[Ma] Mal'cev, A. J. (1958), Homomorphisms onto finite groups, *Ivanov. Gos. Ped. Inst. Učen. Zap. Vol 18*, 49-60.

[Se] Segal, Daniel (1983). *Polycyclic Groups*. Cambridge, England: Cambridge University Press.

[Si] Sims, Charles C. (1994). *Computation with finitely presented groups*. Cambridge, England: Cambridge University Press.

[We] Wehrfritz, B. A. F. (1973). *Infinite Linear Groups*. New York: Springer-Verlag.

of $\mathbf{Q}$ generated by the entries of $g_1, \ldots, g_k, g_1^{-1}, \ldots, g_k^{-1}$; p is an odd prime which does not divide the denominator of any of the entries of the matrices in S; θ is the map from G to $GL(n, F_p)$ defined in the Section 5.1; K is the kernel of θ. We may assume that the entries of a are in the subring S of $\mathbf{Q}$ generated by the entries of elements of G, and as we saw in the Section 5.2, we may assume that we have generators for K. If $|T|$ is small we might simply try each $t \in T$, testing whether or not $at^{-1} \in K$. If $|T|$ is large, we can use techniques for matrices over finite fields to decide whether or not $\theta(a) \in \theta(G)$ and if so to find g in G such that $\theta(a) = \theta(g)$. Then $a \in G$ if and only if $ag^{-1} \in K$. This approach might be particularly efficient in the case when G is polycyclic, since then we can use algorithms developed for working with solvable matrix groups over finite fields (see [Lu]).

6 Future Work

We need to perform experiments to determine the range of input for which the algorithms presented here are practical. In the case of the algorithm to decide whether or not a given matrix group is solvable-by-finite, we need to compare the efficiency of our algorithm with that in [Be2].

References

[BBCIL] Babai, L., Beals, R., Cai, J-y., Ivanyos, G., Luks, E. M. (1994), Multiplicative equations over commuting matrices. Manuscript.

[BCRS] Baumslag, Gilbert, Cannonito, Frank B., Robinson, Derek J., Segal, Dan (1991). The algorithmic theory of polycyclic-by-finite groups. *J. Algebra* **142**, *no. 1*, 118–149.

[Be1] Beals, Robert (1995). Algorithms for matrix groups and the Tits alternative. To appear, *Proc. 36th IEEE FOCS.*

[Be2] Beals, Robert (1995). Testing integrality of matrix groups. In preparation.

[BP] Buchmann, J. Pohst, M. (1989), Computing a lattice basis from a system of generating vectors. *EUROCAL '87 (Leipzig)*, 54–63, *Lecture Notes in Comput. Sci.*, Berlin: Springer.

[Di1] Dixon, John D. (1985). The orbit-stabilizer problem for linear groups. *Can. J. Math. Vol. XXXVII, No. 2*, 238-259.

[Ge] Ge, G. (1993). Algorithms related to multiplicative representations of algebraic numbers, PhD thesis, Math Dept., U. C. Berkeley.

[Lu] Luks, Eugene M. (1992). Computing in solvable matrix groups.*Proc. 33rd IEEE FOCS*, 111-120.

Proof. This follows immediately from the fact that if G is triangularizable over some extension field of $\mathbf{Q}$, then it's triangularizable over some finite extension of $\mathbf{Q}$.

5.2 Deciding if a matrix group is polycyclic-by-finite

Let G be a subgroup of $GL(n,R)$ given by a finite set $\{g_1,\ldots,g_k\}$ of generators. Let S be the subring of $\mathbf{Q}$ generated by the entries of $g_1,\ldots,g_k,g_1^{-1},\ldots,g_k^{-1}$. Let p be an odd prime which does not divide the denominator of any of the entries of the matrices in S. (For example, if $G \leq GL(n,\mathbf{Z})$, we may take $p=3$.) Let $\theta : G \to GL(n,F_p)$ as defined in the Section 5.1, and let K be the kernel of θ. By Lemmas 2 and 3, G is solvable-by-finite if and only if K is triangularizable over $\mathbf{C}$. Furthermore, G is polycyclic-by-finite if and only if K is both triangularizable and polycyclic since if G is polycyclic-by-finite then every subgroup of G is finitely generated (see [Se]). This allows us to reduce problems concerning solvable-by-finite groups to corresponding problems concerning triangularizable groups. We will now elaborate on how such a reduction can be achieved.

First we must obtain a description of K. One way to do so (as in [Di1]) is to get a set T of coset representatives for G/K and to then use the Schreier construction to get a set of $1+|T|(k-1)$ generators for K (see [Si]). If we have generators for K we can decide whether or not G is solvable-by-finite since we can decide whether or not K is triangularizable (see Section 4). Likewise, if G is solvable-by-finite we can decide whether or not G is polycyclic-by-finite, since according to [Be2] it is possible to decide whether or not triangularizable K is polycyclic.

The Schreier construction may be impractical in some cases since even if p is small, $|T|$ might be large: for example, $|GL(10,F_3)| \sim 3\times 10^{47}$. When $|T|$ is large, we can use techniques for working with matrix groups over finite fields to obtain a presentation for G/K and thereby obtain normal generators for K. One way to achieve this is to view G/K as a permutation group on the vectors in F_p^n and to use algorithms for finding presentations of permutation groups. If G is solvable, we can instead use special methods for finding presentations for solvable subgroups of $GL(n,F_p)$ (see [Lu]).

Suppose now that K is given by normal generators, i.e., suppose we have generators for $\tilde{K}$ such that $\tilde{K}^G = K$. We can decide whether or not $\tilde{K}$ is triangularizable, and if it is we can test membership in $\tilde{K}$. Therefore by conjugating elements in $\tilde{K}$ by $g_1,\ldots,g_k,g_1^{-1},\ldots,g_k^{-1}$, we can keep building up $\tilde{K}$ stopping when either it is not triangularizable (in which case G is not solvable-by-finite) or $\tilde{K}$ is both triangularizable and normal in G (in which case $\tilde{K}=K$ and G is solvable-by-finite). Since K is finitely generated, this algorithm is guaranteed to terminate.

5.3 Testing membership

We now discuss the problem of deciding whether or not a given matrix a in $GL(n,\mathbf{Q})$ is an element of G, where G is a polycyclic-by-finite matrix group given by a finite set $\{g_1,\ldots,g_k\}$ of generators. We carry over our notation from Section 5.2: S is the subring

We first show that we can find a presentation for $\psi(G)$ in terms of our given generators, that is, we can find generators for the subgroup K of vectors v in $\mathbf{Z}^k$ such that $\psi(g^v) = 1$. The enveloping algebra B of $\psi(G)$ is the direct sum $F_1 \oplus \cdots \oplus F_r$ of fields. Let π_i be the projection of B onto F_i. As we saw in Section 2, we can find a presentation for the image of $\psi(G)$ under π_i. Thus we can obtain generators for the subgroup K_i of vectors v in $\mathbf{Z}^k$ such that $\pi_i(\psi(g^v)) = 1$. K is then intersection of the K_i's.

As we saw in Section 2, it follows that we can test membership in $\psi(G)$ constructively, that is, we can decide whether or not $\psi(a) \in \psi(G)$, and, if so, we can find $g \in G$ such that $\psi(a) = \psi(g)$. Thus we are left with the problem of deciding whether or not ag^{-1} is in the intersection H of G and the kernel of ψ.

Let $\tilde{H}$ be the subgroup generated by $\{g^v \mid v \in K\}$. H is the normal closure of $\tilde{H}$ in G. Therefore by conjugating elements in $\tilde{H}$ by $g_1, \ldots, g_k$, we can keep building up $\tilde{H}$ until $\tilde{H}$ is normal in G, in which case $\tilde{H} = H$. (Recall that since H is hopfian, we do not need to conjugate by $g_1^{-1}, \ldots, g_k^{-1}$.) This process is guaranteed to terminate since G is assumed to be polycyclic. Now we have generators for H, so we can use the methods of Section 3 to decide whether or not $ag^{-1} \in H$.

5 Polycyclic-by-finite Matrix Groups

5.1 Facts about the p-congruence subgroup

If G is a finitely generated subgroup of $GL(n, \mathbf{Q})$, then the subring S of $\mathbf{Q}$ generated by the entries of the elements of G is finitely generated as a ring. Therefore, we can find a prime p such that if $r \in S$ we can write $r = \frac{u}{v}$ where $u, v \in \mathbf{Z}$ and $(v, p) = 1$. We first notice (as in [Di1]) that G can be embedded in $GL(n, \mathbf{Z}_p)$: the obvious embedding of $\mathbf{Q}$ into $\mathbf{Q}_p$ maps S into $\mathbf{Z}_p$, and in this way we achieve a group embedding of G into $GL(n, \mathbf{Z}_p)$.

Again following Dixon's example, we consider the ring homomorphism $\mathbf{Z}_p \to \mathbf{Z}_p/p\mathbf{Z}_p \cong F_p$ and its extension to a group homomorphism $\theta : GL(n, \mathbf{Z}_p) \to GL(n, F_p)$. The kernel of this homomorphism is called the *principal p-congruence subgroup* of $GL(n, \mathbf{Z}_p)$.

Let p be an odd prime, and let C be the principal p-congruence subgroup of $GL(n, \mathbf{Z}_p)$. In [Di1], Dixon shows that every subgroup G of C is connected. He uses this to prove the following lemma.

Lemma 2 *Let p be an odd prime, and let C be the principal p-congruence subgroup of $GL(n, \mathbf{Z}_p)$. If G is a subgroup of C, and G is solvable-by-finite, then G is triangularizable (over $\overline{\mathbf{Q}_p}$).*

This, together with the lemma which follows, will allow us to reduce problems about polycyclic-by-finite subgroups of $GL(n, \mathbf{Q})$ to problems about subgroups of $GL(n, \mathbf{Q})$ which are both polycyclic and triangularizable (over $\mathbf{C}$).

Lemma 3 *Let G be a subgroup of $GL(n, \mathbf{Q})$. Then G is triangularizable over $\overline{\mathbf{Q}_p}$ if and only if G is triangularizable over $\mathbf{C}$.*

Proof. Let $V = \{v \in R^n \mid v(gh - hg) = 0 \ \forall \ g, h \in G\}$. V is invariant under the action of G since if $v \in R^n$ and $x, g, h \in G$, then

$$vx(gh - hg) = v((xg)h - h(xg)) + (v(hx - xh))g = 0$$

The fact that $V \neq 0$ follows from the fact that G', the commutator subgroup of G, is unipotent since if we let x be a nonzero element of R^n such that $xg = x$ for all $g \in G'$, then for all g, h in G,

$$x(gh - hg) = x(ghg^{-1}h^{-1} - 1_G)hg = 0$$

The image of G under the map to $GL(V)$ is abelian. V has a complement W in R^n. (It is clear that when $R = \mathbf{Z}$, $\mathbf{Z}^n/V$ is torsion-free.) Choose a basis $w_1, \ldots, w_j$ for W and a basis $v_{j+1}, \ldots, v_n$ for V. Let θ be the map from G to $GL(j, R)$ such that $\theta(g)$ describes the action of g on R^n/V relative to the basis $w_1 + V, \ldots, w_j + V$. $\theta(G)$ is unipotent-by-abelian since $\theta(G)' = \theta(G')$ is unipotent. By induction on n, we can find a basis $v_1, \ldots, v_j$ for W such that relative to the basis $v_1 + V, \ldots, v_j + V$, $\theta(G)$ has the desired block structure. The basis $v_1, \ldots, v_n$ for R^n satisfies the criteria of the proposition.

The following corollary is an immediate consequence.

Corollary 1 *Let G be a subgroup of $GL(n, R)$. Then G is triangularizable if and only if G is unipotent-by-abelian.*

It easy to see that the proof of Proposition 1 provides an algorithm to decide whether or not a subgroup G of $GL(n, R)$ given by a finite set of generators is triangularizable, and, if so, to find a basis for R^n satisfying the criteria of the proposition. Find a basis $\{b_1, \ldots, b_d\}$ for A, the enveloping algebra of G. (If $R = \mathbf{Z}$, we choose the b_i's in $GL(n, R)$.) Then $V = \bigcap_{i,j} V_{i,j}$, where $V_{i,j} = \{v \in R^n \mid v(a_i a_j - a_j a_i) = 0\}$. If $V = 0$, then G is not triangularizable. Otherwise, find a complement W to V in R^n. Now proceed inductively to decide whether or not $\theta(G)$ is triangularizable, and, if so, to find a basis $v_1, \ldots, v_j$ for W such that $\theta(G)$ has the desired block structure with respect to $v_1 + V, \ldots, v_j + V$.

4.2 Testing membership

Let G be a triangularizable, polycyclic subgroup of $GL(n, R)$, and let $a \in GL(n, R)$. We will now reduce the problem of deciding whether or not $a \in G$ to two special cases, namely, when G is abelian and the enveloping algebra is a field, or when $G \leq Tr_1(n, R)$. As we saw in the previous section, we may assume that we have found a basis for R^n satisfying the criteria of Proposition 1. We may also assume that a has a block structure like that of G with respect to this basis. Let ψ be the map from $\langle G, a \rangle$ to $GL(n, R)$ given below

$$\begin{pmatrix} a_1 & * & \cdot & \cdot & * & * \\ 0 & a_2 & * & \cdot & \cdot & * \\ \cdot & 0 & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \cdot & \cdot & \cdot & \cdot & * \\ 0 & 0 & \cdot & \cdot & 0 & a_r \end{pmatrix} \longmapsto \begin{pmatrix} a_1 & 0 & \cdot & \cdot & 0 & 0 \\ 0 & a_2 & 0 & \cdot & \cdot & 0 \\ \cdot & 0 & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \cdot & \cdot & \cdot & \cdot & 0 \\ 0 & 0 & \cdot & \cdot & 0 & a_r \end{pmatrix}$$

4 Triangularizable Matrix Groups

4.1 A structure theorem

Recall that an abelian subgroup G of $GL(n,R)$ is triangularizable. We can use this fact to construct other examples of triangularizable subgroups. Let $n = n_1 + \cdots + n_r$, and let G_i be an abelian subgroup of $GL(n_i,R)$. Choose as our generators for G matrices that have the following block structure:

$$\begin{pmatrix} a_1 & * & \cdot & \cdot & * & * \\ 0 & a_2 & * & \cdot & \cdot & * \\ \cdot & 0 & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \cdot & \cdot & \cdot & \cdot & * \\ 0 & 0 & \cdot & \cdot & 0 & a_r \end{pmatrix}$$

where $a_i \in G_i$ for all i. Clearly, G is triangularizable. In this section we show that given a finite set of generators for a triangularizable subgroup G of $GL(n,R)$, we can find a basis for R^n relative to which G has this block structure. Furthermore, we describe an algorithm for deciding whether or not a subgroup of $GL(n,R)$ given by a finite set of generators is triangularizable.

Clearly, a triangularizable subgroup is unipotent-by-abelian: after a change of basis over $\mathbf{C}$ the group is upper triangular, and the commutator of two upper triangular matrices is an upper triangular matrix with 1's on the diagonal. Therefore, it will suffice to show that all unipotent-by-abelian subgroups have the desired form. Before doing so we must recall the following basic fact about unipotent subgroups.

Lemma 1 *If G is a unipotent subgroup of $GL(n,R)$, then there exists an $x \neq 0$ in R^n such that $xg = x$ for all g in G.*

In the case when R is a field, Lemma 1 follows from Corollary 1.21 in [We]. If $R = \mathbf{Z}$, let y be a nonzero element of $\mathbf{Q}^n$ such that $yg = y$ for all g in G, and let x be obtained from y by clearing denominators.

Proposition 1 *Let G be a unipotent-by-abelian subgroup of $GL(n,R)$. There exists a basis B for R^n such that all matrices in G have the following block structure with respect to B*

$$g = \begin{pmatrix} a_1 & * & \cdot & \cdot & * & * \\ 0 & a_2 & * & \cdot & \cdot & * \\ \cdot & 0 & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \cdot & \cdot & \cdot & \cdot & * \\ 0 & 0 & \cdot & \cdot & 0 & a_r \end{pmatrix}$$

where for $1 \leq i \leq k$, the image of G under the map that takes g to a_i is abelian.

exists an element h of $\tilde{H}$ such that $h_{k+1} = -1$, then we take y to be the vector consisting of the first k components of h and then $a = g^y$. Otherwise, $a \notin G$.

3 Unitriangular Matrix Groups

3.1 Unitriangular subgroups of $GL(n, \mathbf{Z})$

Let G be a subgroup of $Tr_1(n, \mathbf{Z})$ given by a finite set $\{g_1, \ldots, g_k\}$ of generators. In order to test membership in G we rely on algorithms which have been developed for working with polycyclic groups given by consistent polycyclic presentations. (See Section 1.2 for a description of POLY SUBGROUP and POLY MEMBER.) $Tr_1(n, \mathbf{Z})$ is a finitely generated nilpotent group and, hence, is polycyclic. It is easy to find a consistent polycyclic presentation $\langle X|R\rangle$ for $Tr_1(n, \mathbf{Z})$: Example 4.1 in Section 9.4 of [Si] is easily generalized. It is also easy to express a given unitriangular matrix in terms of the generators in X. We use POLY SUBGROUP to calculate a polycyclic generating sequence $h_1, \ldots, h_l$ for G and POLY MEMBER to then test membership in G. It is not hard to streamline these algorithms in our specific context.

When G is both unipotent and abelian, we can also find a presentation for G in terms of $g_1, \ldots, g_k$, i.e., we can find generators for the subgroup H of $\mathbf{Z}^k$ consisting of elements z such that $g^z = 1$. There is a homomorphism ϕ from $\mathbf{Z}^k$ to $\mathbf{Z}^l$ taking u in $\mathbf{Z}^k$ to the vector v in $\mathbf{Z}^l$ such that $h^v = g^u$. The kernel of ϕ is H. Since ϕ can be represented by an integer matrix it is easy to find its kernel. As we saw in Section 2, if we can find a presentation for G, it follows that our membership test for G can be made constructive.

3.2 Unitriangular subgroups of $GL(n, \mathbf{Q})$

Let G be a finitely generated subgroup G of $Tr_1(n, \mathbf{Q})$. We reduce the problem of testing membership in G to the problem of testing membership in a subgroup of $Tr_1(n, \mathbf{Z})$. In [Se] (Lemma 2, Chapter 6), Segal shows that if $G = \langle g_1, \ldots, g_k\rangle$ is a finitely generated subgroup of $Tr_1(n, \mathbf{Q})$, then it is easy to find an x in $GL(n, \mathbf{Q})$ such that $x^{-1}Gx \leq Tr_1(n, \mathbf{Z})$: find a natural number m such that $m(g_i - 1)$ is an integer matrix for all $1 \leq i \leq k$ and then let

$$x = \begin{pmatrix} 1 & 0 & \cdot & \cdot & 0 & 0 \\ 0 & m & 0 & \cdot & \cdot & 0 \\ \cdot & 0 & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \cdot & \cdot & \cdot & \cdot & 0 \\ 0 & 0 & \cdot & \cdot & 0 & m^{n-1} \end{pmatrix}$$

Thus, membership testing in a finitely generated subgroup of $Tr_1(n, \mathbf{Q})$ is reduced to the analagous problem in $Tr_1(n, \mathbf{Z})$. As with subgroups of $Tr_1(n, \mathbf{Z})$, if G is also abelian, we can make our membership test constructive and we can find a presentation for G. Alternative methods for working with abelian subgroups of $Tr_1(n, \mathbf{Q})$ are described in [BBCIL].

given matrix a in $GL(n, \mathbf{Z})$ is an element of G, simply verify that $\langle G, a \rangle$ is also polycyclic, get a finite presentation for $\langle G, a \rangle$, and then test whether $a \in G$ using this presentation. In [BCRS] the goal is to prove decidability; our goal here is to sketch algorithms which are actually suitable for computer implementation.

An algorithm for testing membership in an abelian subgroup of $GL(n, R)$ was discovered independently by the author and [BBCIL]. They prove that the run-time of their algorithm is polynomial in the length of the input. They also describe an alternative method for testing membership in a matrix group which is both unipotent and abelian. Both the algorithms described here and those in [BBCIL] rely heavily on the work of Ge ([Ge]) concerning algorithms for multiplicative subgroups of a number field.

In [Be1] Beals describes an algorithm for deciding whether or not a given finitely generated subgroup of $GL(n, R)$ is solvable-by-finite. He proves that the run-time of his algorithm is polynomial in the length of input. His algorithm appears to be suitable for computer implementation. We describe here an alternative to Beals' algorithm. We make no claims regarding the asymptotic run-time of our algorithm, but our algorithm does also appear to be suitable for computer implementation. Experimentation is needed to compare the efficiency of these two algorithms in practice.

Our algorithms for solvable-by-finite matrix groups rely on Dixon's observation ([Di1]) that subgroups of the p-congruence subgroup of $GL(n, \mathbf{Z}_p)$ are connected in the Zariski topology. It is an easy consequence of this result that problems concerning solvable-by-finite matrix groups can be reduced to problems about triangularizable matrix groups. Dixon illustrates this himself by using such a reduction to solve the stabilizer and orbit problems for a nilpotent-by-finite matrix group G: given u in R^n, find the stabilizer of u in G, and given u, v in R^n, decide whether or not u and v are in the same orbit under the action of G. We also rely on an algorithm of Beals ([Be2]) for deciding whether or not a given finitely generated triangularizable group is polycyclic.

2 Abelian Groups Embedded in a Field

Let G be an abelian matrix group given by a finite set $\{g_1, \ldots, g_k\}$ of generators. Assume furthermore that A, the enveloping algebra of G, is a field. We want to find a presentation for G, i.e., we want to find generators for the subgroup H of $\mathbf{Z}^k$ consisting of elements h such that $g^h = 1$. This is precisely the problem solved by Ge in [Ge]. Ge assumes that the field A is given by structure constants, so we must begin by computing a basis for A over $\mathbf{Q}$ and the corresponding structure constants. Ge proves that the run-time of his algorithm is polynomial in the length of the input. He makes no claims concerning the practicality of his algorithm, though others who have used similar techniques were able to do so (see [BP]).

Once we have an algorithm to find H, it is easy to see that we can test membership in G constructively, that is, we can decide whether or not $a \in G$ and, if so, we can express a in terms of the given generators for G. Verify that a commutes with $g_1, \ldots, g_k$. Rename a as g_{k+1} and find generators for $\tilde{H}$, the subgroup of vectors h in $\mathbf{Z}^{k+1}$ such that $g^h = 1$. If there

1 Introduction

1.1 Notation and definitions

Throughout this article, we will let R denote either the ring of integers or a number field. If p is a prime, the field of p-adic numbers will be denoted by $\mathbf{Q}_p$, its algebraic closure by $\overline{\mathbf{Q}_p}$. and the ring of p-adic integers by $\mathbf{Z}_p$. The field with p elements will be denoted by F_p.

Let G be a subgroup of $GL(n,R)$ given by a finite set $\{g_1,\ldots,g_k\}$ of generators. If R is a number field with $[R:\mathbf{Q}]=d$, then we can represent the elements of R as $d\times d$ matrices over $\mathbf{Q}$. Therefore, we may assume R is either $\mathbf{Z}$ or $\mathbf{Q}$. Therefore, when we refer to the *enveloping algebra* of G, we mean the smallest $\mathbf{Q}$-subalgebra of the algebra of $n\times n$ matrices over $\mathbf{Q}$ containing G.

If F is any field and E an extension field of F, and if G is a subgroup of $GL(n,F)$, we say that G is *triangularizable over* E if there is a basis for E^n relative to which every matrix in G is upper triangular, and we say G is *triangularizable* if it is triangularizable over the algebraic closure of F. If G is a subgroup of $GL(n,F)$ and if G is triangularizable over some extension field E of F, then there exists a finite extension K of F over which G is triangularizable (see p. 33 of [Se]). So in our case, a subgroup G of $GL(n,R)$ is triangularizable if and only if it is triangularizable over $\mathbf{C}$. We denote by $Tr_1(n,R)$ the group of upper triangular matrices with entries in R and 1's along the diagonal.

If $x\in\mathbf{Z}^k$ and $g_1,\ldots,g_k\in GL(n,R)$, then g^x denotes $g_1^{x_1}\cdots g_k^{x_k}$.

1.2 Facts about polycyclic groups

In this section we summarize some basic facts about polycyclic groups. Refer to Chapter 9 of [Si] for further definitions and proofs.

An abstract group G is *polycyclic* if it is solvable and every subgroup of G is finitely generated. Every polycyclic group is hopfian, i.e., every surjective homomorphism $f:G\to G$ is an isomorphism.

Let G be a polycyclic group given by a finite presentation $\langle X|R\rangle$. Algorithms exist for testing membership in a subgroup H of G given by a finite set of generators ([Ma]), and if $\langle X|R\rangle$ is a consistent polycyclic presentation, practical algorithms exist. For such presentations, Sims describes in Section 9.6 of [Si] an algorithm POLY SUBGROUP that calculates a polycyclic generating sequence for H and an algorithm POLY MEMBER that uses such a sequence to test membership in H.

1.3 Review of previous work

Let G be a subgroup of $GL(n,\mathbf{Z})$ given by a finite set of generators. In [BCRS] an algorithm is given for deciding whether or not G is polycyclic, and if G is indeed polycyclic, an algorithm is given for finding a presentation for G. Since, as mentioned in Section 1.2, algorithms also exist for testing membership in subgroups of finitely presented polycyclic groups, it is possible to test membership in a polycyclic subgroup of $GL(n,\mathbf{Z})$. To test whether or not a

ABSTRACT

Let R be the ring of integers or a number field. We present several algorithms for working with polycyclic-by-finite subgroups of $GL(n, R)$. Let G be a subgroup of $GL(n, R)$ given by a finite generating set of matrices. We describe an algorithm for deciding whether or not G is polycyclic-by-finite. For polycyclic-by-finite G, we describe an algorithm for deciding whether or not a given matrix is an element of G. We also describe an algorithm for deciding whether or not G is solvable-by-finite, providing an alternative to the algorithm proposed by Beals ([Be1]) for this problem.

Baumslag, Cannonito, Robinson and Segal prove that the problem of determining whether or not a finitely generated subgroup of $GL(n, \mathbf{Z})$ is polycyclic-by-finite is decidable and that the problem of testing membership in a polycyclic-by-finite subgroup of $GL(n, \mathbf{Z})$ is also decidable ([BCRS]). In this report we extend these results by describing algorithms which appear to be suitable for computer implementation. Experimentation is needed to determine the range of input for which they are practical.

Our method is to first reduce each problem to the corresponding problem for triangularizable matrix groups. The reduction is an easy consequence of the result of Dixon ([Di1]) that subgroups of the p-congruence subgroup of $GL(n, \mathbf{Z}_p)$ are connected in the Zariski topology, where $\mathbf{Z}_p$ is the ring of p-adic integers for a prime p.

We then prove a structure theorem for triangularizable matrix groups that allows us to decide whether or not a matrix group is triangularizable and to reduce the problem of testing membership in a polycyclic, triangularizable matrix group to the corresponding problems for finitely generated abelian matrix groups and for finitely generated unitriangular matrix groups. In the case of an abelian matrix group we can find a presentation for the group, and our membership test can be made constructive. For these results we rely heavily on the work of Ge ([Ge]) concerning algorithms for multiplicative subgroups of a number field. We also rely on an algorithm of Beals ([Be2]) to decide whether or not a triangularizable matrix group is polycyclic.

DIMACS Technical Report 95-33
August 1995

Algorithms for Polycyclic-by-finite Matrix Groups: Preliminary Report

by

Gretchen Ostheimer[1]
Dept. of Mathematics
Rutgers University
New Brunswick, New Jersey 08903

[1] Affiliated Graduate Student Member

DIMACS is a cooperative project of Rutgers University, Princeton University, AT&T Bell Laboratories and Bellcore.

DIMACS is an NSF Science and Technology Center, funded under contract STC–91–19999; and also receives support from the New Jersey Commission on Science and Technology.