Zariski density and computing with linear groups

Alla Detinko

Banff International Research Station

11 December 2019

1. Computing with infinite linear groups: set up

How to represent a group in computer?

Main methods:

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

Why linear groups?

- Commonly used representation of groups in group theory and its applications in mathematics and further afield.
- Convenient and efficient way to represent groups in computer.

Main challenges

- Fundamental algorithmic problems are undecidable.
- Complexity issues.
- Lack of methods.

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 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 $\mathbb{F}$.

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 $\mathbb{L}$.

Method of finite approximation: congruence homomorphism techniques.

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.

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 for computing (computer realization of finite approximation):

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

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

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.

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

- 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 developed: outline.

- *Testing finiteness*: test whether the kernel G_ρ of reduction modulo ρ for a W-homomorphism φ_ρ is trivial (if $\mathrm{char}\,\mathbb{F} = 0$).
  Full investigation of structure via an isomorphic copy over a finite field.

- *Testing virtual solvability* (computational realization of the *Tits alternative*:) for a W-homomorphism φ_ρ test whether $G_\rho = \langle N \rangle^G$ is unipotent-by-abelian.

- Testing solvability, (virtual) nilpotency, testing whether the group is abelian-by-finite, central-by-finite etc. Computing 'main' structural components of a (virtually) solvable group; computing Prüfer rank and torsion free rank.

N.B. One maximal ideal ρ is enough for the above algorithms; *software* [1].

2. Zariski density and computation

Further challenges.

- Ubiquity of non solvable-by-finite groups: a linear group 'most likely' is not solvable-by-finite (see e.g. D. Epstein, 1971; R. Aoun, 2011).
- Undecidable basic algorithmic problems, e.g.,

  - 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 subgroups?

- *Approach to computing:*

  Step 1: 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.

  Step 2: H is *thin* or *arithmetic*, i.e. $|\mathcal{G}(R) : H|$ is infinite or, resp. finite; here $H \leq \mathcal{G}(R) := \mathcal{G} \cap \mathrm{GL}(n, R)$.

- 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.

Dense and arithmetic subgroups: set up

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

- $\varphi_m : \mathrm{SL}(n, \mathbb{Z}) \to \mathrm{SL}(n, \mathbb{Z}_m)$;
- Γ_m is the kernel of a homomorphism φ_m (principal congruence subgroup of level m);
- $cl(H)$ is the '*arithmetic closure*' of H (i.e. intersection of arithmetic overgroups of H);
- Level $M(H)$ of H is the level of the (unique) maximal principal congruence subgroup of $cl(H)$, $n \geq 3$.

Scheme of computing.

(i) Test whether $H \leq \mathrm{SL}(n, \mathbb{Z})$ is dense.

(ii) Compute *Level*(H).

(iii) Investigate H using *Level*(H) (via congruence homomorphism technique).

Density testing.

Given a finitely generated $H \leq \mathrm{SL}(n, \mathbb{Z})$, we can test density as follows.

1. *Fact*: $H \leq \mathrm{SL}(n, \mathbb{C})$ is dense iff H is infinite and $ad(H)$ is absolutely irreducible.
   Output: deterministic density test algorithm (of limited practicality).
2. Monte-Carlo algorithm (I. Rivin): returns `true` if detects non-commuting $g, h \in H$ such that h is of infinite order and the Galois group of the characteristic polynomial of g is $Sym(n)$.
3. Further algorithms, i.e. for subgroups of $\mathrm{SL}(n, \mathbb{Z})$ containing a (known) transvection.

Next step: from finite to strong approximation

Questions.

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

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

Exercise. Given

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

Show that

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

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

Theorem. The following are equivalent.

(i) $H \leq \mathrm{SL}(n, \mathbb{Z})$ is dense.

(ii) H surjects onto $\mathrm{SL}(n, p)$ for almost all primes p.

(iii) H surjects onto $\mathrm{SL}(n, p)$ for some $p > 2$.

Notation: $\Pi(H)$ is the set of all primes for which $\varphi_p(H) \neq \mathrm{SL}(n, p)$.

Aim: Given a dense $H \leq \mathrm{SL}(n, \mathbb{Z})$, compute $\Pi(H)$.

Computer realization of the strong approximation theorem.

Approach (based on B. Weisfeiler's method). Given Aschbacher classes $C_1, \ldots, C_9$ of maximal subgroups of $\mathrm{SL}(n, p)$, find all primes p such that $\varphi_p(H)$ is not contained in any group G of C_i, $1 \leq i \leq 9$.

Fact: Let $G \leq \mathrm{SL}(n, p)$. There exists a function $f(n)$, depending only on degree n, such that if $ad(G)$ is absolutely irreducible and $|G| > f(n)$ then $G = \mathrm{SL}(n, p)$.

Method: Find p_0 such that for all $p \geq p_0$, $|\varphi_p(H) > f(n)|$, and $ad(\varphi_p(H))$ is absolutely irreducible.

N.B. Explicit values of $f(n)$ available for $n \leq 12$.

Improved methods: (i) Exclude one-by-one each of Aschbacher classes by special methods avoiding computing $ad(H)$. Done for n prime, and some 'small' values of n.

(ii) Special methods for the case of H containing a (known) transvection.

Computing with dense subgroups

Aim: Given a dense $H \leq \mathrm{SL}(n, \mathbb{Z})$, compute the arithmetic closure $cl(H)$, i.e. $Level(H) := M(H)$.

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

Thus, we have that $\Pi(H)$ is the set of all prime divisors of $M(H)$ (besides probably $p = 2$). Hence to compute $M(H)$ for a dense H, we should find $p^k || M$ for each $p \in \Pi(H)$.

Method: computing in $\mathrm{GL}(n, \mathbb{Z}_m)$; '*trivial Fitting*' approach.

Computing with arithmetic subgroups

Knowing M we can proceed to algorithms for *arithmetic subgroups* (including algorithms for $cl(H)$, H is dense).

Given an arithmetic subgroup $H \leq \mathrm{SL}(n, \mathbb{Z})$, $n \geq 3$, we can

(1) Test whether $g \in \mathrm{SL}(n, \mathbb{Z})$ is contained in H (*membership test*).

(2) Compute the *index* $|\mathrm{SL}(n, \mathbb{Z}) : H|$ (in particular, test whether $H = \mathrm{SL}(n, \mathbb{Z})$).

(3) Investigate (sub)-normal structure of H.

(4) Test whether $u, v \in \mathbb{Q}^n$ are in the same H-orbit, and computing generators of $\mathrm{Stab}_H(u)$ (*orbit-stabilizer problem*).

Method: Computing via reduction to $\mathrm{SL}(n, \mathbb{Z}_M)$.

Remark. Decidability of problems (1), (2) implies that arithmetic subgroups of $\mathrm{SL}(n, \mathbb{Z})$, $n \geq 3$, are *explicitly given* in terms of Grunewald & Segal.

3. Applications and experimental results

Example.

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.

Experiments

Let $\Gamma := \langle x, y, z \mid zxz^{-1} = xy, zyz^{-1} = yxy \rangle$ (the fundamental group of the figure-eight knot complement). Put $F = \langle x, y \rangle$. Consider the representation $\rho_k : \Gamma \to \mathrm{SL}(3, \mathbb{Z})$, $k \in \mathbb{Z}$,

$$\rho_k(x) = \begin{pmatrix} 1 & -2 & 3 \\ 0 & k & -1-2k \\ 0 & 1 & -2 \end{pmatrix}, \rho_k(y) = \begin{pmatrix} -2-k & -1 & 1 \\ -2-k & -2 & 3 \\ -1 & -1 & 2 \end{pmatrix},$$

$$\rho_k(z) = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & -k \\ 0 & 1 & -1-k \end{pmatrix}.$$

Problem ([Long & Reid, 2011]): what are properties of $\rho_k(\Gamma)$?

Motivation: Does $\mathrm{SL}(3, \mathbb{Z})$ have the Howson property? Is $\mathrm{SL}(3, \mathbb{Z})$ coherent?

k	M	Index_Γ	$\mathrm{Index}_{\Gamma,F}$
1	$2^2 3^4$	$2^{10}3^{15}13$	2^2
6	$2^2 31{\cdot}43$	$2^{10}3^3 7{\cdot}43^2 331{\cdot}631$	$2{\cdot}3{\cdot}5$
7	$3^4 5{\cdot}19$	$2^6 3^{17} 5{\cdot}13{\cdot}19^2 31{\cdot}127$	$2^2 3^2$
10	$2^2 3^4 11{\cdot}37$	$2^{14}3^{16}7^2 13{\cdot}19{\cdot}37^2 67$	$2^2 3^2 5$
15	$229{\cdot}241$	$2^6 3^3 5{\cdot}97{\cdot}181{\cdot}241^2 19441$	$2{\cdot}3{\cdot}19$
20	$409{\cdot}421$	$2^4 3^3 5{\cdot}7{\cdot}421^2 55897{\cdot}59221$	$2^2 3{\cdot}17$

Comments: (i) $M = \mathrm{Level}(\rho_k(\Gamma)) = \mathrm{Level}(\rho_k(F))$ for all k in the table.

(ii) The congruence images of $\rho_k(F)$ modulo M available.

(iii) For $k = 1, 6, 10$, $\rho_k(\Gamma)$ surjects onto $\mathrm{SL}(3,2)$, and does not surjects onto $\mathrm{SL}(3,4)$.

(iv) Runtime is less than 15 minutes.

Further experiments.

New experimental results for symplectic monodromy groups of hypergeometric differential equations available. These are 2-generator dense subgroups of $\mathrm{Sp}(n, \mathbb{Q})$ containing a transvection.

Motivation: applications in theoretical physics.

- Experimentation is based on our algorithms for subgroups of $\mathrm{Sp}(n, \mathbb{Z})$.
- Experimental tables provides results (including *Level*(H) and indices in $\mathrm{Sp}(n, \mathbb{Z})$) for

  (i) $n = 4$, 151 groups;
  (ii) $n = 6$, 916 groups.

Justification of arithmeticity in a number of cases obtained.

`https://arxiv.org/abs/1905.02190`

Example. 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.

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

Appendix

1. Magma functions for computing with infinite linear groups: `http://magma.maths.usyd.edu.au/magma/handbook/matrix_groups_over_infinite_fields`.

2. GAP functionality for Zariski dense subgroups: `http://www.math.colostate.edu/~hulpke/arithmetic.g`; Documentation: `https://publications.mfo.de/handle/mfo/1321`.

Acknowledgment: Dane Flannery, and Willem de Graaf, Alexander Hulpke, Eamonn O'Brien.