 0 0;
               0 0 1 1; 0 0 0 -1];

julia> G224 = matrix_group(r1, r2, r3, r4);
```

We determine the Coxeter number of $G(2,2,4)$.

```
julia> N = length(filter(
           is_pseudo_reflection,
           collect(G224)))
12

julia> h = div(2*N, 4)
6
```

This gives the bound $(h+1)^n = 7^4 = 2401$ in Gordon's theorem. To compute the vector space dimension of $\mathbb{Q}[V \oplus V^*]^{\mathrm{co}\, G^{\circledast}}$, we first have to construct the 'doubled' group $G^{\circledast}$.

```
julia> Gd = matrix_group(map(
             g -> diagonal_matrix(g,
                  transpose(inv(g))),
             [r1, r2, r3, r4]));

julia> RG = invariant_ring(Gd)
Invariant ring
  of matrix group of degree 8 over QQ

julia> coRG, _ = quo(polynomial_ring(RG),
       ideal(fundamental_invariants(RG)));

julia> vector_space_dimension(coRG)
2441
```

So, $\dim_{\mathbb{Q}}(\mathbb{Q}[V \oplus V^*]^{\mathrm{co}\, G^{\circledast}}) = 2441 > 2401$ and Gordon's bound is off by (only) 40.

For complex reflection groups

Haiman's conjecture and Gordon's theorem are only concerned with Coxeter groups, but Gordon already expected in [7] that a similar result should hold for more or even all complex reflection groups. However, the first problem already arises in the formulation of the (expected) theorem as one needs to replace the Coxeter number h. Guided by combinatorial considerations, Gordon and Griffeth [8] introduced the *generalized Coxeter number* $h = (N + N^*)/n$ for a complex reflection group where N is the number of pseudo-reflections and N^* the number of distinct reflecting hyperplanes. For a Coxeter group, we have $N = N^*$, so this coincides with the definition given earlier. On the other hand, for example, the two pseudo-reflections $\left(\begin{smallmatrix} \zeta_3 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} \zeta_3^2 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, where ζ_3 is a primitive third root of unity, share the same reflecting hyperplane, so in general we have $N^* \leq N$.

Gordon and Griffeth proved that the lower bound in $(*)$ holds analogously for complex reflection groups with the generalized Coxeter number. As an example, we consider the group $G(5,1,2) = C_5 \wr S_2$. This group is not a Coxeter group as it contains pseudo-reflections of order 5 and accordingly we can only construct it over an extension of $\mathbb{Q}$ containing a fifth root of unity.

```
julia> K, z = cyclotomic_field(5, "z");

julia> r1 = K[z 0; 0 1];

julia> r2 = K[0 1; 1 0];

julia> G512 = matrix_group(r1, r2);
```

We count the pseudo-reflections and distinct hyperplanes.

```
julia> refls = filter(is_pseudo_reflection,
                  collect(G512));

julia> hyperplanes = [ kernel(
         identity_matrix(K, 2) - matrix(g))
         for g in refls ];

julia> N = length(refls)
13

julia> NN = length(unique([
              echelon_form(H)
              for H in hyperplanes ]))
7
```

So, $N = 13$ and $N^* = 7$ which gives $h = 10$ and hence $(h+1)^2 = 121$ as lower bound for the dimension of the doubled coinvariant ring. We compute this dimension.

```
julia> G = matrix_group(map(
             g -> diagonal_matrix(g,
                  transpose(inv(g))),
             [r1, r2]));

julia> RG = invariant_ring(G);

julia> coRG, _ = quo(polynomial_ring(RG),
       ideal(fundamental_invariants(RG)));

julia> vector_space_dimension(coRG)
200
```

We see that 121 is quite a bit off!

In [9], Griffeth considers another (at first glance, straightforward) replacement of the Coxeter number in $(*)$ by taking $g := 2N/n$ instead of the generalized Coxeter number. He proves that the inequality $(*)$ holds for all complex reflection groups with g in place of h. In the example of $G(5,1,2)$, we compute $(g+1)^2 = 14^2 = 196$ which is a much tighter bound for the actual dimension 200 than the one coming from h.

Quaternionic reflections

We have seen that Haiman's conjecture was first proved for 'doubled' real reflection groups and then this result

was generalized to the larger family of 'doubled' complex reflection groups. The latter groups may again be seen as part of an even larger family – the *quaternionic reflection groups*. The definition of a pseudo-reflection group we gave in the beginning can be extended directly to a skew-field K and a left (or right) vector space V. As the name suggests, the quaternionic reflection groups are the pseudo-reflection groups over the skew-field of quaternions $K = \mathbb{H}$. Just like we may consider any real reflection group as a complex reflection group, we can consider a complex reflection group $G \leq \mathrm{GL}(V)$ as a quaternionic reflection group acting on the extension of scalars $V \otimes_{\mathbb{C}} \mathbb{H}$.

Complexification

However, working with quaternionic reflection groups brings some technical complications coming from the non-commutativity of $\mathbb{H}$. The immediate issue for us is that there is no meaningful notion of invariants over $\mathbb{H}$: Extending the action of a quaternionic group G on a left vector space V to an action on $\mathbb{H}[V]$ does in fact not give a well-defined group action as the evaluation of polynomials is not a morphism of rings over a non-commutative coefficient ring. To remedy this problem, we have to consider the quaternionic left vector space V of dimension n as a complex vector space $V|_{\mathbb{C}}$ of dimension $2n$ by restriction of scalars. Doing so induces an embedding $\mathrm{GL}_n(\mathbb{H}) \hookrightarrow \mathrm{GL}_{2n}(\mathbb{C})$ which Cohen [4] dubbed 'complexification'. We refer to [4] for details of this operation and only point out that a complexified quaternionic group in fact turns out to be a subgroup of $\mathrm{Sp}_{2n}(\mathbb{C})$, which is why the quaternionic reflection groups are also called *symplectic reflection groups*.

To come back to the doubled complex reflection groups, let $G \leq \mathrm{GL}(V)$ be a complex reflection group. If we turn G into a quaternionic reflection group by extension of scalars and then complexify the result, we end up with the doubled group $G^{\circledast} \leq \mathrm{GL}(V \oplus V^*)$. This means that in the previous section we actually worked with complexified quaternionic reflection groups.

Proper quaternionic groups

There are quaternionic reflection groups that do not come from complex reflection groups (see [4] for a full classification). Recall that above we considered complex reflection groups of the form $C_m \wr S_n$. These give rise to the complexified quaternionic reflection groups $(C_m \wr S_n)^{\circledast} = C_m^{\circledast} \wr S_n$. Here, $C_m^{\circledast}$ is the subgroup of $\mathrm{SL}_2(\mathbb{C})$ generated by the matrix $\left(\begin{smallmatrix} \zeta_m & 0 \\ 0 & \zeta_m^{-1} \end{smallmatrix}\right)$ where ζ_m is a primitive m-th root of unity. We can construct further quaternionic reflection groups by replacing $C_m^{\circledast}$ by another finite subgroup of $\mathrm{SL}_2(\mathbb{C})$. Let us choose the *binary dihedral group* $\mathsf{D}_m \leq \mathrm{SL}_2(\mathbb{C})$ of order $4m$ which is generated by $C_{2m}^{\circledast}$ together with the matrix $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$. We construct the example $G \coloneqq \mathsf{D}_2 \wr S_3$.

```
julia> K, i = cyclotomic_field(4, "i");

julia> q1 = diagonal_matrix(K[i 0; 0 i^-1],
              identity_matrix(K, 4));

julia> q2 = diagonal_matrix(K[0 -1; 1 0],
              identity_matrix(K, 4));

julia> q3 = K[0 0 1 0 0 0; 0 0 0 1 0 0;
              0 0 0 0 1 0; 0 0 0 0 0 1;
              1 0 0 0 0 0; 0 1 0 0 0 0];

julia> q4 = K[0 0 1 0 0 0; 0 0 0 1 0 0;
              1 0 0 0 0 0; 0 1 0 0 0 0;
              0 0 0 0 1 0; 0 0 0 0 0 1];

julia> G = matrix_group(q1, q2, q3, q4)
Matrix group of degree 6
  over cyclotomic field of order 4
```

This is a complexified quaternionic reflection group of quaternionic rank 3 and order 3072, which does not come from a complex reflection group. The (complexified quaternionic) pseudo-reflections in G are elements with fixed space of codimension 2 due to the complexification operation.

```
julia> quat_refls = filter(
         g -> rank(identity_matrix(K, 6)
                   - matrix(g)) == 2,
         collect(G));

julia> N = length(quat_refls)
45
```

So, G contains 45 quaternionic pseudo-reflections.

Generalizing Haiman's conjecture further

If we simply put the number of pseudo-reflections in G into the inequality $(*)$ using again $2N/n$ for h, we get $(2N/n+1)^n = 31^3 = 29\,791$ on the right hand side. (Notice that $n = 3$ as we need to take the quaternionic rank of G and not the 'complexified' one.)

We compute the left hand side of $(*)$ in our example.

```
julia> RG = invariant_ring(G);

julia> coRG, _ = quo(polynomial_ring(RG),
       ideal(fundamental_invariants(RG)));

julia> vector_space_dimension(coRG)
30148
```

This is only off by 357 from the above lower bound, so barely more than a percent! In January this year, Cartaya and Griffeth [2] published a preprint showing that $(2N/n+1)^n$ gives a lower bound for the dimension of the coinvariant ring of all the complexified quaternionic reflection groups which come as wreath products of rank at least 3. This suggests that Haiman's conjecture can (and maybe should) be seen as a result on quaternionic reflection groups.

However, there are many more infinite families of quaternionic reflection groups in particular in rank 2 for which this generalization of Haiman's conjecture is still

open. In other words: there is still much to discover for pseudo-reflection groups and their (co)invariants.

Acknowledgments

The author is funded by the German Research Foundation (DFG) – project number 286237555 – SFB-TRR 195.

References

[1] J. Bezanson, A. Edelman, S. Karpinski, V. B. Shah, *Julia: A fresh approach to numercial computing*, SIAM Rev. **59** (2017), no. 1, 65–98.

[2] L. Cartaya, S. Griffeth, *Zero fibers of quaternionic quotient singularities*, 2024, preprint, `https://arxiv.org/abs/2402.00158`.

[3] C. Chevalley, *Invariants of finite groups generated by reflections*, Am. J. Math. **77** (1955), 778–782.

[4] A. M. Cohen, *Finite quaternionic reflection groups*, J. Algebra **64** (1980), no. 2, 293–324.

[5] W. Decker, C. Eder, C. Fieker, M. Horn, M. Joswig, *The computer algebra system OSCAR: algorithms and examples*, Springer, 2024.

[6] H. Derksen, G. Kemper, *Computational invariant theory*, Encyclopaedia of Mathematical Sciences, vol. 130, Springer, 2015.

[7] I. Gordon, *On the quotient ring by diagonal invariants*, Invent. Math. **153** (2003), no. 3, 503–518.

[8] I. Gordon, S. Griffeth, *Catalan numbers for complex reflection groups*, Am. J. Math. **134** (2012), no. 6, 1491–1502.

[9] S. Griffeth, *The diagonal coinvariant ring of a complex reflection group*, Algebra Number Theory **17** (2023), no. 11, 2033–2053.

[10] M. Haiman, *Conjectures on the quotient ring by diagonal invariants*, J. Algebra. Comb. **3** (1994), no. 1, 17–76.

[11] M. Horn, *OSCAR: An introduction*, CAR **72** (2023), 16–19.

[12] G. Kemper, G. Malle, *The finite irreducible linear groups with polynomial ring of invariants*, Transform. Groups **2** (1997), no. 1, 57–89.

[13] J.-P. Serre, *Groupes finis d'automorphismes d'anneaux locaux réguliers*, Colloque d'Algèbre (Paris, 1967), Secrétariat mathématique, Paris, 1968, no. 8, 1–11.

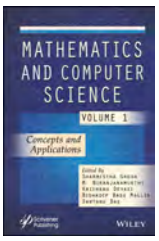
[14] G. C. Shephard, J. A. Todd, *Finite unitary reflection groups*, Canad. J. Math. **6** (1954), 274–304.

[15] U. Thiel, *Symplectic singularities*, CAR **73** (2023), 9–15.

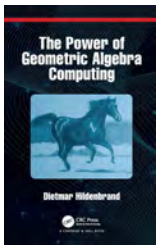
Publikationen über Computeralgebra

Neuerscheinungen:

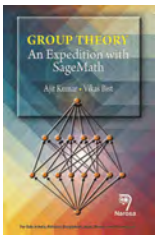
Dirk Colbry,
Matrix Algebra with Computational Applications,
Michigan State Univ.,
Jan. 2021, 446 Seiten,
ISBN 978-1626101074
frei verfügbar



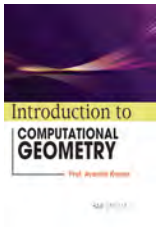
Sharmistha Ghosh et al.,
Mathematics and Computer Science, Vol. 1 und 2,
Wiley - Scrivener,
Jul. 2023, 541+350 Seiten
ISBN 978-1119879671
und 978-1119896326



Dietmar Hildenbrand,
The Power of Geometric Algebra Computing,
Chapman and Hall / CRC,
Sep. 2023, 202 Seiten,
ISBN 978-0367687755

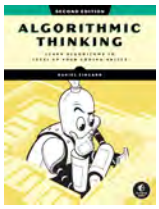


Ajit Kumar, Vikas Bist,
Group Theory: An Expedition with SageMath,
Narosa Publ. House, 2021,
256 Seiten,
ISBN 978-8184877083



Avanish Kumar,
Introduction to Computational Geometry,
Arcler Education Inc.,
Jan. 2024, 252 Seiten,
ISBN 978-1774698471

Daniela Mechkaroska et al.,
Cryptocoding Based on Quasigroups,
Springer, Jan. 2024,
102 Seiten,
ISBN 978-3031501241



Daniel Zingaro,
Algorithmic Thinking, 2nd Edition,
No Starch Press, Jan. 2024,
480 Seiten,
ISBN 978-1718503229

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

Promotionen in der Computeralgebra

Clemens Hofstadler: Noncommutative Gröbner bases and automated proofs of operator statements
Betreuer: Georg Regensburger (Kassel), Clemens G. Raab (Linz)
Weitere Gutachter: Cyrille Chenavier (Limoges)
Oktober 2023

Abstract: Linear operators appear in different forms in various settings all across math- ematics and related disciplines, like engineering or physics. They can be ring elements (as in C^*-algebras), matrices, but also vector space and module homo- morphisms (like (un)bounded operators on Hilbert spaces), or more generally, morphisms in abelian categories. In the thesis, we develop an algebraic framework for automatically proving statements about linear operators by computations with noncommutative poly- nomials. More specifically, arbitrary first-order statements about identities of linear operators can be treated. We present a practical semi-decision procedure for validity of such formulas based on the verification of ideal membership in a free algebra. In contrast to classical approaches for automated theorem prov- ing, these algebraic computations automatically incorporate linearity and they benefit from efficient ideal membership procedures. In particular, we exploit the theory of noncommutative Gröbner bases to verify ideal membership in the free algebra. In order to enhance these computa- tions, we generalise the concept of signature Gröbner bases, originally developed for commutative polynomials, to the free setting, and more generally, to mixed algebras, allowing a mixture of commutative and noncommutative variables. Based on Gröbner basis techniques, we also generalise existing and develop new algorithms for computing elements of specific forms in noncommutative polynomial ideals. These methods serve as one of the key steps in the afore- mentioned semi-decision procedure. Furthermore, we present novel methods for finding short proofs of operator statements, based on the ability to com- pute short certificates of ideal membership. All algorithms are implemented in various software packages for SageMath and Mathematica. We illustrate the capabilities of our framework and software through a case study on statements about the Moore-Penrose inverse, including classical facts and recent results. Furthermore, we showcase that our approach allows to dis- cover new theorems, and we discuss how diagram chases in abelian categories can be automated using our framework.

Stefania Trentin: On the Rapoport-Zink space for GU(2,4) over a ramified prime
Betreuerin: Eva Viehmann (Münster)
Weitere Gutachter: Urs Hartl (Münster), Linus Kramer (Münster)
November 2023

Abstract: In this work, we study the supersingular locus of the Shimura variety associated to the unitary group GU(2, 4) over a ramified prime. We show that the associated Rapoport-Zink space is flat, and we give an explicit description of the irreducible components of the reduction modulo p of the basic locus. In particular, we show that these are universally homeomorphic to either a generalized Deligne-Lusztig variety for a symplectic group or to the closure of a vector bundle over a classical Deligne-Lusztig variety for an orthogonal group. Our results are confirmed in the group-theoretical setting by the reduction method à la Deligne and Lusztig and the study of the admissible set.

Habilitationen in der Computeralgebra

Le Ngoc Long: Zero-Dimensional Schemes and Their Moduli Spaces

Betreuer: Martin Kreuzer (Universität Passau)

Weitere Gutachter: Tobias Kaiser (Universität Passau), Franz Winkler (JKU Linz)

Januar 2024

Abstract: Zero-dimensional schemes in a projective space over a field are important objects in both computer algebra and algebraic geometry. They have been shown to have strong connections with other branches of mathematics such as with singularity theory, coding theory, and algebraic cryptography.

In this thesis, we first look at an important algorithmic task how to check efficiently the structural properties of a zero-dimensional scheme such as the complete intersection, locally/arithmetically Gorenstein and Cayley-Bacharach properties. Using techniques based on the theory of Gröbner bases and the theory of border bases, we provide new characterizations of these properties from which we derive efficient algorithms for checking them.

Secondly, we examine how differential techniques, i.e., techniques based on the structure and module-theoretic properties of Kähler differential modules, can be applied to study the geometric properties of zero-dimensional schemes. In particular, we discuss recent results on the Hilbert functions of the Kähler differential modules of a zero-dimensional scheme, and on differential characterizations of geometric properties like the uniformity and curvilinear properties. Furthermore, we find that the curvilinear property can be checked by calculating the Hilbert function of the Kähler differential algebra instead of having to compute an expensive primary decomposition.

Thirdly, we also investigate how zero-dimensional schemes vary in their moduli spaces. One particularly famous moduli space is the Hilbert scheme $\mathrm{Hilb}^{\mu}(\mathbb{A}^n)$. In an ongoing progress to simplify the representation and understanding of the geometry of this moduli space, one tool which has emerged in the last twenty years is the theory of border basis schemes. These schemes corresponding to order ideals of length μ and form an open affine covering of the Hilbert scheme. In the second part of the thesis, we devise algorithms for computing the defining ideals of subschemes of the border basis scheme parametrizing zero-dimensional schemes having important geometric properties. Moreover, we simplify the defining ideals of certain border basis schemes to allow us to embed them into lower dimensional spaces and study them more efficiently.

Dissertationspreis der Fachgruppe Computeralgebra:

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

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

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

`ca-promotionspreis@mathematik.de`

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

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

Fachgruppe Computeralgebra

Hinweise auf Konferenzen

GAMM - 94th Annual Meeting

Magdeburg, 18.03. – 22.03.2024

jahrestagung.gamm-ev.de

The GAMM Annual Meeting 2024 will be hosted by Otto von Guericke Universität Magdeburg.

It will take place from March 18th to 22nd, 2024 in the "Otto"-City, Magdeburg (Germany).

Submission of Abstracts will be open by October 1st, 2023.

WICA III

Oaxaca, Mexico, 02.06. – 07.06.2024

mathstat.dal.ca/ faridi/WICAIII

The workshop Women in Commutative Algebra III will be held at the BIRS research center located in Oaxaca, Mexico on June 2-7, 2024. Following the model of the first two WICA meetings, this workshop will be entirely dedicated to working on research topics in commutative algebra in a collaborative environment.

Please see the WICA III website for a list of research topics and group leaders in 2024, as well as a link to the application form. If you are interested in participating, please apply by January 30, 2024. We are looking for participants who will have received their PhD by September 2024.

ANTS XVI

Cambridge, MA, USA, 15.07. – 19.07.2024

antsmath.org/ANTSXVI

The ANTS 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 16th edition of ANTS will be held at the Massachusetts Institute of Technology from July 15 to 19 in 2024. Particpants may also be interested in the confrence on the Mordell conecture 100 years later at MIT the preceding week, July 8-12.

ICMS 2024

Durham, Vereinigtes Königreich, 15.07. – 22.07.2024

maths.dur.ac.uk/icms2024/ICMS2024.html

The "International Congress of Mathematical Software" (ICMS) is a bi-annual congress that gathers the mathematicians, scientists and programmers who are interested in the development of mathematical software.

ISSAC 2024

Raleigh, NC, USA, 16.07. – 19.07.2024

www.issac-conference.org/2024

The International Symposium on Symbolic and Algebraic Computation (ISSAC) is the premier conference for research in symbolic computation and computer algebra. ISSAC 2024 will be the 49th meeting in the series, which started in 1966 and has been held annually since 1981. The conference presents a range of invited speakers, tutorials, short communications, software demonstrations and vendor exhibits with a center-piece of contributed research papers.

MEGA 2024

Leipzig, 29.07. – 02.08.2024

mega.sciencesconf.org

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.

MEGA 2024 will take place in MPI, Leipzig, Germany, on 29 July - 2 August, 2024. Mark your calendars!

CASC 2024

Rennes, Frankreich, 02.09. – 06.09.2024

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.

Antrag auf Mitgliedschaft in der Fachgruppe Computeralgebra

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

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

Vorteile einer Mitgliedschaft:

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

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

`https://fachgruppe-computeralgebra.de/aufnahmeantrag`

Fachgruppe Computeralgebra

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

Fachgruppenleitung Computeralgebra 2023–2026

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

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

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

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

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

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

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

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

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

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

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

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

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

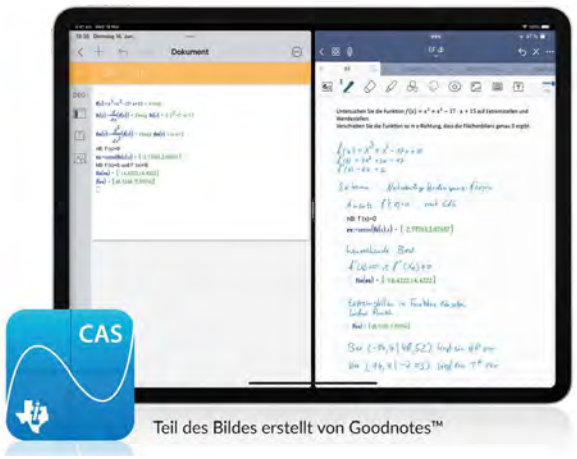
Die TI-Nspire™ CAS App für iPad®

Jetzt UPDATE laden

Für ein riesiges Spektrum an Anwendungen. Für Lernende. Für Lehrende. Für Sie.

Die TI-Nspire™ CAS App für iPad®

- **Vielseitig:** Dynamisch verknüpfte Module
- **Übersichtlich:** Split Screen, Porträtmodus
- **Sicher und einfach:** Der Prüfungsmodus



Lesen Sie hier die komplette Vorteilsliste

education.ti.com/de

Erhältlich im App Store

Texas Instruments