MATHEMATICS OF COMPUTATION
Volume 00, Number 0, Pages 000–000
S 0025-5718(XX)0000-0

ON THE ORBIT-STABILIZER PROBLEM FOR INTEGRAL MATRIX ACTIONS OF POLYCYCLIC GROUPS

BETTINA EICK AND GRETCHEN OSTHEIMER

ABSTRACT. We present an algorithm to solve the orbit-stabilizer problem for a polycyclic group G acting as a subgroup of $GL(d, \mathbb{Z})$ on the elements of $\mathbb{Q}^d$. We report on an implementation of our method and use this to observe that the algorithm is practical.

1. INTRODUCTION

The determination of orbits and stabilizers is one of the most fundamental problems in algorithmic group theory. If the desired orbit is finite or, equivalently, the stabilizer has finite index in the given group, then we can list the orbit and calculate Schreier generators for the stabilizer as outlined in [2]. This method for finite orbits can be improved if the acting group is polycyclic as observed in [10]. However, none of these methods would terminate if the considered orbit is infinite.

The central aim here is to develop a practical algorithm to solve the orbit-stabilizer problem for elements in $\mathbb{Q}^d$ under an integral matrix action of a (possibly infinite) polycyclic group G. Clearly, the desired orbits may be infinite and thus cannot be listed explicitly. Nonetheless we can solve the following problems:

- *stabilizer problem:* for $v \in \mathbb{Q}^d$ construct a generating set for $Stab_G(v)$.
- *orbit problem:* for $v, w \in \mathbb{Q}^d$ decide whether or not there exists an element $g \in G$ with $vg = w$; if so, find such an element g.

These problems arise naturally in algorithms for polycyclic groups G which are given by a polycyclic presentation: the natural conjugation action of G on a normal free abelian subfactor gives rise to an integral matrix action. Thus practical methods to solve the orbit-stabilizer problem will have a variety of applications, such as in the determination of centralizers or intersections of subgroups of G or in solving the conjugacy problem for elements of G. We refer to [8] for details on this topic.

It is well-known that the orbit-stabilizer problem is undecidable for general matrix groups, and yet it is decidable for polycyclic-by-finite integral matrix groups as observed in [1]. The algorithms introduced to establish this decidability were not developed with a view to practicality. A more practical approach to solve the orbit-stabilizer problem in the case of a nilpotent-by-finite rational matrix group has been described in [7], but this method has never been implemented and it is expected to be limited to small dimensions only.

Received by the editor May 31, 2001, and, in revised form, February 4, 2002.
2000 *Mathematics Subject Classification.* primary 20F16, 20-04; secondary 68W30.
Both authors thank Werner Nickel for useful discussions.

The algorithms presented in this paper have been implemented in the computer algebra system GAP [15] using an interface to KANT [4]. This implementation demonstrates that the developed methods are practical for a number of interesting examples. We include a report on this implementation and its applications below.

This paper is organized as follows. Section 2 recalls background information about polycyclic rational matrix groups. Section 3 describes a collection of basic algorithms for polycyclic groups that will be needed for the orbit-stabilizer calculations. Section 4 presents an algorithm for calculating orbits and stabilizers. Section 5 outlines an example application of our method. Section 6 contains a report on our implementation and the results of experiments that illustrate the practicality of our methods.

2. Preliminaries on matrix actions

Throughout, $\mathbb{Z}$ denotes the ring of integers, $\mathbb{Q}$ the field of rationals, and $\mathbb{F}_p$ the field with p elements. We consider a group G acting via $\nu : G \to GL(d, \mathbb{Q}) : g \to \overline{g}$ on $V = \mathbb{Q}^d$. The image of this action $\overline{G}$ is a rational matrix group. In this section we recall the properties and notations related to such actions and their modules which we need in our later methods.

The module V is called *irreducible* if it has no proper $\mathbb{Q}G$-invariant subspaces. Similarly, V is *semisimple* if it is a direct sum of irreducible subspaces and it is *homogeneous* if it is a direct sum of isomorphic irreducible subspaces. If V is irreducible, homogeneous or semisimple, then we also describe G as irreducible, homogeneous or semisimple, respectively. Further, $\overline{G}$ is *unipotent* if it is conjugate to a group of upper unitriangular matrices in $GL(d, \mathbb{Q})$. We say that $\overline{G}$ is $\mathbb{C}$-*triangularizable* if it is conjugate to an upper triangular subgroup of $GL(d, \mathbb{C})$.

Let G be finitely generated. Then there is a finite set of primes π such that the matrix entries of the elements of $\overline{G}$ have denominators divisible by primes in π only. For example, π can be chosen as the prime divisors of the entries in the generators of $\overline{G}$ and their inverses. We obtain that $\overline{G} \leq GL(d, \mathbb{Q}_\pi)$, where $\mathbb{Q}_\pi = \{\frac{a}{b} \in \mathbb{Q} \mid p \not| \; b \text{ for all } p \notin \pi\}$. Thus, if p is a prime with $p \notin \pi$, then the natural ring homomorphism $\iota : \mathbb{Q}_\pi \to \mathbb{F}_p$ extends to the *congruence homomorphism*

$$\psi_p : G \to GL(d, \mathbb{F}_p) : (g_{i,j})_{i,j} \mapsto ((g_{i,j})^\iota)_{i,j}.$$

The kernel G_p of ψ_p is called the *p-congruence subgroup* of G. The following fundamental theorem on the structure of p-congruence subgroups of polycyclic matrix groups is proved in [7], Lemma 9.

Theorem 2.1. (Dixon) *Let $\overline{G} \leq GL(d, \mathbb{Q}_\pi)$ be polycyclic. If $p \notin \pi$ is an odd prime, then $\overline{G}_p$ is torsion-free and $\overline{G}_p'$ is unipotent. Thus $\overline{G}_p$ is unipotent-by-abelian.*

The following lemma from [12] gives further insight into the structure of unipotent-by-abelian polycyclic rational matrix groups and the matrix algebras they generate. For a rational matrix group $\overline{G} \leq GL(d, \mathbb{Q})$ we denote by $\mathbb{Q}[\overline{G}]$ the matrix algebra generated by the matrix elements of $\overline{G}$. Thus $\mathbb{Q}[\overline{G}]$ is a rational algebra of dimension at most d^2.

Lemma 2.2. *Let $\overline{G}$ be a polycyclic subgroup of $GL(d, \mathbb{Q}_\pi)$ and $p \notin \pi$ an odd prime. Let $V = \mathbb{Q}^d$ be the natural $\mathbb{Q}\overline{G}$-module. Then the following are equivalent.*

a) *$\overline{G}$ is unipotent-by-abelian.*
b) *$\overline{G}$ is $\mathbb{C}$-triangularizable.*
c) *There exists a sequence of $\mathbb{Q}\overline{G}$-invariant subspaces $V = V_1 > \ldots > V_l > V_{l+1} = 0$ and a basis $\mathcal{B}$ through this sequence such that each $\overline{g} \in \overline{G}$ has the following form with respect to $\mathcal{B}$:*

$$\overline{g}_{\mathcal{B}} = \begin{pmatrix} \overline{g}^{\nu_1} & * & * & * \\ 0 & \overline{g}^{\nu_2} & * & * \\ 0 & 0 & \ddots & * \\ 0 & 0 & 0 & \overline{g}^{\nu_l} \end{pmatrix}$$

where $\nu_i : \overline{G} \to GL(d_i, \mathbb{Q}_\pi)$ is a homomorphism with an abelian image H_i such that the matrix algebra $\mathbb{Q}[H_i]$ is a field.

The factors V_i/V_{i+1} of a sequence as obtained in Lemma 2.2 c) are homogeneous, since the acting matrix algebra is simple. Thus we call such a sequence an *homogeneous block flag* for $\overline{G}$. The sequence is called an *irreducible block flag* if its factors are irreducible.

Our main application of Lemma 2.2 is to investigate p-congruence subgroups of groups G which act as subgroups of $GL(d, \mathbb{Z})$. Recall that these groups G_p act as unipotent-by-abelian groups by Theorem 2.1 and thus Lemma 2.2 applies. Further, these groups act on the rational space $\mathbb{Q}^d$, but they also act on the integral lattice $\mathbb{Z}^d$. In our later applications we want to exploit this fact and thus we introduce an integral version of Lemma 2.2.

Remark 2.3. Let G be a group acting via $\nu : G \to GL(d, \mathbb{Z})$ on $V = \mathbb{Q}^d$ and on $W = \mathbb{Z}^d$.

a) Let $U \leq V$ be a rational subspace and define $U^* = \{w \in W \mid uw = 0 \text{ for all } u \in U\}$, where uw is the natural scalar product. Then U^{**} is a subgroup of W with a free abelian factor group W/U^{**}. Further, U^{**} spans U as a rational vector space.
b) If $V = V_1 > \ldots > V_l > V_{l+1} = 0$ is a series of G-invariant subspaces of V, then using $W_i = V_i^{**}$ we obtain an equivalent series of G-invariant subgroups $W = W_1 > \ldots > W_l > W_{l+1} = 0$ such that W_i/W_{i+1} is free abelian.

We call the series of $\mathbb{Z}^d$ obtained by Remark 2.3 b) an *integral block flag* for G. Using Remark 2.3 a) it is straightforward to determine an integral block flag from a rational block flag. We denote an integral block flag as homogeneous or irreducible if the factors in the series are homogeneous or irreducible as rational modules. The following lemma from [8] yields an interesting application of integral block flags.

Lemma 2.4. *Let G_p be a p-congruence subgroup for the action $\nu : G \to GL(d, \mathbb{Z})$. Let $W = \mathbb{Z}^d$ and consider an integral homogeneous block flag $W = W_1 > \ldots > W_l > W_{l+1} = 0$ for G_p. Then the action of G_p on each free abelian factor W_i/W_{i+1} induces a homomorphism $\nu_i : G_p \to GL(d_i, \mathbb{Z})$ whose image $G_p^{\nu_i}$ is a free abelian group.*

Proof. Let $b \in GL(d, \mathbb{Z})$ be the base change matrix corresponding to $\mathcal{B}$, where $\mathcal{B}$ is a basis of W exhibiting the given flag. Note that $(\overline{G}_p)^b \leq (GL(d, \mathbb{Z})_p)^b = GL(d, \mathbb{Z})_p$. Thus $(\overline{G}_p)^b$ is a p-congruence subgroup. Hence $\overline{g} \in \overline{G}_p$ yields $\overline{g}^b = 1 + ph$ for a matrix h. The matrix block form of $\overline{g}^b$ implies now that $g^{\nu_i} = 1 + ph_i$ for a matrix h_i. Thus $(G_p)^{\nu_i}$ is a p-congruence subgroup. By Theorem 2.1 we obtain that $(G_p)^{\nu_i}$ is torsion-free and, since it is also abelian, we obtain that it is free abelian. $\square$

3. Basic Algorithms for Polycyclic Groups

Let G be a polycyclic group and let $\mathcal{G} = \{g_1, \ldots, g_n\}$ be a generating set for G. We define $G_i = \langle g_i, \ldots, g_n \rangle$ and $G_{n+1} = 1$. Then $\mathcal{G}$ is called a *polycyclic sequence* for G if $G_{i+1} \trianglelefteq G_i$ for $1 \leq i \leq n$; that is, the series of subgroups $G = G_1 \geq \ldots \geq G_n \geq G_{n+1} = 1$ is a subnormal series with cyclic factors of G. By definition, each polycyclic group has a series of this type and any such series can be used to obtain a polycyclic sequence of G.

Within our algorithm to solve the orbit-stabilizer problem for a polycyclic group G, we assume that G is given by a polycyclic sequence $\mathcal{G}$. In many applications of the orbit-stabilizer algorithm such a sequence will be known *a priori*; for example, the determination of centralizers or intersections of subgroups in polycyclically presented groups as outlined in [8] is an application of this type. Further, if G is a polycyclic rational matrix group given by a generating set, then we can use the practical method of [12] to determine a polycyclic sequence for G. Similarly, the algorithm developed by Lo [11] can be used to determine a polycyclic sequence for a polycyclic finitely presented group.

In the following sections we recall a number of basic methods for polycyclic groups given by polycyclic sequences. We refer to [14] for an introduction and primary applications and to [8] for a detailed discussion and a variety of applications of polycyclic sequences.

3.1. **Orbits and blocks.** Let G be a group acting by multiplication from the right on an arbitrary set Ω and assume that K is a normal subgroup in G. Suppose that we can solve the orbit-stabilizer problem in Ω for K: for given $v, w \in \Omega$ we can find an element $k \in K$ such that $vk = w$ or else we can determine that no such k exists, and we can compute generators for the stabilizer $Stab_K(v)$. The following lemma extends this to a solution for the orbit-stabilizer problem in G.

Lemma 3.1. *Let G be a group acting on Ω and let $K \trianglelefteq G$. Let $v \in \Omega$ and denote $Stab_G(vK) = \{g \in G \mid (vK)g = vK\}$ the setwise stabilizer of vK under the action of G.*

a) *$vG = \bigcup_{t \in T} (vt)K$, where T is a transversal for $Stab_G(vK)$ in G.*
b) *For each $g \in Stab_G(vK)$ there exists an element $k_g \in K$ with $vg = vk_g$.*
c) *$Stab_G(v) = \langle rk_r^{-1}, Stab_K(v) \mid r \in R \rangle$, where $R \subseteq G$ with $Stab_G(vK) = \langle R, K \rangle$.*

Proof. a) Since K is normal in G, we observe that $(vK)g = (vg)K$ for each $g \in G$. Thus $vG = \cup_{g \in G} (vg)K$. If $g = kh$ for an element $k \in Stab_G(vK)$, then $(vg)K = (vK)g = (vK)kh = (vK)h = (vh)K$. Hence we obtain $vG = \cup_{t \in T} (vt)K$.

b) This is obvious and we consider c). Let $g \in Stab_G(vK)$ and let $k_g \in K$ with $vg = vk_g$. Then $gk_g^{-1} \in Stab_G(v)$. Hence $KStab_G(v) = Stab_G(vK)$ and $Stab_G(v)$ is a supplement to K in $Stab_G(vK)$ with intersection $Stab_G(v) \cap K = Stab_K(v)$. This implies c). $\square$

To apply the approach of Lemma 3.1 we need a transversal T and generators R for the stabilizer $Stab_G(vK)$ modulo K. In particular, $Stab_G(vK)$ must have finite index in G.

3.2. **Determining finite orbits and their stabilizers.** The approach of Section 3.1 can be used to compute orbits and stabilizers in a finite set Ω under the action of a polycyclic group G given by a polycyclic sequence $\mathcal{G} = \{g_1, \ldots, g_n\}$. We consider $K = \langle g_2, \ldots, g_n \rangle$. Using the polycyclic sequence $\{g_2, \ldots, g_n\}$ for K, we can assume that we can solve the orbit-stabilizer problem for K by induction. We extend this solution for K to G as follows.

Since Ω is finite, there exists an $e \in \mathbb{N}$ with $(vK)g_1^{e+1} = vK$. If e is minimal with this condition, then $Stab_G(vK) = \langle g_1^{e+1}, K \rangle$. Thus we can choose $T = \{1, g_1, \ldots, g_1^e\}$ and $R = \{g_1^{e+1}\}$ in Lemma 3.1. Moreover, if $\{k_1, \ldots, k_r\}$ is a polycyclic sequence for $Stab_K(v)$, then $\{gk_g^{-1}, k_1, \ldots, k_r\}$ is a polycyclic sequence for $Stab_G(v)$, where $g = g_1^{e+1}$ and k_g is defined as in Lemma 3.1 b).

3.3. **Computing p-congruence subgroups.** We consider the p-congruence subgroup G_p corresponding to an action $\nu : G \to GL(d, \mathbb{Q})$. We can use the finite orbit stabilizer algorithm of Section 3.2 to determine a polycyclic sequence for G_p from that for G. For this purpose we consider a basis $\mathcal{B}$ of $\mathbb{F}_p^d$ and successively stabilize each basis vector in $\mathcal{B}$. Thus we obtain a sequence of stabilizers $S_1 = G$ and $S_{i+1} = Stab_{S_i}(b_i)$. Note that the finite orbit stabilizer algorithm produces a polycyclic sequence for the computed stabilizer. Hence we can iterate the application of this method and eventually obtain a polycyclic sequence for $S_{d+1} = G_p$.

3.4. **Calculating homogeneous and irreducible block flags.** In our orbit-stabilizer algorithm, we will use an irreducible block flag to solve the orbit-stabilizer problem for unipotent-by-abelian p-congruence subgroups G_p by an inductive approach. Hence we need to determine such a flag.

In [12] there is a practical method described to determine a homogeneous block flag for a unipotent-by-abelian matrix group given by a generating set. Using this, it remains to refine a given homogeneous block flag to an irreducible one. Also, for induction purposes we need to be able to refine an irreducible block flag for a unipotent-by-abelian group G to an irreducible block flag for a subgroup $H \leq G$. Both problems are addressed in [8] and practical solutions for them are obtained there. We recall these solutions in the following for completeness.

Lemma 3.2. *Let $\nu : G \to GL(d, \mathbb{Q})$ be such that the image of ν is a finitely generated abelian group $\overline{G}$. Let $V = \mathbb{Q}^d$ be its natural module.*

a) *If V is homogeneous as $\mathbb{Q}G$-module, then each non-trivial vector of V is contained in an irreducible $\mathbb{Q}G$-submodule of V.*
b) *If V is irreducible as $\mathbb{Q}G$-module and $H \leq G$, then V is homogeneous as $\mathbb{Q}H$-module.*

Proof. a) We consider $0 \neq w \in V$ and let U be the submodule of V generated by w. We have to prove that U is irreducible. Since V is homogeneous, there exists a direct factorization $V = V_1 \oplus \ldots \oplus V_r$ into isomorphic irreducible G-submodules. Let $w = w_1 + \ldots + w_r$ with $w_i \in V_i$. Since $w \neq 0$, there exists a component i with $w_i \neq 0$. Let $\psi : U \to V_i$ be the projection onto the i-th component of V. Since $w_i \neq 0$, we obtain that ψ is surjective. It remains to show that ψ is injective.

Let $u \in ker(\psi)$. By construction, $u = wa$ for an element $a \in \mathbb{Q}[\overline{G}]$ and thus $0 = u^\psi = (wa)^\psi = (w^\psi)a = w_i a$. By Schur's lemma we obtain that a acts trivially on V_i. Hence $a = 0$ and $u = wa = 0$ as desired.
b) The matrix algebra $\mathbb{Q}[\overline{G}]$ is abelian and acts irreducibly. Thus each non-zero element of $\mathbb{Q}[\overline{G}]$ is invertible by Schur's lemma. Hence also each non-zero element of the subalgebra $\mathbb{Q}[\overline{H}]$ is invertible. Therefore, $\mathbb{Q}[\overline{H}]$ cannot contain non-trivial ideals and $\mathbb{Q}[\overline{H}]$ is simple. Thus V is homogeneous under the action of $\mathbb{Q}H$. □

Using Lemma 3.2 a) we can now readily refine a homogeneous block flag to an irreducible block flag. For this purpose we consider each factor of the homogeneous block flag and refine it by a series with irreducible factors. Such a series can be determined by iterated computations of irreducible subspaces. In turn, as observed in Lemma 3.2 a), we can determine an irreducible subspace of the homogeneous factor by choosing an arbitrary non-trivial vector and determining the subspace it generates. The latter problem can be solved by a spinning algorithm. This elementary algorithm iteratedly acts with group generators on a basis of a subspace and thus obtains the closure of the subspace under the group action.

Similarly, we can refine an irreducible block flag for a group G to an irreducible block flag for a subgroup H, since by Lemma 3.2 b) the considered block flag is a homogeneous block flag for H and thus the above method applies.

Remark 3.3. Let $\nu : G \to GL(d, \mathbb{Z})$ be an integral action of G. Then we can determine an integral irreducible block flag for G using a rational irreducible block flag and Remark 2.3.

3.5. **Determining centralizers of abelian actions.** The computation of kernels of homomorphisms is one of the main tools in our orbit-stabilizer method. In all applications of the tool we consider a homomorphism of a polycyclic group G given by a polycyclic sequence $\mathcal{G} = \{g_1, \ldots, g_n\}$ into an abelian group: $\nu : G \to \overline{G} : g \mapsto \overline{g}$. Since the image of ν is abelian, we obtain that the relations of the images of $\mathcal{G}$ form a lattice:

$$rl(\overline{\mathcal{G}}) = \{(e_1, \ldots, e_n) \mid \overline{g}_1^{e_1} \cdots \overline{g}_n^{e_n} = 1\} \leq \mathbb{Z}^n.$$

The following lemma shows that the relation lattice determines the kernel of ν. We include a brief sketch of its proof here for completeness and we refer to [8] for a detailed proof and background on kernel computations in polycyclic groups.

Lemma 3.4. *Let G be a polycyclic group with a polycyclic sequence $\mathcal{G} = (g_1, \ldots, g_n)$ and let $\nu : G \to \overline{G}$ be a homomorphism with abelian image. Let $\mathcal{B}$ be a basis in upper triangular form for the relation lattice $rl(\overline{\mathcal{G}})$ and let $\mathcal{K} = \{g_1^{e_n} \cdots g_n^{e_n} \mid (e_1, \ldots, e_n) \in \mathcal{B}\}$ be its corresponding sequence in G. Then $\mathcal{K}$ forms a polycyclic sequence for $ker(\nu)$.*

Proof. We denote $\mathcal{K} = (k_1, \ldots, k_l)$. By construction, $K = \langle \mathcal{K} \rangle \leq ker(\nu)$. We show that $\mathcal{K}$ generates $ker(\nu)$ using induction. Since $\mathcal{G}$ is a polycyclic sequence, each $g \in G$ can be written uniquely in a form $g = g_1^{e_1} \cdots g_n^{e_n}$. The integer vector $(e_1, \ldots, e_n)$ is called the exponent vector of g. In the inductive step we suppose that all elements $g \in ker(\nu)$ whose exponent vectors have depth at least $i+1$ are contained in K. We consider an element $g \in ker(\nu)$ whose exponent vector $e = (e_1, \ldots, e_n)$ has depth i and we show in the following that $g \in K$. By construction, $e \in rl(\overline{\mathcal{G}})$. Since the basis $\mathcal{B}$ is in upper triangular form, there exists an element of depth i in this basis, say b_j, and there exists an integer $a \in \mathbb{N}$ such that $e - ab_j$ has depth greater than i. Now we obtain that $k_j^{-a} \cdot g$ is an element of $ker(\nu)$ whose exponent vector has depth greater than i. Thus, by induction, we obtain that $k_j^{-a} \cdot g \in K$ and therefore $g \in K$. Thus we obtain by induction that $K = ker(\nu)$. In fact, this inductive argument shows that $\mathcal{K}$ is a polycyclic sequence for K, since it determines the polycyclic series with subgroups $K \cap G_i$, where $G = G_1 \geq \ldots \geq G_{n+1} = 1$ is determined by $\mathcal{G}$. □

Remark 3.5. Lemma 3.4 will be applied in the following two cases.

a) $\nu : G \to \mathbb{Q}^d : g_i \mapsto \overline{g}_i$ and the images $\overline{g}_i$ are explicitly given vectors in $\mathbb{Q}^d$. In this case we can use the LLL-algorithm to determine a basis for the lattice $\langle \overline{g}_1, \ldots, \overline{g}_n \rangle$ and, simultaneously, determine the relations between the given images.

b) $\nu : G \to GL(d, \mathbb{Q}) : g_i \mapsto \overline{g}_i$ and the images $\overline{g}_i$ are explicitly given matrices generating a free abelian subgroup of $GL(d, \mathbb{Q})$ which acts irreducibly on $\mathbb{Q}^d$. In this case the matrix algebra $\mathbb{Q}[\overline{G}]$ is a field and finding the relation lattice can be translated into a number theoretic problem.

   In particular, if $\overline{G} \leq GL(d, \mathbb{Z})$, then $\overline{G}$ embeds into the units U of the maximal order of the algebraic number field $\mathbb{Q}[\overline{G}]$. Thus in this case it is sufficient to compute independent generators for U, express the given generators $\overline{g}_i$ in the independent ones and then apply the Hermite normal form algorithm to determine the relation lattice. Alternatively, we can determine the relation lattice by directly using the additive valuation theory which also underpins the unit group computation. For further background on this topic we refer to [3], Section 6.5.4, and to [13].

Remark 3.6. A constructive membership test in irreducible abelian matrix groups can also be obtained using relation lattices and Remark 3.5. More precisely, suppose that the elements $\overline{g}, \overline{g}_1, \ldots, \overline{g}_n$ of an irreducible free abelian group $\overline{G}$ are given and we want to determine an expression $\overline{g} = \overline{g}_1^{e_1} \cdots \overline{g}_n^{e_n}$ if it exists. For this purpose we can determine the relation lattice for $\overline{g}, \overline{g}_1, \ldots, \overline{g}_n$ using Remark 3.5. Then an expression of the desired type exists if and only if there exists a relation of the form $(-1, e_1, \ldots, e_n)$. This can be checked readily once the relation lattice is given.

(We also refer to [12] for methods to test membership in irreducible abelian matrix groups.)

4. Solving the orbit and stabilizer problems

Let G be a polycyclic group which acts on $\mathbb{Q}^d$ via $\nu : G \to GL(d, \mathbb{Z})$ and suppose that a polycyclic sequence for G is known. In this section we introduce a method to solve the orbit-stabilizer problem for elements of $\mathbb{Q}^d$ under the action of G.

First we observe that it is sufficient to solve the orbit-stabilizer problem for elements of $\mathbb{Z}^d$. Let $v, w \in \mathbb{Q}^d$. Then there exists an $0 \neq e \in \mathbb{Q}$ with $ev, ew \in \mathbb{Z}^d$. We obtain that $Stab_G(v) = Stab_G(ev)$ and $vg = w$ if and only if $(ev)g = (ew)g$.

4.1. **Reduction to p-congruence subgroups.** Let G_p be a p-congruence subgroup of G. Since $G_p \trianglelefteq G$ and $[G : G_p]$ is finite, we can use Lemma 3.1 to extend a solution for the orbit-stabilizer problem for G_p to G. Thus we need to determine generators R with $Stab_G(vG_p) = \langle R, G_p \rangle$ and a transversal T for $Stab_G(vG_p)$ in G assuming that we can solve the orbit-stabilizer problem for G_p.

Since G_p has finite index in G, we obtain that the orbit Ω of vG_p under the action of G is finite. Since G is given by a polycyclic sequence, we can compute a set R using the finite orbit-stabilizer algorithm of Section 3.2 and the action of G on Ω. Since Ω is finite, $Stab_G(vG_p)$ has finite index in G. A finite transversal T can be determined together with the action of G on Ω. Therefore, we can reduce the orbit-stabilizer problem for G to finitely many orbit and stabilizer computations for G_p.

Hence it remains to solve the orbit-stabilizer problem for G_p. We use that G_p is polycyclic and unipotent-by-abelian and we describe methods to solve these problems in this case in Sections 4.3 and 4.4. First, in Section 4.2, we consider approaches to optimize the reduction to G_p.

4.2. **Optimizing the reduction.** The extension of the solution for the orbit-stabilizer problem from G_p to G incorporates several calls to the solution of the orbit-stabilizer problem in G_p. While our methods to solve this problem are practical, it will increase the efficiency to reduce the number of such calls as far as possible.

For this purpose we note that if we know *a priori* an intermediate subgroup $Stab_G(vG_p) \leq H \leq G$, then $Stab_G(vG_p) = Stab_H(vG_p)$ and thus the block stabilizer can be determined using a stabilizer computation in the smaller group H. It will be an advantage for the determination of the block stabilizer if $[Stab_G(vG_p) : H]$ is small, since this index corresponds to the orbit length and this, in turn, has an influence on the number of calls to the orbit algorithm for G_p.

Lemma 4.1. *Consider the congruence homomorphism $\psi_p : G \to GL(d, \mathbb{F}_p)$ with kernel G_p. Let v be an element in $\mathbb{Z}^d$ with image v_p in $\mathbb{F}_p^d$. Note that G acts naturally on $\mathbb{F}_p^d$ via ψ_p and let $S_p = Stab_G(v_p)$.*

a) *$Stab_G(v) \leq S_p \leq G$ and thus $Stab_G(v) = Stab_{S_p}(v)$.*
b) *$Stab_G(vG_p) \leq S_p \leq G$ and thus $Stab_G(vG_p) = Stab_{S_p}(vG_p)$.*

Proof. a) is obvious, since ψ_p is an action homomorphism of G. To prove b) we consider an element $g \in Stab_G(vG_p)$. By construction, there exists an element $k \in G_p$ with $vg = vk$. Since G_p is a congruence subgroup,k acts as $1 + pr$ on $\mathbb{Z}^d$ for some matrix r. Thus $vk = v + prv \equiv v \bmod p$. Hence $\psi_p(g)$ stabilizes v_p and b) follows. □

Lemma 4.1 a) shows that we can start the orbit-stabilizer computation by initially computing S_p for a suitable prime p and then replacing G by S_p. This process may be iterated for a number of primes p if desired. Note that S_p can be determined effectively using the finite orbit-stabilizer algorithm of Section 3.2. In particular, we can use the finite field arithmetic for this computation which is more efficient than the rational arithmetic used for our remaining calculations.

Experiments suggest that it is useful to apply this approach for at least one prime p. As indicated by Lemma 4.1 b), the best results are often obtained for the prime p which is also used to determine G_p. In turn, for the computation of G_p it is most effective to choose the smallest possible prime p. Unfortunately, this prime is not always most suitable for this reduction approach as the following example illustrates.

Example 4.2. We consider the matrix $g \in GL(3,\mathbb{Z})$ defined by

$$g = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 3 & 0 & 1 \end{pmatrix}. \quad \text{Then } g^{2i} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 3i & 3i & 1 \end{pmatrix} \text{ for } i \in \mathbb{Z}.$$

We define $G = \langle g \rangle$ and we suppose that we want to determine $Stab_G(v)$ for $v = (0,0,1)$ using the reduction outlined above. Let $B_p = Stab_G(vG_p)$.

First, we choose $p = 3$ and obtain that $vg = (3,0,1) \equiv (0,0,1) \bmod 3$. Hence $S_3 = G$. Further, the 3-congruence subgroup G_3 is generated by g^2 and thus $vG_3 = \{(3i, 3i, 1) \mid i \in \mathbb{Z}\}$. We obtain $G_3 = B_3$. Altogether, we find that $G_3 = B_3 < S_3 = G$ with $[S_3 : B_3] = 2$.

Performing the same calculation with $p = 5$ instead, we find that $G_5 = B_5 = S_5 = \langle g^{10} \rangle < G$. Thus, $p = 5$ is a better choice for this example. But one can also observe in this small example that the generators for G_5 contain larger integer entries which is likely to make subsequent computations with G_5 less effective than similar computations with G_3.

4.3. **Vector stabilizer for p-congruence subgroups.** We consider an action of G via $\nu : G \to GL(d,\mathbb{Z}) : g \to \overline{g}$ and we suppose that G is a p-congruence subgroup with respect to this action for an odd prime p. Thus the image $\overline{G}$ of the action homomorphism is unipotent-by-abelian and we can determine an integral irreducible block flag $V = V_1 > \ldots > V_l > V_{l+1} = 0$ for G by applying Remark 3.3. We use induction down this flag to determine $Stab_G(v)$ for $v \in \mathbb{Z}^d$.

In the inductive step, we assume that $G = Stab_G(v + V_i)$ and we calculate a polycyclic sequence for $Stab_G(v + V_{i+1})$. We then replace G by $Stab_G(v + V_{i+1})$ and proceed by induction. Note that after such an induction step we might have to refine the integral irreducible block flag to such a flag for the computed subgroup. This can be achieved using the method of Lemma 3.2.

To simplify notation, we assume that $V_{i+1} = 0$ and we denote V_i by U. By our induction hypothesis, G stabilizes $v + U$ and thus $v(g-1) = vg - v \in U$ for each $g \in G$. Hence we obtain a map $\delta : G \to U : g \mapsto v(g-1)$. It is straightforward to verify that δ is a derivation of G; that is, $(gh)^\delta = (g^\delta)h + h^\delta$ and $1^\delta = 0$. Further, we observe that $Stab_G(v) = ker(\delta) = \{g \in G \mid g^\delta = 0\}$. Hence we want to determine the kernel of the derivation δ.

Let $K = C_G(U)$; that is, K is the kernel of the natural action of G on the module U. By our setup, $U = \mathbb{Z}^e$ for some $e \in \mathbb{N}$ and thus G acts via a homomorphism $G \to GL(e,\mathbb{Z})$ with free abelian image as observed in Lemma 2.4. Hence a polycyclic sequence for K can be computed from a polycyclic sequence of G using the method of Section 3.5. We consider the restriction of δ to K in the following lemma.

Lemma 4.3. *Let G be a group acting on a module U. Define $K = C_G(U)$ and let $\delta : G \to U$ be a derivation.*

a) *The restriction $\delta_K : K \to U$ is a group homomorphism.*
b) *The image K^δ is a G-invariant sublattice of U.*

Proof. a) Since K centralizes U, we obtain for $k, h \in K$ that $(kh)^\delta = (k^\delta)h + h^\delta = k^\delta + h^\delta$. Thus δ_K is a homomorphism into the additive group U.
b) Since δ is a derivation, we obtain for $k \in K$ and $g \in G$ that $(k^g)^\delta = (g^{-1}kg)^\delta = ((g^{-1})^\delta)kg + (k^\delta)g + g^\delta = (k^\delta)g$, since k centralizes U and thus $((g^{-1})^\delta)kg = ((g^{-1})^\delta)g = -g^\delta$. Hence $(k^\delta)g = (k^g)^\delta \in K^\delta$ using that K is normal in G. ☐

Thus the stabilizer problem for K is easy to solve: $Stab_K(v) = ker(\delta_K)$ which is the kernel of a group homomorphism with abelian image. Further, the abelian image is explicitly given by generators for the lattice K^δ and thus a polycyclic sequence for $Stab_K(v)$ can be computed effectively as described in Remark 3.5 a). The following theorem provides the basis for our solution of the stabilizer problem for G.

Theorem 4.4. *Let G be a polycyclic group acting as irreducible free abelian group on the integral module U. Let $K = C_G(U)$ and let $\delta : G \to U$ be a derivation. Then one of the following cases holds:*

(1) $K^\delta = 0$ *and* $ker(\delta) = G$.
(2) $K^\delta = 0$ *and* $ker(\delta) = K$.
(3) $dim_{\mathbb{Q}} K^\delta = dim_{\mathbb{Q}} U$.

Proof. As observed in Lemma 4.3, the sublattice K^δ of U is G-invariant. Since G acts irreducibly on U, we obtain that K^δ either generates all of U or is trivial. Suppose that $K^\delta = 0$ and $ker(\delta) < G$. We have to show that $ker(\delta) = K$ and we are in case 2). Since $K^\delta = 0$, we have that $K \leq ker(\delta)$. On the other hand, $ker(\delta) < G$ and there exists an element $g \in G$ with $g^\delta \neq 0$. Let $h \in G \setminus K$ be an arbitrary element. First note that $gh = hgk$ for some $k \in K$, since G/K is abelian by our setup. Thus, $(gh)^\delta = (hgk)^\delta = ((hg)^\delta)k + k^\delta = (hg)^\delta$, since k acts trivially on U and $k^\delta = 0$. This yields $(g^\delta)h + h^\delta = (h^\delta)g + g^\delta$ and hence $(g^\delta)(h-1) = (h^\delta)(g-1)$. Both g and h are elements which act non-trivially on U. Since G acts as an abelian irreducible group, we have that the matrix algebra induced by the action of G on U is a field and thus $g-1$ and $h-1$ act as invertible elements on U. Thus $h^\delta = (g^\delta)(h-1)(g-1)^{-1} \neq 0$. Therefore, $h \notin ker(\delta)$. Since $h \in G \setminus K$ is arbitrary, we obtain that $ker(\delta) = K$ as desired. □

This theorem translates into the following approach to determine $Stab_G(v)$ as the kernel of the given derivation δ. First, we can readily check if δ is trivial. In this case, $ker(\delta) = G$ and there is nothing to do. If δ is non-trivial, then we determine K and check if $K^\delta = 0$. In this case, we obtain $ker(\delta) = K$ by Theorem 4.4. It remains to consider the case where $K^\delta \neq 0$. Theorem 4.4 shows that K^δ generates U as a rational vector space in this case and thus $[U : K^\delta] < \infty$. This finiteness condition yields that the remaining kernel computation for $ker(\delta)$ is essentially a finite computation which can be solved by the finite orbit-stabilizer algorithm. This is discussed in more detail in the following theorem.

Theorem 4.5. *Let G be a polycyclic group acting as irreducible free abelian integral matrix group on the integral module U. Let $K = C_G(U)$ and let $\delta : G \to U : g \mapsto v(g-1)$ be a derivation such that $0 \neq K^\delta$. Then we obtain the following.*

a) $\gamma : G \to U/K^\delta : g \to g^\delta + K^\delta$ *is a derivation with* $K \leq ker(\gamma)$.
b) $ker(\gamma) = Stab_G(v + K^\delta)$ *and* $[G : ker(\gamma)] < \infty$.
c) $ker(\gamma) = ker(\delta)K$.

Proof. Denote $I = K^\delta$ and recall that I is a G-invariant sublattice of U. Thus γ is a derivation and, by construction, $K \leq ker(\gamma)$ obtaining a).
For b) we observe that $\delta : G \to U : g \mapsto v(g-1)$ and thus we can read off that the kernel of γ is the stabilizer of the coset of v modulo I. Further, since U/I is a finite set, we obtain that $[G : ker(\gamma)]$ is finite as well.

Let $g \in ker(\gamma)$; that is, $g^\gamma = g^\delta + I = I$. Thus $g^\delta \in I$ and hence there exists an element $k \in K$ with $g^\delta = k^\delta$. Then $(gk^{-1})^\delta = 0$ and thus $gk^{-1} \in ker(\delta)$. Therefore we can write $g = hk$ for an element $k \in K$ and $h \in ker(\delta)$ which proves c). □

We determine $ker(\delta)$ using Theorem 4.5 in two steps. First, we compute a polycyclic sequence for $ker(\gamma)$. By Theorem 4.5 b), we can use the finite orbit-stabilizer algorithm of Section 3.2 for this purpose. Secondly, we use Theorem 4.5 c) to translate a polycyclic sequence of $ker(\gamma)$ into a polycyclic sequence of $ker(\delta)$. Let $g \in ker(\gamma)$. Then $g^\delta \in K^\delta$ and we can use the solution to the orbit problem for K to determine an element $k \in K$ with $g^\delta = k^\delta$. Now $(gk^{-1})^\delta = 0$ and thus $gk^{-1} \in ker(\delta)$. If we apply this process to the elements of a polycyclic sequence of $ker(\gamma)$, then we obtain a polycyclic sequence of $ker(\delta)$.

4.4. **Vector orbit for p-congruence subgroups.** We consider an action of G via $\nu : G \to GL(d, \mathbb{Z}) : g \to \overline{g}$ and we suppose that G is a p-congruence subgroup with respect to this action for an odd prime p. Thus the image $\overline{G}$ of the action homomorphism is unipotent-by-abelian and we can determine an integral irreducible block flag $V = V_1 > \ldots > V_l > V_{l+1} = 0$ for G by applying Remark 3.3. We use induction down this flag to check if the two elements $v, w \in \mathbb{Z}^d$ are in the same G-orbit and if so, then we compute an element $g \in G$ with $vg = w$.

In the inductive step, we assume that we have found an element h in G such that $vh - w$ is an element of V_i. Replacing v with vh, we may assume that $v - w \in V_i$. We want to decide if there exists an element $g \in G$ such that $vg - w \in V_{i+1}$, and, if so, to find such an g. Such an g would fix $v + V_i$, so we may assume that $G = Stab_G(v + V_i)$. This stabilizer can be determined using the method of the previous section. If necessary, we refine the given integral irreducible block flag to such a flag for this subgroup using the method of Lemma 3.2.

To simplify notation, we assume that $V_{i+1} = 0$ and we denote V_i by U. As in Section 4.3, we define a derivation $\delta : G \to U : g \mapsto v(g-1)$ and we compute its kernel $K = C_G(U)$. It remains now to check if the element $u = w - v \in U$ is contained in the image G^δ and if so, then determine $g \in G$ with $u = g^\delta$. This element then yields $v(g-1) = vg - v = w - v = u$ and thus $vg = w$.

Our solution to this problem is based on the same approach as the stabilizer algorithm of Section 4.3. Thus we next determine which case of Theorem 4.4 applies to our given situation and proceed accordingly.

Case (1) In this case $G^\delta = 0$. Thus $u \in G^\delta$ if and only if $u = 0$. In other words, v and w are in the same G-orbit if and only if $v = w$.

Case (2) In this case $K^\delta = 0$ and $G^\delta \neq 0$. Since $K \leq ker(\delta)$, this yields that we can consider δ as a derivation of the free abelian group G/K. The next lemma and its following theorem yield the basis for our method to decide if a given element $u \in U$ is contained in G^δ in this case.

Lemma 4.6. *Let G be a polycyclic group acting as a non-trivial free abelian irreducible group $\overline{G}$ on the module $U = \mathbb{Z}^e$. Then there exist elements $g_1, \ldots, g_e \in G$ such that $\{\overline{g}_1 - 1, \ldots, \overline{g}_e - 1\}$ is a basis of the matrix algebra $\mathbb{Q}[\overline{G}]$.*

Proof. We consider the $\mathbb{Q}$-span W of $\{\overline{g} - 1 \mid \overline{g} \in \overline{G}\}$. Then W is a subspace of the vector space $\mathbb{Q}[\overline{G}]$. Further, $(\overline{g} - 1)\overline{h} = \overline{g}\overline{h} - \overline{h} = (\overline{g}\overline{h} - 1) - (\overline{h} - 1) \in W$ and W is $\overline{G}$-invariant. Since $\overline{G}$ acts as a free abelian irreducible group on U, we obtain that $\mathbb{Q}[\overline{G}]$ is a field and thus $W = \mathbb{Q}[\overline{G}]$. Further, $dim_{\mathbb{Q}}\mathbb{Q}[\overline{G}] = e$ and thus $\mathbb{Q}[\overline{G}]$ is spanned by e elements of the form $\overline{g} - 1$. □

We note that a basis for $\mathbb{Q}[\overline{G}]$ as described in the above lemma can be computed readily. It provides the setup for the following fundamental theorem.

Theorem 4.7. *Let G be a polycyclic group acting as free abelian irreducible group $\overline{G}$ on the module $U = \mathbb{Z}^e$. We consider a derivation $\delta : G \to U$ and an element $u \in U$. We suppose that $K^\delta = 0$ for $K = C_G(U)$ and $G^\delta \neq 0$. Then we obtain the following.*

a) *If $\{\overline{g}_1 - 1, \ldots, \overline{g}_e - 1\}$ is a basis of $\mathbb{Q}[\overline{G}]$, then $\{g_1^\delta, \ldots, g_e^\delta\}$ is a basis of $\mathbb{Q}^e$. Thus we can write $u = a_1 g_1^\delta + \ldots + a_e g_e^\delta$ for certain $a_1, \ldots, a_e \in \mathbb{Q}$.*

b) *Let $a_u = a_1(\overline{g}_1 - 1) + \ldots + a_e(\overline{g}_e - 1) + 1 \in \mathbb{Q}[\overline{G}]$. Then $u \in G^\delta$ if and only if $a_u \in \overline{G}$. In this case we obtain that $u = g^\delta$ for a preimage g of a_u in G.*

Proof. Since $K \leq ker(\delta)$, we can consider δ as a derivation of G/K. To simplify notation, we assume $K = 1$ and thus $G = \overline{G} \leq GL(e, \mathbb{Z})$. In particular, G is an abelian group acting irreducibly on $\mathbb{Q}^e$. We consider the mapping defined by

$$\varphi : G \to GL(e+1, \mathbb{Z}) : g \mapsto \tilde{g} = \begin{pmatrix} g & 0 \\ g^\delta & 1 \end{pmatrix}.$$

Since δ is a derivation, we obtain that φ is a homomorphism and thus an isomorphism from G to $H = \{\tilde{g} \mid g \in G\}$. In particular, H is abelian. If $\hat{h}$ is defined as the upper left $e \times e$-submatrix of an $(e+1) \times (e+1)$-matrix h, then the inverse of φ is obtained by

$$\nu : H \to G : h \mapsto \hat{h}.$$

We consider the matrix algebra $\mathbb{Q}[H]$. The elements of this algebra are of the form

$$a = \begin{pmatrix} \hat{a} & 0 \\ v_a & q_a \end{pmatrix} \text{ with } v_a \in \mathbb{Q}^e \text{ and } q_a \in \mathbb{Q}.$$

Note that for $g \in G$ we have that $v_{\tilde{g}} = g^\delta$. We extend ν to an algebra homomorphism

$$\nu : \mathbb{Q}[H] \to \mathbb{Q}[G] : a \mapsto \hat{a}.$$

In the following we investigate the algebra homomorphism ν in various steps.

1) Let b be an arbitrary element in $\mathbb{Q}[G]$. Since $g_1 - 1, \ldots, g_e - 1$ spans $\mathbb{Q}[G]$, we can write $b - 1 = b_1(g_1 - 1) + \ldots + b_e(g_e - 1)$ for certain $b_1, \ldots, b_e \in \mathbb{Q}$. We define $a = b_1(\tilde{g}_1 - 1) + \ldots + b_e(\tilde{g}_e - 1) + 1 \in \mathbb{Q}[H]$. Then $a^\nu = b$ and a is a preimage of b in $\mathbb{Q}[H]$ with the property that $q_a = 1$ and $v_a = b_1 g_1^\delta + \ldots + b_e g_e^\delta$.

2) We determine the kernel of ν. First, we construct non-trivial elements in $ker(\nu)$: we choose an element $b \in \mathbb{Q}[H]$ with $q_b \neq 1$ (say $b = 2\tilde{g}$ for some $\tilde{g} \in H$), determine $a \in \mathbb{Q}[H]$ with $a^\nu = b^\nu$ and $q_a = 1$ as in 1) and obtain $c = a - b \in ker(\nu)$ with $q_c = q_a - q_b = 1 - q_b \neq 0$. Thus $\dim_{\mathbb{Q}} ker(\nu) \geq 1$.

Now let $a \in ker(\nu)$; that is, $a^\nu = 0$. Since H is an abelian group,$\mathbb{Q}[H]$ is an abelian algebra and thus a commutes with each element $\tilde{g} \in H$. We compute

$$\tilde{g}a = \begin{pmatrix} g & 0 \\ g^\delta & 1 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ v_a & q_a \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ v_a & q_a \end{pmatrix} \text{ and } a\tilde{g} = \begin{pmatrix} 0 & 0 \\ v_a g + q_a g^\delta & q_a \end{pmatrix}$$

and we obtain $v_a g + q_a g^\delta = v_a$ and thus $v_a(g - 1) = -q_a g^\delta$. Hence, if $q_a = 0$, then $v_a = 0$, since g stabilizes v_a for all $g \in G$ in this case and G acts irreducibly.

Otherwise, if $q_a \neq 0$, then $-\frac{v_a}{q_a} = g^\delta(g-1)^{-1}$ for all $1 \neq g \in G$. Thus $\frac{v_a}{q_a}$ is constant over all $a \in ker(\nu)$ with $q_a \neq 0$ and $\dim_{\mathbb{Q}} ker(\nu) \leq 1$. In summary, we obtain that $ker(\nu)$ has dimension 1.

3) We define $A = \{a \in \mathbb{Q}[H] \mid \hat{a} \neq 0 \text{ and } q_a = 1\}$. Then each $a \in A$ is invertible with

$$\begin{pmatrix} \hat{a} & 0 \\ v_a & 1 \end{pmatrix}^{-1} = \begin{pmatrix} \hat{a}^{-1} & 0 \\ -v_a\hat{a}^{-1} & 1 \end{pmatrix}$$

and thus A is a multiplicative group. We show that the restriction $\nu_A : A \to \mathbb{Q}[G] \setminus \{0\} : a \mapsto \hat{a}$ is an isomorphism of multiplicative groups. Clearly, it is a homomorphism, since ν is an algebra homomorphism. It is surjective by 1). Thus it remains to observe that ν_A is injective. Suppose that $a \in A$ with $a^\nu = 1$. Then $a - 1 \in \mathbb{Q}[H]$ with $(a-1)^\nu = 0$. Thus $a - 1 \in ker(\nu)$ and $q_{a-1} = 0$, since $q_a = 1$ and $q_1 = 1$. By the discussion in 2) we obtain that $v_{a-1} = 0$ and thus $a = 1$. Hence ν_A is injective and thus an isomorphism.

4) Clearly, $H \leq A$. Further, for $a \in A$ the element v_a depends only on $\hat{a} \in \mathbb{Q}[G]$ by 3).

Now we are in the position to prove the theorem as follows.

a) Let W be the rational space spanned by $g_1^\delta, \ldots, g_e^\delta$. Using 1) and 4) we observe that $W = \langle v_a \mid a \in A\rangle$. Since

$$a\tilde{g} = \begin{pmatrix} \hat{a} & 0 \\ v_a & 1 \end{pmatrix}\begin{pmatrix} g & 0 \\ g^\delta & 1 \end{pmatrix} = \begin{pmatrix} \hat{a}g & 0 \\ v_ag + g^\delta & 1 \end{pmatrix} \text{ and } a\tilde{g} = \begin{pmatrix} \widehat{a\tilde{g}} & 0 \\ v_{a\tilde{g}} & 1 \end{pmatrix}$$

we obtain $v_ag = v_{a\tilde{g}} - g^\delta = v_{a\tilde{g}} - v_{\tilde{g}} \in W$ and W is a G-invariant subspace of $\mathbb{Q}^e$. As G acts irreducibly on $\mathbb{Q}^e$ and $W \neq 0$, this yields $W = \mathbb{Q}^e$ proving a).

b) Let $u \in \mathbb{Q}^e$ and write $u = a_1g_1^\delta + \ldots + a_eg_e^\delta$. Let $a = a_1(\tilde{g}_1 - 1) + \ldots + a_e(\tilde{g}_e - 1) + 1 \in \mathbb{Q}[H]$. Then by 1) and 4) we observe that a is the unique element in A with $v_a = u$. Hence $u \in G^\delta$ if and only if $a \in H$. Equivalently, $u \in G^\delta$ if and only if $\hat{a} \in G$. Since $\hat{a} = a_1(g_1 - 1) + \ldots + a_e(g_e - 1) + 1$, we obtain b). □

Using Theorem 4.7 we can now readily decide if $u \in \overline{G}^\delta$. First we determine a basis of the form $g_1 - 1, \ldots, g_e - 1$ of $\mathbb{Q}[\overline{G}]$ using a spinning algorithm as in Section 3.4. Then we can readily determine $u = a_1\overline{g}_1^\delta + \ldots + a_e\overline{g}_e^\delta$. This defines the element $a_u \in \mathbb{Q}[\overline{G}]$ as in Theorem 4.7 b). Now it remains to check if $a_u \in \overline{G}$ and, if so, to find a preimage in G of a_u. Since $\overline{G}$ is an abelian irreducible matrix group, this can be achieved using the constructive membership test of Remark 3.6.

Case (3) In this case $K^\delta \neq 0$ and hence $[U : K^\delta] < \infty$. We first check if $u \in K^\delta$. If so, then we obtain an element $k \in K$ with $u = k^\delta$ and this solves the problem. Note that a basis for the lattice K^δ can be computed readily and thus the membership test in K^δ is straightforward.

If $u \notin K^\delta$, then we determine the (finite) G-orbit of $v + K^\delta \in U/K^\delta$. Similar to Theorem 4.5, we can now observe that v and w are in the same G-orbit if and only if $v + K^\delta$ is in the same G-orbit as $w + K^\delta$. If this is the case, then we obtain an element $g \in G$ with $wg = v + k^\delta = v + v(k-1) = vk$ and thus $wgk^{-1} = v$.

5. An example application

Let $G = \langle a, b, c\rangle$ with

$$a = \begin{pmatrix} -1 & 1 & 8 \\ -5 & -2 & 20 \\ -1 & 0 & 5 \end{pmatrix}, b = \begin{pmatrix} -47 & -24 & 192 \\ 0 & 1 & 0 \\ -12 & -6 & 49 \end{pmatrix} \text{ and } c = \begin{pmatrix} -23 & 0 & 96 \\ 0 & 1 & 0 \\ -6 & 0 & 25 \end{pmatrix}.$$

It is a determinant computation to observe that $G \le GL(3, \mathbb{Z})$. We want to determine $Stab_G(v)$ for $v = (-1, 0, 5)$ using the methods introduced in the above sections. These need as input a polycyclic sequence of the considered group. We note that $\mathcal{G} = (a, b, c)$ is such a sequence; in fact, the elements a, b, c fulfill the relations of the polycyclic presentation

$$b^a = c, \;\; b^{a^{-1}} = b^{-1}c, \;\; c^a = bc, \;\; c^{a^{-1}} = b, \;\; c^b = c, \;\; c^{b^{-1}} = c.$$

Step 1. We choose $p = 3$ as an admissible odd prime for G. As an initial step for the desired stabilizer computation, we determine a polycyclic sequence for the 3-congruence subgroup G_3 as described in Section 3.3. We obtain that G acts as a cyclic group of order 8 on $\mathbb{F}_3^3$ and $G_3 = \langle a^8, b, c\rangle$.

In Section 4.1 we observed that the stabilizer problem for G reduces to a solution for the orbit-stabilizer problem for G_3. This reduction has been improved in Section 4.2. To apply this improvement, we consider the action of G on $\mathbb{F}_3^3$ and determine the orbit and the stabilizer of the element v in this induced action. Using the finite orbit-stabilizer methods of Section 3.2, we obtain that the orbit of the image $v_3 \in \mathbb{F}_3^3$ of v has length 4 under the action of G. The preimage of the stabilizer of v_3 in G is given by $S_3 = \langle a^4, b, c\rangle$. Hence, as outlined in Section 4.2, we may replace G by S_3 and thus simplify the desired stabilizer computation.

Step 2. Now we determine a polycyclic sequence for $Stab_{G_3}(v)$ using the method for p-congruence subgroups introduced in Section 4.3. As a first step we construct an irreducible block flag for G_3 by applying Section 3.4. We observe that the base change matrix

$$g = \begin{pmatrix} 4 & 0 & -5 \\ 0 & -1 & 2 \\ 1 & 0 & -1 \end{pmatrix}$$

conjugates the generators of G_3 such that

$$\overline{a} = (a^8)^g = \begin{pmatrix} 1 & 54 & 87 \\ 0 & 13 & 21 \\ 0 & 21 & 34 \end{pmatrix}, \overline{b} = b^g = \begin{pmatrix} 1 & 6 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \overline{c} = c^g = \begin{pmatrix} 1 & 0 & 6 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Further, $\overline{v} = vg = (1, 0, 0)$. It remains now to compute the stabilizer $Stab_{G_3}(\overline{v})$ using the new action of G_3. This new action exhibits the irreducible block flag $\mathbb{Z}^3 = V_1 > V_2 > V_3 = 0$ with $V_2 = \langle (0, 1, 0), (0, 0, 1)\rangle$. Obviously, $\overline{v} + V_2$ is stabilized by G_3 and thus we can proceed directly to the next iteration step considering the action of G_3 on V_2.

Following the notation in Section 4.3, we denote $U = V_2$. Next, we set up the derivation δ. For this purpose we compute the values of δ on the polycyclic sequence of G_3 and we obtain that

$$\overline{a}^\delta = \overline{v}(\overline{a}-1) = (0,54,87),\ \ \overline{b}^\delta = \overline{v}(\overline{b}-1) = (0,6,0),\ \ \overline{c}^\delta = \overline{v}(\overline{c}-1) = (0,0,6).$$

Note that the values of δ on the polycyclic sequence are sufficient to determine the value of g^δ for an arbitrary element g: we can write g as a product of the generators and then use the relation $(hk)^\delta = (h^\delta)k + k^\delta$. Recall that we want to determine the kernel of the derivation δ to obtain $ker(\delta) = Stab_{G_3}(\overline{v})$.

Obviously, the considered derivation δ is non-trivial. Hence we have to determine the kernel K of the action of G_3 on U. Generally, we use the methods of Section 3.5 for this purpose. However, in this case it is straightforward to read off from the conjugated generators of G_3 that $K = C_{G_3}(U) = \langle \overline{b}, \overline{c}\rangle$ and $\{\overline{b}, \overline{c}\}$ forms a polycyclic sequence for K.

As a major tool in the computation of $ker(\delta)$ we use the restriction of δ to the centralizer K. This restriction can be computed readily for the polycyclic sequence of K. We obtain that

$$K^\delta = \langle (0,6,0), (0,0,6)\rangle = 6U.$$

In this case, the images of δ on the polycyclic sequence of K yield a lattice basis for K^δ. In general, we only obtain generators for the considered lattice and a basis is then determined easily by applying a Hermite normal form computation on the images. We note that the image K^δ is indeed a G_3-invariant sublattice of U as observed in Lemma 4.3 b). Further, the restriction δ_K is a group homomorphism by Lemma 4.3 a) and thus we can use the methods of Section 3.5 to compute that $ker(\delta_K) = 1$.

As our next step we have to check which case of Theorem 4.4 applies to the given situation. Since $K^\delta \neq 0$, we are in case (3) of this theorem. Thus we have to consider Theorem 4.5 and determine the induced derivation γ from δ. Since $K \leq ker(\gamma)$, we can consider γ as derivation of G_3/K. We determine $ker(\gamma)$ as described in Theorem 4.5 b) using the finite orbit-stabilizer algorithm of Section 3.2. We obtain that $\overline{v} + K^\delta$ has an orbit of length 3 under the action of G_3; in fact, we obtain

$$\begin{aligned}
\overline{va} &= (1,54,87) \equiv (1,0,3) \bmod K^\delta\\
\overline{va}^2 &\equiv (1,0,3)\overline{a} = (1,117,189) \equiv (1,3,3) \bmod K^\delta\\
\overline{va}^3 &\equiv (1,3,3)\overline{a} = (1,156,252) \equiv (1,0,0) = \overline{v} \bmod K^\delta
\end{aligned}$$

Thus $ker(\gamma) = \langle \overline{a}^3, \overline{b}, \overline{c}\rangle$ with index 3 in G_3. Using Theorem 4.5 d) we now translate $ker(\gamma)$ into $ker(\delta)$. As described in Section 4.3, we consider the polycyclic sequence of $ker(\gamma)$ and lift it to a polycyclic sequence of $ker(\delta)$. Note that $ker(\delta_K) = ker(\delta) \cap K$. Thus the polycyclic sequence of $ker(\delta_K)$ can be used as the initial part of the desired sequence, while the remaining part of K is avoided by $ker(\delta)$. In our case $ker(\delta_K) = 1$, while $\overline{b}, \overline{c} \in K$ and thus these two elements are avoided by $ker(\delta)$. Hence it remains to consider $\overline{a}^3$. Here we obtain

$$\overline{va}^3 = (1, 121392, 196416) = \overline{v} + 20232\,(0,6,0) + 32736\,(0,0,6).$$

Hence $\overline{a}^3 \cdot \overline{b}^{-20232} \cdot \overline{c}^{-32736}$ stabilizes $\overline{v}$. Using the original basis and the original generators a, b, c of G we obtain as resulting stabilizer

$$Stab_{G_3}(v) = ker(\delta) = \langle a^{24} \cdot b^{-20232} \cdot c^{-32736}\rangle.$$

Step 3. Finally, we extend the solution for the stabilizer problem in G_3 to the corresponding solution in S_3. Since $[S_3 : G_3] = 2$ and $S_3 = \langle a^4, G_3\rangle$, we determine $w = va^4 = (-26, -7, 105)$ and obtain $\overline{w} = wg = (1, 7, 11)$. Now we have to check if $\overline{v}$ and $\overline{w}$ are contained in the same G_3-orbit. Thus we have to apply the solution to the orbit problem in G_3.

This orbit problem for G_3 is solved using the same machinery as the stabilizer computation of step 2. Thus we use induction down the irreducible block flag of G_3 and we consider the action of G_3 on $U = V_2$. We observe that $\overline{w} \equiv (1, 1, 5) \bmod K^\delta$. Since this element is not contained in the G_3-orbit of $\overline{v} + K^\delta$, we can read off that $\overline{w}$ is not in the same G_3-orbit as $\overline{v}$.

Result: We obtain $Stab_G(vG_3) = G_3$ and thus $Stab_G(v) = Stab_{G_3}(v)$. Hence by Step 2 we can now read off

$$Stab_G(v) = \langle a^{24} \cdot b^{-20232} \cdot c^{-32736}\rangle = \langle \begin{pmatrix} 838801 & 231840 & -3355200 \\ -231840 & -64079 & 927360 \\ 167760 & 46368 & -671039 \end{pmatrix} \rangle.$$

6. Implementation and experiments

Our algorithms have been implemented in the computer algebra system GAP incorporating an interface to KANT to solve the number theoretic problems of Remark 3.5 b). The GAP part of the implementation builds on the POLYCYCLIC [9] package for computations with infinite polycyclic groups defined by polycyclic presentations.

It is rather difficult to give precise limits for the range of applications of the considered methods. Clearly, the efficiency of applications depends on the number and the dimensions of an integral irreducible block flag for the considered group. The orbit lengths arising in applications of the finite orbit-stabilizer algorithm are a further limiting factor. However, the most unpredictable difficulties arise from integer arithmetic problems if large integers turn up in the acting matrices or the underlying lattices.

We estimate that the orbit-stabilizer computation is usually practical for modules $\mathbb{Q}^d$ up to dimension $d \leq 10$ if no integer arithmetic problems occur. Our experiments suggest that it can also be practical for larger dimensions depending on the action of the considered polycyclic group.

In the following sections we give a more detailed report on the practicality of the methods and we include an outline of various runtimes for our methods. All timings have been obtained on a PC with 128 MB Ram and a Celeron 500 Mhz processor running under Linux and they are given in seconds.

6.1. **Almost crystallographic groups.** Almost crystallographic groups can be defined as finitely generated nilpotent-by-finite groups with trivial normal torsion subgroup. Dekimpe [5] introduced a library of almost crystallographic groups of Hirsch lengths 3 and 4. This catalog of groups is available in GAP as share package Aclib [6]. All groups in this catalog are polycyclic and they can be accessed in two different representations: as rational matrix groups in dimension 4 or 5 and as polycyclically presented groups.

We consider the almost crystallographic groups of Hirsch length 4 in their matrix representation in $GL(5, \mathbb{Q})$ and we determine of stabilizers of elements in $\mathbb{Q}^5$ under the action of these groups. These matrix groups are unipotent-by-finite and we can conjugate them such that the unipotent normal subgroup is integral. In this setting we can then apply the method of Section 4.

The Aclib classification contains 95 different types of groups of Hirsch length 4. The runtimes to determine the stabilizer of a random element of $\mathbb{Z}^5$ under a group from this list range between 0.03 seconds and 1.1 seconds. This shows that the stabilizer method for such groups is practical.

In the following table we consider the groups G_1 and G_2 which are defined by the types $(4, 41)$ and $(4, 82)$ in [5] in more detail. These groups have a polycyclic series with factors of the orders $(2, 2, 2, \infty, \infty, \infty, \infty)$ and $(2, 6, \infty, \infty, \infty, \infty)$, respectively. The following table contains runtimes in seconds for some stabilizer computations of elements in $\mathbb{Q}^5$ and it includes the orders of the factors of a polycyclic series for the stabilizers.

	$(4, -7, 2, -1, 3)$		$(1, 0, 0, 0, 0)$		$(0, 0, 1, 0, 0)$	
	stabilizer	time	stabilizer	time	stabilizer	time
G_1	(∞)	0.5	$(2, \infty)$	0.3	$(2, \infty, \infty, \infty)$	0.1
G_2	(∞)	0.7	(∞)	1.1	$(2, \infty, \infty, \infty)$	0.2

6.2. **Further examples.** In Table 1 we report runtimes for the stabilizer computation applied to the example $G = \langle a, b, c \rangle$ of Section 5 and some randomly chosen elements of $\mathbb{Z}^3$. While this example is of rather small dimension, it is still interesting, since almost all the features of our algorithm are used in the computations with this example. In particular, the number theoretic method of Remark 3.5 is used frequently. This part of the algorithm is performed by KANT and we note that the runtimes for the application of KANT are not incorporated in the timings of the following table. However, these runtimes are negligible in all cases considered here. The stabilizer is cyclic in all of the listed cases and it is described by a generator.

element	stabilizer	time
$(1, 4, -3)$	$a^{24}\ b^{-47496}\ c^{-76848}$	0.12
$(3, 3, 1)$	$a^{56}\ b^{-64223866204}\ c^{-103916398407}$	0.7
$(-1, 4, -1)$	$a^{120}\ b^{-279046542389632386371112}\ c^{-451506790029563504521296}$	0.15
$(-1, -3, 0)$	$a^{24}\ b^{-18582}\ c^{-30066}$	0.12
$(-3, 2, -1)$	$a^{84}\ b^{-31422136657942756}\ c^{-50842085111695408}$	0.7
$(-1, -2, -2)$	$a^{24}\ b^{-14776}\ c^{-23908}$	0.12
$(-2, -5, 0)$	$a^{24}\ b^{-17247}\ c^{-27906}$	0.11
$(-2, 0, -2)$	$a^{120}\ b^{-126638925791829255497592}\ c^{-204906086229955426121889 6}$	0.14
$(0, 5, 2)$	$a^{6}\ b^{-7}\ c^{-10}$	0.27
$(1, -5, 2)$	$a^{24}\ b^{-2316}\ c^{-3748}$	0.13

TABLE 1. Action on a 3-dimensional module

In Section 5 we introduced an action of the group $G = \langle a, b, c \rangle$ on $\mathbb{Q}^3$. Now we use this action to define a new operation of G on $\mathbb{Q}^3 \otimes \mathbb{Q}^3 \cong \mathbb{Q}^9$ via $(v \otimes w)g = vg \otimes wg$. Thus we obtain a new action $G \to GL(9, \mathbb{Z})$ for this group. As above, we choose some random elements of $\mathbb{Q}^9$ and collect runtimes and stabilizers in Table 2. We note that the computation of a homogeneous integral block flag for the 3-congruence

element	stabilizer	time
$(-3, 0, -3, 3, 1, 0, 2, 0, 4)$	1	1.28
$(-2, 1, 1, -1, 1, 1, 2, 2, -5)$	1	1.18
$(0, -3, -1, 1, 1, 1, 2, -1, 0)$	1	1.13
$(2, 5, -3, -2, -2, -2, -5, 5, -3)$	1	1.19
$(-1, -3, 0, -4, -1, -4, 3, 4, 1)$	1	1.23

TABLE 2. Action on a 9-dimensional module

subgroup of G takes about 1.1 seconds for this action and hence this forms the major part of the computation.

Let $G = \langle a, b, c \mid b^a = bc\rangle$ and consider the rationally irreducible action of G on $\mathbb{Q}^4$ via

$$a \mapsto \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{pmatrix} \text{ and } b \mapsto \begin{pmatrix} 1 & 1 & 0 & -1 \\ -1 & 0 & 1 & 0 \\ 0 & -1 & 0 & 1 \\ 1 & 1 & -1 & 0 \end{pmatrix}.$$

This action induces a natural diagonal action on the tensor product $\mathbb{Q}^4 \otimes \mathbb{Q}^4$ and this yields an action of G as a subgroup of $GL(16, \mathbb{Z})$. In Table 3 we give runtimes for the stabilizer algorithm applied to randomly chosen elements of $\mathbb{Q}^{16}$. We note that the factors in a homogeneous series for the 3-congruence subgroup of G have dimensions 4 and 12 and it takes about 5.5 seconds to compute such a homogeneous series. Hence, again, the calculation of the series is the main time-consuming part of the algorithm. The stabilizer is described by a generator in the following table.

element	stabilizer	time
$(1, 2, -1, 0, 0, -4, -1, 1, 3, -2, 0, -1, -2, 3, 0, 0)$	c	6.47
$(-1, 0, 1, -2, -3, 2, -3, 4, 0, -1, -1, 0, 1, 1, -4, -2)$	c	5.65
$(-1, 2, 1, 2, 1, 2, 0, -4, -2, 2, 1, -1, 1, 2, 0, -1)$	c	6.46
$(1, 2, 4, 0, 4, 1, -2, 1, 5, -1, 0, 0, 1, 1, 1, 1)$	c	5.69
$(-2, 1, -2, 2, -2, 4, 3, 2, 1, -2, 0, 1, -1, -2, -2, 2)$	c	5.72

TABLE 3. Action on a 16-dimensional module

7. FINAL COMMENTS

Using the methods of Section 4 we obtain a practical approach to solve the orbit-stabilizer problem for elements of $\mathbb{Q}^d$ under action of a polycyclic group G which acts as a subgroup of $GL(d, \mathbb{Z})$.

The methods introduced in Section 4 heavily rely on the fact that a polycyclic sequence for G is given. Such a sequence is known in many applications of our methods or otherwise it can be computed as described in Section 3. However, it is possible to modify our algorithm to use an arbitrary generating set for G. In this case it substitutes a number of the methods outlined in Section 3 by algorithms to compute with integral polycyclic matrix groups which have been introduced in [12]. It would be interesting to investigate the practicality of this variation as well.

The methods presented here apply to integral polycyclic matrix groups only. A particularly interesting extension of our methods would be the case of rational matrix representations. Many of the approaches outlined in this paper extend to rational representations as well. It seems that the primary limitation to integral representations derives from the fact that we need to obtain an application of the finite orbit stabilizer algorithm for solving the problem in Case (3) of Theorem 4.4.

References

1. Gilbert Baumslag, Frank B. Cannonito, Derek J. S. Robinson, and Dan Segal, *The algorithmic theory of polycyclic-by-finite groups*, J. Algebra **142** (1991), 118–149.
2. Gregory Butler, *Fundamental algorithms for permutation groups*, Lecture Notes in Comput. Sci., vol. 559, Springer-Verlag, New York, Heidelberg, Berlin, 1991.
3. Henri Cohen, *A course in computational algebraic number theory*, Graduate texts in mathematics, vol. 138, Springer-Verlag, New York, 1995.
4. M. Daberkow, C.Fieker, J. Klüners, M. Pohst, K.Roegner, and K. Wildanger, *Kant V4*, J. Symb. Comput. **24** (1997), 267 – 283.
5. Karel Dekimpe, *Almost-bieberbach groups: Affine and polynomial structures*, Lecture notes in Math., vol. 1639, Springer, 1996.
6. Karel Dekimpe and Bettina Eick, *Aclib*, 2000, A GAP share package, see [15].
7. John D. Dixon, *The orbit-stabilizer problem for linear groups*, Can. J. Math. **37** (1985), 238–259.
8. Bettina Eick, *Algorithms for polycyclic groups*, Habilitationsschrift, Universität Kassel, 2001.
9. Bettina Eick and Werner Nickel, *Polycyclic*, 2000, A GAP share package, see [15].
10. R. Laue, J. Neubüser, and U. Schoenwaelder, *Algorithms for finite soluble groups and the SOGOS system*, Computational Group Theory, Durham, 1982, Academic Press, 1984, pp. 105 – 135.
11. Eddie H. Lo, *A polycyclic quotient algorithm*, J. Symbolic Computation **25** (1998), 61–97.
12. Gretchen Ostheimer, *Practical algorithms for polycyclic matrix groups*, J. Symbolic Computation **28** (1999), 361–379.
13. Michael E. Pohst, *Computational algebraic number theory*, DMV Seminar, vol. 21, Birkäuser, 1993.
14. Charles C. Sims, *Computation with finitely presented groups*, Encyclopedia of mathematics and its applications, Cambridge University Press, New York, 1994.
15. The GAP Group, *GAP – Groups, Algorithms and Programming*, www.gap-system.org, 2000.

Institut für Geometrie, Universität Braunschweig, 38106 Braunschweig, Germany
E-mail address: `beick@tu-bs.de`

Department of Computer Science, 103 Hofstra University, NY 11549, USA
E-mail address: `cscgzo@husun3.Hofstra.edu`