MATHEMATICS OF COMPUTATION
Volume 76, Number 259, July 2007, Pages 1669–1682
S 0025-5718(07)01979-5
Article electronically published on March 9, 2007

TESTING POLYCYCLICITY OF FINITELY GENERATED RATIONAL MATRIX GROUPS

BJÖRN ASSMANN AND BETTINA EICK

ABSTRACT. We describe algorithms for testing polycyclicity and nilpotency for finitely generated subgroups of $\mathrm{GL}(d,\mathbb{Q})$ and thus we show that these properties are decidable. Variations of our algorithm can be used for testing virtual polycyclicity and virtual nilpotency for finitely generated subgroups of $\mathrm{GL}(d,\mathbb{Q})$.

1. INTRODUCTION

The Tits' alternative states that a finitely generated subgroup of $\mathrm{GL}(d,\mathbb{Q})$ is either virtually solvable or contains a non-abelian free subgroup. Algorithms for deciding the Tits' alternative are described in [2], [6] and [12].

Polycyclic groups form a large and interesting subclass of the class of virtually solvable finitely generated groups. Many properties are algorithmically decidable for polycyclic groups as shown in [5], and various practical algorithms for polycyclically presented groups are described in [8].

An algorithm for checking whether a given finitely generated subgroup of $\mathrm{GL}(d,\mathbb{Q})$ is polycyclic has not been available so far. It is the central aim of this paper to present a solution for this problem. More precisely, given a finitely generated subgroup G of $\mathrm{GL}(d,\mathbb{Q})$, we describe algorithms for

(1) testing whether G is polycyclic (or virtually polycyclic),
(2) testing whether G is nilpotent (or virtually nilpotent).

Our methods for (1) and (2) rely on an algorithm for testing whether a virtually polycyclic group $G \leq \mathrm{GL}(d,\mathbb{Q})$ conjugates into $\mathrm{GL}(d,\mathbb{Z})$. We describe such an algorithm in Section 5. An alternative method for this purpose can be found in [3].

Our solutions for the algorithms in (1) and (2) are closely related to each other. They heavily rely on an application of the Mal'cev correspondence for upper unitriangular matrix groups. Based on that, they reduce to some simple applications of linear algebra methods.

Received by the editor February 21, 2006 and, in revised form, August 3, 2006.
2000 *Mathematics Subject Classification.* Primary 20F16, 20-04; Secondary 68W30.
Key words and phrases. Finitely generated matrix group, Tits' alternative, polycyclicity, nilpotency, Mal' cev correspondence.
The first author was supported by a Ph.D. fellowship of the "Gottlieb Daimler- und Karl Benz-Stiftung" and the UK Engineering and Physical Science Research Council (EPSRC).
The second author was supported by a Feodor Lynen Fellowship from the Alexander von Humboldt Foundation and by the Marsden Fund of New Zealand via grant UOA412.

We implemented our algorithm for testing polycyclicity using the computer algebra system GAP [14] as a basis. A report and comments on this implementation with runtimes for some example groups is included below.

Our algorithms also apply to finitely generated subgroups of $\mathrm{GL}(d, K)$, where K is an algebraic number field, since such matrix groups can be considered as subgroups of $\mathrm{GL}(d[K:\mathbb{Q}], \mathbb{Q})$.

2. Deciding the Tits' alternative

Let $G \leq \mathrm{GL}(d, \mathbb{Q})$ be finitely generated and denote $V = \mathbb{Q}^d$. In this section we briefly recall the method of [2] for testing whether G is solvable or virtually solvable, since we need various parts of it later.

2.1. **Computing a semisimple series.** A series $V = V_1 > \ldots > V_l > V_{l+1} = \{0\}$ of G-submodules through V is called *semisimple* if V_i/V_{i+1} is semisimple as a G-module for $1 \leq i \leq l$. In this subsection we briefly recall a method to determine a semisimple series for G.

Recall that the radical $Rad_G(V)$ is defined as the intersection of all maximal G-submodules in V and it is the smallest G-submodule in V with a semisimple factor module. Thus the determination of a semisimple series can be reduced to an iterated computation of radicals.

A method to compute the radical $Rad_G(V)$ has been introduced by L.E. Dickson in [7]. It uses that $Rad_G(V) = VRad_G(\mathbb{Q}[G])$, where $\mathbb{Q}[G]$ is the matrix algebra generated by G, and determines a basis for $Rad_G(\mathbb{Q}[G])$. For this purpose, it takes a basis for $\mathbb{Q}[G]$ and then reduces to solving a linear equation of size $\dim \mathbb{Q}[G]$.

2.2. **The p-congruence subgroup.** Since G is finitely generated, there exists a finite set of primes π such that $G \leq \mathrm{GL}(d, \mathbb{Q}_\pi)$, where $\mathbb{Q}_\pi$ is the set of all rational numbers $\frac{a}{b}$ with b divisible by primes in π only. Let $p > 2$ be a prime with $p \notin \pi$. Then the natural homomorphism $\psi_p : \mathbb{Q}_\pi \to \mathbb{F}_p$ extends to a homomorphism

$$\varphi_p : G \to \mathrm{GL}(d, \mathbb{F}_p)$$

defined by applying ψ_p to every entry in a matrix element of G. The kernel H of φ_p is called the *p-congruence subgroup* and the image I of φ_p is the *p-congruence image* of G. By construction, the group H has finite index in G. As G is finitely generated, this implies that H is finitely generated. Generators for H can be computed from generators for G using an orbit-stabilizer algorithm, since $H = Stab_G(B)$, where B is a basis of $\mathbb{F}_p^d$ and G acts via φ_p on $\mathbb{F}_p^d$. However, the resulting generating set for H is often too large to allow efficient computations. A usually significantly smaller set of normal subgroup generators for H can be determined from generators for G as described in [2].

2.3. **Testing (virtual) solvability.** The following theorem provides a characterisation of the finitely generated solvable or virtually solvable subgroups of $\mathrm{GL}(d, \mathbb{Q})$. This characterisation can be checked easily with available computational tools, and thus it yields an algorithm for checking solvability and virtual solvability. If the group G acts on a module W, then $G_W \leq \mathrm{GL}(W)$ denotes the group induced by the action of G on W. A proof for the following theorem can be found in [2].

1. **Theorem.** *Let $G \leq \mathrm{GL}(d, \mathbb{Q})$ be finitely generated with p-congruence subgroup H and p-congruence image I. Let $V = V_1 > \ldots > V_l > V_{l+1} = \{0\}$ be a semisimple series for G. Then:*

a) G is virtually solvable if and only if $H_{V_i/V_{i+1}}$ is abelian for $1 \leq i \leq l$.
b) G is solvable if and only if G is virtually solvable and I is solvable.

2.4. **Comparing classes of groups.** The polycyclic groups form a large subclass of the class of finitely generated solvable groups. For example, it is known that every finitely generated solvable subgroup of $\mathrm{GL}(d,\mathbb{Z})$ and every finitely generated nilpotent group is polycyclic. Thus, for example, since every finitely generated group U of upper unitriangular matrices in $\mathrm{GL}(d,\mathbb{Q})$ is nilpotent, U is also polycyclic. However, not every finitely generated solvable subgroup of $\mathrm{GL}(d,\mathbb{Q})$ is polycyclic, as the following example shows:

$$G = \langle \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \rangle.$$

The group G contains the normal subgroup $U = \{ \left(\begin{smallmatrix} 1 & \frac{a}{2^e} \\ 0 & 1 \end{smallmatrix}\right) \mid a \in \mathbb{Z}, e \in \mathbb{N}_0 \}$. The quotient G/U is infinite cyclic and U is abelian; thus G is solvable. However U is not finitely generated and hence G is not polycyclic.

3. The Mal'cev correspondence

In this section we recall the Mal'cev correspondence introduced in [11] restricted to the case that we want to use later and we summarise some of its fundamental properties. For more background we refer to [13, Chapter 6], [10, Chapter 9,10] and [4, Chapter 4].

Let $\mathrm{Tr}_1(d,\mathbb{Q}) \leq \mathrm{GL}(d,\mathbb{Q})$ denote the subgroup of all upper unitriangular matrices, and let $\mathrm{Tr}_0(d,\mathbb{Q})$ denote the Lie algebra of all upper triangular $d \times d$-matrices over $\mathbb{Q}$ having zeros on the diagonal, where the Lie bracket is defined in the standard form $[x,y] = xy - yx$. We define the *logarithm* and the *exponential* maps as follows:

$$\begin{aligned} \log &: \mathrm{Tr}_1(d,\mathbb{Q}) \to \mathrm{Tr}_0(d,\mathbb{Q}) \\ &: g \mapsto (g-1) - \frac{1}{2}(g-1)^2 + \cdots + \frac{(-1)^d}{(d-1)}(g-1)^{d-1}, \\ \exp &: \mathrm{Tr}_0(d,\mathbb{Q}) \to \mathrm{Tr}_1(d,\mathbb{Q}) \\ &: x \mapsto 1 + x + \frac{1}{2}x^2 + \cdots + \frac{1}{(d-1)!}x^{d-1}. \end{aligned}$$

These mappings are mutually inverse bijections which facilitate the Mal'cev correspondence between $\mathrm{Tr}_1(d,\mathbb{Q})$ and $\mathrm{Tr}_0(d,\mathbb{Q})$. We recall some of the features of this correspondence in the following.

3.1. **The interplay between subgroups and subalgebras.** The following theorem exhibits the interplay between the subgroups of $\mathrm{Tr}_1(d,\mathbb{Q})$ and the Lie subalgebras of $\mathrm{Tr}_0(d,\mathbb{Q})$ via the Mal'cev correspondence. Recall that a group G is *radicable* if for every $g \in G$ and $n \in \mathbb{N}$ there exists an $h \in G$ such that $h^n = g$. For a subgroup $U \leq \mathrm{Tr}_1(d,\mathbb{Q})$ we denote with $\mathcal{L}(U) := \mathbb{Q} \log U$ the $\mathbb{Q}$-vector space spanned by $\log U$.

2. **Theorem.** *Let $U \leq \mathrm{Tr}_1(d,\mathbb{Q})$ and $L \leq \mathrm{Tr}_0(d,\mathbb{Q})$ a Lie subalgebra. Then:*
a) $\exp L$ is a radicable torsion-free nilpotent subgroup of $\mathrm{Tr}_1(d,\mathbb{Q})$.
b) $\mathcal{L}(U)$ is a Lie subalgebra of $\mathrm{Tr}_0(d,\mathbb{Q})$.
c) $U \leq \exp \mathcal{L}(U)$ and every element of $\exp \mathcal{L}(U)$ has some power lying in U.

Proof. See [13, Chapter 6, Theorem 2]. □

A group $\hat{U}$ is a *radicable hull* of a torsion-free nilpotent group U if $\hat{U}$ is a radicable torsion-free nilpotent group that contains U and if every element in $\hat{U}$ has some power lying in U. Theorem 2 asserts that $\exp \mathcal{L}(U)$ is a radicable hull for $U \leq \mathrm{Tr}_1(d, \mathbb{Q})$. By [10, Theorem 9.20.] a radicable hull is unique up to isomorphism.

3.2. **Compatibility of actions.** The following theorem shows that the action of automorphism groups on subgroups of $\mathrm{Tr}_1(d, \mathbb{Q})$ is compatible with the Mal'cev correspondence.

3. **Theorem.** *Let $U \leq \mathrm{Tr}_1(d, \mathbb{Q})$ and let $\Gamma = \{\alpha \in \mathrm{Aut}(\mathcal{L}(U)) \mid (\log U)^\alpha \subseteq \log U\}$. Then $\phi : \mathrm{Aut}(U) \to \Gamma : \beta \mapsto \exp \circ\, \beta \circ \log$ is an isomorphism, where $l^{\exp \circ \beta \circ \log} = ((l^{\exp})^\beta)^{\log}$.*

Proof. See [13, Chapter 6, Theorem 6]. □

Theorem 3 has the following application which will be fundamental for our algorithms. For the proof of the following theorem note that the Baker-Campbell-Hausdorff formula [10, Definition 9.6] allows us to define a group multiplication on $\mathrm{Tr}_0(d, \mathbb{Q})$. This has the form $x * y = x + y + \frac{1}{2}[x, y] + \dots$ and allows us to express the group mulitplication in terms of Lie algebra operations. The logarithm map is then an isomorphism of groups between $\mathrm{Tr}_1(d, \mathbb{Q})$ and $(\mathrm{Tr}_0(d, \mathbb{Q}), *)$.

4. **Theorem.** *Let $U \leq \mathrm{Tr}_1(d, \mathbb{Q})$ and $H \leq \mathrm{Aut}(U)$ such that $U = \langle u_1, \dots, u_l \rangle^H$ for certain elements $u_1, \dots, u_l \in U$. Let $W \leq \mathrm{Tr}_0(d, \mathbb{Q})$ be the Lie algebra generated by $\log u_1, \dots, \log u_l$. Then $\mathcal{L}(U) = W^{\phi(H)}$.*

Proof. Let $S = \langle u_1, \dots, u_l \rangle$. Since W is a Lie algebra, we have that $x * y \in W$ for all $x, y \in W$. Since $\log : \mathrm{Tr}_1(d, \mathbb{Q}) \to (\mathrm{Tr}_0(d, \mathbb{Q}), *)$ is an isomorphism, it follows that $\log S \subset W$ and therefore $\mathcal{L}(S) = \mathbb{Q} \log S \subset W$. On the other hand, $\log u_i \in \mathcal{L}(S)$ for all i and so $W \subset \mathcal{L}(S)$. This yields that $\mathcal{L}(S) = W$.

An element $g \in S^H$ is of the form $g = u_{i_1}^{h_{i_1}} \cdots u_{i_l}^{h_{i_l}}$ for certain $h_{i_j} \in H$. Therefore $\log g = (\log u_{i_1})^{\phi(h_{i_1})} * \cdots * (\log u_{i_l})^{\phi(h_{i_l})}$ which is contained in $\mathcal{L}(S)^{\phi(H)}$. It follows that $\mathcal{L}(U) = \mathcal{L}(S^H) \subset \mathcal{L}(S)^{\phi(H)} \subset \mathcal{L}(U)^{\phi(H)} = \mathcal{L}(U)$. Thus $\mathcal{L}(S)^{\phi(H)} = \mathcal{L}(U)$. □

Theorem 4 yields that a basis for $\mathcal{L}(U)$ can be computed if $U \leq \mathrm{Tr}_1(d, \mathbb{Q})$ is given as $U = \langle u_1, \dots, u_l \rangle^H$ for a finitely generated group $H \leq \mathrm{Aut}(U)$. For this purpose we determine $\log u_1, \dots, \log u_l$ and then use a spinning algorithm (see for example [2]) to compute a basis for the smallest vector space that contains these elements and is closed under taking Lie brackets and acting with the generators of H. This yields a Lie algebra which is finite dimensional, since it is a subalgebra of the finite dimensional algebra $\mathrm{Tr}_0(d, \mathbb{Q})$, and hence the spinning algorithm terminates.

A similar approach could be considered for computing a generating set for U. However, the group U might not be finitely generated, even if it is finitely generated as an H-module, and in this case the spinning algorithm would not terminate.

3.3. **Finite generation.** A subgroup $U \leq \mathrm{Tr}_1(d, \mathbb{Q})$ is a *lattice group* if $\log U$ is closed under addition in $\mathrm{Tr}_0(d, \mathbb{Q})$. For example, the group $\mathrm{Tr}_1(d, \mathbb{Q})$ is a lattice group, since $\log \mathrm{Tr}_1(d, \mathbb{Q}) = \mathrm{Tr}_0(d, \mathbb{Q})$. For a subgroup $U \leq \mathrm{Tr}_1(d, \mathbb{Q})$ we define the *lattice hull* U^{lat} as the intersection of all lattice groups in $\mathrm{Tr}_1(d, \mathbb{Q})$ containing U. If U is finitely generated, then U has finite index in U^{lat} by [13, Chapter 6].

5. **Lemma.** *a) If $U \leq \mathrm{Tr}_1(d,\mathbb{Q})$ is finitely generated, then the additive group $\mathbb{Z}\log U$ is free abelian of finite rank and spans $\mathcal{L}(U)$ over $\mathbb{Q}$.*

b) If M is a finitely generated subgroup of the additive group $\mathrm{Tr}_0(d,\mathbb{Q})$, then $\langle \exp M\rangle$ is a finitely generated subgroup of $\mathrm{Tr}_1(d,\mathbb{Q})$.

Proof. a) See [13, Chapter 6].

b) The group $\mathrm{Tr}_0(d,\mathbb{Q})$ is torsion-free. Thus M has a $\mathbb{Z}$-basis $\log u_1,\dots,\log u_l$ for certain $u_1,\dots,u_l \in \mathrm{Tr}_1(d,\mathbb{Q})$. Let $U = \langle u_1,\dots,u_l\rangle$. Since U has finite index in U^{lat}, it follows that U^{lat} is finitely generated. Since $\log u_i \in \log U^{\mathrm{lat}}$ for $i = 1,\dots,l$, we find that M is contained in the lattice $\log U^{\mathrm{lat}}$. Therefore, we obtain that $\exp M \subset U^{\mathrm{lat}}$ and thus $\langle \exp M\rangle$ is finitely generated. □

4. Polycyclic sequences

In this section we briefly recall the basic notations used for computations with polycyclic groups. We refer to [9, Chapter 10], for further information.

Every polycyclic group G has a subnormal series $G = G_1 > \ldots > G_n > G_{n+1} = \{1\}$ with cyclic factors. Choose $g_i \in G$ with $G_i = \langle g_i, G_{i+1}\rangle$ for $1 \leq i \leq n$. Then the sequence $(g_1,\dots,g_n)$ is called a *polycyclic sequence* for G. The following lemma shows that a polycyclic sequence is a generating set for its underlying group and it has some particularly useful features. For a proof see [9], Lemma 8.3.

6. **Lemma.** *Let $(g_1,\dots,g_n)$ be a polycyclic sequence for a polycyclic group G. Then every element g of G can be written as $g = g_1^{e_1}\cdots g_n^{e_n}$ for certain $e_1,\dots,e_n \in \mathbb{Z}$.*

Polycyclic sequences are a fundamental tool in effective computations with polycyclic groups. In particular, every polycyclic sequence defines a finite presentation for its underlying group G: a so-called polycyclic presentation; see [9]. The algorithm in [2] can be used to determine a polycyclic sequence and its corresponding presentation for a polycyclic subgroup of $\mathrm{GL}(d,\mathbb{Q})$ and for certain of its factor groups.

5. Checking conjugacy into $\mathrm{GL}(d,\mathbb{Z})$

Let $G \leq \mathrm{GL}(d,\mathbb{Q})$ be a virtually polycyclic group. In this section we exhibit an effective test to check whether G can be conjugated into $\mathrm{GL}(d,\mathbb{Z})$; that is, whether there exists an element $h \in \mathrm{GL}(d,\mathbb{Q})$ such that $G^h \leq \mathrm{GL}(d,\mathbb{Z})$. Note that not every polycyclic subgroup of $\mathrm{GL}(d,\mathbb{Q})$ conjugates into $\mathrm{GL}(d,\mathbb{Z})$ as the example $G = \langle(\frac{1}{2})\rangle$ shows.

As a first step towards this aim, we recall two well-known characterisations of the groups which conjugate into $\mathrm{GL}(d,\mathbb{Z})$. For a subset M of a vector space we denote by $\langle M\rangle_{\mathbb{Q}}$ and $\langle M\rangle_{\mathbb{Z}}$ its $\mathbb{Q}$-span and its $\mathbb{Z}$-span, respectively. Further, we denote with $\mathbb{Z}[G]$ the subring of $M_d(\mathbb{Q})$ which is generated by the matrices in G. By a $\mathbb{Z}$-order in the matrix algebra $\mathbb{Q}[G]$ we mean a subring of $\mathbb{Q}[G]$ that is finitely generated as a $\mathbb{Z}$-module, contains the same identity as $\mathbb{Q}[G]$ and spans $\mathbb{Q}[G]$ over $\mathbb{Q}$. Therefore $\mathbb{Z}[G]$ is a $\mathbb{Z}$-order in $\mathbb{Q}[G]$ if and only if $\mathbb{Z}[G]$ is finitely generated as an additive group.

7. **Lemma.** *The following properties are equivalent:*

a) G is conjugated to a subgroup of $\mathrm{GL}(d,\mathbb{Z})$.

b) There exists a G-invariant lattice $L \leq V = \mathbb{Q}^d$ with $\langle L\rangle_{\mathbb{Q}} = V$.

c) $\mathbb{Z}[G]$ is a $\mathbb{Z}$-order.

Proof. $a) \Rightarrow c)$: Suppose that G is conjugated to a subgroup H of $\mathrm{GL}(d,\mathbb{Z})$. Then $\mathbb{Z}[H]$ is a $\mathbb{Z}$-order in $M_d(\mathbb{Z})$ and thus also $\mathbb{Z}[G]$ is a $\mathbb{Z}$-order.

$c) \Rightarrow b)$: Suppose that $\mathbb{Z}[G]$ is a $\mathbb{Z}$-order and let $B = \{b_1, \dots, b_s\}$ be a $\mathbb{Z}$-basis for $\mathbb{Z}[G]$. Then for all $g \in G$ there exist $a_{g,k} \in \mathbb{Z}$ such that $b_i g = \sum_{k=1}^{s} a_{g,k} b_k$ for $1 \le i \le s$. Let $r_{i,j}$ be the j-th row of b_i. Then $r_{i,j} g = \sum_{k=1}^{s} a_{g,k} r_{k,j}$ follows. Thus $L = \langle r_{i,j} \mid 1 \le i \le s, 1 \le j \le d \rangle_{\mathbb{Z}}$ is a G-invariant lattice. Further $\langle L \rangle_{\mathbb{Q}} = V$, because the rows of $1 \in \mathbb{Z}[G]$ are linear independent.

$b) \Rightarrow a)$: Let L be a G-invariant lattice. Then G acts on L as a subgroup of $\mathrm{GL}(d,\mathbb{Z})$. Since a basis for L is also a basis for V, it follows that G is conjugate to a subgroup of $\mathrm{GL}(d,\mathbb{Z})$. □

As a next step, we introduce an effective method to check whether $\mathbb{Z}[G]$ is a $\mathbb{Z}$-order. We first consider the special case of a cyclic group. For $g \in \mathrm{GL}(d,\mathbb{Q})$ denote with χ_g the minimal polynomial of g.

8. **Lemma.** *Let $g \in \mathrm{GL}(d,\mathbb{Q})$ and $U = \langle g \rangle$. Then the following are equivalent:*

a) $\mathbb{Z}[U]$ is a $\mathbb{Z}$-order.

b) $\chi_g, \chi_{g^{-1}} \in \mathbb{Z}[x]$.

c) $\chi_g \in \mathbb{Z}[x]$ and χ_g has the constant term ± 1.

Proof. $a) \Rightarrow b)$ and $a) \Rightarrow c)$: If $\mathbb{Z}[U]$ is a $\mathbb{Z}$-order, then U conjugates into $\mathrm{GL}(d,\mathbb{Z})$. As the minimal polynomial is invariant under conjugation, it follows that $\chi_g, \chi_{g^{-1}} \in \mathbb{Z}[x]$. As the constant term of χ_g is the determinant of g, it also follows that this constant term is ± 1.

$b) \Rightarrow a)$: Let $n = deg \chi_g$ and $m = deg \chi_{g^{-1}}$. As χ_g and $\chi_{g^{-1}}$ are normed polynomials over $\mathbb{Z}$, it follows that $\{g^{-m+1}, \dots, g^{-1}, 1, g, \dots, g^{n-1}\}$ generates $\mathbb{Z}[U]$ as an additive group and hence $\mathbb{Z}[U]$ is a $\mathbb{Z}$-order.

$c) \Rightarrow a)$: Let $\chi_g = x^n + \alpha_{n-1} x^{n-1} + \cdots + \alpha_1 x + \alpha_0$. Then

$$g(g^{n-1} + \alpha_{n-1} g^{n-2} + \cdots + \alpha_1) = -\alpha_0.$$

As $\alpha_0 = \pm 1$, it follows that $g^{-1} = \mp(g^{n-1} + \alpha_{n-1} g^{n-2} + \cdots + \alpha_1)$. Thus $\{1, g, \dots, g^{n-1}\}$ generates $\mathbb{Z}[U]$ as an additive group and so $\mathbb{Z}[U]$ is a $\mathbb{Z}$-order. □

The following theorem yields a reduction to the case of cyclic groups.

9. **Theorem.** *Let $\{g_1, \dots, g_n\}$ be a generating set of $G \le \mathrm{GL}(d,\mathbb{Q})$ such that every element of g can be written as a collected word $g = g_1^{e_1} \dots g_n^{e_n}$ with $e_1, \dots, e_n \in \mathbb{Z}$. Then $\mathbb{Z}[G]$ is a $\mathbb{Z}$-order if and only if $\mathbb{Z}[\langle g_i \rangle]$ is a $\mathbb{Z}$-order for $1 \le i \le n$.*

Proof. Write $U_i = \langle g_i \rangle$. If $\mathbb{Z}[G]$ is a $\mathbb{Z}$-order, then $\mathbb{Z}[U_i]$ is a $\mathbb{Z}$-order. Thus it suffices to show the converse. Let $a_{i,1}, \dots, a_{i,l_i}$ be a $\mathbb{Z}$-basis for $\mathbb{Z}[U_i]$. Then for every $g \in G$ there exist $\alpha_{ij_i} \in \mathbb{Z}$ with

$$\begin{aligned} g &= g_1^{e_1} \cdots g_n^{e_n} \\ &= \left(\sum_{j_1=1}^{l_1} \alpha_{1j_1} a_{1j_1} \right) \cdots \left(\sum_{j_n=1}^{l_n} \alpha_{nj_n} a_{nj_n} \right) \\ &= \sum_{j_1=1}^{l_1} \cdots \sum_{j_n=1}^{l_n} \alpha_{1j_1} \cdots \alpha_{nj_n} a_{1j_1} \cdots a_{nj_n}. \end{aligned}$$

Thus

$$S = \{a_{1j_1} \cdots a_{nj_n} | 1 \leq j_i \leq l_i\}$$

is a finite generating set for $\mathbb{Z}[G]$ as an additive group. □

As G is virtually polycyclic, there exists a polycyclic normal subgroup N of finite index in G. Let T be a transversal for N in G and let $R = (r_1, \ldots, r_l)$ be a polycyclic sequence for N. Then every element g in G can be written as $g = tr_1^{e_1} \cdots r_l^{e_l}$ for some $t \in T$ and $e_1, \ldots, e_l \in \mathbb{Z}$. Thus $T \cup R$ is a generating set for G which satisfies the hypothesis of Theorem 9. Hence we obtain the following corollary to Theorem 9 which provides an effective check whether G conjugates into $\mathrm{GL}(d, \mathbb{Z})$.

10. **Corollary.** *Let G be virtually polycyclic with normal polycyclic subgroup N of finite index. Let T be a transversal for N in G and let R be a polycyclic sequence for N. Then G is conjugated to a subgroup of $\mathrm{GL}(d, \mathbb{Z})$ if and only if $\chi_g, \chi_{g^{-1}} \in \mathbb{Z}[x]$ for every $g \in T \cup R$.*

6. Testing polycyclicity

In this section we introduce an effective method to test whether a finitely generated subgroup G of $\mathrm{GL}(d, \mathbb{Q})$ is polycyclic. Every polycyclic group is solvable. Thus as a first step in our method, we use the algorithm of Section 2.3 to check whether G is solvable. We then assume throughout that the considered group G is solvable.

Let $V = \mathbb{Q}^d$ and let $V = V_1 > \ldots > V_l > V_{l+1} = \{0\}$ be an arbitrary, fixed semisimple series of G. Then the centralizer of this series $U = \cap_{i=1}^{l} C_G(V_i/V_{i+1})$ is called a *unipotent radical* of G. Note that by choosing a basis for V exhibiting the semisimple series, we can assume that $U \leq \mathrm{Tr}_1(d, \mathbb{Q})$.

The following lemma summarizes some information of the structure of G and U which will be used throughout.

11. **Lemma.** *Let $G \leq \mathrm{GL}(d, \mathbb{Q})$ be finitely generated and solvable and let U be a unipotent radical of G. Then U is nilpotent and G/U is polycyclic.*

Proof. As $U \leq \mathrm{Tr}_1(d, \mathbb{Q})$, it follows that U is nilpotent. Let $V = V_1 > \ldots > V_l > V_{l+1} = \{0\}$ be the semisimple series underlying U. Then the factor G/U embeds into the direct product $G_{V_1/V_2} \times \ldots \times G_{V_l/V_{l+1}}$. It follows from Theorem 1 (see also [2]) that this direct product is (finitely generated abelian)-by-(finite solvable) and hence G/U is polycyclic. □

The following theorem provides a characterisation for polycyclic rational matrix groups.

12. **Theorem.** *Let $G \leq \mathrm{GL}(d, \mathbb{Q})$ be finitely generated and solvable and let U be a unipotent radical of G. Then G is polycyclic if and only if U is finitely generated.*

Proof. If G is polycyclic, then every subgroup of G is finitely generated and hence U is finitely generated. Conversely, if U is finitely generated, then U is polycyclic, because U is nilpotent by Lemma 11. As G/U is also polycyclic by Lemma 11, the result follows. □

As described in [2], we can compute a polycyclic presentation for G/U. By evaluating the relators of such a presentation, we obtain a finite set of normal

subgroup generators for U; that is, $U = \langle u_1, \dots, u_l \rangle^G$ for certain $u_1, \dots, u_l \in U$. By Theorem 12, it remains to check whether U is finitely generated.

We employ the Lie algebra $\mathcal{L}(U)$ for this purpose. First, we note that a basis for the finite dimensional $\mathcal{L}(U)$ can be computed using Theorem 4. The conjugation action of G on U induces a subgroup $H \leq \mathrm{Aut}(U)$. In turn, this subgroup H acts on $\mathcal{L}(U)$ by Theorem 3. Let $\phi_{\mathcal{B}} : \mathrm{Aut}(U) \to \mathrm{GL}(e, \mathbb{Q})$ describe this action with respect to the basis $\mathcal{B}$ of $\mathcal{L}(U)$ and let $\phi = \phi_{\mathcal{B}}$ for some arbitrary, fixed basis $\mathcal{B}$.

Our aim in the following is to show that we can read off from the action of G on $\mathcal{L}(U)$ whether U is finitely generated. The following theorem is a first step into that direction.

13. **Theorem.** *Let $U \leq \mathrm{Tr}_1(d, \mathbb{Q})$ and $H \leq \mathrm{Aut}(U)$ such that $U = \langle u_1, \dots, u_l \rangle^H$ for certain $u_1, \dots, u_l \in U$. Then U is finitely generated if and only if $\phi(H)$ can be conjugated into $\mathrm{GL}(e, \mathbb{Z})$.*

Proof. Assume that U is finitely generated. By Lemma 5, the additive group $\mathbb{Z} \log U$ is free abelian of finite rank and spans $\mathcal{L}(U)$ over $\mathbb{Q}$. Thus there exists a $\mathbb{Z}$-basis $\mathcal{B}$ for $\mathbb{Z} \log U$ which is also a $\mathbb{Q}$-basis for $\mathcal{L}(U)$. By Theorem 3, the lattice $\mathbb{Z} \log U$ is invariant under the action of H. Hence $\phi_{\mathcal{B}}(H) \leq \mathrm{GL}(e, \mathbb{Z})$ and $\phi(H)$ can be conjugated into $\mathrm{GL}(e, \mathbb{Z})$.

Now assume that $\phi(H)$ can be conjugated into $\mathrm{GL}(e, \mathbb{Z})$. Let $\mathcal{B}$ be a basis of $\mathcal{L}(U)$ such that $\phi_{\mathcal{B}}(H) \leq \mathrm{GL}(e, \mathbb{Z})$ and let L be the $\mathbb{Z}$-span of $\mathcal{B}$. Denote $W = \langle u_1, \dots, u_l \rangle$. Then $\mathbb{Z} \log W$ is finitely generated by Lemma 5 and hence there exists $z \in \mathbb{N}$ such that $\mathbb{Z} \log W \subset M := \frac{1}{z} L$. As $\phi_{\mathcal{B}}(H) \leq \mathrm{GL}(e, \mathbb{Z})$, the lattice M is invariant under the action of H. Therefore for all $u \in W$ and $h \in H$, it follows that $\log(u^h) = \log(u)^h \in M$. Thus $U = W^H \subseteq \langle \exp(M) \rangle$. By Lemma 5, the group $\langle \exp(M) \rangle$ is finitely generated. Hence U is finitely generated. □

Let $\varphi : G \to \mathrm{GL}(e, \mathbb{Q})$ denote the action of G on $\mathcal{L}(U)$ with respect to an arbitrary, fixed basis $\mathcal{B}$ of $\mathcal{L}(U)$. Then Theorem 13 yields that the group U is finitely generated if and only if $\varphi(G)$ can be conjugated into $\mathrm{GL}(e, \mathbb{Z})$. Section 5 contains a method to check whether a polycyclic subgroup of $\mathrm{GL}(e, \mathbb{Q})$ conjugates into $\mathrm{GL}(e, \mathbb{Z})$. However, this method does not apply directly, as $\varphi(G)$ might not be polycyclic. The next theorem shows that the method of Section 5 generalises to the case considered here. For $g \in G$ we denote with $\chi_{\varphi(g)} \in \mathbb{Q}[x]$ the minimal polynomial of $\varphi(g)$.

14. **Theorem.** *Let $G \leq \mathrm{GL}(d, \mathbb{Q})$ be finitely generated and solvable and let U be a unipotent radical of G. Let $(g_1 U, \dots, g_n U)$ be a polycyclic sequence for G/U. Then G is polycyclic if and only if $\chi_{\varphi(g_i)}, \chi_{\varphi(g_i^{-1})} \in \mathbb{Z}[x]$ for $1 \leq i \leq n$.*

Proof. Suppose that G is polycyclic. Then U is finitely generated and thus $\varphi(G)$ can be conjugated into $\mathrm{GL}(e, \mathbb{Z})$ by Theorem 13. Thus $\chi_{\varphi(g_i)}, \chi_{\varphi(g_i^{-1})} \in \mathbb{Z}[x]$ follows.

Conversely, suppose that $\chi_{\varphi(g_i)}, \chi_{\varphi(g_i^{-1})} \in \mathbb{Z}[x]$ for $1 \leq i \leq n$. Let $\mathcal{L}(U) = L_1 > \cdots > L_{l+1} = \{0\}$ be a refinement of the upper central series of $\mathcal{L}(U)$ to a $\mathbb{Q}G$-composition series. We use induction on l to show that $\varphi(G)$ can be conjugated into $\mathrm{GL}(e, \mathbb{Z})$. As U is finitely generated as a G-normal subgroup, this yields by Theorem 13 and Theorem 12 that G is polycyclic.

First consider the case $l = 1$. Then U acts trivially on $\mathcal{L}(U)$ and thus $\varphi(G)$ is polycyclic with polycyclic sequence $(\varphi(g_1), \dots, \varphi(g_n))$. Corollary 10 now yields that $\varphi(G)$ can be conjugated into $\mathrm{GL}(e, \mathbb{Z})$.

Now let $l > 1$. We assume by induction that there exists a basis $\mathcal{B}$ of $\mathcal{L}(U)$ which exhibits $L_1 > L_2 > \{0\}$ and with respect to which G_{L_1/L_2} and G_{L_2} have integral matrix representations and thus are polycyclic. With respect to $\mathcal{B}$ every element $\varphi(g)$ is represented by a matrix of the form

$$\begin{pmatrix} \alpha(g) & \gamma(g) \\ & \beta(g) \end{pmatrix}$$

where $\alpha(g)$, respectively $\beta(g)$, are the representations of the action of g on L_1/L_2, respectively L_2. For $g, h \in G$, it follows that $\gamma(gh) = \alpha(g)\gamma(h) + \gamma(g)\beta(h)$. Thus, since $\alpha(G), \beta(G)$ are integral matrix groups and by assumption G is finitely generated, we deduce that the denominators of the entries of $\gamma(G)$ are bounded. Since $\alpha(G)$ and $\beta(G)$ are polycyclic, it follows that $\varphi(G)$ is polycyclic. Therefore there exists a polycyclic sequence $(\varphi(g_1), \ldots, \varphi(g_n), \varphi(u_1), \ldots, \varphi(u_l))$ of $\varphi(G)$, where $u_1, \ldots, u_l \in U$. Since U is unipotent, the minimal polynomial of $\varphi(u_j^{\pm 1})$ is of the form $(x-1)^{m_j}$ for some $m_j \in \mathbb{N}$ and $1 \leq j \leq l$. By Corollary 10, $\varphi(G)$ can be conjugated into $\mathrm{GL}(e, \mathbb{Z})$. □

The results of this section yield the following algorithm to test polycyclicity. Let G be a finitely generated subgroup of $\mathrm{GL}(d, \mathbb{Q})$ and let $V = \mathbb{Q}^d$.

IsPolycyclic(G **)**

1: test whether G is solvable and return false if this is not the case.
2: compute a pc-sequence $(g_1U, \ldots, g_nU)$ for G/U where U is a unipotent radical.
3: compute normal subgroup generators for U.
4: compute a basis $\mathcal{B}$ for the Lie algebra $\mathcal{L}(U)$.
5: compute the induced action $\varphi(g_i)$ with respect to $\mathcal{B}$ for $1 \leq i \leq n$.
6: let $\chi_{\varphi(g_i)}$ be the minimal polynomial of $\varphi(g_i)$ for $1 \leq i \leq n$.
7: **if** $\chi_{\varphi(g_i)} \in \mathbb{Z}[x]$ and has constant term ± 1 for $1 \leq i \leq n$, **then**
8: return true
9: **else**
10: return false
11: **end if**

7. Testing virtual polycyclicity

A variation of the method to test polycyclicity yields a method to determine whether a finitely generated subgroup of $\mathrm{GL}(d, \mathbb{Q})$ is virtually polycyclic. The following theorem characterises the virtually polycyclic groups in a computationally useful form.

15. **Theorem.** *Let $G \leq \mathrm{GL}(d, \mathbb{Q})$ be finitely generated and virtually solvable, and let H be a p-congruence subgroup of G. Then G is virtually polycyclic if and only if H is polycyclic.*

Proof. If H is polycyclic, then G is virtually polycyclic, because $[G : H] < \infty$. If G is virtually polycyclic, then there exists a normal polycyclic subgroup K with $[G : K] < \infty$. Being a subgroup of K, the group $H \cap K$ is polycyclic. We have that $H/H \cap K \cong KH/H \leq G/K$ and thus $H/H \cap K$ is finite. Since H is solvable by Theorem 1, $H/H \cap K$ is solvable. Thus $H/H \cap K$ is polycyclic. Therefore H is polycyclic. □

Generators for a p-congruence subgroup H of G can be computed from a generating set of G as discussed in Section 2.2. Thus the method of Section 6 extends to testing virtual polycyclicity.

8. Testing nilpotency

Let $G \leq \mathrm{GL}(d, \mathbb{Q})$ be finitely generated. In this section we describe a method to test whether G is nilpotent. Every finitely generated nilpotent group is polycyclic. Hence as a first step to our algorithm we check whether the given group G is polycyclic using the method of Section 6. Thus we can assume in the following that G is polycyclic.

A possible approach towards testing nilpotency is to determine a polycyclic presentation for G using the method of [2] and, based on that, to check nilpotency as described in [8]. In the following we outline an alternative approach. This alternative shows that testing nilpotency is closely related to testing polycyclicity as in Section 6 and, further, the alternative extends to testing virtual nilpotency as shown in Section 9 below.

As a first step, we characterise the nilpotent matrix groups among the polycyclic matrix groups. For this purpose we use the following notation: if H is a group which acts by automorphisms on a group U, then H *acts nilpotently* on U if there exists a series of H-invariant normal subgroups through U such that H centralizes every factor of the series. For a proof of the following lemma and more background on nilpotency see [13, Chapter 1].

16. **Lemma.** *Let G be a polycyclic subgroup of $\mathrm{GL}(d, \mathbb{Q})$ and let U be a unipotent radical of G. Then G is nilpotent if and only if G/U is nilpotent and G acts nilpotently on U.*

As side-results of the algorithm IsPolycyclic of Section 6, we have given normal subgroup generators for a unipotent radical U of G and a polycyclic sequence $\mathcal{G} = (g_1U, \ldots, g_kU)$ of G/U. We can use this to determine a polycyclic presentation for G/U and, based on that, we can test whether G/U is nilpotent.

It remains to find a criterion which decides whether G acts nilpotently on U. As in the test for polycyclicity, one can use the action of G on the Lie algebra $\mathcal{L}(U)$ for this purpose. The following theorem provides a first step towards proving this.

17. **Theorem.** *Let $U \leq \mathrm{Tr}_1(d, \mathbb{Q})$ and let $H \leq \mathrm{Aut}(U)$. Then H acts nilpotently on U if and only if H acts nilpotently on $\mathcal{L}(U)$.*

Proof. Assume that H acts nilpotently on U. Then there exists a central series $1 = U_k < \cdots < U_1 = U$ of U with H-central factors. Define a chain of Lie subalgebras of $\mathcal{L}(U)$ by $\mathcal{L}_i = \mathcal{L}(U_i)$. Using [10, Lemma 10.12.], a straightforward calculation shows that this is an H-central series of $\mathcal{L}(U)$.

Assume conversely that H acts nilpotently on $\mathcal{L}(U)$. Then $\mathcal{L}(U)$ has a central series $0 = \mathcal{L}_k < \cdots < \mathcal{L}_1 = \mathcal{L}(U)$ with H-central factors. Define a descending chain of subgroups of U by $U_i = \exp(\mathcal{L}_i) \cap U$. Again using [10, Lemma 10.12], a straightforward calculation shows that this is a central series of U with H-central factors. □

Let $\varphi : G \to \mathrm{GL}(e, \mathbb{Q})$ denote the action of the polycyclic group G on the Lie algebra $\mathcal{L}(U)$ of a unipotent radical of G with respect to an arbitrary, fixed basis

of $\mathcal{L}(U)$. The following theorem shows how the nilpotency of G can be read off the action φ in a similar form as polycyclicity can be read off.

A polycyclic sequence $(g_1, \ldots, g_k)$ is called a *nilpotent sequence* if its corresponding polycyclic series $G_i = \langle g_i, \ldots, g_k \rangle$ is a central series (and hence the underlying group is nilpotent).

18. **Theorem.** *Let $G \leq \mathrm{GL}(d, \mathbb{Q})$ be polycyclic and let U be a unipotent radical of G. Let G/U be nilpotent with nilpotent sequence $(g_1U, \ldots, g_nU)$. Then G is nilpotent if and only if $\chi_{\varphi(g_i)}(x) = (x-1)^{m_i}$ for certain $m_i \in \mathbb{Z}$ and for $1 \leq i \leq n$.*

Proof. Assume that G is nilpotent. Then G acts nilpotently on U by Lemma 16 and thus on $\mathcal{L}(U)$ by Theorem 17. Hence $\chi_{\varphi(g_i)}(x) = (x-1)^{m_i}$ for certain m_i and $1 \leq i \leq n$ follows.

Conversely, assume that $\chi_{\varphi(g_i)}(x) = (x-1)^{m_i}$ for all i. Denote by $\zeta_k(\mathcal{L}(U))$ the k-th term of the upper central series of $\mathcal{L}(U)$. That is $\zeta_1(\mathcal{L}(U)) = \{x \in \mathcal{L}(U) \mid [y, x] = 0 \ \forall y \in \mathcal{L}(U)\}$ and $\zeta_{i+1}(\mathcal{L}(U))/\zeta_i(\mathcal{L}(U)) = \zeta_1(\mathcal{L}(U)/\zeta_i(\mathcal{L}(U)))$. Note that $\zeta_i(\mathcal{L}(U))$ is an ideal of $\mathcal{L}(U)$ and so in particular a Lie subalgebra. Further $\zeta_i(\mathcal{L}(U))$ is invariant under autmorphisms of $\mathcal{L}(U)$ and therefore invariant under the action of G.

We show that G acts nilpotently on the factors $F_k = \zeta_k(\mathcal{L}(U))/\zeta_{k+1}(\mathcal{L}(U))$. This implies that G acts nilpotently on $\mathcal{L}(U)$ and thus on U by Theorem 17. In turn, this yields the desired result by Lemma 16.

Let $k \in \mathbb{N}$ and let $\varphi_k(G)$ denote the action induced by G on F_k. Using [10, Lemma 10.12] we deduce that U acts trivially on F_k. Thus the sequence $(\varphi_k(g_1), \ldots, \varphi_k(g_n))$ is a polycyclic sequence of $\varphi_k(G)$. Let $G_i = \langle g_i, \ldots, g_n \rangle$. Then the groups $\varphi_k(G_i)$ for $1 \leq i \leq n$ form a central series of $\varphi_k(G)$. Let $l \in \{1, \ldots, n\}$ be maximal such that $\varphi_k(g_l) \neq 1$. Let W be the eigenspace of $\varphi_k(g_l)$. Then $F_k > W > \{0\}$, since $\varphi_k(g_l)$ is non-trivial and satisfies $(x-1)^{m_l} = 0$. By the choice of l, the element $\varphi_k(g_l)$ is contained in the center of $\varphi_k(G)$. This implies that W is a G-invariant subspace of F_k. The actions induced by G on F_k/W and W satisfy the assumption of the theorem. Thus by induction on the dimension, we can assume that G acts nilpotently on F_k/W and W. Thus G acts nilpotently on F_k. □

The results of this section yield the following algorithm to test nilpotency. Let G be a finitely generated subgroup of $\mathrm{GL}(d, \mathbb{Q})$ and let $V = \mathbb{Q}^d$.

IsNilpotent(G **)**

1: test whether G is polycyclic and return false if this is not the case.
2: as side-results of step 1, obtain a polycyclic sequence $\mathcal{G}$ of G/U and a basis $\mathcal{B}$ of $\mathcal{L}(U)$ for a unipotent radical U of G,
3: using $\mathcal{G}$, test whether G/U is nilpotent and return false if this is not the case.
4: compute a nilpotent sequence $(g_1U, \ldots, g_nU)$ for G/U.
5: compute the induced action $\varphi(g_i)$ with respect to $\mathcal{B}$ for $1 \leq i \leq n$.
6: compute the minimal polynomial $\chi_{\varphi(g_i)}(x)$ of $\varphi(g_i)$ for $1 \leq i \leq n$.
7: **if** $\chi_{\varphi(g_i)}(x) = (x-1)^{m_i}$ for $1 \leq i \leq n$, **then**
8: return true
9: **else**
10: return false
11: **end if**

9. Testing virtual nilpotency

A modification of the nilpotency testing algorithm yields a method for testing virtual nilpotency. Let $G \leq \mathrm{GL}(d, \mathbb{Q})$ be finitely generated. As a first step, we check whether G is virtually polycyclic with the method of Section 7. As a side-result of this algorithm, we obtain normal subgroup generators for a unipotent radical U of G and a polycyclic sequence for H/U where H is a p-congruence subgroup of G.

Note that H/U is free abelian; see [2]. Since $[G : H] < \infty$ and two subgroups of finite index intersect in a subgroup of finite index, G is virtually nilpotent if and only if H is virtually nilpotent. The latter condition can be checked with the following theorem. Recall that for $h \in \mathrm{GL}(e, \mathbb{Q})$ we denote by $\chi_h(x)$ the minimal polynomial of h.

19. **Theorem.** *Let $H \leq \mathrm{GL}(d, \mathbb{Q})$ and let U be a unipotent radical of H. Suppose that H/U is finitely generated abelian with polycyclic sequence $(g_1U, \ldots, g_nU)$. Then H is virtually nilpotent if and only if all roots of $\chi_{\varphi(g_i)}(x) = 0$ are roots of unity for $1 \leq i \leq n$.*

Proof. Assume that H is virtually nilpotent. Let $K \leq H$ with $s = [H : K] < \infty$ and K nilpotent. Then K acts nilpotently on $U \cap K$ and therefore, by Theorem 17, K acts nilpotently on $\mathcal{L}(U \cap K)$. Since $[U : U \cap K] = [KU : K] \leq [H : K] < \infty$, $\mathcal{L}(U \cap K) = \mathcal{L}(U)$ and thus K acts nilpotently on $\mathcal{L}(U)$. Therefore, since $g_i^s \in K$, the minimal polynomial of $\varphi(g_i^s) = \varphi(g_i)^s$ is $(x-1)^{m_i}$ for some $m_i \in \mathbb{N}$. Thus $\chi_{\varphi(g_i)}(x)$ divides $(x^s - 1)^{m_i}$. This implies that all roots of $\chi_{\varphi(g_i)}(x) = 0$ are roots of unity.

Assume conversely that $E \subset \mathbb{C}$, the set of all eigenvalues of $\varphi(g_1), \ldots, \varphi(g_n)$, contains only roots of unity. Let $l \in \mathbb{N}$ such that $\lambda^l = 1$ for all $\lambda \in E$. Define $K = \langle g_1^l, \ldots, g_n^l, U \rangle$. In order to show that K acts nilpotently on U, by Theorem 18, it is sufficient to show that $\chi_{\varphi(g_i{}^l)} = (x-1)^{m_i}$ for some $m_i \in \mathbb{N}$ for $1 \leq i \leq n$. Let θ be an eigenvalue of $\varphi(g_i^l)$. From the Jordan-Normal form of $\varphi(g_i)$ it can be read off that $\theta = \lambda^l$ for some eigenvalue λ of $\varphi(g_i)$. Since $\lambda \in E$, $\theta = 1$ follows and thus $\chi_{\varphi(g_i{}^l)} = (x-1)^{m_i}$ for some $m_i \in \mathbb{N}$. □

10. Implementation and examples

We illustrate our algorithms on the simple example group G, already mentioned in Section 2.4, which is generated by

$$g = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad h = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

The series $V = \mathbb{Q}^2 > W = \langle (0,1) \rangle_{\mathbb{Q}} > \{0\}$ is a semisimple series for G. The induced actions $G_{V/W}$ and G_W are both polycyclic, and thus G is solvable. Let U be the centraliser of the semisimple series; thus U is a unipotent radical for G. Then G/U is an infinite cyclic group and (gU) is a polycyclic sequence for G/U. Further $U = \langle h \rangle^G$. It follows that

$$\mathcal{L}(U) = \mathcal{L}(\langle h \rangle)^{\varphi(g)} = (\mathbb{Q} \log \langle h \rangle)^{\varphi(g)} = \left(\langle \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \rangle_{\mathbb{Q}} \right)^{\varphi(g)} = \langle \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \rangle_{\mathbb{Q}}.$$

It can be seen that the induced action of g on $\mathcal{L}(U)$ with respect to the basis $\mathcal{B} = \{ \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right) \}$ is given by the matrix $\varphi(g) = (\frac{1}{2})$. The minimal polynomial of $\varphi(g)$ is not in $\mathbb{Z}[X]$ and thus G is not polycyclic.

10.1. **Runtimes.** The algorithm IsPolycyclic of Section 6 was implemented in GAP [14] as a part of the Polenta package [1]. Instead of computing minimal polynomials in step 6 of the algorithm we determine characteristic polynomials because this is more efficient and because the minimal polynomial of a rational matrix is integral if and only if the characteristic polynomial is integral.

Alternatively the method in [3], which is also implemented in GAP, could be used to test whether the induced action of G to $\mathcal{L}(U)$ conjugates into $\mathrm{GL}(e,\mathbb{Z})$. Therefore this method could replace the steps 6 to 11 of our algorithm "IsPolycyclic". We compared this variation with our method and did not notice any difference in the runtimes for our example groups.

A method for testing virtual polycyclicity has not yet been implemented. To handle this case it is necessary to compute short finite presentations of finite non-soluble matrix groups.

In Table 1 we display runtimes for some example matrix groups and we also summarise some of the properties of the considered groups. All example groups considered in Table 1 are solvable and not contained in $\mathrm{GL}(d,\mathbb{Z})$. The groups G_1, G_2 are unipotent, G_3, G_4 are almost crystallographic groups. G_5 was constructed using the Kronecker product of generators of an almost crystallographic group. The group G_6 is a randomly generated subgroup of the direct product of a unipotent and a free-abelian-by-finite group. The group G_7 is the group G from the beginning of Section 10. G_8, G_9 are randomly generated upper-block-triangular matrix groups.

Every example group G_i is available in the package Polenta via the function "SolvableMatGroupExams(i)". A group $G \leq \mathrm{GL}(d,\mathbb{Q})$ given by generators can be tested to be polycyclic using the command "IsPolycyclicMatGroup(G)". All computations where carried out in GAP Version 4.4.7 on a Pentium 4 machine with 3.2 gigahertz and 90 MB of memory for GAP.

TABLE 1. Testing polycyclicity: The columns display the degree d, the number of generators, the rank (or Hirsch length) and the dimension of $\mathcal{L}(U)$ for every of the considered examples $G_1, \ldots, G_9$. If no rank is given, then the example group is not polycyclic. The last column contains the time which is needed by the algorithm IsPolycyclic of Section 6 in minutes:seconds.milliseconds.

Group	Degree	No. gens	Rank	Dim $\mathcal{L}(U)$	Runtime
G_1	4	2	4	4	0.047
G_2	5	2	6	6	0.109
G_3	5	5	4	4	0.822
G_4	5	5	4	4	0.568
G_5	16	5	3	3	0.557
G_6	20	11	7	4	6:13.083
G_7	2	2	-	1	0.150
G_8	6	4	-	10	15.966
G_9	8	4	-	13	14.379

ACKNOWLEDGMENT

We thank Gabriele Nebe for discussions on checking conjugacy into $\mathrm{GL}(d,\mathbb{Z})$.

References

1. B. Assmann. *Polenta - Polycyclic presentations for matrix groups*, 2006. A refereed GAP 4 package, see [14].
2. B. Assmann and B. Eick. Computing polycyclic presentations for polycyclic rational matrix groups. *Accepted by J. Symb. Comput.*, 2005. MR2178086 (2006g:20044)
3. L. Babai, R. Beals, and D. Rockmore. Deciding finiteness of matrix groups in deterministic polynomial time. In *Proc. of International Symposium on Symbolic and Algebraic Computation* ISSAC '93, pages 117–126. (Kiev), ACM Press, 1993.
4. G. Baumslag. *Lecture notes on nilpotent groups*. Amer. Math. Soc., Providence, 1971. MR0283082 (44:315)
5. G. Baumslag, F. B. Cannonito, D. J. S. Robinson, and D. Segal. The algorithmic theory of polycyclic-by-finite groups. *J. Alg.*, 142:118–149, 1991. MR1125209 (92i:20036)
6. R. Beals. Improved algorithms for the Tits alternative. In W. M. Kantor and A. Seress, editors, *Groups and Computation III*, pages 63–77. (DIMACS, 1999), 2001. MR1829471 (2002g:20085)
7. L. E. Dickson. *Algebras and their arithmetics*. University of Chicago, 1923.
8. B. Eick. Algorithms for polycyclic groups. Habilitationsschrift, Universität Kassel, 2001.
9. D. F. Holt, B. Eick, and E. A. O'Brien. *Handbook of Computational Group Theory*. Discrete Mathematics and its Applications. CRC Press, 2005. MR2129747 (2006f:20001)
10. E. Khukhro. *p-Automorphisms of Finite p-Groups*, volume 246 of *Lecture Note Series*. London Mathematical Soc., 1998. MR1615819 (99d:20029)
11. A. J. Mal'cev. On certain classes of infinite soluble groups. *Mat. Sb.*, 28:567–588, 1951. MR0043088 (13:203k)
12. G. Ostheimer. Practical algorithms for polycyclic matrix groups. *J. Symb. Comput.*, 28:361–379, 1999. MR1716421 (2000h:20004)
13. D. Segal. *Polycyclic Groups*. Cambridge University Press, Cambridge, 1983. MR713786 (85h:20003)
14. The GAP Group. *GAP–Groups, Algorithms and Programming*. www.gap-system.org, 2006.

Centre for Interdisciplinary Research in Computational Algebra (CIRCA), University of St Andrews, North Haugh, St Andrews, KY16 9SS Fife, Scotland

E-mail address: bjoern@mcs.st-and.ac.uk

Institut Computational Mathematics, Fachbereich Mathematik und Informatik, Technische Universität Braunschweig, Braunschweig, Germany

E-mail address: beick@tu-bs.de