Computing with infinite linear groups: methods, algorithms, and applications

Alla Detinko

University of St Andrews

Hausdorff Research Institute for Mathematics
25 October 2018

PART 1. Linear groups and computation: set up

Why linear groups?

- Commonly used representation of groups in group theory and its applications.
- Applications in other areas of mathematics and further afield (number theory, geometry, theoretical physics);
  fundamental mathematical model of transformations in science.
- Convenient and efficient way to represent groups in computer.

Aim:

- Design practical methods, algorithms, and software for computing with linear groups over an *arbitrary* infinite field.
- Solution of mathematical problems by computer experiments.

How to represent a group in computer?

Commonly used methods:

- Permutations.
- Matrices over finite fields.
- Generators and relations.

How to represent a *linear* group in computer?

Methods:

- Finite set of matrices: finitely generated groups.
- Finite set of polynomials: linear algebraic groups.

How to represent a *finitely generated* linear group in computer?

Given $G = \langle g_1, \ldots, g_r \rangle \leq \mathrm{GL}(n, \mathbb{F})$, $\mathbb{F}$ is a (infinite) field.

Aim: *symbolic* representation of G over an arbitrary infinite field.

Method.

- G is defined over a finitely generated extension of the prime subfield of $\mathbb{F}$.
- G is defined over a finitely generated integral domain $R \subset \mathbb{F}$.

Examples: main fields

1. $\mathbb{Q}$ and algebraic number fields.
2. $\mathbb{L} = \mathbb{P}(x_1, \ldots, x_m)$, $\mathbb{P}$ is a number field or $\mathbb{F}_q$.
3. A finite extension of $\mathbb{L}$.

What are finitely generated linear groups?

(i) Residual finiteness: finite approximation.

Given $G = \langle S \rangle$. Then $G \leq \mathrm{GL}(n, R)$ for a finitely generated integral domain $R \subseteq \mathbb{F}$ determined by the entries of matrices in $S \cup S^{-1}$.

Theorem. The group G is residually finite. Moreover, G is approximated by matrix groups of degree n over finite fields R/ρ, ρ is maximal.

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

Method for computing: computer realization of finite approximation.

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

(ii) The Tits alternative.

Theorem (J. Tits, 1972)**.** A finitely generated linear group over a field is either solvable-by-finite or it contains a non-cyclic free subgroup.

Strategy for computing:

1. Algorithms for solvable-by-finite groups.
2. Algorithms for groups with a free non-abelian subgroup.

PART 2. Computing with virtually solvable groups

Method of finite approximation: congruence homomorphism techniques.

Notation: Given an ideal $\rho \subseteq R$, define the congruence homomorphism $\varphi_\rho : \mathrm{GL}(n, R) \to \mathrm{GL}(n, R/\rho)$.

- $\ker \varphi_\rho := \Gamma_\rho$ (principal congruence subgroup).
- $G \cap \Gamma_\rho := G_\rho$ (congruence subgroup).

Method: Reduction to, e.g., finite fields via construction of a congruence homomorphism φ_ρ such that G_ρ satisfies some *special* properties.

Theorem (Wehrfritz et al.). There exists a maximal ideal $\rho < R$ such that
(i) All torsion elements of Γ_ρ are unipotent,i.e. Γ_ρ is torsion-free if $\mathrm{char}\, R = 0$.
(ii) If G is solvable-by-finite then G_ρ is unipotent-by-abelian.

Notation: We call φ_ρ as in the theorem a *W-homomorphism*.

Examples: Main domains and construction of W-homomorphisms.

- Let $\mathbb{F} = \mathbb{Q}$. Then $R = \frac{1}{c}\,\mathbb{Z}$, $c \in \mathbb{Z}$. Define $\rho = p\mathbb{Z}$, p is prime, $p \neq 2$, $p \nmid c$. Then φ_ρ is a W-homomorphism; in particular, G_ρ is *torsion-free* (Minkowski).

- Let $\mathbb{F} = \mathbb{Q}(\alpha)$ be a number field, $f(t)$ be the minimal polynomial of α. Then $R = \frac{1}{c}\,\mathcal{O}$, $\mathcal{O}$ is the ring of integers of $\mathbb{Q}(\alpha)$, $c \in \mathbb{Z}$, $c \neq 0$. If $p > 2$ is a prime dividing neither c nor the discriminant of $f(t)$ then reduction modulo p is a W-homomorphism.

- Let $\mathbb{F} := \mathbb{F}_p(x)$. Then $R = \frac{1}{c}\,\mathbb{F}_p[x]$, $c = c(x) \in \mathbb{F}_p[x]$. If $\alpha \in \bar{\mathbb{F}}_p$, $c(\alpha) \neq 0$ then reduction modulo $\rho := \langle (x - \alpha) \rangle$ is a W-homomorphism.

N.B. We can construct W-homomorphisms for all finitely generated integral domains R.

Which algorithms do we need?

1. Recognition algorithms, i.e. testing the type of an input group.
2. Investigation of the structure and properties of the input group.
3. Library of basic functions.

Algorithms: recognizing types of groups.

- Testing finiteness.

  Method ($\mathrm{char}\,\mathbb{F} = 0$): test whether the kernel G_ρ of reduction modulo ρ for a W-homomorphism φ_ρ is trivial.

- Testing virtual solvability (computational realization of the *Tits alternative*).

  Method: for a W-homomorphism φ_ρ test whether $G_\rho = \langle N \rangle^G$ is unipotent-by-abelian (*via computing in enveloping algebras*, i.e. no need to compute $\langle N \rangle^G$).

- Testing solvability, (virtual) nilpotency, testing whether the group is abelian-by-finite, central-by-finite etc.

N.B. One maximal ideal ρ is enough for the above algorithms.

Algorithms: investigating structure.

- **Finite groups**.

  Method:
  Construct an isomorphic copy over a finite field via W-homomorphisms, and then apply algorithms for matrix groups over finite fields.

- **Solvable-by-finite groups**.

  Motivation: theory of infinite soluble groups.

  Challenges (solvable vs polycyclic):

  - May not be finitely presentable;
  - Contain subgroups which are not finitely generated.

Given a finitely generated solvable-by-finite group over a field $\mathbb{F}$ we can:

- Construct a generating set of the completely reducible (i.e. block-diagonal) part of G. This includes testing whether G is completely reducible and whether G is unipotent (i.e. upper uni-triangular in some basis).
- Compute Prüfer rank and torsion free rank of G; compute a 'basis' of the unipotent radical of G; test whether the index $|G : H|$ a finitely generated subgroup H of G is finite.
- Library of functions for computing with (virtually) nilpotent linear groups: this is a premium class of groups.

Software: Magma package `http://magma.maths.usyd.edu.au/magma/handbook/matrix_groups_over_infinite_fields`.

PART 3. Zariski density and computing

Groups with free non-abelian subgroups: challenges

- 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.

  - Membership testing is *decidable* in finitely generated solvable-by-finite subgroups of $\mathrm{GL}(n, \mathbb{Q})$ (Kopytov, 1968);

  - Membership testing is *undecidable* in $\mathrm{SL}(4, \mathbb{Z})$ (Michailova, 1958).
- Lack of computational methods: to proceed with non-solvable-by-finite groups *one ideal* may not be enough.

Why dense and arithmetic subgroups?

- Approach to computing:

  (i) Each finitely generated linear group H is a subgroup of a linear algebraic group $\mathcal{G}$; without loss of generality H is (Zariski) dense in $\mathcal{G}$.

  N.B. Algorithms computing Zariski closure exist.

  (ii) $H \leq \mathcal{G}(R) := \mathcal{G} \cap \mathrm{GL}(n, R)$; $|\mathcal{G}(R) : H|$ is finite (H is arithmetic) or infinite (H is *thin*).

- Algorithms for dense subgroups are in high demand, particularly due to applications of in number theory, topology, physics, etc. (cf. P. Sarnak, *Notes on thin matrix groups*, 2012).

- Fundamental algorithmic problems for arithmetic subgroups are known to be decidable (under some conditions!): Grunewald & Segal, 1980.

What are dense and arithmetic subgroups?

Set up: $\mathcal{G} := \mathrm{SL}(n, \mathbb{C})$, $R = \mathbb{Z}$.

(i) The congruence subgroup property and computing

Theorem (Bass, Mennicke et al, 1965-67). $\mathrm{SL}(n, \mathbb{Z})$, $n \geq 3$, satisfies the *congruence subgroup property* (CSP), i.e. each arithmetic subgroup H of $\mathrm{SL}(n, \mathbb{Z})$, $n \geq 3$, contains the kernel Γ_m 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).

N.B. H contains a unique maximal principal congruence subgroup Γ_M. The level M of Γ_M is the *level* of H.

Fact. Each dense subgroup $H \leq \mathrm{SL}(n, \mathbb{Z})$ is contained in the unique 'minimal' arithmetic overgroup $\mathrm{cl}(H)$ (*arithmetic closure* of H).

N.B. If H is dense the *level* of H is defined as the level of $\mathrm{cl}(H)$.

(ii) Strong approximation

Questions.
(1) To which extent do congruence images define a linear group H?

(2) Can we compute all congruence images of H?
Example. Given

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

(i) $H \equiv \mathrm{SL}(3, \mathbb{Z}) \bmod m, \forall m \in \mathbb{N}$.
(ii) H is of infinite index in $\mathrm{SL}(3, \mathbb{Z})$.
Exercise: prove (i) and (ii).

Theorem (Weisfeiler et al.). If $H \leq \mathrm{SL}(n, \mathbb{Z})$ is dense then H surjects onto $\mathrm{SL}(n, p)$ for all but a finite number of primes p (Strong Approximation Theorem).

Proposition. Dense H surjects onto $\mathrm{SL}(n, p)$ iff p does not divide the level M of H (besides small exceptions for $n = 3, 4$, $p = 2$).

Method for computing: from finite to strong approximation

Given a finitely generated subgroup $H \leq \mathrm{SL}(n, \mathbb{Z})$, we can:

- Test density of H.
  Method: a number of Monte-Carlo and deterministic algorithms (e.g., Rivin's algorithms).
- For dense H compute the set $\Pi(H)$ of all primes p for which H does not surject onto $\mathrm{SL}(n, p)$ (computational realization of the *strong approximation theorem*).
  Method: based on the classification of maximal subgroups of $\mathrm{SL}(n, p)$.

  N.B. More generally, we can compute all congruence quotients of H ($n > 2$).
- Compute the level M of a dense (in particular, arithmetic) subgroup H and, thereby, compute $\mathrm{cl}(H)$.
  Method: computing in $\mathrm{GL}(n, \mathbb{Z}_m)$; '*trivial Fitting*' approach.

Knowing M we can proceed to algorithms for *arithmetic subgroups*.

Computing with arithmetic subgroups: sample algorithms.

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

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

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

`IsSL`(H): test whether $H = \mathrm{SL}(n, \mathbb{Z})$.

`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 $\langle H \rangle^{\Gamma_n}$, H any finitely generated subgroup of Γ_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 $\mathrm{Stab}_H(u)$.

N.B.: `Stabilizer`(H, u) is finitely generated.

Method: solution of orbit-stabilizer problem for the congruence image $\varphi_M(H)$ acting on $\mathbb{Z}_M^n$ and the principal congruence subgroup $\Gamma_M \leq H$ acting on $\mathbb{Z}^n$.

Remark: We justified decidability of the above problems (cf. results by Grunewald & Segal).

Applications and experimental results

Experiments.

Given

$$\mathrm{H} = \left\langle \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 4 & 7 \\ 0 & -2 & -3 \\ 0 & 1 & 1 \end{bmatrix} \right\rangle.$$

`IsFinite`(H);
'false'
N.B. Generators of H are of finite order.

`IsSolvableByFinite`(H);
'false'
`IsDense`(H);# density test in $\mathrm{SL}(3, \mathbb{Z})$.
'true'

`PrimesForDense`(H);
$\Pi(H) = \{2\}$

`LevelMaxPCS`(H); # computing the level M of H.
$M = 2^3$

N.B. Now we know $\mathrm{cl}(H)$.

`Index`(H); # computing the index of $\mathrm{cl}(H)$ in $\mathrm{SL}(3, \mathbb{Z})$.
$2^7 \cdot 7$

Question: Is H arithmetic in $\mathrm{SL}(3, \mathbb{Z})$ (or, equivalently, $H = \mathrm{cl}(H)$)?

Experimental evidence: 'most likely, H is not arithmetic'

Fact (Long & Reid, 2011): $H \cong \Delta(3, 3, 4)$.

Conclusion: H is not arithmetic; e.g. has a finite quotient isomorphic to $\mathrm{Alt}(20)$ which does not have faithful representation in $\mathrm{SL}(3, p)$ for any p.

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 $\mathrm{G}(d,k) = \langle U, T \rangle \leq \mathrm{Sp}(4,\mathbb{Z})$ 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