Computing with infinite linear groups: recent advances and open problems

Alla Detinko

University of St Andrews

MFO
2 August 2016

1. Set up

Given a finitely generated subgroup $G \leq \mathbb{GL}(n, \mathbb{F})$, $\mathbb{F}$ is an infinite field.

Aim: Design practical methods, algorithms, and software for computing in this class of groups.

Motivation:

- Applications in mathematics and further afield.
- Convenient way to represent groups in computer.

Obstacle: Lack of methods for computing in this class of groups.

1.1 Finite approximation.

Given $G \leq \mathrm{GL}(n, R)$, R is a finitely generated integral domain. For an ideal $\rho \leq R$ denote $\varphi_\rho : \mathrm{GL}(n, R) \to \mathrm{GL}(n, R/\rho)$.

Fact: G is residually finite and approximated by matrix groups of degree n over finite fields R/ρ, ρ is maximal

Reason: R is approximated by fields R/ρ, i.e. for any non-zero $a \in R$ there exists a maximal ideal ρ which does not contain a.

Advantage: Reduction to computing with matrix groups over finite fields.

1.3 Example: solvable-by-finite groups.

Method: One maximal ideal is enough for computing with (virtually) solvable linear groups.

Recognition algorithms:

- Testing whether G is (virtually) solvable, (virtually) nilpotent, abelian-by-finite, central-by-finite, etc.
- Testing whether G is finite.

Structural investigation. If G is solvable-by-finite we can:

- Compute completely reducible part of G, including testing whether G is completely reducible or unipotent.
- Compute Prüfer and torsion free ranks of G.
- Do structural investigation of finite groups over $\mathbb{F}$ via construction of an isomorphic copy over a finite field.

Ongoing project with Dane Flannery and Eamonn O'Brien.

2. Next step: from finite to strong approximation

(joint work with Alexander Hulpke and Dane Flannery)

2.1 Groups with free non-abelian subgroups

- Ubiquity of non solvable-by-finite groups: a finitely generated linear group most likely is not solvable-by-finite (see e.g. D. Epstein, 1971; R. Aoun, 2011).
- Undecidable basic algorithmic problems.
- Lack of computational methods: to proceed with non solvable-by-finite groups one ideal may not be enough.

2.2 Strong approximation

Questions

(1) To which extent do congruence images define the group G?

(2) Can we compute all congruence images of G?

Example 1. Given

$$G = \left\langle \begin{bmatrix} 1 & 122 & 11 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 11 & 1 & 12 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -10 & 122 & 1 \end{bmatrix} \right\rangle,$$

(i) $G \equiv \mathrm{SL}(3,\mathbb{Z}) \bmod m, \forall m \in \mathbb{N}$.

(ii) G is of infinite index in $\mathrm{SL}(3,\mathbb{Z})$.

Exercise. Prove (i), (ii). Recognize the type of G and investigate its structure.

Example 2. Strong approximation. Let $G \leq \mathrm{SL}(n,\mathbb{Z})$ be Zariski dense in $\mathrm{SL}(n,\mathbb{R})$. Then $G \equiv \mathrm{SL}(n,\mathbb{Z}) \bmod p$ for all but a finite number of primes p.

2.3 Computing in dense subgroups.

Given a finitely generated $H \leq \mathrm{SL}(n, \mathbb{Z})$, $n > 2$, dense subgroup. In particular, H can be arithmetic, i.e. of finite index in $\mathrm{SL}(n, \mathbb{Z})$.

N.B. Density testing algorithms available (implemented).

Dense non-arithmetic subgroups are called *thin*.

Recall. $\mathrm{SL}(n, \mathbb{Z})$, $n \geq 3$, satisfies the *congruence subgroup property* (CSP), i.e. each arithmetic subgroup H of $\mathrm{SL}(n, \mathbb{Z})$, $n \geq 3$, contains the kernel of a homomorphism $\varphi_m : \mathrm{SL}(n, \mathbb{Z}) \to \mathrm{SL}(n, \mathbb{Z}_m)$ for some $m \in \mathbb{N}$: the *principal congruence subgroup* of level m (PCS).
Moreover, H contains the unique maximal principal congruence subgroup Γ_M. The level M of Γ_M is the level of H.

Main result

- Given a dense subgroup H, we can compute its 'arithmetic closure' $cl(H)$, i.e. the minimal arithmetic subgroup of $\mathrm{SL}(n, \mathbb{Z})$ containing H.
- In particular, if H is arithmetic then we compute its level.

Method.

- H surjects onto $\mathrm{SL}(n, p)$ iff p does not divide the level M of the maximal principal congruence subgroup of H (besides small exceptions for $n = 3, 4$, $p = 2$). This yields fast algorithms for computing the level M of the maximal principal congruence subgroup of $cl(H)$.

- Further computing is based on algorithms for matrix groups over a finite ring $\mathbb{Z}_m$ (including, in particular, trivial Fitting method).

Sample algorithms.

Let H be an arithmetic subgroup of $\mathrm{SL}(n, \mathbb{Z})$.

`IsIn`(H, g): membership test of $g \in \Gamma_n$ in H.

`Index`$(\Gamma_n : H)$: computing the index.

`IsSubnormal`(H): tests whether H is subnormal in Γ_n.

`Normalizer`(H): returns a generating set of $N_{\Gamma_n}(H)$.

`NormalClosure`(H): returns a generating set of $\langle H \rangle^{\Gamma_n}$.

Orbit-stabilizer problem.

Given an arithmetic subgroup H of $\mathrm{SL}(n, \mathbb{Z})$, and vectors $u, v \in \mathbb{Q}^n$.

`Orbit`(H, u, v): tests whether $\exists\, g \in H$ such that $g(u) = v$ and find a g if such exists.

`Stabilizer`(H, u): returns a generating set of $\mathrm{Stab}_H(u)$.

2.4 Sample application: computing with monodromy groups.

Let

$$U := \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ d & d & 1 & 0 \\ 0 & -k & -1 & 1 \end{bmatrix}, \quad T := \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

with $d, k \in \mathbb{Z}$. Then $\mathrm{G}(d,k) \leq \mathrm{Sp}(4,\mathbb{Z})$ is the monodromy group of a generalized hypergeometric ordinary differential equation.

For 14 pairs (d,k) the group $\mathrm{G}(d,k)$ is a monodromy group associated to Calabi-Yau threefolds; seven of these are arithmetic while the rest are thin.

Problem (D. van Straten et. al.).
Find an arithmetic subgroup $\hat{\mathrm{G}}(d,k)$ of $\mathrm{Sp}(4,\mathbb{Z})$ which contains $\mathrm{G}(d,k)$, and compute the index $|\mathrm{Sp}(4,\mathbb{Z}) : \hat{\mathrm{G}}(d,k)|$.

(d,k)	M	index	t(sec)
$(1,3)$	2	6	3.910
$(1,2)$	2	10	3.306
$(2,3)$	8	$2^6 \cdot 3 \cdot 5$	4.797
$(3,4)$	$2^2 \cdot 3^2$	$2^9 \cdot 3^5 \cdot 5^2$	7.155
$(4,4)$	2^6	$2^{20} \cdot 3^2 \cdot 5$	8.064
$(6,5)$	$2^3 \cdot 3^2$	$2^{10} \cdot 3^6 \cdot 5^2$	9.988
$(9,6)$	$2 \cdot 3^5$	$2^8 \cdot 3^{14} \cdot 5^2$	10.671
$(5,5)$	$2 \cdot 5^3$	$2^8 \cdot 3^3 \cdot 5^8 \cdot 13$	10.312
$(2,4)$	2^4	$2^{11} \cdot 3^2 \cdot 5$	5.106
$(1,4)$	2^2	$2^5 \cdot 5$	3.515
$(16,8)$	2^{10}	$2^{40} \cdot 3^2 \cdot 5$	16.841
$(12,7)$	$2^5 \cdot 3^2$	$2^{17} \cdot 3^6 \cdot 5^2$	21.446
$(8,6)$	2^7	$2^{24} \cdot 3^2 \cdot 5$	10.771
$(4,5)$	2^5	$2^{13} \cdot 3 \cdot 5$	7.605

3. Further computing: list of problems

Let $n > 2$ and $H \leq \mathrm{SL}(n, \mathbb{Z})$ be finitely generated dense.

Sample computational problems

Recognition:

1. Arithmeticity testing: decide whether $|\mathrm{SL}(n, \mathbb{Z}) : H|$ is finite.
2. If $|\mathrm{SL}(n, \mathbb{Z}) : H| = \infty$ then test whether H is maximal in $\mathrm{SL}(n, \mathbb{Z})$. Also, construct a finitely generated maximal subgroup of $\mathrm{SL}(n, \mathbb{Z})$ of infinite index.

Structure:

3. Construct a finitely generated (dense) free subgroup of H.
4. If H is free then test whether each finitely generated non-abelian subgroup of H is dense (strong density).

Motivation: applications.