Recent advances in computing with infinite linear groups

Alla Detinko
(joint work with Dane Flannery)

National University of Ireland, Galway

St Andrews, 3rd-11th August 2013

1. Preliminaries: computing with finitely generated linear groups

1. Preliminaries: computing with finitely generated linear groups

1.1 Set up

Given a finite set S of invertible matrices of degree n over a field F, consider the group $G = \langle S \rangle \subseteq GL(n, F)$. Then $G \subseteq GL(n, R) \subseteq GL(n, F)$ for a finitely generated integral domain $R \subseteq F$ determined by entries of matrices in $S \cup S^{-1}$.

1. Preliminaries: computing with finitely generated linear groups

1.1 Set up

Given a finite set S of invertible matrices of degree n over a field F, consider the group $G = \langle S \rangle \subseteq GL(n, F)$. Then $G \subseteq GL(n, R) \subseteq GL(n, F)$ for a finitely generated integral domain $R \subseteq F$ determined by entries of matrices in $S \cup S^{-1}$.

Given an ideal $\rho \subset R$, define the *congruence homomorphism*
$\varphi_\rho : GL(n, R) \to GL(n, R/\rho)$.
The kernel $ker\varphi_\rho(G) := G_\rho$ is a *congruence subgroup* of G.

1.2 Properties of a finitely generated linear group G

(i) G is residually finite, and is approximated by matrix groups of degree n over finite fields (Mal'cev).

1.2 Properties of a finitely generated linear group G

(i) G is residually finite, and is approximated by matrix groups of degree n over finite fields (Mal'cev).
(ii) There exist ideals $\rho \subset R$ such that G_ρ is torsion-free ($char\,F = 0$), and G_ρ is unipotent-by-abelian if G is solvable-by-finite (Selberg-Wehrfritz).

1.2 Properties of a finitely generated linear group G

(i) G is residually finite, and is approximated by matrix groups of degree n over finite fields (Mal'cev).
(ii) There exist ideals $\rho \subset R$ such that G_ρ is torsion-free ($char\, F = 0$), and G_ρ is unipotent-by-abelian if G is solvable-by-finite (Selberg-Wehrfritz).

Method developed (computational analogue of method of finite approximation).

1.2 Properties of a finitely generated linear group G

(i) G is residually finite, and is approximated by matrix groups of degree n over finite fields (Mal'cev).
(ii) There exist ideals $\rho \subset R$ such that G_ρ is torsion-free ($char F = 0$), and G_ρ is unipotent-by-abelian if G is solvable-by-finite (Selberg-Wehrfritz).

Method developed (computational analogue of method of finite approximation).

Implementation of congruence homomorphism techniques

- providing reduction to subgroups of $GL(n, \mathbb{F}_q)$ (by (i))
- with the kernel G_ρ satisfying (ii).

1.3 Problems solved

Using the above method we solved the following problems (over a broad range of domains).

1.3 Problems solved

Using the above method we solved the following problems (over a broad range of domains).

- `IsFinite`: testing finiteness of G, and investigation of structure of G if G is finite.

1.3 Problems solved

Using the above method we solved the following problems (over a broad range of domains).

- `IsFinite`: testing finiteness of G, and investigation of structure of G if G is finite.
- `IsSolvableByFinite`: computational analogue of the Tits alternative.

1.3 Problems solved

Using the above method we solved the following problems (over a broad range of domains).

- `IsFinite`: testing finiteness of G, and investigation of structure of G if G is finite.
- `IsSolvableByFinite`: computational analogue of the Tits alternative.
- Further properties: `IsAbelianByFinite`, `IsNilpotentByFinite`, `IsSolvable` etc., along with structural investigation of the groups.

1.3 Problems solved

Using the above method we solved the following problems (over a broad range of domains).

- `IsFinite`: testing finiteness of G, and investigation of structure of G if G is finite.
- `IsSolvableByFinite`: computational analogue of the Tits alternative.
- Further properties: `IsAbelianByFinite`, `IsNilpotentByFinite`, `IsSolvable` etc., along with structural investigation of the groups.

Feature of the method: test related properties of G_ρ without computing G_ρ.

1.4 Further development

1.4 Further development

The Tits Alternative: A finitely generated subgroup of $GL(n, F)$ is either solvable-by-finite, or contains a free non-abelian subgroup (J. Tits, 1972).

1.4 Further development

The Tits Alternative: A finitely generated subgroup of $GL(n, F)$ is either solvable-by-finite, or contains a free non-abelian subgroup (J. Tits, 1972).

Approach to further computing: consider two different classes separately.

1.4 Further development

The Tits Alternative: A finitely generated subgroup of $GL(n, F)$ is either solvable-by-finite, or contains a free non-abelian subgroup (J. Tits, 1972).

Approach to further computing: consider two different classes separately.

Obstacles for computing with solvable-by-finite groups G (cf. related classes of groups, e.g., polycyclic-by-finite groups).

1.4 Further development

The Tits Alternative: A finitely generated subgroup of $GL(n, F)$ is either solvable-by-finite, or contains a free non-abelian subgroup (J. Tits, 1972).

Approach to further computing: consider two different classes separately.

Obstacles for computing with solvable-by-finite groups G (cf. related classes of groups, e.g., polycyclic-by-finite groups).

- G may not be finitely presentable.

1.4 Further development

The Tits Alternative: A finitely generated subgroup of $GL(n, F)$ is either solvable-by-finite, or contains a free non-abelian subgroup (J. Tits, 1972).

Approach to further computing: consider two different classes separately.

Obstacles for computing with solvable-by-finite groups G (cf. related classes of groups, e.g., polycyclic-by-finite groups).

- G may not be finitely presentable.
- Subgroups of G may not be finitely generated.

1.4 Further development

The Tits Alternative: A finitely generated subgroup of $GL(n, F)$ is either solvable-by-finite, or contains a free non-abelian subgroup (J. Tits, 1972).

Approach to further computing: consider two different classes separately.

Obstacles for computing with solvable-by-finite groups G (cf. related classes of groups, e.g., polycyclic-by-finite groups).

- G may not be finitely presentable.
- Subgroups of G may not be finitely generated.
- Lack of methods for computing with SF linear groups: e.g., standard algorithms based on computing normal closure may not terminate.

2. Linear groups of finite rank

2. Linear groups of finite rank

A group G has *finite Prüfer rank* $rk(G)$ if each finitely generated subgroup of G can be generated by $rk(G)$ elements, and $rk(G)$ is the least such integer.

2. Linear groups of finite rank

A group G has *finite Prüfer rank* $rk(G)$ if each finitely generated subgroup of G can be generated by $rk(G)$ elements, and $rk(G)$ is the least such integer.

- How strong is this restriction?

2. Linear groups of finite rank

A group G has *finite Prüfer rank* $rk(G)$ if each finitely generated subgroup of G can be generated by $rk(G)$ elements, and $rk(G)$ is the least such integer.

- How strong is this restriction?
- Why groups of finite rank, i.e., what are computational advantages of such groups?

2. Linear groups of finite rank

A group G has *finite Prüfer rank* $rk(G)$ if each finitely generated subgroup of G can be generated by $rk(G)$ elements, and $rk(G)$ is the least such integer.

- How strong is this restriction?
- Why groups of finite rank, i.e., what are computational advantages of such groups?

2.1 What are linear groups of finite rank?

Theorem. If $G \subseteq GL(n, F)$ has finite Prüfer rank then G is solvable-by-finite.

2. Linear groups of finite rank

A group G has *finite Prüfer rank* $rk(G)$ if each finitely generated subgroup of G can be generated by $rk(G)$ elements, and $rk(G)$ is the least such integer.

- How strong is this restriction?
- Why groups of finite rank, i.e., what are computational advantages of such groups?

2.1 What are linear groups of finite rank?

Theorem. If $G \subseteq GL(n, F)$ has finite Prüfer rank then G is solvable-by-finite.

Proposition. A finitely generated subgroup G of $GL(n, F)$ has finite Prüfer rank if it is solvable-by-finite and $\mathbb{Q}$-linear.

Further properties.

A group G has *finite torsion-free rank* if it has a (subnormal) series of finite length whose factors are either infinite cyclic or periodic. The number $h(G)$ of infinite cyclic factors is the *torsion-free rank* of G.

Further properties.

A group G has *finite torsion-free rank* if it has a (subnormal) series of finite length whose factors are either infinite cyclic or periodic. The number $h(G)$ of infinite cyclic factors is the *torsion-free rank* of G.

Proposition. Let G be a finitely generated subgroup of $GL(n, \mathbb{Q})$. Then the following are equivalent.

- G is solvable-by-finite.
- G is of finite Prüfer rank.
- G is of finite torsion-free rank.

2.2. Structure of finitely generated linear groups of finite rank

2.2. Structure of finitely generated linear groups of finite rank

2.2.1 Polyrational groups

A group is *polyrational* if it has a series of finite length with each factor isomorphic to a subgroup of the additive group $\mathbb{Q}^+$.

2.2. Structure of finitely generated linear groups of finite rank

2.2.1 Polyrational groups

A group is *polyrational* if it has a series of finite length with each factor isomorphic to a subgroup of the additive group $\mathbb{Q}^+$.

Proposition. A finitely generated subgroup G of $GL(n, F)$ has finite Prüfer rank if and only if G is polyrational-by-finite.

In this case $h(G) \leq rk(G)$, and $h(G) = rk(G)$ if G is polyrational.

2.2.2 Unipotent radicals

2.2.2 Unipotent radicals

Given $G \subseteq GL(n, F)$, denote by G_u the *unipotent radical* of G, i.e., the maximal unipotent normal subgroup of G.

2.2.2 Unipotent radicals

Given $G \subseteq GL(n, F)$, denote by G_u the *unipotent radical* of G, i.e., the maximal unipotent normal subgroup of G.

Lemma. If $G \subseteq GL(n, F)$ is finitely generated solvable-by-finite then G/G_u is a finitely generated abelian-by-finite completely reducible group.

2.2.2 Unipotent radicals

Given $G \subseteq GL(n, F)$, denote by G_u the *unipotent radical* of G, i.e., the maximal unipotent normal subgroup of G.

Lemma. If $G \subseteq GL(n, F)$ is finitely generated solvable-by-finite then G/G_u is a finitely generated abelian-by-finite completely reducible group.

Remark. G_u is not necessarily finitely generated.

2.2.2 Unipotent radicals

Given $G \subseteq GL(n, F)$, denote by G_u the *unipotent radical* of G, i.e., the maximal unipotent normal subgroup of G.

Lemma. If $G \subseteq GL(n, F)$ is finitely generated solvable-by-finite then G/G_u is a finitely generated abelian-by-finite completely reducible group.

Remark. G_u is not necessarily finitely generated.

Proposition. Let $G \subseteq GL(n, \mathbb{Q})$ be finitely generated solvable-by-finite. Then there exists a finitely generated subgroup H of G_u such that $G_u = \langle H \rangle^G$ and $h(H) = h(G_u) = rk(G_u)$.

2.2.2 Unipotent radicals

Given $G \subseteq GL(n, F)$, denote by G_u the *unipotent radical* of G, i.e., the maximal unipotent normal subgroup of G.

Lemma. If $G \subseteq GL(n, F)$ is finitely generated solvable-by-finite then G/G_u is a finitely generated abelian-by-finite completely reducible group.

Remark. G_u is not necessarily finitely generated.

Proposition. Let $G \subseteq GL(n, \mathbb{Q})$ be finitely generated solvable-by-finite. Then there exists a finitely generated subgroup H of G_u such that $G_u = \langle H \rangle^G$ and $h(H) = h(G_u) = rk(G_u)$.

- G_u is polyrational, and H is poly-$\mathbb{Z}$.
- G_u is the isolator of H in G_u, i.e., for each $g \in G_u$ there exists $m \in \mathbb{Z}$ such that $g^m \in H$.

3. Computing ranks

Set up: Given a finitely generated group $G \leq GL(n, \mathbb{P})$, $|\mathbb{P} : \mathbb{Q}| < \infty$.

3. Computing ranks

Set up: Given a finitely generated group $G \leq GL(n, \mathbb{P})$, $|\mathbb{P} : \mathbb{Q}| < \infty$.

Method. All algorithms are based on congruence homomorphism techniques, i.e., selection of a maximal ideal $\rho \subset R \subset \mathbb{P}$ such that G_ρ is torsion-free (and unipotent-by-abelian if G is solvable-by-finite), and construction of $\varphi_\rho(G) \subset GL(n, \mathbb{F}_q)$, $\mathbb{F}_q \cong R/\rho$.

3. Computing ranks

Set up: Given a finitely generated group $G \leq GL(n, \mathbb{P})$, $|\mathbb{P} : \mathbb{Q}| < \infty$.

Method. All algorithms are based on congruence homomorphism techniques, i.e., selection of a maximal ideal $\rho \subset R \subset \mathbb{P}$ such that G_ρ is torsion-free (and unipotent-by-abelian if G is solvable-by-finite), and construction of $\varphi_\rho(G) \subset GL(n, \mathbb{F}_q)$, $\mathbb{F}_q \cong R/\rho$.

3.1. First steps

3. Computing ranks

Set up: Given a finitely generated group $G \leq GL(n, \mathbb{P})$, $|\mathbb{P} : \mathbb{Q}| < \infty$.

Method. All algorithms are based on congruence homomorphism techniques, i.e., selection of a maximal ideal $\rho \subset R \subset \mathbb{P}$ such that G_ρ is torsion-free (and unipotent-by-abelian if G is solvable-by-finite), and construction of $\varphi_\rho(G) \subset GL(n, \mathbb{F}_q)$, $\mathbb{F}_q \cong R/\rho$.

3.1. First steps

We can test whether G is of finite rank.

3. Computing ranks

Set up: Given a finitely generated group $G \leq GL(n, \mathbb{P})$, $|\mathbb{P} : \mathbb{Q}| < \infty$.

Method. All algorithms are based on congruence homomorphism techniques, i.e., selection of a maximal ideal $\rho \subset R \subset \mathbb{P}$ such that G_ρ is torsion-free (and unipotent-by-abelian if G is solvable-by-finite), and construction of $\varphi_\rho(G) \subset GL(n, \mathbb{F}_q)$, $\mathbb{F}_q \cong R/\rho$.

3.1. First steps

We can test whether G is of finite rank.

`IsOfFiniteRank`: returns `true` if $rk(G)$ is finite (i.e., $h(G)$ is finite); otherwise returns `false`.

3.2 Reduction to completely reducible case

3.2 Reduction to completely reducible case

(i) `CompletelyReduciblePart`: constructs a completely reducible part $\pi(G)$ of a finitely generated solvable-by-finite subgroup G of $GL(n, F)$, i.e., a generating set of the completely reducible abelian-by-finite group $\pi(G) \cong G/G_u$.

Method: computing in enveloping algebra of G_ρ.

3.2 Reduction to completely reducible case

(i) `CompletelyReduciblePart`: constructs a completely reducible part $\pi(G)$ of a finitely generated solvable-by-finite subgroup G of $GL(n, F)$, i.e., a generating set of the completely reducible abelian-by-finite group $\pi(G) \cong G/G_u$.
Method: computing in enveloping algebra of G_ρ.

(ii) `RankCR`: for a finitely generated completely reducible solvable-by-finite group G returns $h(G) = h(G_\rho)$; here G_ρ is completely reducible finitely generated abelian.

3.3 Rank of unipotent radical

`RankOfUnipotentRad`

1. Construct a finitely generated $H \leq G_u$ such that $h(H) = h(G_u)$, $G_u = \langle H \rangle^G$ (via a presentation of $\pi(G)$, and normal subgroup generators method).
2. Return $h(H)$.

3.4 General case

Compute two main structural components:

3.3 Rank of unipotent radical

`RankOfUnipotentRad`

1. Construct a finitely generated $H \leq G_u$ such that $h(H) = h(G_u)$, $G_u = \langle H \rangle^G$ (via a presentation of $\pi(G)$, and normal subgroup generators method).
2. Return $h(H)$.

3.4 General case

Compute two main structural components:

1. Completely reducible part $\pi(G)$ of G.

3.3 Rank of unipotent radical

`RankOfUnipotentRad`

1. Construct a finitely generated $H \leq G_u$ such that $h(H) = h(G_u)$, $G_u = \langle H \rangle^G$ (via a presentation of $\pi(G)$, and normal subgroup generators method).
2. Return $h(H)$.

3.4 General case

Compute two main structural components:

1. Completely reducible part $\pi(G)$ of G.
2. $H \leq G_u$ as in (3.2).

3.3 Rank of unipotent radical

`RankOfUnipotentRad`

1. Construct a finitely generated $H \leq G_u$ such that $h(H) = h(G_u)$, $G_u = \langle H \rangle^G$ (via a presentation of $\pi(G)$, and normal subgroup generators method).
2. Return $h(H)$.

3.4 General case

Compute two main structural components:

1. Completely reducible part $\pi(G)$ of G.
2. $H \leq G_u$ as in (3.2).

   Then
3. Apply the formula $h(G) = h(G/G_u) + h(G_u)$ as $G_u \lhd G$.

4. Applications: subgroups of finite index

4. Applications: subgroups of finite index

4.1 Ranks and subgroups of finite index

4. Applications: subgroups of finite index

4.1 Ranks and subgroups of finite index

Theorem (D. Robinson, 2012). Let H be a subgroup of a finitely generated solvable FAR group G. Then $|G : H|$ is finite if and only if $h(H) = h(G)$.

4. Applications: subgroups of finite index

4.1 Ranks and subgroups of finite index

Theorem (D. Robinson, 2012). Let H be a subgroup of a finitely generated solvable FAR group G. Then $|G : H|$ is finite if and only if $h(H) = h(G)$.

Remark. Here solvable FAR group means that G has finite abelian ranks.

4. Applications: subgroups of finite index

4.1 Ranks and subgroups of finite index

Theorem (D. Robinson, 2012). Let H be a subgroup of a finitely generated solvable FAR group G. Then $|G : H|$ is finite if and only if $h(H) = h(G)$.

Remark. Here solvable FAR group means that G has finite abelian ranks.

Corollary. Let $H \leq G \leq GL(n, F)$ where G is finitely generated and of finite Prüfer rank. Then $|G : H|$ is finite if and only if $h(H) = h(G)$.

4. Applications: subgroups of finite index

4.1 Ranks and subgroups of finite index

Theorem (D. Robinson, 2012). Let H be a subgroup of a finitely generated solvable FAR group G. Then $|G : H|$ is finite if and only if $h(H) = h(G)$.

Remark. Here solvable FAR group means that G has finite abelian ranks.

Corollary. Let $H \leq G \leq GL(n, F)$ where G is finitely generated and of finite Prüfer rank. Then $|G : H|$ is finite if and only if $h(H) = h(G)$.

`IsOfFiniteIndex(`S_1, S_2`)`: for finite subsets S_1, S_2 of $GL(n, \mathbb{P})$ such that $G = \langle S_1 \rangle$ is solvable-by-finite and $H = \langle S_2 \rangle \leq G$ returns `true` if and only if $h(G) = h(H)$.

5. Example: arithmeticity of solvable linear groups

5. Example: arithmeticity of solvable linear groups

Notation. Given $K \leq GL(n, \mathbb{C})$ and a subring $R \leq \mathbb{C}$, denote $K \cap GL(n, R)$ by K_R.

Definition. Let G be an algebraic group defined over $\mathbb{Q}$. A subgroup H of $G_{\mathbb{Q}}$ is said to be *arithmetic* if H is commensurable with $G_{\mathbb{Z}}$, i.e. $H_{\mathbb{Z}}$ has finite index in both H and $G_{\mathbb{Z}}$.

5. Example: arithmeticity of solvable linear groups

Notation. Given $K \leq GL(n, \mathbb{C})$ and a subring $R \leq \mathbb{C}$, denote $K \cap GL(n, R)$ by K_R.

Definition. Let G be an algebraic group defined over $\mathbb{Q}$. A subgroup H of $G_\mathbb{Q}$ is said to be *arithmetic* if H is commensurable with $G_\mathbb{Z}$, i.e. $H_\mathbb{Z}$ has finite index in both H and $G_\mathbb{Z}$.

Problem. Given a finitely generated subgroup H of $G_\mathbb{Q}$, is H arithmetic (in G)?

Solution. `IsArithmeticSolvable`(S, G).

For a solvable algebraic group G and a finite subset S of $G_{\mathbb{Q}}$ returns `true` if $H = \langle S \rangle$ is arithmetic; `false` otherwise.

Solution. `IsArithmeticSolvable`(S, G).

For a solvable algebraic group G and a finite subset S of $G_{\mathbb{Q}}$ returns `true` if $H = \langle S \rangle$ is arithmetic; `false` otherwise.

Main steps:

- `GeneratingArithmetic`(G): returns a generating set of a finite index subgroup of $G_{\mathbb{Z}}$ (de Graaf, 2013).

Solution. `IsArithmeticSolvable`(S, G).

For a solvable algebraic group G and a finite subset S of $G_{\mathbb{Q}}$ returns `true` if $H = \langle S \rangle$ is arithmetic; `false` otherwise.

Main steps:

- `GeneratingArithmetic`(G): returns a generating set of a finite index subgroup of $G_{\mathbb{Z}}$ (de Graaf, 2013).
- `IsIntegralSF`(H): tests whether H is integral.

Solution. `IsArithmeticSolvable`(S, G).

For a solvable algebraic group G and a finite subset S of $G_{\mathbb{Q}}$ returns `true` if $H = \langle S \rangle$ is arithmetic; `false` otherwise.

Main steps:

- `GeneratingArithmetic`(G): returns a generating set of a finite index subgroup of $G_{\mathbb{Z}}$ (de Graaf, 2013).
- `IsIntegralSF`(H): tests whether H is integral.
- Computing ranks of $G_{\mathbb{Z}}$ and $H = \langle S \rangle$.

6. Conclusion: implementation

Implementation of algorithms in MAGMA:

- For SF linear groups (Eamonn O'Brien, 2012);
- For arithmetic subgroups of solvable algebraic groups (Willem de Graaf, 2013).