Irreducibility Testing of Nilpotent Matrix Groups

Tobias Rossmann

Galway, 6 May 2011

NUI Galway
OÉ Gaillimh

science foundation ireland
fondúireacht eolaíochta éireann

This work is supported by the Research Frontiers Programme of Science Foundation Ireland

Matrix groups

Definition

A **matrix group** over a field K is a subgroup of $\mathrm{GL}_d(K)$.

- Matrix groups arise naturally in mathematics (and elsewhere).
- They are one of the basic ways of representing groups on a computer. In practice, they are usually given by finite sequences of generating matrices.

Computing with matrix groups

Computing with matrix groups over finite fields

- The *"Matrix Group Recognition Project"* has essentially been completed (≈ 20 years).
- Many problems have efficient solutions (up to basic oracles).
- Implementations exist (or are being developed) in GAP or MAGMA.

Computing with matrix groups over infinite fields

- Fundamental problems are undecidable (e.g. membership).
- Many computational problems are open.

Recent project (Detinko & Flannery, Eick, O'Brien, . . .)

Develop and implement practical algorithms for basic computational problems related to finitely generated matrix groups over infinite fields.

Fundamental problems

Let $G \leqslant \mathrm{GL}_d(K)$ be given by finitely many generators.

Group-theoretic problems

- Decide if G is finite, soluble, nilpotent, ...
- Compute centralisers, normalisers, ...
- Find a finite presentation for G (if possible).
- ...

Geometric problems

- Decide irreducibility, primitivity, ... of G.
- Orbit-stabiliser problem.
- Decide membership in G of a given $x \in \mathrm{GL}_d(K)$.
- ...

Irreducibility testing

Definition

Let $G \leqslant \mathrm{GL}_d(K)$. Then G is **reducible** if there exists a proper G-invariant subspace of K^d. Otherwise, G is **irreducible**.

Computational tasks

1. Decide if G is irreducible.
2. If G is reducible, construct an invariant subspace.

Relevance

- Irreducibility is the most fundamental module-theoretic property.
- Reduction to irreducible groups is a common technique in the theory of matrix groups.
- Starting point of MGRP over finite fields.

Irreducibility testing

Computational tasks (again)

1. Decide if G is irreducible.
2. If G is reducible, construct an invariant subspace.

The state of the art

- Irreducibility of matrix groups over finite fields can be tested using the MEAT-AXE algorithm. (Parker 1984, Holt & Rees 1994, ...)
- Irreducibility of finite matrix groups over the rationals can be tested effectively (Nebe & Steel 2009). Implemented in MAGMA.

Computing with nilpotent matrix groups

- Nilpotent matrix groups have been studied extensively (Suprunenko).
- They have been shown to be well-suited for computations.
- Nilpotency and finiteness can be tested (Detinko & Flannery 2008).
- In (Detinko & Flannery 2006), an algorithm which simultaneously tests irreducibility and primitivity of nilpotent matrix groups over finite fields was developed.

This talk

Let K be a number field. We describe an algorithm for deciding irreducibility of f.g. nilpotent matrix groups over K. In the case of finite nilpotent groups, we obtain a fully constructive algorithm. Time permitting, we also consider primitivity testing of finite nilpotent groups.

Matrix groups and algebras

Definition

Let $G \leqslant \mathrm{GL}_d(K)$.

- The **enveloping algebra** $K[G]$ of G is the subalgebra of $\mathrm{M}_d(K)$ generated by G.
- If $K[G]$ is semisimple, then G is **completely reducible**.
- If $K[G]$ is simple, then G is **homogeneous**.

Fact

G irreducible $\Rightarrow$ G homogeneous $\Rightarrow$ G completely reducible.

Fact (Detinko & Flannery 2008)

If G is f.g. nilpotent, then we can either prove that G is completely reducible or we can construct a proper $K[G]$-submodule.

The strategy

Let $G \leqslant \mathrm{GL}_d(K)$ be f.g., nilpotent, and completely reducible.

Goal: decide irreducibility of G.

We proceed as follows:

0. The case that G is abelian is easily treated.
1. Find an abelian normal subgroup $A \triangleleft G$ which is either inhomogeneous or homogeneous and maximal (i.e. $A = \mathrm{C}_G(A)$).
2. If A is inhomogeneous, then we can either prove reducibility of G or we reduce irreducibility testing to a problem in smaller dimension.
3. If A is homogeneous and maximal, then we can use computational Galois cohomology to decide irreducibility of G.

Step 1: constructing abelian normal subgroups

Let $G \leqslant \mathrm{GL}_d(K)$ be finitely generated, nilpotent and completely reducible.

Using congruence homomorphisms

We can find a homomorphism $G \xrightarrow{\pi} H$ onto a finite group H with the following property: a subgroup $A \leqslant G$ is abelian iff A^π is abelian.

Explicitly:

- Let R be the ring of integers of K.
- Choose an odd unramified prime $\mathfrak{p} \triangleleft R$ such that $G \leqslant \mathrm{GL}_d(R_\mathfrak{p})$.
- Take π to be the natural map $G \to G \bmod \mathfrak{p} \leqslant \mathrm{GL}_d(R/\mathfrak{p})$.
- By a theorem of Suprunenko and basic ANT, $\mathrm{Ker}(\pi)$ is torsion-free.
- Another result of Suprunenko implies that $[G, G]$ is finite.
- Hence, if A^π is abelian, then $[A, A] \leqslant \mathrm{Ker}(\pi) \cap [G, G] = 1$.

Step 1: constructing abelian normal subgroups

Goal: find an abelian $A \lhd G$ which is inhomgs or homgs and maximal.

Fact

A completely reducible abelian $A \leqslant \mathrm{GL}_d(K)$ is homg iff $K[A]$ is a field.

Fact (Dixon; Eberly)

For a completely reducible abelian $A \leqslant \mathrm{GL}_d(K)$, "most" elements $x \in K[A]$ satisfy $K[A] = K[x]$.

Let $G \xrightarrow{\pi} H$ be as on the previous slide. Using a presentation of H we find generators of $\mathrm{Ker}(\pi)$; note that $\mathrm{Ker}(\pi) \leqslant \mathrm{Z}(G)$.

1. Let $B \lhd H$ be abelian.
2. If $B^{\pi^{-1}}$ is inhomogeneous, then stop.
3. If B is maximal abelian, then stop.
4. Enlarge $B < \mathrm{C}_H(B)$ and go to 2.

Step 2: reduction

Goal: make use of an inhomogeneous normal subgroup.

Theorem (Clifford 1937 + Detinko & Flannery 2006)

Let $G \leqslant \mathrm{GL}_d(K)$ *be completely reducible,* $N \triangleleft G$*, and* $K^d = U_1 \oplus \cdots \oplus U_r$ *be the homgs decompn over* $K[N]$*. Then* G *is irreducible if and only if*

1. G *acts transitively on* $\mathcal{U} = \{U_1, \ldots, U_r\}$*, and*
2. $\mathrm{Stab}_G(U_1)$ *acts irreducibly on* U_1*.*

- $\mathcal{U}$ can be easily computed if N is abelian.
- We may test transitivity of G on $\mathcal{U}$ using perm. group algorithms.
- The action of $\mathrm{Stab}_G(U_1)$ on U_1 can be computed using linear algebra.

Reduction

If N is inhomogeneous (i.e. $|\mathcal{U}| > 1$), then we can either prove reducibility of G or we continue irreducibility testing in smaller dimension.

A reminder: crossed products

Let L/Z be a finite Galois extension of number fields, $\Gamma = \mathrm{Gal}(L/Z)$, and $\phi \in \mathrm{Z}^2(\Gamma, L^\times)$. Define

$$L \star_\phi \Gamma = \bigoplus_{\sigma \in \Gamma} u_\sigma L$$

with multiplication $a u_\sigma = u_\sigma a^\sigma$ $(a \in L, \sigma \in \Gamma)$ and $u_\sigma u_\tau = u_{\sigma\tau} \cdot (\sigma, \tau)\phi$. The algebra $L \star_\phi \Gamma$ is the **crossed product** of L by Γ determined by ϕ.

Facts

- $\mathcal{A} = L \star_\phi \Gamma$ is a central simple Z-algebra.
- $\mathrm{index}(\mathcal{A}) =$ L-dimension of the irreducible $\mathcal{A}$-module.
- $\mathrm{index}(\mathcal{A}) =$ order of $[\phi] \in \mathrm{H}^2(\Gamma, L^\times)$. (Brauer-Hasse-Noether 1932)
- The order of $[\phi]$ can be determined algorithmically. (Fieker 2009)

Step 3: cohomology

Goal: decide irreducibility of G if $A \triangleleft G$ is homogeneous and max. abelian.

Proposition

Let $G \leqslant \mathrm{GL}_d(K)$ be nilpotent and let $A \triangleleft G$ be max. abelian and homgs.

1. *Let $L = K[A]$. Then G/A acts faithfully on L by conjugation.*
2. *Let $Z = L^{G/A}$. Then $K[G] \cong_Z L \star G/A$ in the natural way.*

We may thus decide irreducibility of G as follows:

1. Construct $\phi \in \mathrm{Z}^2(G/A, A)$ corr. to $1 \to A \to G \to G/A \to 1$.
2. Compute $m =$ order of $[\phi] \in \mathrm{H}^2(G/A, L^\times)$.
3. Check if $d = m|L : K|$.

Summary (deciding irreducibility)

Deciding irreducibility of a f.g. nilpotent group $G \leqslant \mathrm{GL}_d(K)$ (main steps):

1. Construct an abelian normal subgroup $A \triangleleft G$ which is inhomogeneous or maximal abelian and homogeneous.
2. If A is inhomogeneous, then either prove reducibility or reduce to smaller dimension and start again.
3. If A is maximal abelian and homogeneous, then compute the index of $K[G]$ and read off irreducibility of G.

Remark

We don't (in general) obtain a submodule in case 3.

Example: cyclic algebras

Suppose that K contains a primitive mth root of unity ζ_m. Let $\lambda, \nu \in K^\times$ and suppose that $X^m - \nu$ is irreducible over K. Let $\beta = \sqrt[m]{\nu}$ and define

$$G = \left\langle \underbrace{\begin{bmatrix} \beta & & & \\ & \beta \cdot \zeta_m & & \\ & & \ddots & \\ & & & \beta \cdot \zeta_m^{m-1} \end{bmatrix}}_{u}, \begin{bmatrix} 0 & 1 & & \\ & \ddots & \ddots & \\ & & 0 & 1 \\ \lambda & & & \end{bmatrix} \right\rangle.$$

Note that G has class 2. Regard G as a matrix group over K of degree m^2. Then $A = \langle \lambda, u, \zeta_m \rangle$ is a homgs maximal abelian normal subgroup of G with $G/A \cong \mathrm{C}_m$. It is well-known that $K[G]$ is a **cyclic algebra**.

Fact

Let m be a prime. Then G is reducible iff $\mathrm{N}_{K(\beta)/K}(x) = \lambda$ has a soln.

The finite case

- We obtain a fully constructive algorithm for irreducibility testing of finite nilpotent matrix groups.
- We can handle a considerably larger class of fields of char. zero.
  - In theory: any field of characteristic zero with algorithms for polynomial factorisation and for solving $x^2 + y^2 = -1$.
  - In practice: number fields and rational function fields over these.
- The algorithm is quite practical. An implementation is available in MAGMA V2.17 and as a stand-alone package.
- Primitivity can be tested too.

The strategy (finite case)

Fact

If $A \leqslant \mathrm{GL}_d(K)$ is finite non-cyclic abelian, then A is inhomogeneous.

Strategy (based on (Detinko & Flannery 2006) for finite fields)

Let $G \leqslant \mathrm{GL}_d(K)$ be finite nilpotent.

1. Find a non-cyclic abelian normal subgp of G or prove that none exists.
2. In the first case, reduce.
3. In the second case, test irreducibility of G directly.

Theorem (Roquette 1958, ...)

Let G be finite nilpotent. All abelian normal subgroups of G are cyclic iff

- *G_2 is cyclic or isomorphic to Q_8 or to D_{2^k}, SD_{2^k}, Q_{2^k} for $k \geqslant 4$, and*
- *$G_{2'}$ is cyclic.*

Finding non-cyclic abelian normal subgroups

We can find $A \triangleleft G$ which is non-cyclic or cyclic and max. abelian.

Lemma

Let G be a finite nilpotent group such that $[G, G]$ is cyclic. Define $H = \mathrm{C}_G([G, G])$.

1. *If $H_{2'}$ is cyclic and H_2 is cyclic or $H_2 \cong \mathrm{Q}_8$, then all abelian normal subgroup of G are cyclic.*
2. *Suppose that $H_p \ncong \mathrm{Q}_8$ is non-abelian. Then $\langle \mathrm{Z}(H_p), h \rangle$ is a non-cyclic abelian normal subgroup of G for some $h \in H_p$.*

Proof.

1. Follows from (Berger, Kovács, Newman 1980).
2. Note that $\mathrm{class}(H_p) = 2$. If $\langle \mathrm{Z}(H_p), h \rangle$ were cyclic for all $h \in H_p$, then H_p would contain a unique subgroup of order p. But then H_p would be cyclic or generalised quaternion, which is impossible. ◆

Enter $x^2 + y^2 = -1$

Let all abelian normal subgps of a non-abelian $G \leqslant \mathrm{GL}_d(K)$ be cyclic.

- Let $A \triangleleft G$ be cyclic of index 2. We may assume that A is homgs.
- Let $Z = \mathrm{Z}(K[G]) = K[A]^G$. We find that

$$K[G] \cong_Z \left(\frac{-1, \pm 1}{Z}\right) = Z(\sqrt{-1}) \star \mathrm{C}_2.$$

Lemma

1. *If G_2 is (semi)dihedral, then G is irreducible iff $d = 2|Z : K|$.*
2. *Let G_2 be quaternion. If $x^2 + y^2 = -1$ is soluble in Z, then G is irreducible iff $d = 2|Z : K|$. Otherwise, G is irreducible iff $d = 4|Z : K|$.*

Enter $x^2 + y^2 = -1$

Example

We have $K[G] \cong \left(\frac{-1,-1}{K}\right)$, where

$$G = \left\langle \begin{bmatrix} . & 1 & . & . \\ -1 & . & . & . \\ . & . & . & -1 \\ . & . & 1 & . \end{bmatrix}, \begin{bmatrix} . & . & 1 & . \\ . & . & . & 1 \\ -1 & . & . & . \\ . & -1 & . & . \end{bmatrix} \right\rangle \leqslant \mathrm{GL}_4(K).$$

Hence, G is reducible iff $x^2 + y^2 = -1$ is soluble in K. If this is the case, then finding a proper $K[G]$-submodule is equivalent to finding a solution of $x^2 + y^2 = -1$.

Primitivity testing

Definition

Let $G \leqslant \mathrm{GL}_d(K)$ be irreducible. If there exists a non-trivial decomposition

$$K^d = U_1 \oplus \cdots \oplus U_r$$

permuted by G, then G is **imprimitive**. Otherwise, G is **primitive**. A subspace U_i is a **block** and a subgp $\mathrm{Stab}_G(U_i)$ is **block stabiliser** for G.

Computational tasks

1. Decide if G is primitive.
2. If G is imprimitive, construct a system of imprimitivity.

Elementary facts

Facts

Let $G \leqslant \mathrm{GL}_d(K)$ be irreducible.

- *$H < G$ is a block stabiliser iff there is an irreducible $K[H]$-submodule $U < K^d$ with $d = |G : H||U : K|$.*
- *G is imprimitive iff some max. subgp of G is a block stabiliser.*
- *If $H < G$ has index 2, then H is a block stabiliser iff H is reducible.*
- *If G is primitive, then all normal subgroups of G are homogeneous.*

Maximal subgroups

Let $G \leqslant \mathrm{GL}_d(K)$ be finite, nilpotent, and irreducible.

- If $A \triangleleft G$ is non-cyclic abelian G, then G is imprimitive.
- We obtain a reduction to the case that all abelian $A \triangleleft G$ are cyclic.
- The abelian case is easily treated (again).
- Let $A \triangleleft G$ be cyclic of index 2. We may assume that A is irreducible.
- It suffices to test if any of the max. subgps of G is a block stabiliser.
- The interesting ones correspond to the prime divisors of $|G|$.

Lemma

$|G| = \mathcal{O}(d^{1+\varepsilon})$ *for* $\varepsilon > 0$.

Maximal subgroups

Proposition

1. *Let $H < G$ have prime index p ($+$ conditions for $p = 2$, e.g. $A \neq H$). Suppose that one of the following conditions is satisfied:*
   - *G_2 is (semi)dihedral,*
   - *$|G_2| \geqslant 32$, or*
   - *p is odd.*

   Then H is a block stabiliser iff $|K[A] : K[A^p]| = p$.
2. *If $G_2 \cong \mathrm{Q}_8$, then subgroups of index 2 of G are irreducible.*
3. *Suppose that $\mathrm{Q}_8 \times \mathrm{C}_m \cong H < G \cong \mathrm{Q}_{16} \times \mathrm{C}_m$ for odd m. Then H is a block stabiliser iff $|K[A] : K[A^2]| = 2$ and the following condition is satisfied: $\mathrm{ord}(2 \bmod m)|K_{\mathfrak{p}} : \mathbf{Q}_2|$ is even for all $\mathfrak{p} \mid 2$.*

We can thus test primitivity of G by looping over its maximal subgroups and testing the conditions in the proposition.