Linear groups and computation

Alla Detinko

RWTH Aachen University
25 May 2016

1. Why linear groups?

- Fundamental mathematical model of transformations in science.
- Commonly used representation of groups in group theory and its applications.
- Convenient and efficient way to represent groups in computer.

2. Computing with linear groups

How to represent a group in computer?

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

Project. Computing with groups given by a finite set of matrices over an infinite field.

- Develop general methods and techniques for computing with linear groups over an arbitrary infinite field.
- Obtain practical algorithms for solution of fundamental computational problems.
- Design software for computing in this class of groups aimed at solution of mathematical problems by straightforward computing.

History.

- L. Babai, R. Beals et. al.
- G. Nebe, W. Plesken et. al.
- B. Eick, G. Ostheimer et. al. (polycyclic groups).
- A. Cohen, W. de Graaf et. al. (algebraic groups).

Obstacles.

- Undecidability of basic computational problems.
- Complexity issues (e.g. such as growth of size of matrix entries).
- Lack of established methods for computing in this class of groups.

3. Finitely generated linear groups and computing.

3.1 Methods of computing.

3.1.1 Representation in computer: main domains.

Given $G := \langle S \rangle$, $S = \{g_1, \ldots, g_r\}$, $g_i \in \mathrm{GL}(n, \mathbb{F})$, $1 \leq i \leq r$, $\mathbb{F}$ is a field. Since G is finitely generated, it is defined over a finitely generated extension of the prime subfield of $\mathbb{F}$. Moreover

Lemma. For a subfield $\mathbb{P} \subseteq \mathbb{F}$ there exist $x_1, \ldots, x_m \in \mathbb{F}$ $(m \geq 0)$ algebraically independent over $\mathbb{P}$ such that $\mathbb{F}$ is a finite extension of $\mathbb{P}(x_1, \ldots, x_m)$.

Examples: main domains

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 $\mathbb{L}$.

3.1.2 Method of finite approximation.

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

Lemma. R is 'approximated' by finite fields, i.e.

- for each maximal ideal ρ of R, R/ρ is a finite field;
- the intersection of maximal ideals of R is zero.

Theorem (Mal'cev). The group G is residually finite. Moreover, G is approximated by matrix groups of degree n over finite fields.

3.1.3 Congruence homomorphism techniques.

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

Notation

- $\ker \varphi_\rho := \Gamma_\rho$ (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 satisfy some special properties.

3.2 What are finitely generated linear groups: classes and structure.

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.

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.

Theorem (Selberg, Wehrfritz). A finitely generated linear group contains a normal subgroup N of finite index such that the torsion elements of N are all unipotent. In particular, if $\mathrm{char}\,\mathbb{F} = 0$ then N is torsion-free.

Theorem (Lie-Kolchin-Mal'cev)**.** A linear group G over a field $\mathbb{F}$ is solvable-by-finite iff G contains a unipotent-by-abelian subgroup of finite index.

4. Computing in solvable-by-finite groups.

4.1 Computational analogue of the method of finite approximation.

Theorem. Given a finitely generated subgroup G of $\mathrm{GL}(n, R)$ there exist maximal ideals ρ of R such that

(i) torsion elements of G_ρ are unipotent, i.e. G_ρ is torsion free if $\mathrm{char}\, R = 0$.

(ii) G_ρ is unipotent-by-abelian if G is solvable-by-finite.

We call φ_ρ for ρ as above an *W-homomorphism*.

Method.

1. Select ρ such that φ_ρ is an W-homomorphism.
2. Construct $\varphi_\rho(G)$ (which is a matrix group over the finite field R/ρ).
3. Find a (finite) normal generating set N of the kernel G_ρ, i.e. $G_\rho = \langle N \rangle^G$.

Examples: W-homomorphisms.

- Let $\mathbb{F} = \mathbb{Q}$. Then $R = \frac{1}{c}\,\mathbb{Z}$, $c \in \mathbb{Z}$. Define $\rho = p\mathbb{Z}$, $p \neq 2$, $p \nmid c$. 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 $\rho := (x - \alpha)$ is a W-homomorphism.

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

4.2 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 analogue 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).

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

4.3 Algorithms: investigating structure.

- Finite groups: 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.

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

  - Construction of 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).
  - Computing a 'basis' of the unipotent radical $U(G)$, i.e. a finite set of matrices T such that torsion-free ranks of $\langle T \rangle$ and $U(G)$ are the same. This includes computing Prüfer rank and torsion free rank of G.
  - 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`.

5. Next step: computing with non-solvable-by-finite groups.

5.1 What are non- solvable-by-finite groups?

- 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).

- Computational obstacles:

  - Undecidable basic algorithmic problems:

    - membership test is *decidable* in finitely generated solvable-by-finite subgroups of $\mathrm{GL}(n, \mathbb{Q})$ (Kopytov, 1968);
    - membership test is *undecidable* in $\mathrm{SL}(4, \mathbb{Z})$ (Michailova, 1958).

  - Too wide class of groups.
  - Lack of computational methods.

5.2 Why arithmetic groups ?

A subgroup $H \leq \mathrm{GL}(n, \mathbb{Q})$ of an algebraic $\mathbb{Q}$-group $\mathcal{G} \leq \mathrm{GL}(n, \mathbb{C})$ is *arithmetic* if H is commensurable with $\mathcal{G}_{\mathbb{Z}} := \mathcal{G} \bigcap \mathrm{GL}(n, \mathbb{Z})$, i.e., $H \bigcap \mathcal{G}_{\mathbb{Z}}$ has finite index in both H and $\mathcal{G}_{\mathbb{Z}}$.

N.B. Arithmetic subgroups are finitely generated.

Example. If $\mathcal{G} = \mathrm{SL}(n, \mathbb{C})$ or $\mathrm{Sp}(n, \mathbb{C})$ then finite index subgroups of $\mathrm{SL}(n, \mathbb{Z})$, (resp. $\mathrm{Sp}(n, \mathbb{Z})$) are arithmetic.

Motivation.

- One of the central classes of linear groups.
- Fundamental algorithmic problems are known to be decidable (under some conditions!): Grunewald & Segal, 1980.
- Computing with arithmetic subgroups is currently in high demand (in particular, due to impact on number theory, topology, physics: see, e.g., P. Sarnak, *Notes on thin matrix groups*, preprint, 2012).

5.3 Arithmetic groups with the congruence subgroup property: computing

5.3.1 Set up: congruence subgroup property.

Examples: $\mathrm{SL}(n, \mathbb{Q})$ vs $\mathrm{SL}(n, \mathbb{Z})$.

1. The only proper normal subgroups of $\mathrm{SL}(n, \mathbb{Q})$ lie in the finite center consisting of scalar matrices (i.e. $\mathrm{SL}(n, \mathbb{Q})$ is 'close' to simple).

2. $\Gamma_n := \mathrm{SL}(n, \mathbb{Z})$ contains infinitely many normal subgroups of finite index. For example, *principal congruence subgroups (PCS)* $\Gamma_{n,m}$ *of level* m, i.e. kernels of $\varphi_m : \mathrm{SL}(n, \mathbb{Z}) \to \mathrm{SL}(n, \mathbb{Z}_m)$; here $\mathbb{Z}_m := \mathbb{Z}/m\mathbb{Z}$.

3. $\Gamma_2 := \mathrm{SL}(2, \mathbb{Z})$ contains normal subgroups of finite index which do not contain a principal congruence subgroup $\Gamma_{2,m}$ for any m (XIXth century; Klein, Fricke). Moreover, $\mathrm{SL}(2, \mathbb{Z})$ contains non-central normal subgroups of infinite index (e.g. $\langle t_{21}(m) \rangle^{\Gamma_n}$ is of infinite index for $m > 5$).

Theorem (Bass, Mennicke et al, 1965-67). Every normal non-central subgroup of $\mathrm{SL}(n, \mathbb{Z})$, $n > 2$, contains a principal congruence subgroup $\Gamma_{n,m}$ for some m.

Corollary. Each arithmetic subgroup of $\mathrm{SL}(n, \mathbb{Z})$, $n \geq 3$, contains a principal congruence subgroup $\Gamma_{n,m}$ for some m.

In other terms $\mathrm{SL}(n, \mathbb{Z})$, $n \geq 3$, satisfies the *congruence subgroup property* (CSP).

Examples. $\mathrm{SL}(2,\mathbb{Z})$ does not have CSP, while $\mathrm{SL}(n,\mathcal{O}_{\mathbb{F}})$, $n \geq 3$, $\mathrm{Sp}(2n,\mathcal{O}_{\mathbb{F}})$, $n \geq 2$, satisfy CSP, $\mathcal{O}_{\mathbb{F}}$ is ring of integers of a number field $\mathbb{F}$ that is not totally imaginary.

For details see current surveys on the *congruence subgroup problem.*

5.3.2 Approach to computing with arithmetic subgroups which satisfy CSP.

(i) Find a principal congruence subgroup $\Gamma_{n,m}$ of H;

(ii) Reduce computing to matrix groups over $\mathbb{Z}_m$.

N.B. A principal congruence subgroup $\Gamma_{n,m}$ of H is not unique, but the maximal PCS $\Gamma_{n,M}$ is unique.

5.4 Structure of arithmetic subgroups and computing

5.4.1 Principal congruence subgroup and computing

Notation. Let $t_{ij} = 1_n + e_{ij}(m)$ be an elementary matrix of level m, $i \neq j$; here $e_{ij}(m)$ is $n \times n$ matrix with m in position (i, j) and zeros everywhere else.
Denote $E_{n,m} = \langle t_{ij}(m) | 1 \leq i, j \leq n, i \neq j \rangle$ *elementary group of level* m.

Properties of $\Gamma_{n,m}$.

Fact 1. $\Gamma_{n,m} = \langle E_{n,m} \rangle^{\Gamma_n}$.

Fact 2. $\Gamma_{n,m^2} \leq E_{n,m}$.

Fact 3. If $|\Gamma_n : H| \leq c$ then $H \geq \Gamma_{n,m^2}$, $m = lcm\{1, \ldots, c\}$.

Proposition. Construction of a PCS in an arithmetic subgroup of $\mathrm{SL}(n, \mathbb{Z})$, $n > 2$, is decidable.

Proof. Follows from Todd-Coxeter procedure and Fact 3. $\square$

Proposition. Let H be an arithmetic subgroup of $\mathrm{SL}(n, \mathbb{Z})$. Then the following problems are decidable.

- Membership test of $g \in \mathrm{SL}(n, \mathbb{Z})$ in H.
- Computing an upper bound on the index $|\mathrm{SL}(n, \mathbb{Z}) : H|$.

Proof. Computing a PCS of H is decidable. $\square$

Conclusion. Arithmetic subgroups of $\mathrm{SL}(n, \mathbb{Z})$, $n > 2$, are *explicitly given* in terms of Grunewald & Segal.
Hence solution of all decision problems obtained by Grunewald & Segal valid for arithmetic subgroups of $\mathrm{SL}(n, \mathbb{Z})$, $n > 2$.

N.B.: most of algorithms of Grunewald & Segal are not practical.

5.4.1 Computing in congruence images: subgroups of $\mathrm{GL}(n, \mathbb{Z}_m)$.

Let $m = p_1^{k_1} \dots p_t^{k_t}$ where p_i are distinct primes and $k_i \geq 1$. Then $\mathrm{GL}(n, \mathbb{Z}_m) \cong \mathrm{GL}(n, \mathbb{Z}_{p_1^{k_1}}) \times \dots \times \mathrm{GL}(n, \mathbb{Z}_{p_t^{k_t}})$.

Denote $K := \{h \in \mathrm{GL}(n, \mathbb{Z}_{p^k}) | \ h \equiv 1_n \bmod p^{k-1}\}$ (congruence subgroup of level p^{k-1}). Then K is a (finite) p-group and $\mathrm{GL}(n, \mathbb{Z}_{p^k})/K \cong \mathrm{GL}(n, p)$.

Conclusion: computing with matrix groups over $\mathbb{Z}_m$ is reduced via congruence homomorphism method to computing over finite fields and computing in finite p-groups.

6. Algorithms for computing with arithmetic subgroups

6.1 Computing principal congruence subgroups: from finite approximation to strong approximation.

Aim. Find the level M of the maximal principal congruence subgroup of an arithmetic subgroup H of $\Gamma_n := \mathrm{SL}(n, \mathbb{Z})$, $n > 2$.

Feature. The method requires computing congruence images of H modulo *all* primes.

N.B.: no need for a generating set of the principal congruence subgroup $\Gamma_{n,M}$, although we can compute it too.

What is the strong approximation?

Example: $\mathrm{GL}(n,\mathbb{Z})$ vs $\mathrm{SL}(n,\mathbb{Z})$.

- $\mathrm{GL}(n,\mathbb{Z})$ does not surject onto $\mathrm{GL}(n,p)$ modulo all primes $p \geq 5$.
- $\mathrm{SL}(n,\mathbb{Z})$ surjects onto $\mathrm{SL}(n,p)$ modulo all primes.

Let H be an arithmetic subgroup of $\mathrm{SL}(n,\mathbb{Z})$, $n > 2$.

Fact 1. H surjects onto $\mathrm{SL}(n,p)$ modulo all but a finite number of primes p.
Reason: H is Zariski dense in SL_n (strong approximation theorem).

Moreover

Fact 2. 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 $n = 3, 4$, $p = 2$).

These provide fast algorithms for computing the level M of the maximal principal congruence subgroup of H.

6.2 Algorithms: library of functions

6.2.1 Computing the level and related procedures

Given: arithmetic subgroup H of $\mathrm{SL}(n, \mathbb{Z})$.

`LevelMaxPCS`(H): computes the level M of the maximal principal congruence subgroup $\Gamma_{n,M}$ of H.

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

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

6.2.1 Subnormal structure

`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 $\langle H \rangle^{\Gamma_n}$.

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

6.2.3 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.: $\mathrm{Stab}_H(u)$ is a finitely generated group.
Method: solution of orbit-stabilizer problem for $\varphi_m(H)$ acting on $\mathbb{Z}^n$ and $\Gamma_{n,m} \leq H$.

Details: see in Section 4 in Journal of Algebra 421 (2015) 234-259.

6.3 Applications and experimental results

6.3.1 Arithmetic groups and low dimensional topology.

Example(Long & Reid, 2011). Define $\beta_T(F) = \langle X_T, Y_T \rangle \leq \mathrm{SL}(3, \mathbb{Z})$, where

$$X_T = \begin{bmatrix} -1+T^3 & -T & T^2 \\ 0 & -1 & 2T \\ -T & 0 & 1 \end{bmatrix}, Y_T = \begin{bmatrix} -1 & 0 & 0 \\ -T^2 & 1 & -T \\ T & 0 & -1 \end{bmatrix}, T \in \mathbb{Z}.$$

Theorem (Long & Reid, 2011) Fix an integer $T \neq 0$. Then the groups $\beta_T(F)$ are arithmetic and $\cap_{T>0}\beta_T(F) = 1$.

Problem (Long & Reid): what are the indices $|\mathrm{SL}(3, \mathbb{Z}) : \beta_T(F)|$?

N.B.: $|\mathrm{SL}(3, \mathbb{Z}) : \beta_T(F)| \to \infty$ as $T \to \infty$.

T	M	index	t(sec.)
1	5	$2^3 31$	0.3
2	2^5	$2^{20} 3 \cdot 7$	0.7
3	$3^3 73$	$2^5 3^{13} 13 \cdot 1801$	5.8
4	$2^7 23$	$2^{33} 3 \cdot 7^2 11 \cdot 79$	3.5
5	$5^3 367$	$2^4 3^3 5^{10} 13 \cdot 31 \cdot 61 \cdot 3463$	62.8
11	$5 \cdot 11^3 797$	$2^6 3 \cdot 5^2 7 \cdot 11^{10} 19 \cdot 31 \cdot 157 \cdot 199 \cdot 4051$	616.4
15	$3^3 5^3 67 \cdot 151$	$2^9 3^{15} 5^{12} 7^3 11 \cdot 13 \cdot 31^2 1093$	56.4
19	$19^3 67 \cdot 307$	$2^4 3^{10} 5 \cdot 7^2 11 \cdot 17 \cdot 19^{10} 31 \cdot 43 \cdot 127 \cdot 733$	108.1
50	$2^5 5^6 23 \cdot 1019$	$2^{27} 3^2 5^{25} 7^3 11 \cdot 31 \cdot 79 \cdot 509 \cdot 148483$	1137.9
100	$2^7 5^6 29 \cdot 67 \cdot 193$	$2^{46} 3^6 5^{25} 7^5 11 \cdot 13 \cdot 31^2 67 \cdot 1783$	186.2

6.3.2 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