The conjugacy problem in $\mathrm{GL}(n, \mathbf{Z})$

Tommy Hofmann (joint with Bettina Eick & Eamonn O'Brien)

Bordeaux, December 1st, 2020

Saarland University

The conjugacy problem

Dehn's problems (1911)

Let G be a group..

1. [...] (Word problem)
2. Given $g, h \in G$, decide whether g and h conjugated, that is, whether there exists $k \in G$ such that $k^{-1}gk = h$. (*Conjugacy problem*)
3. [...] (Isomorphism problem)

Building block for advanced algorithms in algorithm group theory.

Group based cryptography

- Public key cryptography protocols from "any" group G.
- Security is connected to the hardness of the conjugacy problem in G.

Originally formulated for finitely presented groups, where all three problems are *undecidable*.

The problem

Problem

Let $A, B \in \mathrm{M}_n(\mathbf{Z})$ be matrices over $\mathbf{Z}$. Decide if there exists a matrix $P \in \mathrm{GL}_n(\mathbf{Z}) = \{A \in \mathrm{M}_n(\mathbf{Z}) \mid \det(A) = \pm 1\}$ such that

$$P^{-1}AP = B \quad (\Leftrightarrow \quad AP = PB).$$

Find such a P in case it exists.

Example

Consider

$$A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \quad B = \begin{pmatrix} 5 & -2 \\ -1 & 0 \end{pmatrix}.$$

Do there exist $a, b, c, d \in \mathbf{Z}$ such that

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 5 & -2 \\ -1 & 0 \end{pmatrix} \text{ and } ad - bc = \pm 1?$$

(Or $a, b, c, d, e \in \mathbf{Z}$ with ... and $(ad - bc) \cdot e = 1$).

Conjugacy of matrices over fields

- Over $\mathbf{C}$ we have the *Jordan canonical form*.
- A matrix $A \in \mathrm{M}_n(\mathbf{C})$ is conjugate to a unique matrix of the form

$$\begin{pmatrix} J_1 & & \\ & \ddots & \\ & & J_r \end{pmatrix}, \text{ where } J_i = \begin{pmatrix} \lambda_i & 1 & & & \\ & \lambda_i & 1 & & \\ & & \ddots & \ddots & \\ & & & \lambda_i & 1 \\ & & & & \lambda_i \end{pmatrix} \text{ and } \lambda_i \in \mathbf{C}.$$

- For arbitrary fields, there is the rational normal form (Frobenius normal form).
- Rational normal forms can be efficiently computed.
- Conjugacy problem over fields is solved (in the case the conjugating element is in GL_n)

Conjugacy of matrices over the integers

Now let $A, B \in \mathrm{M}_n(\mathbf{Z})$. We want to decide if there exists $P \in \mathrm{GL}_n(\mathbf{Z})$ with $P^{-1}AP = B$.

- It is necessary that there exists $P \in \mathrm{GL}_n(\mathbf{Q})$ with $A = P^{-1}BP$.
- This is not sufficient:

$$\begin{pmatrix} 1 & -5 \\ 3 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -5/3 \end{pmatrix}^{-1} \begin{pmatrix} 1 & 3 \\ -5 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -5/3 \end{pmatrix}, \text{ but}$$

$$\begin{pmatrix} 1 & -5 \\ 3 & -1 \end{pmatrix} \neq P^{-1} \begin{pmatrix} 1 & 3 \\ -5 & -1 \end{pmatrix} P, \text{ for all } P \in \mathrm{GL}_2(\mathbf{Z}).$$

From now on we assume that A and B are conjugated over $\mathbf{Q}$. In particular A and B have the same characteristic polynomial.

Conjugacy of matrices over the integers

Theorem (Latimer–MacDuffee 1933)

Let $A, B \in \mathrm{M}_n(\mathbf{Z})$ with irreducible characteristic polynomial $f \in \mathbf{Z}[x]$. Let $\mathcal{O} = \mathbf{Z}[x]/(f)$. Then there are "canonical" $\mathcal{O}$-ideals I_A and I_B such that

$$A,\ B \text{ are conjugated in } \mathrm{GL}_n(\mathbf{Z}) \quad \Longleftrightarrow \quad I_A \cong I_B \text{ as } \mathcal{O}\text{-ideals.}$$

- The ring $\mathcal{O}$ is an order in the algebraic number field $\mathbf{Q}[x]/(f)$.
- We enter the domain of (computational) algebraic number theory.
- There exist ("efficient") algorithms to solve this.
- Worst case: Subexponential complexity in the size of A and B (assuming GRH and other heuristics).

Conjugacy of matrices over the integers

Theorem can be used to determine all (conjugacy classes) of integer matrices with a given irreducible characteristic polynomial.

Example

- Let $f = x^2 + 13 \in \mathbf{Z}[x]$.
- $\mathcal{O} = \mathbf{Z}[x]/(x^2+13) = \mathbf{Z}[\sqrt{-13}] = \mathcal{O}_K$, where $K = \mathbf{Q}(\sqrt{-13})$.
- $\mathrm{Cl}(\mathcal{O}) = \{\overline{\langle 1, \sqrt{-13}\rangle}, \overline{\langle 2, 1+\sqrt{-13}\rangle}\}$.
-
$$\langle 1, \sqrt{-13}\rangle \longrightarrow \begin{pmatrix} 0 & 1 \\ -13 & 0 \end{pmatrix}, \quad \langle 2, 1+\sqrt{-13}\rangle \longrightarrow \begin{pmatrix} -1 & 2 \\ -7 & 1 \end{pmatrix}.$$
- There are exactly two conjugacy classes of integer matrices with characteristic polynomial $x^2 + 13$.

Conjugacy of matrices over the integers

Theorem (Sarkisyan 1977, Grunewald 1980)

There exists an algorithm that decides if two given matrices $A, B \in \mathrm{M}_n(\mathbf{Z})$ are conjugated in $\mathrm{GL}_n(\mathbf{Z})$. The algorithm also finds a conjugating element.

Decidable yes, but practical?

Grunewald 1980:

> *We have not tried to write out very effective algorithms, a lot of them depend highly exponentially on the data. But for dimension 2 and 3 it is possible to modify the procedure [...] to actually obtain not too inefficient computer programs.*

Remark

For a matrix $T \in \mathrm{M}_n(\mathbf{Z})$ the algorithm of Grunewald also gives a finite generating set of the arithmetic group

$$C_{\mathbf{Z}}(T) = \{X \in \mathrm{GL}_n(\mathbf{Z}) \mid XT = TX\}.$$

Conjugacy of matrices over the integers

Special cases:

- Latimer–MacDuffee 1933: Algorithm for matrices with irreducible characteristic polynomial.
- Opgenorth–Plesken–Schultz 1998: Algorithm for matrices of finite order (implemented in Magma by Kirschmer).
- Husert 2016: Algorithm for nilpotent and semisimple matrices (implemented in Magma for nilpotent matrices and matrices with irreducible minimal polynomial).
- Marseglia 2018: Algorithm for matrices with squarefree characteristic polynomial (Magma and Oscar/Hecke).
- Nebe 2019: Algorithms (based on a local-global principle) for certain semisimple matrices.

(All of them are more or less practical).

Conjugacy of matrices over the integers

Theorem (Eick–H.–O'Brien 2019)

There exists an "efficient" algorithm for solving the conjugacy problem of integer matrices. It can also compute generators of centralizers.

- Based on the approach of Grunewald.
- Corrections and improved theoretical results.
- A mix of computational number and group theory.

How it works—from matrices to modules

$A, B \in \mathrm{M}_n(\mathbf{Z})$.

- Decompose $A = S + N$ with $SN = NS$, S semisimple with minimal polynomial $f \in \mathbf{Z}[x]$ and N nilpotent ($N^l = 0$).
- Let $R = \mathbf{Z}[x, y]$ and consider $\mathbf{Z}^n$. Let x act as S and y as N. Since $f(x)$ and y^l act as zero (and commute), $\mathbf{Z}^n$ is naturally a $\mathbf{Z}[x, y]/(f, y^l)$-module (call it M_A).
- Now $\mathbf{Z}[x]/(f) = \mathcal{O}$ is an order in the étale $\mathbf{Q}$-algebra $\mathbf{Q}[x]/(f)$ and M_A is an $\mathcal{O}[y]/(y^l)$-module.

Proposition

The matrices A and B are conjugated in $\mathrm{GL}_n(\mathbf{Z})$ if and only if M_A and M_B are isomorphic $\mathcal{O}[y]/(y^l)$-modules.

- Now reduction to f irreducible and $\mathcal{O} = \mathcal{O}_K$, where $K = \mathbf{Q}[x]/(f)$.
- Solve the isomorphism problem (and more) for $\mathcal{O}_K[y]/(y^l)$-modules.

How it works—fun with modules

Standard submodules

A $\mathcal{O}_K[y]/(y^l)$-module N is *standard*, if

$$N \cong (\mathcal{O}_K[y]/(y))^{r_1} \oplus (\mathcal{O}_K[y]/(y^2))^{r_2} \oplus \cdots \oplus (\mathcal{O}_K[y]/(y^l))^{r_l}$$

for some integers $r_1, \ldots, r_l \in \mathbf{Z}_{\geq 0}$ (the *type*).

- Play a similar role like free submodules for finitely generated projective $\mathcal{O}_K$-modules.
- Can solve the isomorphism problem (just compare the type).
- Can compute automorphism group $\mathrm{Aut}_{\mathcal{O}_K[y]/(y^l)}(N)$ of a standard module N. (Involves computing

$$\mathrm{GL}_{r_1}(\mathcal{O}_K) \times \cdots \times \mathrm{GL}_{r_l}(\mathcal{O}_K).$$

  This is "easy" except when $r_1 = 2$ and K imaginary quadratic.)

How it works—fun with modules

Standard submodules

A $\mathcal{O}_K[y]/(y^l)$-module N is *standard*, if

$$N \cong (\mathcal{O}_K[y]/(y))^{r_1} \oplus (\mathcal{O}_K[y]/(y^2))^{r_2} \oplus \cdots \oplus (\mathcal{O}_K[y]/(y^l))^{r_l}$$

for some integers $r_1, \ldots, r_l \in \mathbf{Z}_{\geq 0}$ (the *type*).

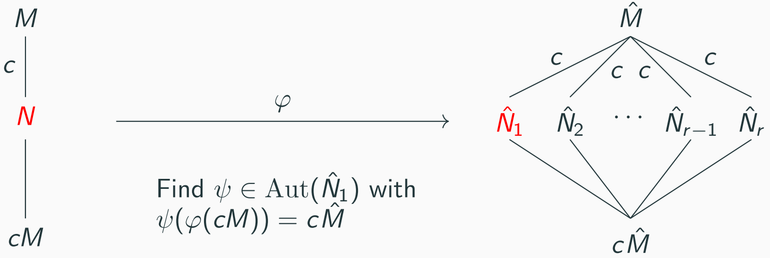
- Theoretical results on the location (in the submodule lattice) and the number of standard submodules of a given module. (Similar to locating free submodules of f.g. projective $\mathcal{O}_K$-modules using Cl_K.)
- One can efficiently determine the standard submodules of a given $\mathcal{O}_K[y]/(y^l)$-module.

How it works—fun with modules

Now let M, $\hat{M}$ be $\mathcal{O}_K[y]/(y^l)$-modules. We want to decide if $M \cong \hat{M}$.

Theorem

Let $N \subseteq M$ be standard of index c and $\{\hat{N}_1, \ldots, \hat{N}_r\}$ all standard submodules of $\hat{M}$ with index c. Then $M \cong \hat{M}$ if and only if there exist $1 \leq i \leq r$ and an isomorphism $\varphi\colon N \to \hat{N}_i$ such that $\varphi(cM) = \varphi(c\hat{M})$ (that is, the unique extension of φ to $\mathbf{Q} \otimes N$ maps M to $\hat{M}$).



How it works—in practice

Full implementation with no restriction on the input (in Magma).

Example

Consider the 10 by 10 matrices

$$
\begin{pmatrix}
-14 & -4 & 0 & 0 & -1 & 1 & 0 & 0 & 0 & 0 \\
-7 & -2 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
-3 & -1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & -14 & -4 & 0 & 0 & -1 \\
0 & 0 & 0 & 0 & 0 & -7 & -2 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & -3 & -1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0
\end{pmatrix},
\begin{pmatrix}
-9 & 9 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & -7 \\
0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\
-4 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -3 \\
0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & -7 & -9 & 1 & 0 & 0 & 0 \\
-1 & 1 & 0 & 0 & -7 & -9 & 0 & 0 & 0 & 0 \\
9 & -7 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 6 \\
0 & 0 & 1 & 0 & 3 & 4 & 0 & 0 & 0 & 0 \\
-9 & 8 & 0 & -1 & 0 & 0 & 0 & 1 & 0 & -7 \\
-9 & 8 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -7
\end{pmatrix}.
$$

- Minimal polynomial is $(x^5 + 16x^4 - 3x + 1)^2$.
- Implementation takes 8 seconds to find a conjugating matrix.

Very difficult to estimate the runtime of the algorithm (theory and practice).

How it works—in practice

Example

Consider

$$T = \begin{pmatrix} -5 & 8 & -5 \\ 4 & -7 & 5 \\ 1 & -2 & 2 \end{pmatrix} \in \mathrm{M}_3(\mathbf{Z}).$$

Our implementation shows in 0.3 seconds that

$$C_{\mathbf{Z}}(T) = \left\langle \begin{pmatrix} 860 & 1206 & -975 \\ 603 & 1001 & -795 \\ 195 & 318 & -253 \end{pmatrix}, \begin{pmatrix} 4 & 6 & -5 \\ 3 & 5 & -5 \\ 1 & 2 & -3 \end{pmatrix}, \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \right\rangle.$$

Practical limitations

Practical limitations fall into two categories:

Number theory

- Computation of ring of integers (given $\mathcal{O} = \mathbf{Z}[x]/(f)$, find $\mathcal{O}_K$).
- Computation of the class group (to solve principal ideal problems).

Group theory

- Large number of standard submodules.
- Computations with orbit-stabilizer algorithm (and large orbits).

Other applications and limitations

The algorithm can be applied to solve the problem for $\mathrm{SL}_n(\mathbf{Z})$ (requires generators $C_{\mathbf{Z}}(X)$) and $\mathrm{PGL}_n(\mathbf{Z})$.

What the algorithm cannot do:

- Find a canonical form for the conjugacy classes in $\mathrm{GL}_n(\mathbf{Z})$ (similar to the Jordan normal form or rational canonical form over fields).
- Determine the finitely many $\mathrm{GL}_n(\mathbf{Z})$-conjugacy classes for a fixed semisimple $\mathrm{GL}_n(\mathbf{Q})$-conjugacy class.

Outlook—What now?

Find an algorithm with nice complexity (as in the Latimer–MacDuffee theorem).

There are lots of variations of this problem, which are all known to be decidable (but no efficient algorithms are known).

- *Simultaneous* conjugacy problem: $P^{-1}A_iP = B_i$ for all $1 \leq i \leq r$, where $A_1, \ldots, A_r, B_1, \ldots, B_r \in \mathrm{M}_n(\mathbf{Z})$.

Replace $\mathrm{GL}_n(\mathbf{Z})$ with

- $\mathrm{GL}_n(\mathcal{O})$ (for some "arithmetic" ring $\mathcal{O}$),
- $\mathrm{Sp}_{2n}(\mathbf{Z})$ or $\mathrm{O}_n(f)$, where f is an integral quadratic form,
- an arithmetic group $\Gamma \subseteq G(\mathbf{Z})$, where $G = \langle f_1, \ldots, f_l \rangle$ is an algebraic subgroup of GL_n given by a finite set of polynomial equations over $\mathbf{Q}$ (Grunewald–Segal 1980).

```
julia> using Hecke

julia> A = matrix(ZZ, 2, 2, [1, 2, 3, 4])
[1 2]
[3 4]

julia> B = matrix(ZZ, 2, 2, [5, -2, -1, 0])
[5 -2]
[-1 0]

julia> isconjugate(A, B)
(true, [1 0]
       [2 -1])
```

Thank you.