J. Symbolic Computation (1999) **11**, 1–000

A Practical Algorithm for Finding Matrix Representations for Polycyclic Groups

Eddie H. Lo and Gretchen Ostheimer

National Security Agency, Fort Meade, MD 20755
Mathematics Department, Tufts University, Medford, MA 02155

(Received 24 August 1999)

In this paper we describe a new algorithm for constructing a representation by integer matrices for a polycyclic group given by a finite presentation. This is a first step toward finding a practical algorithm for this problem. We used our algorithm to construct representations for various polycyclic groups. The examples which we studied included a collection of free nilpotent groups, and our results here led us to a new theoretical result concerning such groups.

1. Introduction

In this paper we consider the representation problem: given a finite presentation for a group G, decide whether or not G has a faithful representation as a matrix group and, if so, construct such a representation. Clearly, there does not exist an algorithm to solve this problem in general: if such an algorithm existed, we could use it to decide whether or not a given finitely presented group were trivial, and this latter problem is known to be undecidable. However if we insist that G define a polycyclic group, then G has a faithful matrix representation (Chapter 5, Segal (1983)), and, furthermore, there exists an algorithm to construct such a representation. This latter fact follows implicitly from the results in Baumslag *et al.* (1991), and in that paper the authors raise the question of whether practical algorithms exist for this and other fundamental problems concerning polycyclic groups. This paper constitutes a first step toward answering their question. Preliminary experiments suggest that the algorithm described here is practical enough to be useful in studying some interesting presentations (Section 5). Among the examples considered were a collection of free nilpotent groups; our results here led us to a new theoretical result concerning such groups (Section 6).

The algorithm for embedding polycyclic groups implicit in Baumslag *et al.* (1991) is described in Section 2. Segal also developed an algorithm for the representation problem for polycyclic groups as a step toward establishing the decidability of the isomorphism problem for such groups (Segal, 1990). For a comparison of our practical algorithm with earlier algorithms, see Section 4.

This paper is based on the second author's Ph. D. thesis (Ostheimer, 1996a). In that thesis, a practical algorithm is given for embedding a polycyclic group provided that the group satisfies a certain technical restriction. The restriction is weak in the sense

0747–7171/90/000000 + 00 \$03.00/0

that every polycyclic group has a finite index subgroup satisfying it. In this paper, we extend the results in Ostheimer (1996a) by removing the restriction. We do so by relying on algorithms in Lo (1997) and Ostheimer (1996b). We also discuss some heuristics for improving on the algorithm in Ostheimer (1996a) based on new experimental results. Further experiments are needed to better understand which kinds of presentations can be represented practically using our techniques.

1.1. Notation and definitions

Throughout this paper let $\mathbf{Z}$ denote the ring of integers, $\mathbf{Q}$ the field of rationals, and $\mathbf{C}$ the field of complex numbers. If n is a positive integer and if R is any ring, the group of $n \times n$ matrices which are invertible over R is denoted by $\mathrm{GL}(n, R)$. The ring of $n \times n$ matrices over R is denoted by $M(n, R)$.

Let F be any field, and let E be an extension field of F. If G is a subgroup of $\mathrm{GL}(n, F)$, then G is *triangularizable over* E if there is a basis for E^n relative to which every matrix in G is upper triangular, and G is *triangularizable* if it is triangularizable over the algebraic closure of F. If G is a subgroup of $\mathrm{GL}(n, F)$ and if G is triangularizable over some extension field E of F, then there exists a finite extension L of F over which G is triangularizable. (See p. 33 of Segal (1983).) Therefore, a subgroup G of $\mathrm{GL}(n, \mathbf{Q})$ is triangularizable if and only if it is triangularizable over $\mathbf{C}$.

Let $\mathrm{Tr}_1(n, R)$ denote the group of upper triangular matrices with entries in R and ones along the diagonal. Elements of $\mathrm{Tr}_1(n, R)$ are called *unitriangular*. An element of $\mathrm{GL}(n, R)$ is *unipotent* if all of its eigenvalues are 1. If G, a subgroup of $\mathrm{GL}(n, R)$, consists entirely of unipotent elements, then G is said to be *unipotent*. If G is unipotent and if R is $\mathbf{Z}$ or $\mathbf{Q}$, then there is a basis for R^n with respect to which G is unitriangular. (The case when $R = \mathbf{Q}$ is proved as Corollary 1.21 in Wehrfritz (1973), and the case when $R = \mathbf{Z}$ follows easily.) Lemma 7 of Chapter 5 of Segal (1983) gives an alternative condition which guarantees the existence of such a basis, namely, that G act nilpotently on R^n: the group G *acts nilpotently* on R^n if there exists a chain

$$0 \leq V_0 \leq V_1 \leq \cdots \leq V_k = R^n$$

of G-invariant subgroups of R^n such that the induced action of G on each factor V_i/V_{i-1} is trivial.

1.2. Basic algorithms for polycyclic groups

Chapter 9 in Sims (1994) gives a good introduction to polycyclic groups. A group G is *polycyclic* if there is a sequence of subgroups $G_1, \ldots, G_{k+1}$ for G such that

$$G = G_1 \triangleright G_2 \triangleright \cdots \triangleright G_k \triangleright G_{k+1} = 1,$$

where for each i, G_i/G_{i+1} is cyclic. In this case, if $g_i G_{i+1}$ is a generator for G_i/G_{i+1}, then $g_1, \ldots, g_k$ is called a *polycyclic generating sequence* for G. A group G is polycyclic if and only if G is solvable and all of the subgroups of G are finitely generated.

Polycyclic groups are finitely presented. It is often convenient to assume that a polycyclic group is given by a special presentation known as a *consistent polycyclic presentation*. Intuitively, a consistent polycyclic presentation is one from which the polycyclic structure of the group is easily gleaned. In particular, the generators in a consistent polycyclic presentation form a polycyclic generating sequence for G. (See Section 9.6 of Sims (1994) for a precise definition.)

Throughout this paper we rely on the following algorithms in Sims (1994) and Lo (1998a) for working with a polycyclic group G given by a consistent polycyclic presentation. These include:

testing membership in a subgroup of G,
finding the normal closure of a subgroup of G,
finding generating sets for the terms in the lower central series of G, and
finding a consistent polycyclic presentation for a subgroup or a quotient of G.

We also rely on the fact that a polycyclic group satisfies the ascending chain condition on subgroups. See Section 9.3 in Sims (1994) for a proof.

For a polycyclic group G define the *torsion subgroup* of G, $T(G)$, to be

$$\langle N \mid N \triangleleft G \text{ and } N \text{ finite}\rangle.$$

It follows from the ascending chain condition that $T(G)$ is finite. In Section 3.2 we will need a practical algorithm to find the torsion subgroup of a nilpotent group given by a consistent polycyclic presentation. In Theorem 3.11 of Baumslag *et al.* (1991), the authors describe an algorithm for finding $T(G)$ for polycyclic G. In the case when G is actually nilpotent, their algorithm (modified slightly) appears to be practical. The modified algorithm is described as follows. Begin by finding the last nontrivial term $A = \gamma_c(G)$ in the lower central series for G. By induction on the class of G, we can find the torsion subgroup of G/A and hence its preimage C under the map $G \to G/A$. We can then find the torsion subgroup of C/C' and its preimage T under the map $C \to C/C'$. It is obvious that $T(G) \leq T$. Since A is central in G, A is contained in $Z(C)$, the center of C. Therefore $|C : Z(C)| \leq |C : A| < \infty$. By a theorem of Schur (Corollary 10.1.4 in Robinson (1982)), it follows that C' is finite. Therefore, T is finite and $T = T(G)$.

1.3. Algorithms for the group ring

In order to construct a representation of a polycyclic group G, we let G act on the group ring $\mathbf{Z}[H]$ for various subgroups H of G. In this section we recall some basic facts about group rings. We also discuss a generalization of the Gröbner basis method in commutative ring theory to the group ring of a polycyclic group. (See Lo (1998b) or Lo (1996b).)

Throughout this paper, the term *ideal* will be used to refer to a two-sided ideal of a ring. However, the algorithms in Lo (1998b) work with right ideals. Therefore, our ideals will be described by a finite set of right ideal generators. (Recall that each right ideal in the group ring of a polycyclic-by-finite group is finitely generated as a right ideal. For two different proofs of this, see Hall (1954) and Lo (1996b).) Note that if R is any ring and $\mathcal{A}$ and $\mathcal{B}$ are ideals of R generated as right ideals by sets A and B respectively, then $\mathcal{AB}$ is generated as a right ideal by $\{ab \mid a \in A,\, b \in B\}$.

The *augmentation ideal* $\mathcal{G}$ of $\mathbf{Z}[G]$ is the kernel of the ring homomorphism of $\mathbf{Z}[G]$ to $\mathbf{Z}$ taking $\sum n_g g$ to $\sum n_g$. If G is generated by $a_1, \ldots, a_k$ as a group, then the set $\{a_1 - 1, \ldots, a_k - 1\}$ generates $\mathcal{G}$ as a right ideal. To see this, let $\mathcal{J}$ be the right ideal generated by $\{a_1 - 1, \ldots, a_k - 1\}$. Since $\mathcal{G}$ is generated by

$$\{g - 1 \mid g \in G,\ g \neq 1\}$$

as an abelian group, it suffices to show that for all g in G, $g-1 \in \mathcal{J}$. But suppose that $w \in G$ and $w-1 \in \mathcal{J}$. Then $wa_i - 1 = (w-1)a_i + (a_i - 1) \in \mathcal{J}$, and $wa_i^{-1} - 1 = ((w-1)-(a_i-1))a_i^{-1} \in \mathcal{J}$. By induction on the word length of w, it can be shown that for all $g \in G$, $g-1 \in \mathcal{J}$, and hence $\mathcal{J} = \mathcal{G}$.

Let G be a polycyclic group and let $\mathcal{I}$ be an ideal of $\mathbf{Z}[G]$. Suppose we are given a consistent polycyclic presentation for G and a finite set of elements in the group ring that generates $\mathcal{I}$ as a right ideal. In Lo (1996a), algorithms have been implemented to solve the following problems.

Decide whether or not a given element of the group ring is an element of $\mathcal{I}$.
Decide whether or not $\mathbf{Z}[G]/\mathcal{I}$ is finitely generated as an abelian group.
If so, find a finite set of elements of $\mathbf{Z}[G]$ whose images generate $\mathbf{Z}[G]/\mathcal{I}$ as an abelian group, and find a finite set of elements of $\mathbf{Z}[G]$ whose images generate the torsion subgroup of $\mathbf{Z}[G]/\mathcal{I}$ (considered as an abelian group).

If, in addition, $\mathbf{Z}[G]/\mathcal{I}$ is a free abelian group, then the following problems can be solved.

Find a set of elements of $\mathbf{Z}[G]$ whose images form a basis for $\mathbf{Z}[G]/\mathcal{I}$.
Given an element x of the group ring, express $x + \mathcal{I}$ in terms of that basis.

Let H be a finitely generated group acting on $\mathbf{Z}[G]/\mathcal{I}$ by $\mathbf{Z}$-automorphisms, where $\mathbf{Z}[G]/\mathcal{I}$ is finitely generated free abelian. In this paper we will consider several situations in which we start with a concrete description of the action of H; that is, if h is a given element of H and if x is a given element of $\mathbf{Z}[G]$, then we can find an element y of $\mathbf{Z}[G]$ such that the image of $x+\mathcal{I}$ under h is $y+\mathcal{I}$. In such situations a matrix representation for H can be found as follows. Find elements $b_1, \ldots, b_n$ of $\mathbf{Z}[G]$ whose images form a basis for $\mathbf{Z}[G]/\mathcal{I}$. Then for each generator h of H, find a matrix representing the action of h on $\mathbf{Z}[G]/\mathcal{I}$ by expressing the image of each $b_i + \mathcal{I}$ (under the action of h) as a $\mathbf{Z}$-linear combination of $b_1 + \mathcal{I}, \ldots, b_n + \mathcal{I}$.

2. Decidability

Let G be a polycyclic group given by a finite presentation. In this section we show that it follows implicitly from the results in Baumslag *et al.* (1991) that there exists an algorithm to find an embedding for G. Among the results in Baumslag *et al.* (1991) are algorithms to do the following.

Find a presentation for a polycyclic subgroup of $\mathrm{GL}(n, \mathbf{Z})$ given by a finite generating set of matrices.
Find the kernel of a homomorphism between two polycyclic groups given by finite presentations.

To find an embedding for G we can proceed as follows. Let X be the given generating set. Begin by enumerating the set maps f from X into $\{M(n,\mathbf{Z}), n = 1, 2, \ldots\}$. It is easy to decide whether or not f defines a homomorphism from G into $\mathrm{GL}(n, \mathbf{Z})$: check whether or not $f(X) \subseteq \mathrm{GL}(n,\mathbf{Z})$ and, if so, check whether or not the matrices in $f(X)$ satisfy the relations for G. For each such homomorphism f, proceed as follows. Find a presentation for $f(G)$. Let Y be the generating set for this presentation. For each x in

X, express $f(x)$ as a word in the elements of Y and their inverses. In this way, we get a definition of f as a homomorphism between two groups defined by finite presentations. Next, find the kernel of f. If that kernel is trivial, stop: f is an embedding. If not, keep looking; eventually this algorithm will terminate.

Clearly, this algorithm is not practical. A practical algorithm is described in the next section.

3. A practical algorithm

Let G be a polycyclic group given by a finite presentation. In this section we describe a practical algorithm for constructing an embedding of G into $\mathrm{GL}(n, \mathbf{Z})$ for some n. Section 3.2 describes the algorithm for the special case when G can be embedded in a unitriangular group, Sections 3.5 and 3.6 generalize the algorithm to the case when G can be embedded in a triangularizable group, and Section 3.7 considers the most general case–when G can be embedded in a solvable matrix group. In describing these algorithms, we need to refer to earlier proofs of the existence of such embeddings; for completeness these proofs are summarized in Sections 3.1 and 3.4. We also describe practical algorithms for deciding whether or not G falls into either of the above special cases (Sections 3.3 and 3.6).

3.1. Existence of an embedding into $\mathrm{Tr}_1(n, \mathbf{Z})$

In Chapter 5 of Segal (1983), Segal proves the existence of an embedding of a finitely generated torsion-free nilpotent group into a unitriangular matrix group. In Section 3.2 we describe an algorithm for constructing this embedding. In this section we summarize the results from Segal (1983) to which we will need to refer when describing our construction.

Proposition 3.1. *Let $G = X \ltimes H$ be a semidirect product. Then the action of H on $\mathbf{Z}[H]$ by right multiplication and the action of X on $\mathbf{Z}[H]$ by conjugation extend simultaneously to give an action of G on $\mathbf{Z}[H]$. Thus, there is a homomorphism*

$$^* : G \to Aut_{\mathbf{Z}}(\mathbf{Z}[H])$$

such that for h in H, x in X and $a = \sum_{c \in H} a_c c$ in $\mathbf{Z}[H]$,

$$a^{h^*} = ah, \text{ and } a^{x^*} = a^x = \sum_{c \in H} a_c c^x.$$

Now let H be a finitely generated torsion-free nilpotent group of class c. Segal defines the ideal $\mathcal{I}(H)$ of $\mathbf{Z}[H]$ as follows. Let $\mathcal{H}$ be the augmentation ideal of $\mathbf{Z}[H]$. Then $\mathbf{Z}[H]/\mathcal{H}^{c+1}$ is finitely generated as an abelian group. Let T be the torsion subgroup of $\mathbf{Z}[H]/\mathcal{H}^{c+1}$ considered as an abelian group under addition. Define $\mathcal{I}(H)$ to be the pullback of T under the quotient map that takes $\mathbf{Z}[H]$ to $\mathbf{Z}[H]/\mathcal{H}^{c+1}$. Segal proves the following theorem, thereby establishing the existence of a representation of $X \ltimes H$ in which H is represented by a unitriangular matrix group.

Theorem 3.2. *Let H be a finitely generated torsion-free nilpotent group. Then the quotient $\mathbf{Z}[H]/\mathcal{I}(H)$ is a finitely generated free abelian group. Let $X = Aut(H)$ and define the map*

$$^* : X \ltimes H \to Aut_{\mathbf{Z}}(\mathbf{Z}[H])$$

as in Proposition 3.1. Then $\mathcal{I}(H)$ is invariant under $(X \ltimes H)^*$, and $X \ltimes H$ acts faithfully via * on $\mathbf{Z}[H]/\mathcal{I}(H)$. Furthermore, there exists a basis for $\mathbf{Z}[H]/\mathcal{I}(H)$ relative to which H is represented by unitriangular matrices.

Recall that for all n, $\mathrm{Tr}_1(n, \mathbf{Z})$ is finitely generated torsion-free nilpotent. Therefore, it follows from Theorem 3.2 that an abstract group H can be embedded in $\mathrm{Tr}_1(n, \mathbf{Z})$ for some n if and only if H is finitely generated torsion-free nilpotent.

Segal's proof of Theorem 3.2 yields a bound on the size of the faithful representation, as follows.

PROPOSITION 3.3. *Let H be a finitely generated torsion-free nilpotent group of class c. Then the rank of $\mathbf{Z}[H]/\mathcal{I}(H)$ as a free abelian group is less than or equal to $1+k+\cdots+k^c$, where k is the number of generators for H/H'.*

PROOF. In Lemma 2 of Chapter 5, Segal proves that $\mathcal{H}/\mathcal{H}^2$ is isomorphic to H/H' (as an abelian group). In the proof of Lemma 3, he notes that there is a a $\mathbf{Z}$-module epimorphism

$$\pi_i : \mathcal{H}^{i-1}/\mathcal{H}^i \otimes \mathcal{H}/\mathcal{H}^2 \to \mathcal{H}^i/\mathcal{H}^{i+1}$$

given by

$$(x + \mathcal{H}^i) \otimes (y + \mathcal{H}^2) \to xy + \mathcal{H}^{i+1}.$$

Therefore, if we have a generating set for $\mathcal{H}^{i-1}/\mathcal{H}^i$ consisting l elements, then we can find a generating set for $\mathcal{H}^i/\mathcal{H}^{i+1}$ consisting of lk elements. By induction it follows that there is a generating set for $\mathcal{H}^i/\mathcal{H}^{i+1}$ consisting of k^i elements. Since $\mathbf{Z}[H]/\mathcal{H}$ is a cyclic group, there is a generating set for $\mathbf{Z}[H]/\mathcal{H}^{c+1}$ consisting of $1 + k + \cdots + k^c$ elements. □

The special case when H is a finitely generated free nilpotent group is discussed in Section 6. The bound is tight in this case.

The following proposition turns out to be very useful in Section 5 where we perform experiments for obtaining representations.

PROPOSITION 3.4. *Suppose that G is a group isomorphic to the semidirect product $H \rtimes X$, where H is isomorphic to Z^n and the conjugation action of X on H is faithful. Let $\phi : X \to GL(n, Z)$ correspond to the conjugation action with respect to some basis of H. Let $\psi : G \to GL(n+1, Z)$ be defined by*

$$\psi(xh) = \begin{pmatrix} 1 & h \\ 0 & \phi(x) \end{pmatrix},$$

where $h \in H$ is written as a row vector with respect to the basis and $x \in X$. Then ψ is a faithful representation of G.

PROOF. Since H is free abelian, it is torsion-free and is nilpotent of class 1. The quotient of $\mathbf{Z}[H]$ by the augmentation ideal $\mathcal{I}(H) = \mathcal{H}^2$ is free and has rank $n+1$ as an abelian group; in fact, if $h_1, h_2, \ldots, h_n$ is a basis of H, then $\{1 + \mathcal{H}^2, h_1 - 1 + \mathcal{H}^2, h_2 - 1 + \mathcal{H}^2, \ldots, h_n - 1 + \mathcal{H}^2\}$ is a basis for the abelian group $\mathbf{Z}[H]/\mathcal{H}^2$. (For a proof of this, consult the proof of Proposition 6.1.) It is easy to check that the matrix in Proposition 3.4 is just the matrix constructed by using this basis. □

3.2. Constructing an embedding into $\mathrm{Tr}_1(n, \mathbf{Z})$

Suppose we are given a consistent polycyclic presentation for H and that H is torsion-free nilpotent. Let $\mathcal{H}$ and $\mathcal{I}(H)$ be defined as in Section 3.1. We can use the algorithms of Lo as described in Section 1.3 to construct the embedding in Theorem 3.2, provided that we can find a finite set of elements of the group ring that generates $\mathcal{I}$ as a right ideal. We will now show how to find such a generating set.

Let $\{a_1, \ldots, a_k\}$ be a set of generators for H. As we saw in Section 1.3, $\{a_1 - 1, \ldots, a_k - 1\}$ generates $\mathcal{H}$ as a right ideal. Hence we can obtain a set of k^{c+1} elements of $\mathbf{Z}[H]$ that generates $\mathcal{H}^{c+1}$ as a right ideal. Use the algorithms in Lo (1998b) to obtain a generating set

$$\{b_1 + \mathcal{H}^{c+1}, \ldots, b_r + \mathcal{H}^{c+1}\}$$

for the torsion subgroup of $\mathbf{Z}[H]/\mathcal{H}^{c+1}$ (considered as an abelian group). Then $b_1, \ldots, b_r$ together with the right ideal generators for $\mathcal{H}^{c+1}$ generate $\mathcal{I}$ as a right ideal.

3.3. Testing for nilpotency

In Section 3.1 we saw that a group H can be embedded in $\mathrm{Tr}_1(n, \mathbf{Z})$ for some n if and only if H is finitely generated torsion-free nilpotent. Suppose we are given a consistent polycyclic presentation for a group H. In this section we describe an algorithm for deciding whether or not H is torsion-free nilpotent.

Before describing the algorithm, we prove the following lemma. This lemma seems to be common knowledge, but we have been unable to find a reference for it.

Lemma 3.5. *Let H be a finitely generated group such that $|\gamma_i(H) : \gamma_{i+1}(H)| < \infty$ for some i. Then $|\gamma_j(H) : \gamma_{j+1}(H)| < \infty$ for all $j \geq i$.*

Proof. Let r be the exponent of $\gamma_i(H)/\gamma_{i+1}(H)$. Let $g_1, \ldots, g_m$ be elements of $\gamma_i(H)$ whose images generate $\gamma_i(H)/\gamma_{i+1}(H)$. Suppose H is generated by $\{a_1, \ldots, a_k\}$. Then the image of

$$\{[g_i, a_j] \mid 1 \leq i \leq m,\ 1 \leq j \leq k\}$$

generates $\gamma_{i+1}(H)/\gamma_{i+2}(H)$. (See Proposition 9.2.6 of Sims (1994).) Let g be in $\{g_1, \ldots, g_m\}$ and a be in $\{a_1, \ldots, a_k\}$. Using a commutator identity (Proposition 9.1.6 of Sims (1994)), we see that

$$[g^m, a]\gamma_{i+2}(H) = [g^{m-1}, a][g^{m-1}, a, g][g, a]\gamma_{i+2}(H).$$

Since $\gamma_{i+1}(H)/\gamma_{i+2}(H)$ is abelian and $[g^{m-1}, a, g] \in \gamma_{i+2}$,

$$[g^m, a]\gamma_{i+2}(H) = [g^{m-1}, a][g, a]\gamma_{i+2}(H).$$

By induction it follows that

$$[g^r, a]\gamma_{i+2}(H) = [g, a]^r\gamma_{i+2}(H)$$

where r is a positive integer. Since $g^r \in \gamma_{i+1}(H)$, it follows that $[g, a]^r \in \gamma_{i+2}(H)$. Therefore, $\gamma_{i+1}(H)/\gamma_{i+2}(H)$ is a finitely generated abelian group of finite exponent, and hence is finite. □

Lemma 3.5 gives us an algorithm for deciding whether or not H is torsion-free nilpotent. Begin by computing generators for each of the terms in the lower central series for H. If in so doing we find that for some i,

$$1 < |\gamma_i(H) : \gamma_{i+1}(H)| < \infty, \tag{3.1}$$

then we can deduce by Lemma 3.5 that either H is not nilpotent or $\gamma_i(H)$ is a nontrivial finite normal subgroup. If, on the other hand,

$$|\gamma_i(H) : \gamma_{i+1}(H)| = 1, \text{ and } \gamma_i(H) \neq 1, \tag{3.2}$$

then H is not nilpotent. If, for all i, neither 3.1 nor 3.2 occurs, then each time we move down the lower central series, the Hirsch number of $\gamma_i(H)$ decreases and in a finite number of steps we find that for some c, $\gamma_{c+1}(H) = 1$, i.e., that H is class c nilpotent. Having found the last term in the lower central series for H, we can now compute the torsion subgroup of H (using the algorithm described in Section 1.2), and thereby decide whether or not H is torsion-free.

3.4. Existence of an embedding into a solvable matrix group

In Chapter 5 of Segal (1983), Segal proves the existence of an embedding of an abstract polycyclic group G into $\mathrm{GL}(n, \mathbf{Z})$ for some n. In Section 3.6 we describe an algorithm for constructing a similar embedding in the case when G' is torsion-free nilpotent. In this section, we summarize the results from Segal (1983) to which we will need to refer when describing our construction.

For the key step in the proof, Segal makes the following inductive assumption. Throughout this paper we will refer to this assumption as Hypothesis (†).

Hypothesis (†) :

> *H and K are normal subgroups of a polycyclic group L,*
> *$H \leq K$ and L/H is abelian, and*
> *there is an embedding μ of K into $GL(m, \mathbf{Z})$ such that $\mu(H) \subseteq Tr_1(m, \mathbf{Z})$.*

Segal shows that there is an integer n and an embedding ν of L into $\mathrm{GL}(n, \mathbf{Z})$ such that $\nu(H) \leq Tr_1(n, \mathbf{Z})$. We begin by considering the most difficult and interesting case – the case in which L/K is infinite cyclic and generated by aK.

Let L act on $\mathbf{Z}[K]$ as in Proposition 3.1. Since $\mathbf{Z}[K]$ isn't finitely generated as an abelian group, our first goal is to find an ideal $\mathcal{I}$ of $\mathbf{Z}[K]$ such that

1 $\mathcal{I}$ is invariant under the action of a, giving us an action of L on $\mathbf{Z}[K]/\mathcal{I}$, and
2 $\mathbf{Z}[K]/\mathcal{I}$ is a finitely generated free abelian group. (Thus we get a matrix representation for L.)

We begin by finding two ideals $\mathcal{J}$ and $\overline{\mathcal{K}}$, each of which satisfies one of these two criteria, and then we show how $\mathcal{I}$ can be constructed from $\mathcal{J}$ and $\overline{\mathcal{K}}$.

Our embedding μ of K into $\mathrm{GL}(m, \mathbf{Z})$ extends to a ring homomorphism of $\mathbf{Z}[K]$ to the ring of integer matrices $M(m, \mathbf{Z})$. Let $\mathcal{J}$ be the kernel of this action. The quotient $\mathbf{Z}[K]/\mathcal{J}$ is a finitely generated free abelian group, but $\mathcal{J}$ might not be invariant under the action of a.

Let $\mathcal{H}$ be the augmentation ideal of $\mathbf{Z}[H]$. We define $\overline{\mathcal{H}}$ to be $\mathcal{H}\mathbf{Z}[K]$. Since $H \triangleleft K$,

$\overline{\mathcal{H}} = \mathbf{Z}[K]\mathcal{H}$. Not only is $\overline{\mathcal{H}}$ invariant under the action of a, but a acts trivially on $\mathbf{Z}[K]/\overline{\mathcal{H}}$. To see this, let k be an element of K, and use the fact that L/H is abelian:

$$k^a - k = k([k,a]-1) \in k(L'-1) \subseteq k(H-1) \subseteq \overline{\mathcal{H}}.$$

Unfortunately, $\mathbf{Z}[K]/\overline{\mathcal{H}}$ might not be finitely generated.

Let $\mathcal{S}$ be the ideal $(\mathcal{J}+\overline{\mathcal{H}})^m$ and let T be the torsion subgroup of $\mathbf{Z}[K]/\mathcal{S}$, considered as an abelian group. Let $\mathcal{I}$ be the pullback of T under the map $\mathbf{Z}[K] \to \mathbf{Z}[K]/\mathcal{S}$. Clearly, $\mathcal{I}$ is an ideal of $\mathbf{Z}[K]$. Segal proves that $\mathcal{I}$ satisfies the two criteria above. The following lemma follows directly from Segal's proof of Theorem 4 in Section 5.C. For completeness we include a proof similar to his proof.

LEMMA 3.6. *Suppose that H, K and L satisfy Hypothesis (†) and that L/K is infinite cyclic and generated by aK. Let $\mathcal{I}$ be the ideal of $\mathbf{Z}[K]$ defined above. Then $\mathcal{I}$ is invariant under the action of a and $\mathbf{Z}[K]/\mathcal{I}$ is a finitely generated free abelian group. If τ is the homomorphism*

$$\tau : L \to Aut_{\mathbf{Z}}(\mathbf{Z}[K]/\mathcal{I})$$

*induced from the homomorphism * in Proposition 3.1, then the kernel of τ is the centralizer $C_{\langle a\rangle}(K)$. There is a basis for $\mathbf{Z}[K]/\mathcal{I}$ with respect to which $\tau(H)$ is unitriangular.*

PROOF. Since a acts trivially on $\mathbf{Z}[K]/\overline{\mathcal{H}}$, the ideal $\mathcal{J}+\overline{\mathcal{H}}$ is invariant under a. Therefore $\mathcal{I}$ is also invariant.

Since $\mathbf{Z}[K]/\mathcal{J}$ is finitely generated as an abelian group, so is $\mathbf{Z}[K]/(\mathcal{J}+\overline{\mathcal{H}})$. By Lemma 9 in Section 5.C of Segal (1983), $\mathbf{Z}[K]/\mathcal{S}$ is also finitely generated as an abelian group. Therefore $\mathbf{Z}[K]/\mathcal{I}$ is finitely generated free abelian.

Before finding the kernel of τ, we show that $(1+\mathcal{I}) \cap K = 1$. Since μ is injective, $(1+\mathcal{J}) \cap K = 1$. Therefore, it suffices to show that $\mathcal{I} \subseteq \mathcal{J}$. Since H is embedded in $\mathrm{Tr}_1(m,\mathbf{Z})$, $\mathcal{H}^m \subseteq \mathcal{J}$. Since $\mathcal{J}$ is an ideal of $\mathbf{Z}[K]$, it follows that $(\overline{\mathcal{H}})^m \subseteq \mathcal{J}$. Therefore,

$$\mathcal{S} = (\mathcal{J}+\overline{\mathcal{H}})^m \subseteq (\overline{\mathcal{H}})^m + \mathcal{J} \subseteq \mathcal{J}.$$

The quotient $\mathbf{Z}[K]/\mathcal{J}$ is torsion-free. Therefore $\mathcal{I} \subseteq \mathcal{J}$ and $(1+\mathcal{I}) \cap K = 1$.

We are now ready to find the kernel of τ. Clearly, $C_{\langle a\rangle}(K)$ is contained in the kernel of τ. Suppose that $k \in K$ and r is a nonnegative integer such that ka^r is in the kernel of τ. Then $1+\mathcal{I}$ is fixed by $\tau(ka^r)$, and therefore $k^{a^r} \in (1+\mathcal{I}) \cap K = 1$. Thus, $k=1$. Now for all j in K, $j+\mathcal{I}$ is fixed by a^r. Therefore, $j^{a^r} - j \in \mathcal{I}$. But

$$j^{a^r} - j = j([j,a^r]-1).$$

Hence $[j,a^r]-1 \in \mathcal{I}$ and $[j,a^r] \in (\mathcal{I}+1) \cap K = 1$. Therefore, a^r centralizes K and the kernel of τ is precisely $C_{\langle a\rangle}(K)$.

Let $M = \mathbf{Z}[K]/\mathcal{I}$, considered as a $\mathbf{Z}[H]$-module. Then $M\mathcal{H}^m = 0$, since

$$\mathbf{Z}[K]\mathcal{H}^m \subseteq \overline{\mathcal{H}}^m \subseteq \mathcal{S} \subseteq \mathcal{I}.$$

Let M_i be the subgroup of M generated by $\{xy+\mathcal{I} : x \in \mathbf{Z}[K], y \in \mathcal{H}^i\}$. Then H stabilizes the following chain:

$$M \geq M_1 \geq M_2 \geq \cdots \geq M_m = 0.$$

Therefore, H acts nilpotently on M, and hence (Section 1.1) there is a basis for M with respect to which $\tau(H)$ is unitriangular. □

With this key lemma in hand, it is now relatively easy to prove the existence of a matrix representation for a polycyclic-by-finite group. The following lemma is an exercise in Segal (1983) (p. 92).

LEMMA 3.7. *Let G be a polycyclic-by-finite group. There exists a normal torsion-free subgroup G_1 with finite index in G such that $G_1/Fitt(G_1)$ is free abelian.*

Let $G_1 \lhd G$ as above. Lemma 8 of Section 5.C of Segal (1983) shows that in order to find an embedding of G, it suffices to find an embedding for G_1. Since we will use Segal's Lemma 8 in a somewhat different context, we give a more complete statement and proof of it here. The proof given here is basically that sketched in Segal (1983).

LEMMA 3.8. *Let H be a subgroup of finite index d in a group G. Suppose that there exists an embedding μ of H into $GL(n, \mathbf{Z})$. Then there exists an embedding ν of G into $GL(nd, \mathbf{Z})$. If, furthermore, $K \leq H$, $K \lhd G$ and $\mu(K) \leq Tr_1(n, \mathbf{Z})$, then we can choose ν such that $\nu(K) \leq Tr_1(nd, \mathbf{Z})$.*

PROOF. Let $M = \mathbf{Z}^n$, considered as a right $\mathbf{Z}[H]$-module via μ. Let $V = M \otimes \mathbf{Z}[G]$ where $\otimes$ denotes $\otimes_{\mathbf{Z}[H]}$ and $\mathbf{Z}[G]$ is viewed as a left $\mathbf{Z}[H]$-module. Let $\{x_1, \ldots, x_d\}$ be a set of coset representatives for the right cosets of H in G. Then

$$V = M \otimes \mathbf{Z}[H]x_1 \ \oplus \ \cdots \ \oplus \ M \otimes \mathbf{Z}[H]x_d.$$

Let $b_1, \ldots, b_n$ be a basis for M over $\mathbf{Z}$. Then

$$\mathcal{B} = b_1 \otimes x_1, \ldots, b_n \otimes x_1, b_1 \otimes x_2, \ldots, b_n \otimes x_2, \ldots, b_1 \otimes x_d, \ldots, b_n \otimes x_d$$

is a basis for V over $\mathbf{Z}$. Fix g in G. Let Σ_d be the symmetric group on d letters. Let $h_1, \ldots, h_d$ in H and σ_d in Σ_d be given by $x_i g = h_i x_{\sigma(i)}$. Then define

$$\begin{aligned} \nu : G &\rightarrow \mathrm{Aut}_{\mathbf{Z}}(V) \\ g &\mapsto \nu(g) \end{aligned}$$

as follows:

$$(b_k \otimes x_i)\nu(g) = b_k \mu(h_i) \otimes x_{\sigma(i)}$$

for $1 \leq k \leq n$ and $1 \leq i \leq d$. It is easy to check that ν is an embedding. Suppose $K \lhd G$. For all h in K, there exist $h_1, \ldots, h_d$ such that $x_i h = h_i x_i$, in which case the matrix for $\nu(h)$ with respect to the basis $\mathcal{B}$ is

$$\begin{pmatrix} \mu(h_1) & 0 & \cdot & \cdot & 0 & 0 \\ 0 & \mu(h_2) & 0 & \cdot & \cdot & 0 \\ \cdot & 0 & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \cdot & \cdot & \cdot & \cdot & 0 \\ 0 & 0 & \cdot & \cdot & 0 & \mu(h_d) \end{pmatrix}.$$

Therefore, if $\mu(K) \leq \mathrm{Tr}_1(n, \mathbf{Z})$, then $\nu(K) \leq \mathrm{Tr}_1(nd, \mathbf{Z})$. □

Since $\mathrm{Fitt}(G_1)$ is finitely generated torsion-free nilpotent, it can be embedded in $\mathrm{Tr}_1(m, \mathbf{Z})$ for some m as in Theorem 3.2. Suppose that

$$G_1 \rhd K \rhd \mathrm{Fitt}(G_1)$$

where G_1/K is infinite cyclic and generated by xK. It is not hard to show that $\mathrm{Fitt}(K) = \mathrm{Fitt}(G_1)$. By induction on the Hirsch length of G, there exists a positive integer k and an embedding of K into $\mathrm{GL}(k, \mathbf{Z})$ mapping $\mathrm{Fitt}(G_1)$ into $\mathrm{Tr}_1(k, \mathbf{Z})$. It can be shown that $C_{\langle x \rangle}(K) = 1$. By Lemma 3.6, there exists a positive integer n and an embedding $\tau : G_1 \to \mathrm{GL}(n, \mathbf{Z})$ such that $\tau(\mathrm{Fitt}(G_1)) \leq \mathrm{Tr}_1(n, \mathbf{Z})$. By Lemma 3.8 it follows that there exists an embedding ν of G into $\mathrm{GL}(nd, \mathbf{Z})$ such that $\nu(\mathrm{Fitt}(G_1)) \leq \mathrm{Tr}_1(nd, \mathbf{Z})$, where $|G : G_1| = d$.

3.5. Constructing an embedding for a cyclic extension

In the previous section, we saw that a key step in Segal's proof of the existence of an embedding involved subgroups H, K and L satisfying Hypothesis (†); an embedding for K implied the existence of an embedding for L. In this section, we describe an algorithm for constructing the embedding for L.

We begin with the easy case– that in which L/K is finite. Let d be the order of L/K. By Lemma 3.8 there exists an embedding ν of L into $\mathrm{GL}(md, \mathbf{Z})$ such that $\nu(H) \subseteq \mathrm{Tr}_1(md, \mathbf{Z})$. By examining the proof of Lemma 3.8, we see that for a given l in L, we find a matrix representing $\nu(l)$ as follows. Find σ in Σ_d and $h_1, \ldots, h_d$ in H such that $x_i l = h_i x_{\sigma(i)}$, where $\{x_1, \ldots, x_d\}$ is a set of coset representatives for L/K. Let $\mathcal{B}$ be the basis for $\mathbf{Z}^{nd}$ defined in the proof of Lemma 3.8. Then the matrix for $\nu(l)$ with respect to $\mathcal{B}$ is ap, where a in $\mathrm{GL}(nd, \mathbf{Z})$ is given by

$$a = \begin{pmatrix} \mu(h_1) & 0 & \cdot & \cdot & 0 & 0 \\ 0 & \mu(h_2) & 0 & \cdot & \cdot & 0 \\ \cdot & 0 & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \cdot & \cdot & \cdot & \cdot & 0 \\ 0 & 0 & \cdot & \cdot & 0 & \mu(h_d) \end{pmatrix}$$

and p is obtained by taking the tensor product of the $n \times n$ identity matrix and the $d \times d$ permutation matrix associated with σ.

For the rest of this section, we consider the more difficult case– that in which L/K is infinite. Suppose that aK is a generator for L/K.

Lemma 3.9. *There exists a positive integer n and an embedding $\nu : L \to GL(n, \mathbf{Z})$ such that $\nu(H) \leq Tr_1(n, \mathbf{Z})$.*

Proof. If $C_{\langle a \rangle}(K)$ is trivial, then the homomorphism τ of Lemma 3.6 is an embedding. If instead $C_{\langle a \rangle}(K) = \langle a^r \rangle$ for some positive integer r, then refine the series $L \triangleright K$ as follows:

$$L \triangleright K\langle a^r \rangle \triangleright K.$$

Then $K\langle a^r \rangle$ is the direct product of $\langle a^r \rangle$ and K, and the map λ from $K\langle a^r \rangle$ to $\mathrm{GL}(m + 2, \mathbf{Z})$ given by

$$\lambda : a^{ri}k \hookrightarrow \begin{pmatrix} \mu(k) & 0 \\ 0 & \begin{pmatrix} 1 & i \\ 0 & 1 \end{pmatrix} \end{pmatrix}$$

is an embedding such that $\lambda(H)$ is unitriangular. By Lemma 3.8, there exists an embedding ν from L to $\mathrm{GL}(n, \mathbf{Z})$ such that $\nu(H)$ is unitriangular. □

We now discuss the way in which Lemma 3.9 gives us an algorithm to construct an embedding of L into $\mathrm{GL}(n, \mathbf{Z})$. We begin by constructing the embedding τ of Lemma 3.6. Let us assume that we are given a consistent polycyclic presentation for K and an element a of L such that aK generates L/K. Assume that the embedding μ of K into $\mathrm{GL}(m, \mathbf{Z})$ is also given (by matrices representing $\mu(k)$ for each generator for K). If we can find a finite set of right ideal generators for $\mathcal{I}$, then we can use the Gröbner basis algorithm described in Section 1.3 to find $\tau(l)$ for each generator l of L.

We first show that we can find a finite set of right ideal generators for $\mathcal{J}$. Our embedding $\mu : K \to \mathrm{GL}(n, \mathbf{Z})$ can be extended to a ring homomorphism (which we also denote by μ) from $\mathbf{Z}[K]$ to the ring of $n \times n$ matrices over $\mathbf{Z}$. Suppose K is generated by $g_1, \ldots, g_s$. Since $\{\mu(g_1), \ldots, \mu(g_s)\}$ generates $\mu(\mathbf{Z}[K])$ as a ring and since $\mu(\mathbf{Z}[K])$ is a free abelian group of rank less than or equal to m^2, we can find elements $x_1, \ldots, x_r$ of $\mathbf{Z}[K]$ whose images form a $\mathbf{Z}$-basis for $\mathbf{Z}[K]/\mathcal{J}$. Fix i such that $1 \leq i \leq s$. For $1 \leq j \leq s$, let $\alpha(i,j)$ and $\beta(i,j)$ be the integers such that $g_i - \sum_j \alpha(i,j)x_j \in \mathcal{J}$ and $g_i^{-1} - \sum_j \beta(i,j)x_j \in \mathcal{J}$. Next fix i, j such that $1 \leq i, j \leq s$. For $1 \leq k \leq s$, let $\gamma(i,j,k)$ be the integer such that $x_i x_j - \sum_k \gamma(i,j,k)x_k \in \mathcal{J}$. Now let

$$R = \{g_i - \sum_j \alpha(i,j)x_j,\ g_i^{-1} - \sum_j \beta(i,j)x_j,\ x_i x_j - \sum_k \gamma(i,j,k)x_k : 1 \leq i,j,k \leq s\}.$$

It is easy to see that R generates $\mathcal{J}$ as a right ideal.

Since $\overline{\mathcal{H}} = \mathcal{H}\,\mathbf{Z}[K]$ and (as we saw in Section 1.3) we can find generators for $\mathcal{H}$ as a right ideal of $\mathbf{Z}[H]$, it follows that we can find generators for $\overline{\mathcal{H}}$ as a right ideal of $\mathbf{Z}[K]$. Therefore, we can find a finite set Q of right ideal generators for $\mathcal{S} = (\mathcal{J} + \overline{\mathcal{H}})^m$. Use the methods of Section 1.3 to find a finite set P of elements of $\mathbf{Z}[K]$ whose images generate the torsion subgroup of $\mathbf{Z}[K]/\mathcal{S}$. Then $Q \cup P$ generates $\mathcal{I}$ as a right ideal of $\mathbf{Z}[K]$.

Now we may assume that we have constructed the homomorphism τ of Lemma 3.6. In Ostheimer (1996b), a practical algorithm is given for finding a presentation for an abelian matrix group; in this context, that algorithm finds a nonnegative integer r such that $\langle r \rangle$ is the kernel of the homomorphism from $\mathbf{Z}$ to $\langle \tau(a) \rangle$ taking i to $\tau(a)^i$. If $r = 0$ then $\tau(a)$ has infinite order. In this case, $C_{\langle a \rangle}(K)$ is trivial and τ is an embedding satisfying all the desired properties.

If r is positive, then the order of $\tau(a)$ is r, and our construction is much simpler. Refine the series $L \rhd K$ as in the proof of Lemma 3.9:

$$L \rhd K\langle a^r \rangle \rhd K.$$

It is easy to construct the embedding λ from $K\langle a \rangle$ to $\mathrm{GL}(m+2, \mathbf{Z})$ (defined in the proof of Lemma 3.9), and as we saw above, we can then construct an embedding ν from L to $\mathrm{GL}(n, \mathbf{Z})$ as needed.

We see that the size n of the embedding ν might depend on our choice of a coset representative for L/K. For example, suppose that the action of a is inner; i.e., there exists a $k \in K$ such that for all $x \in K$, $x^a = x^k$. Then ak^{-1} centralizes K. Therefore, with this choice of coset representative for L/K, we obtain a different (and probably considerably smaller) representation of L.

3.6. Constructing an embedding into a triangularizable matrix group

In the Section 3.4 we sketched a proof of the existence of an embedding of a polycyclic group G into a (solvable) subgroup of $\mathrm{GL}(n, \mathbf{Z})$ for some n. In this section we describe an algorithm for constructing a somewhat different embedding in the special case when G can be embedded in a triangularizable subgroup of $\mathrm{GL}(n, \mathbf{Z})$ for some n. In order to develop a practical algorithm for constructing the embedding of Section 3.4, we would need a practical algorithm for finding the Fitting subgroup of a polycyclic group given by a finite presentation. While algorithms for this problem are known to exist, a practical algorithm has yet to be found. (See Section 4.) The algorithm we describe here does not require computing the Fitting subgroup.

The following proposition follows easily from well-known results.

Proposition 3.10. *If G is a triangularizable subgroup of $GL(n, \mathbf{Z})$, then G is polycyclic and G' is torsion-free nilpotent.*

Proof. As noted in Section 1.1, since G' is unipotent there is a basis for $\mathbf{Z}^n$ with respect to which G' is contained in $\mathrm{Tr}_1(n, \mathbf{Z})$. Therefore G' is finitely generated torsion-free nilpotent. Since G' is solvable, it follows that G is solvable, and Mal'cev showed that all solvable subgroups of $\mathrm{GL}(n, \mathbf{Z})$ are polycyclic. (For a proof of this see Section 2.B in Segal (1983).) □

The converse of Proposition 3.10 also holds:

Proposition 3.11. *If G is a polycyclic group and G' is torsion-free nilpotent, then there exists a positive integer n and an embedding $\psi : G \hookrightarrow GL(n, \mathbf{Z})$ mapping G into a triangularizable group.*

Proof. There exist subgroups $H_0, H_1, \ldots, H_r$ of G such that

$$G = H_0 \triangleright H_1 \triangleright H_2 \triangleright \cdots \triangleright H_r = G',$$

where H_0/H_1 is finite and H_i/H_{i+1} is infinite cyclic for all i. By Theorem 3.2 there exists a positive integer m and an embedding $\mu : G' \to \mathrm{Tr}_1(m, \mathbf{Z})$. By repeated applications of Lemma 3.9, there exists a positive integer n' and an embedding $\nu' : H_1 \to \mathrm{GL}(n', \mathbf{Z})$ such that $\nu'(G') \leq \mathrm{Tr}_1(n', \mathbf{Z})$. By Lemma 3.8 it now follows that there exists a positive integer n and an embedding $\nu : G \to \mathrm{GL}(n, \mathbf{Z})$ such that $\nu(G') \leq \mathrm{Tr}_1(n, \mathbf{Z})$. □

Notice that as a consequence of Propositions 3.10 and 3.11, we can decide whether or not G (given by a consistent polycyclic presentation) can be embedded in a triangularizable subgroup of $\mathrm{GL}(n, \mathbf{Z})$ for some n: begin by finding generators for G' (Section 1.2) and then use the methods in Section 3.3 to decide whether or not G' is torsion-free nilpotent. For the rest of this section, assume that G' is torsion-free nilpotent.

We are now in a position to describe an algorithm for embedding G. Use the methods of Section 9.6 of Sims (1994) to find generators for G'. As we showed in Section 3.2, we can construct an embedding from G' into $\mathrm{Tr}_1(m, \mathbf{Z})$. The methods of Section 9.6 of Sims (1994) can also be used to find a consistent polycyclic presentation for G/G'. Find generators for subgroups $H_0, \ldots, H_r$ such that

$$G = H_0 \triangleright H_1 \triangleright \ldots \triangleright H_r = G',$$

H_0/H_1 is finite and H_i/H_{i+1} is infinite cyclic for all $1 \leq i < r$. For i such that $0 \leq i < r$, use the methods of Section 3.5 to construct a representation for H_i from our representation for H_{i+1}.

Procedure Embedding(G)
Input: G : A polycyclic group G given by a consistent polycyclic presentation;
Output: A faithful representation of G.
Begin
  Find a finite-index (torsion-free nilpotent)-by-abelian subgroup H of G as follows:
    Use the finite index program to enumerate the finite index subgroups H of G;
    Find H' and use the test in Section 3.3 to determine whether H' is
      torsion-free nilpotent;
    Stop when such a subgroup H is found;
  Find a consistent polycyclic presentation of H;
  Construct an embedding from H' into $\mathrm{Tr}_1(m, \mathbf{Z})$ as in Section 3.2;
  Find generators for subgroups $H_0, H_1, \ldots, H_r$ such that
    $H = H_0 \rhd H_1 \rhd \ldots \rhd H_r = H'$,
    H_0/H_1 is finite and H_i/H_{i+1} is infinite cyclic for $1 \le i < r$;
  For $1 \le i < r$, inductively construct a representation for H_i from H_{i+1} using
    the methods in Lemma 3.9;
  Construct a representation of H_0 from H_1 using the methods of Lemma 3.8;
  Construct a representation of G from H using the methods of Lemma 3.8;
End.

Figure 1. Procedure to Construct Embedding

3.7. Constructing an embedding into a solvable matrix group

It is a well-known fact (Segal, 1983) that polycyclic groups are (torsion-free nilpotent)-by-abelian-by-finite. In the previous section we saw how a group whose commutator subgroup is torsion-free nilpotent can be embedded into a triangularizable matrix group. Here we will solve the embedding problem for general polycyclic groups.

Let G be a polycyclic group. The method suggested here is to enumerate finite index subgroups of G until a (torsion-free nilpotent)-by-abelian subgroup H is found. Using the method described in 3.3 it can be determined whether H is (torsion-free nilpotent)-by-abelian. Usually enumerating finite index subgroups can be time-consuming. However, enumerating finite index subgroups of a polycyclic group given by a consistent polycyclic presentation seems to be a much easier problem. Coset tables for the subgroups of polycyclic groups can be found using a wreath-product ordering on the rows and from the coset tables, generators for the subgroups can be found. For details refer to Lo (1997) and Sims (1994). The algorithm for constructing a representation of polycyclic groups is shown in Figure 1.

The size n of the resulting embedding depends on many factors, including the following parameters: let p be the number of generators for H'; let c be the nilpotency class of H', let d be the index of H_1 in G, and let r be the rank of H_1/G'. By examining the proofs of the results leading up to Proposition 3.11, it is not difficult to prove the existence of a primitive recursive function $B(p, c, d, r)$ such that $n < B(p, c, d, r)$. However, easily obtained bounds for $B(p, c, d, r)$ appear to grow very rapidly as a function of these parameters, and preliminary experiments suggest that such bounds vastly overestimate the actual size of the embedding obtained. (See Section 5 for details about these experiments.) Further experimentation is needed to understand how the size of the embedding obtained for G depends on the group structure of G.

4. Comparisons with earlier algorithms

In Grunewald and Segal (1980), the authors describe an algorithm for finding an embedding of a finitely-generated torsion-free nilpotent group H into $\mathrm{Tr}_1(n, \mathbf{Z})$. Their embedding is the same as that described in Section 3.4. Recall that we found an ideal $\mathcal{I}(H)$ of $\mathbf{Z}[H]$ such that $\mathbf{Z}[H]/\mathcal{I}(H)$ is finitely generated free abelian and such that there is a faithful action of H on $\mathbf{Z}[H]/\mathcal{I}(H)$. We then used the Gröbner basis algorithms described in Section 1.3 to find a basis for $\mathbf{Z}[H]/\mathcal{I}(H)$ and thereby find a matrix representation for H. In Grunewald and Segal (1980) the authors describe another method for finding a basis for $\mathbf{Z}[H]/\mathcal{I}(H)$. It is not clear which algorithm will be faster in practice.

Let G be a polycyclic group given by a consistent polycyclic presentation. In Section 3.3 an algorithm for deciding whether or not G is torsion-free nilpotent is described. A proof of decidability can also be found in Baumslag *et al.* (1991) where the authors describe an algorithm for deciding whether or not G is nilpotent as well as an algorithm for finding the maximal normal finite subgroup of T of G. As discussed in Section 3.3, their algorithm for finding T appears to be practical for nilpotent G. Their algorithm to decide nilpotence depends on the following theorem. (See Section 1.C in Segal (1983).)

THEOREM 4.1. *Let G be a polycyclic-by-finite group such that G is not nilpotent. Then there exists a finite quotient of G which is not nilpotent.*

Nilpotence can therefore be decided by a method which the authors of Baumslag *et al.* (1991) call the *local-global method*. Imagine two processes running simultaneously. The first process attempts to prove that G is nilpotent by computing the terms of the lower central series, stopping if it is discovered that $\gamma_k(G) = 1$. The second attempts to prove that G is not nilpotent by enumerating all the finite quotients $\overline{G}$ of G and stopping if it is discovered that $\overline{G}$ is not nilpotent. Eventually, one of these two processes stops, at which point we know whether or not G is nilpotent. This algorithm is unlikely to be practical even for very simple examples.

In Segal (1990), Segal describes an algorithm for finding an embedding of a polycyclic group G (given by a finite presentation) into $\mathrm{GL}(n, \mathbf{Z})$. The main result in (Segal, 1990) is an algorithm to decide whether or not two polycyclic groups are isomorphic. That goal places extra requirements on the embedding for G, and hence the construction of the embedding in Segal (1990) is considerably more complicated than that described in Section 3.4 of this paper.

In Segal (1990), no attempt was made to find a practical algorithm to construct the embedding. For example, at one point in the construction, Segal relies on an algorithm to solve the following problem, known as the *generalized conjugacy problem*.

> Let G be a polycyclic-by-finite group given by a finite presentation. Let A and B be subgroups of G (given by finite generating sets). Decide whether or not A and B are conjugate in G.

The following theorem (Section 4.D in Segal (1983)) shows that the local-global method can be used to decide whether or not A and B are conjugate.

THEOREM 4.2. *Let G be a polycyclic-by-finite group and let A and B be two subgroups of G. If A and B have conjugate images in every finite quotient of G, then A and B are conjugate in G.*

In this case one process enumerates all the elements g of G, stopping if it finds that $A^g = B$, and the other process enumerates all the finite quotients $\overline{G}$ of G, stopping if it finds that $\overline{A}$ is not conjugate to $\overline{B}$. As with the algorithm to decide nilpotence, this algorithm is unlikely to be practical even for very simple examples. Moreover, the problem of finding a practical algorithm to solve the generalized conjugacy problem is generally believed to be quite difficult. Nonetheless, there may be a practical algorithm for finding the embedding described in Segal (1990).

As we remarked in Section 3.6, we did not follow the construction in Section 3.4 exactly, because to do so we would need to find the Fitting subgroup of a polycyclic group G given by a consistent polycyclic presentation. An algorithm for finding the Fitting subgroup of a polycyclic-by-finite group given by a finite presentation is described in Baumslag *et al.* (1991). Once again, the authors of Baumslag *et al.* (1991) were not trying to find a practical algorithm. For example, at one point in the algorithm they find a certain finite section F/T of the group, where $F \triangleleft G$ and $T \triangleleft F$. They then enumerate each of the subgroups of this section, computing for each its preimage L under the map $F \to F/T$ and then testing whether or not L is nilpotent and $L \triangleleft G$. The practicality of such a step is suspect.

In addition to comparing the efficiency of various algorithms for finding a matrix representation for a polycyclic group, we should also compare the sizes of the matrices produced by such algorithms. The embedding described in Segal (1990) is canonical in the following sense. Segal defines, for a given polycyclic-by-finite group G, a positive integer n_G and an embedding β_G of G into $\mathrm{GL}(n_G, \mathbf{Z})$. Let G and H be isomorphic polycyclic groups, where $\theta : G \to H$ is an isomorphism. Then $n_G = n_H = n$, say, and there exists an inner automorphism γ of $\mathrm{GL}(n, \mathbf{Z})$ such that

$$\gamma(\beta_G(G)) = \beta_H(\theta(G)).$$

On the other hand, the sizes of the matrices produced by the algorithm described in Section 3.6 appear to vary depending on things like the given generating set for the group.

5. Experiments

In this section we describe a series of experiments in which matrix representations were constructed from consistent polycyclic presentations using the algorithm listed in Section 3.7. Note that this algorithm has not been fully implemented. Instead, we stepped through the algorithm by hand using as tools a Maple implementation of the algorithms for working with the enveloping algebra of a matrix group and the Gröbner basis method for integral group rings of polycyclic groups as implemented in Lo (1996a). (See Section 1.3.) Along the way, methods to simplify the construction were used to reduce the amount of the computation and the size of the representation. In general, the algorithm seems to work well as stated. However, it seems that a good approach is to first find a normal free abelian subgroup of large rank, then change the polycyclic presentation accordingly and use Prop. 3.4 to obtain an embedding if possible. However, at this point, we don't have an algorithm for finding such a subgroup and ad hoc methods are used to find such subgroups in these experiments. We expected most of the time would be used in computing Gröbner bases. However, in all cases, the matrices obtained had small entries (at most two digits), and at no time did we experience unreasonable delays while the Gröbner basis calculations were performed.

In the first series of experiments, we constructed embeddings from presentations for the groups $\mathrm{Tr}_1(n, \mathbf{Z})$. For $n = 2, 3, 4, 5$, we followed Example 4.1 in Chapter 9 of Sims (1994) to obtain a consistent polycyclic presentation for $\mathrm{Tr}_1(n, \mathbf{Z})$. For example, when $n = 5$, we define g_i, $1 \leq i \leq 10$, to be the matrix

$$\begin{pmatrix} 1 & \delta_{1,i} & \delta_{5,i} & \delta_{8,i} & \delta_{10,i} \\ 0 & 1 & \delta_{2,i} & \delta_{6,i} & \delta_{9,i} \\ 0 & 0 & 1 & \delta_{3,i} & \delta_{7,i} \\ 0 & 0 & 0 & 1 & \delta_{4,i} \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

where $\delta_{j,i}$ is the Kronecker delta. The polycyclic series is $G_1 \triangleright G_2 \triangleright G_3 \triangleright \dots G_{10} \triangleright 1$ where $G_i = \langle g_i, g_{i+1}, \dots, g_{10} \rangle$ for $1 \leq i \leq 10$. The techniques in Section 3.2 are used to construct embeddings from these presentations. We indicate in Table 1 the sizes of the embeddings obtained which seem to grow like $n!$. With a different presentation, we can use Proposition 3.4 directly to construct a representation for $\mathrm{Tr}_1(n, \mathbf{Z})$. Let $1 \leq n_1, n_2 < n$ and $n_1 + n_2 = n$. Every element in $\mathrm{Tr}_1(n, \mathbf{Z})$ is of the form

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$$

where a is in $\mathrm{Tr}_1(n_1, \mathbf{Z})$ and c is in $\mathrm{Tr}_1(n_2, \mathbf{Z})$. Let H be the set of all matrices in $\mathrm{Tr}_1(n, \mathbf{Z})$ where a and c are identity matrices. Then H is free abelian of rank $n_1 n_2$. Let X be the set of all matrices in $\mathrm{Tr}_1(n, \mathbf{Z})$ with $b = 0$. Notice that $\mathrm{Tr}_1(n, \mathbf{Z}) = H \circ X$. In the next paragraph, we prove that the conjugation action of X on H is faithful. Thus by Proposition 3.4, a representation of degree $n_1 n_2 + 1$ can be obtained. In the case when $n_1 = 1$ and $n_2 = n - 1$, the representation is of degree n and the representation map ψ in Proposition 3.4 maps every matrix in $\mathrm{Tr}_1(n, \mathbf{Z})$ to itself.

To see that the conjugation action of X on H is faithful, we suppose $x \in X$ fixes H. Let $u \in \mathrm{Tr}_1(n_1, \mathbf{Z})$ and $v \in \mathrm{Tr}_1(n_2, \mathbf{Z})$ be given by

$$x = \begin{pmatrix} u & 0 \\ 0 & v \end{pmatrix}.$$

Let h denote an element in H,

$$h = \begin{pmatrix} I_{n_1} & c \\ 0 & I_{n_2} \end{pmatrix},$$

where I_{n_1} is the identity in $\mathrm{GL}(n_1, \mathbf{Z})$, I_{n_2} is the identity in $\mathrm{GL}(n_2, \mathbf{Z})$ and c is an $n_1 \times n_2$ matrix. Then $x^{-1}hx = h$. So

$$\begin{pmatrix} I_{n_1} & u^{-1}cv \\ 0 & I_{n_2} \end{pmatrix} = \begin{pmatrix} u^{-1} & 0 \\ 0 & v^{-1} \end{pmatrix} \begin{pmatrix} I_{n_1} & c \\ 0 & I_{n_2} \end{pmatrix} \begin{pmatrix} u & 0 \\ 0 & v \end{pmatrix} = \begin{pmatrix} I_{n_1} & c \\ 0 & I_{n_2} \end{pmatrix}$$

and $uc = cv$. Let $1 \leq i, k \leq n_1$ and $1 \leq j, l \leq n_2$. Let c^{ij} be the $n_1 \times n_2$ matrix whose ij-th entry is 1 and zero everywhere else. Comparing the kl-th entry of uc^{ij} and $c^{ij}v$, we get $u_{ki}\delta_{jl} = \delta_{ki}v_{jl}$. By varying i, j, k, l, we can see that $u = I_{n_1}$ and $v = I_{n_2}$. Hence the conjugacy action of X on H is faithful.

Next we describe four unrelated experiments. Since a consistent polycyclic presentation is usually long and redundant, the group in each case is presented using a subset of the relations in a consistent polycyclic presentation sufficient to define the group. All power

Table 1. Unitriangular Groups

Group	Size of embedding
$\mathrm{Tr}_1(2, \mathbf{Z})$	2
$\mathrm{Tr}_1(3, \mathbf{Z})$	7
$\mathrm{Tr}_1(4, \mathbf{Z})$	35
$\mathrm{Tr}_1(5, \mathbf{Z})$	132

relations are given if they exist. In the first one, take

$$L_1 = \langle a, b, c \mid bc = cb, b^a = b^2c, c^a = bc\rangle.$$

The group L_1 is in fact the semidirect product $\langle b, c\rangle \rtimes \langle a\rangle$, where the action of a on the rank 2 free abelian group $\langle b, c\rangle$ with basis $\{b, c\}$ is given by the matrix

$$\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}.$$

Since this matrix has eigenvalues of modulus not equal to 1, the order of the matrix is infinite and the action of a on $\langle b, c\rangle$ is faithful. By Prop. 3.4, a representation ψ of degree 3 can be obtained, in which

$$\psi(a) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 1 & 1 \end{pmatrix}, \psi(b) = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \text{ and } \psi(c) = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Following directly the algorithm described in Section 3.7, a representation of L_1 can also be obtained. However, the degree of this representation is 6.

In the second experiment, take

$$\begin{aligned} L_2 = \langle a, b, c, d \quad \mid \quad & b^a = c, c^a = b^{-1}c^3d, d^a = d, \\ & c^b = cd^{-1}, d^b = d, d^c = d\rangle \end{aligned}$$

and $K_2 = \langle b, c, d\rangle$. We embedded K_2 into $\mathrm{Tr}_1(3, \mathbf{Z})$ by sending b, c, d to the usual generators for $\mathrm{Tr}_1(3, \mathbf{Z})$. Then the method in Section 3.5 is used to find an embedding of L_2 into a matrix group. The degree of this embedding is 7. It seems that in this example, Proposition 3.4 cannot be applied to obtain a smaller representation.

In the third and fourth experiments, we illustrate the effect of changing the presentation on the size of the representation obtained. Let

$$\begin{aligned} L_3 = \langle a_1, a_2, a_3, a_4, a_5 \quad \mid \quad & a_2a_1 = a_1a_2a_4^{-1}, a_3a_1 = a_1a_3, a_4a_1 = a_1a_4, a_5a_1 = a_1a_5, \\ & a_3a_2 = a_2a_5, a_4a_2 = a_2a_3a_4^{-1}a_5, a_5a_2 = a_2a_4, \\ & a_4a_3 = a_3a_4, a_5a_3 = a_3a_5, a_5a_4 = a_4a_5\rangle. \end{aligned}$$

This group is the metabelian quotient of G_5 from Lo (1998b). Applying the algorithm directly to this presentation, we obtain a representation of degree 35. Notice, however, that $\{a_1, a_3, a_4, a_5\}$ generates a normal free abelian subgroup of rank 4 in L_3. Using Prop.

3.4, a representation ψ of degree 5 can be obtained. In fact, for integers x_1, x_3, x_4, x_5,

$$\psi(a_1^{x_1}a_3^{x_3}a_4^{x_4}a_5^{x_5}) = \begin{pmatrix} 1 & x_1 & x_3 & x_4 & x_5 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \text{ and } \psi(a_2) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & -1 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

Take L_4 to be the polycyclic group

$$\langle a, b, c \mid b^a = bc^{-3}, c^a = c^{-1}, c^b = c^{-1} \rangle.$$

We embedded $K_4 = \langle b, c \rangle$ as follows:

$$b = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \text{ and } c = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

We let $H_4 = \langle c \rangle$. We then used the methods of Section 3.5 to construct a representation for L_4. In this case we found the size of the embedding, but we did not calculate the matrices explicitly. The degree of the embedding obtained is 24. However, by changing the presentation, we were able to find a representation of smaller degree for L_4. Via the Tietze transformation $b = da^{-1}$, L_4 can be presented as

$$\langle a, d, c \mid d^a = c^3 d, c^a = c^{-1}, c^d = c \rangle.$$

Now the subgroup $\langle d, c \rangle$ generates a free abelian group of rank 2 in L_4, and the action of a on this subgroup is given by the matrix

$$\begin{pmatrix} 1 & 3 \\ 0 & -1 \end{pmatrix},$$

with respect to the basis $\{d, c\}$. This matrix has order 2. So the action of a on $\langle d, c \rangle$ is not faithful and Proposition 3.4 does not apply. However, using the method in Section 3.5, a representation of degree 5 can be obtained. Here,

$$\psi(a) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 3 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}, \psi(b) = \begin{pmatrix} 1 & 1 & 3 & 0 & 0 \\ 0 & 1 & 3 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$$\text{and } \psi(c) = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

6. A Note about Free Nilpotent Groups

Let $F(k, c)$ denote the free nilpotent group of rank k and class c. (The free nilpotent group $F(k, c)$ is defined to be $F(k)/\gamma_{c+1}(F(k))$, where $F(k)$ is the free group on k generators.) In this series of experiments, we constructed embeddings for $F(2, 1)$, $F(2, 2)$,

Table 2. Free Nilpotent Groups

Group	Size of embedding
$F(2,1)$	3
$F(2,2)$	7
$F(2,3)$	15
$F(2,4)$	31

$F(2,3)$ and $F(2,4)$. We first used Lo (1996a) to obtain presentations for these groups. We then used the techniques in Section 3.2 to construct embeddings from these presentations. The sizes of the embeddings obtained are listed in Table 2. Note that for each of these groups, the size of the embedding obtained is equal to the bound $1+k+k^2+\cdots+k^c$ calculated in Proposition 3.3.

We finish this section by proving that our algorithm will produce a representation for $F(k,c)$ of size $1+k+k^2+\cdots+k^c$ for all k and c. In Hall (1957), the same representation is constructed by looking at actions of H on the group algebra $\mathbf{Q}[H]$, and the size of the representation is calculated. In Passi (1979), many of Hall's lemmas are proved in the context of the group ring of H over a ring R. Here, we will state the result in $\mathbf{Z}[H]$ and prove it by referring to Hall (1957) and Passi (1979). As in Section 3.1, $\mathcal{H}$ denotes the augmentation ideal of $\mathbf{Z}[H]$.

Proposition 6.1. *Let H be the free nilpotent group of rank k and class c. Then $\mathbf{Z}[H]/\mathcal{H}^{c+1}$ is free as an abelian group and has rank $1+k+k^2+\cdots+k^c$.*

Proof. The quotients in the lower central series for H are all free abelian (Hall (1957), p. 441). Let $x_1,\ldots,x_M$ be a polycyclic generating sequence for H which refines the lower central series for H to a series with infinite cyclic quotients. Let $\mathcal{V}$ be the set of all products

$$v = v_1 v_2 \cdots v_M$$

where $v_i = (1-x_i)^{r_i}$ for some nonnegative r_i, or $v_i = (1-x_i)^{c+1}x_i^{-s_i}$ for some positive s_i. Then $\mathcal{V}$ is a basis for the group ring $\mathbf{Z}[H]$ (Passi (1979), p. 26). Define a weight function on the elements of $\mathcal{V}$ as follows. If each factor of v is of the form $v_i = (1-x_i)^{r_i}$ for some nonnegative r_i, then $\mu(v)$ is defined to be

$$\sum_1^M r_i w_i,$$

where w_i is the positive integer such that

$$x_i \in \gamma_{w_i}(H) - \gamma_{w_{i+1}}(H).$$

If $v_i = (1-x_i)^{c+1}x_i^{-s_i}$ for some positive s_i, then $\mu(v)$ is defined to be $c+1$. For $1 \le j \le c+1$, let $\mathcal{V}_j$ be

$$\{v \in \mathcal{V} \;:\; \mu(v) = j\},$$

and for $j > c+1$, let $\mathcal{V}_j$ be the empty set.

Our first goal is to show that for $j = 1, 2, \ldots, c$, $\mathcal{H}^j/\mathcal{H}^{j+1}$ is free as an abelian group and that the images of the elements in $\mathcal{V}_j$ (under the map from $\mathbf{Z}[H]$ to $\mathbf{Z}[H]/\mathcal{H}^{j+1}$) form a basis for $\mathcal{H}^j/\mathcal{H}^{j+1}$. Let E_j be the $\mathbf{Z}$-span of $\mathcal{V}_j \cup \mathcal{V}_{j+1} \cup \cdots$ for $j \leq c+1, E_j = E_{c+1}$ for $j > c+1$. Then $E_r E_s \subseteq E_{r+s}$ for all r, s (Passi (1979), p. 27). For all $j = 1, 2, \ldots, c+1$, since $E_j \subseteq \mathcal{H}^j$, it can be seen that $\mathcal{H}^j = E_j$ (Passi (1979), p. 33). Since $\mathcal{V}$ is linearly independent over $\mathbf{Z}$, it follows that $\mathcal{V}_j$ is a basis for $\mathcal{H}^j$ mod $\mathcal{H}^{j+1}$ (and hence that $\mathcal{H}^j/\mathcal{H}^{j+1}$ is free).

Finally, we would like to show that $|\mathcal{V}_j| = k^j$ for $j = 1, 2, \ldots, c$. (Since $\mathbf{Z}[H]/\mathcal{H}$ is free of rank 1, our proposition will then follow.) Note that

$$\sum_{j=0}^{\infty} |\mathcal{V}_j| t^j = \prod_{j=1}^{\infty} \frac{1}{(1-t^j)^{m_j}},$$

where for $i = 1, 2, \ldots, c$, m_i is the rank of $\gamma_i(H)/\gamma_{i+1}(H)$ as a free abelian group (Hall (1957) p. 452). Note also that

$$\frac{1}{1-kt} = \prod_{j=1}^{\infty} \frac{1}{(1-t^j)^{m_j}},$$

by Hall (1957) p. 441. The proposition now follows. □

7. Implementation Notes

It has been mentioned that the algorithm described in Section 3.7 has not been fully implemented yet. In this section, we discuss what would be involved to make a full implementation possible.

The algorithm relies on the ability to do fundamental computations in the group ring of a polycyclic group, as outlined in Section 1.3. In the experiments we performed, the tool we used is the program Lo (1996a). Originally used to compute polycyclic quotients of finitely presented groups, Lo (1996a) also allows users to perform the group ring calculations needed here. Readers are referred to the examples in Lo (1996a) on how this can be done.

For a full implementation, it is also necessary to be able to compute in the enveloping algebra of a matrix group. This can be done easily when simple matrix multiplications and integer row Hermite normal form calculations are provided.

If the polycyclic group whose representation needs to be found is not (torsion-free nilpotent)-by-abelian, then it is necessary to find a finite index (torsion-free nilpotent)-by-abelian subgroup first. A program to enumerate finite index subgroups of a polycyclic group has been developed. See Lo (1997) for details. We also need to be able to determine whether a subgroup of a polycyclic group is torsion-free nilpotent. An algorithm has been sketched in Section 3.3. An implementation of this algorithm would require procedures to work with subgroups of polycyclic groups as described in Section 1.2.

8. Acknowledgments

Here, we would like express our sincere thanks to Professor Charles Sims, who served as Ph.D. thesis advisor for both of us, for all the helpful discussion and encouragement over the years. We would also like to thank the reviewers for their thoughtful comments.

References

Baumslag, G., Cannonito, F. B., Robinson, D. J. S., Segal, D. (1991). The algorithmic theory of polycyclic-by-finite groups. *J. Algebra*, **142**:118–149.

Grunewald, F., Segal, D. (1980). Some general algorithms II: Nilpotent groups. *Ann. of Math.*, **112**:585–617.

Hall, P. (1954). Finiteness conditions for soluble groups. *Proc. London Math. Soc.*, **4**(3):419–436.

Hall, P. (1957). Nilpotent groups. In Gruenberg, K. W., Roseblade, J. E., editors, *Collected Works of Philip Hall*, chapter 23, pages 415–462. Clarendon Press, Oxford.

Lo, E. H. (1996a). A Polycyclic Quotient Algorithm Package. Department of Mathematics, Rutgers University, New Jersey, ftp@math.rutgers.edu.

Lo, E. H. (1996b). A polycyclic quotient algorithm. In Finkelstein, L., Kantor, W. M., editors, *Groups and Computation II*, volume 28 of *DIMACS Series in Discrete Mathematics and Computer Science*, pages 159–168, Providence, RI. American Mathematical Society.

Lo, E. H. (1997). Enumerating the finite index subgroups of a polycyclic group. Unpublished.

Lo, E. H. (1998a). Finding intersection and normalizer in finitely generated nilpotent groups. *J. Symbolic Computation*, **25**:45–59.

Lo, E. H. (1998b). A polycyclic quotient algorithm. *J. Symbolic Computation*, **25**:61–97.

Ostheimer, G. (1996a). *Algorithms for Polycyclic-by-Finite Groups.* PhD thesis, Rutgers University, Math Dept.

Ostheimer, G. (1996b). Algorithms for polycyclic-by-finite matrix groups. In Finkelstein, L., Kantor, W. M., editors, *Groups and Computation II*, volume 28 of *DIMACS Series in Discrete Mathematics and Computer Science*, pages 297–307, Providence, RI. American Mathematical Society.

Passi, I. B. S. (1979). *Group Rings and Their Augmentation Ideals*, volume 715 of *Lecture notes in mathematics.* Springer-Verlag, New York.

Robinson, D. J. S. (1982). *A Course in the Theory of Groups.* Springer-Verlag, New York.

Segal, D. (1983). *Polycyclic Groups*, volume 82 of *Cambridge tracts in mathematics.* Cambridge University Press, New York.

Segal, D. (1990). Decidable properties of polycyclic groups. *Proc. London Math. Soc. (3)*, **61**:497–528.

Sims, C. C. (1994). *Computation with Finitely Presented Groups*, volume 48 of *Encyclopedia of mathematics and its applications.* Cambridge University Press, New York.

Wehrfritz, B. A. F. (1973). *Infinite Linear Groups.* Springer-Verlag, Berlin.