ALGORITHMS FOR LINEAR GROUPS OF FINITE RANK

A. S. DETINKO, D. L. FLANNERY, AND E. A. O'BRIEN

ABSTRACT. Let G be a finitely generated solvable-by-finite linear group. We present an algorithm to compute the torsion-free rank of G and a bound on the Prüfer rank of G. This yields an algorithm to decide whether a finitely generated subgroup of G has finite index. The algorithms are implemented in MAGMA for groups over algebraic number fields.

In [7, 8] we developed practical methods for computing with linear groups over an infinite field $\mathbb{F}$. Those methods were used to test whether a finitely generated subgroup of $\mathrm{GL}(n, \mathbb{F})$ is solvable-by-finite (SF). We now proceed to the design of further algorithms for finitely generated SF linear groups. Such a group may not be finitely presentable (see [21, 4.22, p. 66]), so obviously cannot be studied using approaches that **require** a presentation; in contrast to, say, polycyclic-by-finite (PF) groups. Extra restrictions are necessary to make computing feasible. Groups of finite rank are suitable candidates from this point of view, because they are well-behaved algorithmically [13, Section 9.3]. They also have convenient structural features (see [13, Section 5.2] and Section 1).

In this paper we develop initial results to enable computing with finitely generated linear groups of finite rank. Since such groups are $\mathbb{Q}$-linear (Proposition 1.4), our primary focus is the case that $\mathbb{F}$ is an algebraic number field. We first test whether $G \leq \mathrm{GL}(n, \mathbb{F})$ has finite rank. If so, we compute its torsion-free rank and an upper bound on its Prüfer rank. This furnishes an algorithm to decide whether a finitely generated subgroup of G has finite index. We determine various asymptotic bounds of interest in their own right. Algorithms for the structural investigation of G are provided as well: these construct a completely reducible part, and a finitely generated subgroup with the same rank as the unipotent radical. Our algorithms have been implemented in MAGMA [5]. We emphasize that computations are performed with a given group in its original representation, avoiding enlargement of matrices to get an isomorphic copy over $\mathbb{Q}$.

Naturally, it is possible to take advantage of additional properties of G when they are known. If G is polycyclic then one could obtain its torsion-free rank from a consistent polycyclic presentation of G, the latter found as in [2]. An even more tractable class is nilpotent-by-finite groups (cf. [10, Section 7]).

We summarize the layout of the paper. Section 1 gives background on linear groups of finite rank, including a reduction to SF groups over a number field. Section 2 is an extended treatment of such groups. In Section 3 we discuss ranks of finite index subgroups; we are indebted to D.J.S. Robinson for a vital theorem here. Section 3 also shows how to find the rank of a unipotent normal subgroup. In Section 4 we present our algorithms and some experimental results.

Unless stated otherwise, $\mathbb{F}$ is an (infinite) field. The rational field is denoted as usual by $\mathbb{Q}$, and $\mathbb{P}$ is a number field with ring of integers $\mathcal{O}_{\mathbb{P}}$.

1. PRELIMINARIES

A general reference for this section is [13, Chapter 5].

1.1. **Prüfer rank and torsion-free rank.** Recall that a group G has finite Prüfer rank $\mathrm{rk}(G)$ if each finitely generated subgroup of G can be generated by $\mathrm{rk}(G)$ elements, and $\mathrm{rk}(G)$ is the least such integer.

Theorem 1.1. *Let $G \leq \mathrm{GL}(n, \mathbb{F})$ have finite Prüfer rank. Then G is SF, and if $\mathrm{char}\, \mathbb{F} > 0$ then G is abelian-by-finite (AF).*

Proof. See [21, 10.9, p. 141]. □

Corollary 1.2. *Let G be a finitely generated subgroup of $\mathrm{GL}(n, \mathbb{F})$. If G is AF then it has finite Prüfer rank; if G is completely reducible and has finite Prüfer rank then it is AF.*

Proof. If G is AF then it has a normal finitely generated abelian subgroup A of finite index. Since A and G/A have finite rank, so does G. On the other hand, if G is completely reducible and has finite rank, then it is AF by Theorem 1.1 and [21, 3.5 (ii), p. 44]. □

Remark 1.3. The converse of Theorem 1.1 is not true even when G is finitely generated. However, see Proposition 2.3.

Proposition 1.4. *If G is a finitely generated subgroup of $\mathrm{GL}(n, \mathbb{F})$ of finite Prüfer rank then G is $\mathbb{Q}$-linear, i.e., isomorphic to a subgroup of $\mathrm{GL}(d, \mathbb{Q})$ for some d.*

Proof. Suppose that $\mathrm{char}\, \mathbb{F} = 0$. By [21, 4.8, p. 56], G is (torsion-free)-by-finite, and by Theorem 1.1, G is SF. Thus G contains a torsion-free solvable normal subgroup of finite index and finite rank. The result now follows from [11, Theorem 2].

Suppose that $\mathrm{char}\, \mathbb{F} > 0$. By Theorem 1.1, G is PF. It is well-known that a PF group is $\mathbb{Z}$-linear; see [13, 3.3.1, p. 57]. □

Theorem 1.1 and Proposition 1.4 essentially reduce the investigation of finitely generated linear groups of finite rank to the case of SF groups over $\mathbb{Q}$. In Section 2.2 we show conversely that finitely generated SF subgroups of $\mathrm{GL}(n, \mathbb{P})$ always have finite rank. Hence we restrict attention mainly to groups over number fields.

Now recall that a group G has finite torsion-free rank if it has a subnormal series of finite length whose factors are either periodic or infinite cyclic. The number $\mathrm{h}(G)$ of infinite cyclic factors is the *Hirsch number*, or *torsion-free rank*, of G.

Lemma 1.5. *An SF group with finite Prüfer rank has finite torsion-free rank.*

Proof. See [13, p. 85]. □

Lemma 1.6. *Let G be a group with normal subgroup N.*

(i) *If G has finite Prüfer rank then $\mathrm{rk}(G) \leq \mathrm{rk}(N) + \mathrm{rk}(G/N)$.*
(ii) *If G has finite torsion-free rank then $\mathrm{h}(G) = \mathrm{h}(N) + \mathrm{h}(G/N)$.*

1.2. **Polyrational groups.** Let $U(G)$ be the unipotent radical of $G \leq \mathrm{GL}(n, \mathbb{F})$; namely, the largest unipotent normal subgroup of G. Note that $G/U(G)$ is isomorphic to a completely reducible subgroup of $\mathrm{GL}(n, \mathbb{F})$. If we exhibit G in block triangular form with completely reducible blocks, then $U(G)$ is the kernel of the projection of G onto its main diagonal. Denote the largest periodic normal subgroup of G by $\tau(G)$.

Lemma 1.7. *Let G be a finitely generated subgroup of* $\mathrm{GL}(n, \mathbb{F})$ *of finite Prüfer rank. Then* $\tau(G)$ *is finite.*

Proof. Theorem 1.1 and Proposition 1.4 imply that G is SF and we may assume that $\operatorname{char}\mathbb{F} = 0$. Then $\tau(G)$ is isomorphic to a subgroup of $\tau(G/U(G))$, and $G/U(G)$ is finitely generated AF by Corollary 1.2. So we may further assume that G has a normal abelian subgroup A of finite index. Since A is finitely generated, $\tau(G) \cap A \leq \tau(A)$ is finite. Thus $|\tau(G)| = |\tau(G)A : A| \cdot |\tau(G) \cap A|$ is finite. □

A group is *polyrational* if it has a series of finite length with each factor isomorphic to a subgroup of the additive group $\mathbb{Q}^+$. So a polyrational group has finite torsion-free and Prüfer ranks.

Proposition 1.8. *If G is polyrational then* $\mathrm{rk}(G) = \mathrm{h}(G)$.

Proof. See [13, 5.2.7, p. 93]. □

Theorem 1.9. *A finitely generated subgroup G of* $\mathrm{GL}(n, \mathbb{F})$ *has finite Prüfer rank if and only if it is polyrational-by-finite. In this case,* $\mathrm{h}(G) \leq \mathrm{rk}(G)$.

Proof. The first statement follows from Theorem 1.1, Lemmas 1.5 and 1.7, and [13, 5.2.5, p. 92]. For the second, let N be a normal polyrational finite index subgroup of G; then $\mathrm{h}(G) = \mathrm{h}(N) = \mathrm{rk}(N) \leq \mathrm{rk}(G)$. □

From now on, the term 'rank' without a qualifier means either Prüfer or torsion-free rank.

2. Solvable-by-finite groups over a number field

We now focus on finitely generated SF subgroups of $\mathrm{GL}(n, \mathbb{P})$. Set $|\mathbb{P} : \mathbb{Q}| = m$. In this section we obtain more detailed information about these groups that will be used in our algorithms.

A finitely generated subgroup G of $\mathrm{GL}(n, \mathbb{F})$ is contained in $\mathrm{GL}(n, R)$ where $R \subseteq \mathbb{F}$ is a finitely generated integral domain. The quotient ring R/ρ is a finite field for any maximal ideal ρ of R. We explain in [7, Section 2] how to construct a congruence homomorphism $\varphi_\rho : \mathrm{GL}(n, R) \to \mathrm{GL}(n, R/\rho)$ for a maximal ideal ρ such that

- the kernel G_ρ of φ_ρ on G is unipotent-by-abelian (UA) if G is SF;
- G_ρ is torsion-free if $\operatorname{char}\mathbb{F} = 0$.

To be more explicit, let $\mathbb{F} = \mathbb{P} = \mathbb{Q}(\alpha)$ where α has minimal polynomial $f(X)$, and let $G = \langle \mathcal{S} \rangle$. Then φ_ρ on $R \cap \mathbb{Q}$ is reduction modulo an odd prime $p \in \mathbb{Z}$ not dividing the discriminant of $f(X)$ nor the denominators of entries in elements of $\mathcal{S} \cup \mathcal{S}^{-1}$. Hence φ_ρ maps R into the finite field $\mathbb{Z}_p(\beta)$, where β is a root of the mod p reduction of $f(X)$. We adhere to this notation from [7].

2.1. Unipotent groups.

Denote the group $\mathrm{UT}(n, K)$ of upper unitriangular matrices over a commutative unital ring K by T. Define T_i to be the subgroup of T consisting of all matrices with their first $i-1$ superdiagonals equal to zero. Then $T = T_1 > T_2 > \cdots > T_n = 1$ is the lower (and upper) central series of T. The homomorphism on T_i that maps each element to its ith superdiagonal has kernel T_{i+1} and image the $(n-i)$-fold direct sum $K^+ \oplus \cdots \oplus K^+$.

Lemma 2.1. *If* $G \leq \mathrm{UT}(n, \mathbb{Q})$ *then*

(i) *G is polyrational,*
(ii) $\mathrm{rk}(G) = \mathrm{h}(G) \leq n(n-1)/2$.

Proof. Let $K = \mathbb{Q}$ in the notation introduced just before the lemma. Since $(G \cap T_i)/(G \cap T_{i+1})$ is isomorphic to a subgroup of T_i/T_{i+1}, (i) is clear. Then $\mathrm{rk}(G) = \mathrm{h}(G)$ by Proposition 1.8. Also, by Lemma 1.6 (ii),

$$\mathrm{h}(T) = \mathrm{h}(T_1/T_2) + \mathrm{h}(T_2/T_3) + \cdots + \mathrm{h}(T_{n-1}/T_n) = \textstyle\sum_{i=1}^{n-1} i = n(n-1)/2. \qquad \square$$

Corollary 2.2. *If* $G \leq \mathrm{UT}(n, \mathbb{P})$ *then* G *is polyrational and* $\mathrm{rk}(G) = \mathrm{h}(G) \leq nm(nm-1)/2$.

2.2. **Ranks of solvable-by-finite groups over number fields.** In this section G is a finitely generated subgroup of $\mathrm{GL}(n, \mathbb{P})$. We prove that if G is SF then it has finite rank. Although $\mathrm{rk}(G)$ can be arbitrarily large, the ranks of finitely generated SF subgroups of $\mathrm{GL}(n, \mathcal{O}_{\mathbb{P}})$ are bounded by functions of n and m, which we give below.

Proposition 2.3. *Suppose that* G *is SF. Then* G *is polyrational-by-finite, hence of finite Prüfer rank.*

Proof. Select an ideal ρ such that G_ρ is UA and G/G_ρ is finite. Let U be the unipotent radical of G_ρ; then G_ρ/U is finitely generated abelian. Write $G_\rho/U = H/U \times \tau(G_\rho/U)$. Since H/U is a finitely generated free abelian group and U is conjugate to a subgroup of $\mathrm{UT}(n, \mathbb{P})$, H is polyrational. Thus G_ρ has a polyrational normal subgroup of finite index. Consequently the same is true for G. $\square$

Remark 2.4. Retaining the notation in the proof of Proposition 2.3, $\mathrm{h}(G) = \mathrm{h}(G_\rho)$ and $\mathrm{rk}(G) \leq \mathrm{rk}(G_\rho) + \mathrm{rk}(\varphi_\rho(G))$ by Lemma 1.6. Furthermore $\mathrm{rk}(G_\rho) \leq \mathrm{h}(H) + \mathrm{rk}(\tau(G_\rho/U))$. If we know $x \in \mathrm{GL}(n, \mathbb{P})$ that conjugates G to block upper triangular form with completely reducible diagonal blocks, then we can choose ρ so that the torsion-free group G_ρ is polyrational, and thus $\mathrm{rk}(G_\rho) = \mathrm{h}(G_\rho)$. In particular, G_ρ is polyrational for any ρ when G is completely reducible.

Remark 2.4 underpins our algorithm to calculate ranks.

Corollary 2.5. *A finitely generated subgroup of* $\mathrm{GL}(n, \mathbb{F})$ *has finite Prüfer rank if and only if it is SF and* $\mathbb{Q}$*-linear.*

Proposition 2.6. *The following are equivalent.*

(i) G *is SF.*
(ii) G *has finite Prüfer rank.*
(iii) G *has finite torsion-free rank.*

Proof. Theorem 1.1 and Proposition 2.3 give (i) ⇔ (ii). Then (i) ⇔ (iii) by Lemma 1.5 and the Tits alternative. $\square$

Remark 2.7. Thus, we can test whether G has finite rank using the algorithm of [7, Section 3.2], which decides the Tits alternative for G. This algorithm accepts a finitely generated linear group over any $\mathbb{F}$; if it returns `false`, then the input does not have finite rank.

In fact, Proposition 2.3 holds for a wider class of groups: what is most important here is that unipotent subgroups of $\mathrm{GL}(n, \mathbb{P})$ have finite rank.

Lemma 2.8. *If* R *is a finitely generated subring of* $\mathbb{P}$ *then an SF subgroup* H *of* $\mathrm{GL}(n, R)$ *has finite Prüfer rank.*

Proof. It suffices to confirm that $H/U(H)$ has finite rank. Indeed, $H/U(H)$ is finitely generated AF by [21, 4.10, p. 57]. □

Proposition 2.9. *Suppose that* $G \leq \mathrm{GL}(n, \mathcal{O}_\mathbb{P})$ *is SF. Then* $\mathrm{h}(G) \leq nm(nm+1)/2$ *and* $\mathrm{rk}(G) \leq nm(2nm+3)/2$.

Proof. Since $\mathrm{GL}(n, \mathcal{O}_\mathbb{P})$ embeds into $\mathrm{GL}(nm, \mathbb{Z})$, we may assume without loss of generality that $G \leq \mathrm{GL}(n, \mathbb{Z})$.

(i) Suppose that G is abelian and $\mathbb{Q}$-irreducible. Then the enveloping algebra $\langle G\rangle_\mathbb{Q}$ is a number field of degree n over $\mathbb{Q}$. Moreover, G is contained in the unit group of the ring of integers of $\langle G\rangle_\mathbb{Q}$. Hence $\mathrm{rk}(G) \leq n$ by Dirichlet's Units Theorem [19, Theorem 12.6, p. 227].

(ii) If G is abelian and completely reducible over $\mathbb{Q}$, then [20, Lemma 4, p. 173] implies that G is conjugate to a group of block diagonal matrices $\{\mathrm{diag}(\mu_1(g), \ldots, \mu_k(g)) \mid g \in G\}$ where $\mu_i(G) \leq \mathrm{GL}(n_i, \mathbb{Z})$ is $\mathbb{Q}$-irreducible. Therefore, by (i),

$$\mathrm{rk}(G) \leq \textstyle\sum_{i=1}^k \mathrm{rk}(\mu_i(G)) = \sum_{i=1}^k n_i = n.$$

(iii) If G is UA then $\mathrm{rk}(G) \leq \frac{n(n-1)}{2} + n = n(n+1)/2$ by (ii) and Lemma 2.1.

(iv) By Remark 2.4, there is an odd prime p such that $\mathrm{h}(G) = \mathrm{rk}(G_\rho)$ and $\mathrm{rk}(G) \leq \mathrm{rk}(G_\rho) + \mathrm{rk}(\varphi_\rho(G))$ for $\rho = pR$. Thus $\mathrm{h}(G) \leq n(n+1)/2$. By [12], a finite completely reducible linear group of degree n can be generated by $\lfloor 3n/2 \rfloor$ elements. Since $\mathrm{rk}(\mathrm{UT}(n,p)) \leq n(n-1)/2$, we deduce that $\mathrm{rk}(\varphi_\rho(G)) \leq n(n+2)/2$. The stated bound on $\mathrm{rk}(G)$ follows. □

Remark 2.10. (i) If $n \geq 4$ then the bound on $\mathrm{rk}(G)$ in Proposition 2.9 can be improved using $\mathrm{rk}(\mathrm{GL}(n,p)) \leq \frac{n^2}{4} + 1$; see [15, p. 199].

(ii) $\mathrm{rk}(\mathrm{GL}(n,p)) \geq \lfloor n^2/4 \rfloor$ because $\mathrm{UT}(n,p)$ has an elementary abelian subgroup of order $p^{\lfloor n^2/4 \rfloor}$.

3. Subgroups of finite index

In this section we first derive a rank-based criterion to recognize when a subgroup of a finitely generated linear group of finite rank has finite index. Subsequently we prove a result about the unipotent radical that forms a key piece of our main algorithm.

3.1. **Ranks and isolators.** We recall some definitions from [13, pp. 83–86]. The *p-rank* (p prime) of an abelian group is the cardinality of a maximal $\mathbb{Z}_p$-linearly independent subset of elements of order p. A solvable group G has *finite abelian ranks* (G is a *solvable FAR group*) if there is a series of finite length in G with each factor abelian, and of finite torsion-free rank and finite p-rank for every prime p. A *minimax group* is a group that has a series of finite length whose factors satisfy either the maximal condition or the minimal condition on subgroups. The minimality $m(G)$ of a solvable minimax group G is the number of infinite factors in a series of G with each factor finite, cyclic, or quasicyclic. For finitely generated solvable groups, the notions of FAR, minimax, and finite Prüfer rank all coincide [13, pp. 175–176].

The following theorem and its proof were communicated to us by D.J.S. Robinson.

Theorem 3.1 (D.J.S. Robinson)**.** *Let H be a subgroup of a finitely generated solvable FAR group G. Then $|G : H|$ is finite if and only if* $\mathrm{h}(H) = \mathrm{h}(G)$.

Proof. The 'only if' direction being clear, assume that $\mathrm{h}(H) = \mathrm{h}(G)$. For $N \trianglelefteq G$,

$$\begin{aligned}\mathrm{h}(HN/N) &= \mathrm{h}(H) - \mathrm{h}(H \cap N)\\ &\geq \mathrm{h}(G) - \mathrm{h}(N) = \mathrm{h}(G/N).\end{aligned}$$

Thus $\mathrm{h}(HN/N) = \mathrm{h}(G/N)$. We prove that $|G : H|$ is finite by induction on $m(G)$. If $m(G) = 0$ then G is finite, so let $m(G) > 0$.

Denote the finite residual of G by D; this is a divisible periodic abelian group [13, 5.3.1, p. 96]. Suppose that $D \neq 1$. Then $m(G/D) < m(G)$, and by the inductive hypothesis $|G : HD|$ is finite. Hence HD is finitely generated, so $HD = HD_0$ where $D_0 \leq D$ is finitely generated, i.e., finite. This implies that $|HD : H|$ is finite, as is $|G : H|$.

Suppose now that $D = 1$. Then G has a non-trivial torsion-free abelian normal subgroup A (for example, the penultimate term in the derived series of a non-trivial torsion-free normal subgroup of G). Since $m(G/A) < m(G)$, by induction $|G : HA|$ is finite. Next, $H \cap A \neq 1$; otherwise $\mathrm{h}(H) = \mathrm{h}(HA/A) = \mathrm{h}(G/A) < \mathrm{h}(G)$. So the result holds for $HA/(H \cap A)$ and its subgroup $H/(H \cap A)$ by induction. Therefore $|HA : H|$ is finite, as is $|G : H|$. □

Remark 3.2. Finitely generated linear groups are residually finite [21, 4.2, p. 51], so for our algorithms we only need that part of the proof of Theorem 3.1 in which $D = 1$.

Corollary 3.3. *Let $H \leq G \leq \mathrm{GL}(n, \mathbb{F})$ where G is finitely generated and of finite Prüfer rank. Then $|G : H|$ is finite if and only if $\mathrm{h}(H) = \mathrm{h}(G)$.*

The *isolator* in G of a subgroup H is

$$I_G(H) = \{x \in G \mid x^k \in H \text{ for some positive integer } k\}.$$

Theorem 3.4. *Let G be a finitely generated SF group, and let $H \leq G$. Then $|G : H|$ is finite if and only if $I_G(H) = G$.*

Proof. See [13, 2.3.14, p. 45]. □

Lemma 3.5. *Suppose that G is a solvable FAR group with a finitely generated subgroup H such that $\mathrm{h}(H) = \mathrm{h}(G)$. Then $I_G(H) = G$.*

Proof. Since $\mathrm{h}(\langle g, H\rangle) = \mathrm{h}(H)$ for every $g \in G$, the lemma follows from Theorem 3.1. □

Lemma 3.6. *Suppose that G is a group of finite torsion-free rank, and H is a subgroup of G such that $I_G(H) = G$. Then $\mathrm{h}(G) = \mathrm{h}(H)$.*

We consider an illustrative example. Let $G \leq \mathrm{UT}(n, \mathbb{C})$ be an algebraic group defined over $\mathbb{Q}$, and set $G_S := G \cap \mathrm{GL}(n, S)$ for a subring S of $\mathbb{C}$. Recall that $L \leq G_{\mathbb{Q}}$ is an arithmetic subgroup of G if L is commensurable with $G_{\mathbb{Z}}$; i.e., $L \cap G_{\mathbb{Z}}$ has finite index in both L and $G_{\mathbb{Z}}$.

Lemma 3.7. *A finitely generated subgroup L of $G_{\mathbb{Q}}$ is an arithmetic subgroup of G if and only if $\mathrm{rk}(L) = \mathrm{rk}(G_{\mathbb{Q}})$.*

Proof. By [17, Lemma 6, p. 138], $H := L \cap G_{\mathbb{Z}}$ has finite index in L. Since L is polyrational and nilpotent, $\mathrm{rk}(H) = \mathrm{rk}(L)$ by Theorem 3.1. Similarly (as $G_{\mathbb{Z}}$ is finitely generated) $|G_{\mathbb{Z}} : H| < \infty$ if and only if $\mathrm{rk}(G_{\mathbb{Z}}) = \mathrm{rk}(H)$. Also, it is not difficult to verify that $G_{\mathbb{Q}} = I_{G_{\mathbb{Q}}}(G_{\mathbb{Z}})$. Hence $\mathrm{rk}(G_{\mathbb{Q}}) = \mathrm{rk}(G_{\mathbb{Z}})$ by Lemma 3.6. □

Remark 3.8. By Lemma 3.7 and [6, Corollary 7.2], if L is arithmetic in G then $\mathrm{h}(L)$ is the dimension of G as an algebraic group.

3.2. **Prüfer rank of a unipotent normal subgroup.** Let G be a finitely generated SF subgroup of $\mathrm{GL}(n, \mathbb{P})$. We show how to construct a finitely generated subgroup of $U(G)$ with the same Prüfer rank as $U(G)$.

Suppose that $G = \langle x_1, \ldots, x_r \rangle$, and let Y be a finite subset of $U(G)$. The normal closure $N = \langle Y \rangle^G$ is in $U(G)$. Define subgroups $H_1 \leq H_2 \leq \cdots$ of N as follows: let $H_1 = \langle Y \rangle$, and for $i \geq 1$, if $H_i = \langle y_{i1}, \ldots, y_{is_i} \rangle$ then

$$H_{i+1} = \langle y_{ij}, y_{ij}^{x_k}, y_{ij}^{x_k^{-1}} : 1 \leq j \leq s_i,\, 1 \leq k \leq r \rangle.$$

Since $\mathrm{rk}(H_i) \leq \mathrm{rk}(H_{i+1}) \leq \mathrm{rk}(N)$, there exists t such that $\mathrm{rk}(H_t) = \mathrm{rk}(H_{t+1})$.

Lemma 3.9. $\mathrm{rk}(H_t) = \mathrm{rk}(N)$.

Proof. By Lemma 3.5, $I_{H_{t+1}}(H_t) = H_{t+1}$. So for $1 \leq i \leq r$ and $1 \leq j \leq s_t$, there are positive integers $m_{ij}, \bar{m}_{ij}$ such that $(y_{tj}^{x_i})^{m_{ij}}$, $(y_{tj}^{x_i^{-1}})^{\bar{m}_{ij}} \in H_t$. We claim that $y_{tj}^{x} \in I_G(H_t)$ for all j and $x \in G$. First,

$$(y_{tj}^{x_v x_u^{\pm 1}})^{m_{vj}} = ((y_{tj}^{x_v})^{m_{vj}})^{x_u^{\pm 1}} \in H_{t+1}$$

since $H_i^{x_k^{\pm 1}} \leq H_{i+1}$. Similarly $(y_{tj}^{x_v^{-1} x_u^{\pm 1}})^{\bar{m}_{vj}} \in H_{t+1}$. Induction on the word length of x then establishes that $y_{tj}^{x} \in I_G(H_t)$ as claimed. Hence $N = H_1^G \leq H_t^G \subseteq I_G(H_t)$; i.e., $N = I_N(H_t)$. By Lemma 3.6, the proof is complete. ☐

4. COMPUTING RANKS OF SOLVABLE-BY-FINITE LINEAR GROUPS

Let $\mathcal{S}$ be a finite subset of $\mathrm{GL}(n, \mathbb{P})$ where $|\mathbb{P} : \mathbb{Q}| = m$, and let $G = \langle \mathcal{S} \rangle$. In this section we present algorithms to compute $\mathrm{h}(G)$ and a bound on $\mathrm{rk}(G)$. These lead directly to an algorithm that tests whether a finitely generated subgroup of G has finite index.

Proposition 2.6 allows us first to test whether G has finite Prüfer (and thereby torsion-free) rank: $\texttt{IsFiniteRank}(G)$ returns $\texttt{true}$ precisely when the procedure $\texttt{IsSolvableByFinite}(G)$ as in [7, p. 402] returns $\texttt{true}$. Henceforth G has finite rank.

4.1. **Auxiliary procedures.**

4.1.1. Suppose that G is abelian and irreducible. Methods to construct a presentation of G are reasonably standard; see [1, Chapter 4] for details. We can find the homogeneous components of G (e.g., by [16]), so the methods extend to completely reducible abelian G. For such input we have procedures (i) $\texttt{PresentationA}$, which returns a presentation of G; and (ii) $\texttt{RankA}$, which returns the torsion-free rank of G. Then $\mathrm{rk}(G) = \texttt{RankA}(G) + \varepsilon$ where $\varepsilon = 0$ if G is torsion-free and $\varepsilon = 1$ otherwise.

4.1.2. If $G \leq \mathrm{UT}(n, \mathbb{P})$ then G is isomorphic to a subgroup of $\mathrm{UT}(nm, \mathbb{Z})$ [17, Lemma 2, p. 111]. Since $\mathrm{UT}(nm, \mathbb{Z})$ is polycyclic, a constructive polycyclic sequence for G may be calculated as in [18, Chapter 9] or [1, Chapter 5]. From this one immediately reads off $\texttt{RankU}(G) := \mathrm{h}(G) = \mathrm{rk}(G)$.

4.2. **Completely reducible groups.** If G is completely reducible then G_ρ is completely reducible abelian and $\mathrm{h}(G) = \mathrm{h}(G_\rho)$. Thus $\mathtt{RankCR}(G) := \mathrm{h}(G) = \mathtt{RankA}(G_\rho)$ as per 4.1.1.

Now let $\mathbb{F}$ be arbitrary and $G \leq \mathrm{GL}(n, \mathbb{F})$ be finitely generated SF. In [7, Section 4] we show how to test whether G is completely reducible. Here we describe a more general procedure.

We refer to [7, Section 3.2]. The computations carried out in a run of $\mathtt{IsSolvableByFinite}(G)$ yield a change of basis matrix x such that G^x is block upper triangular and all diagonal blocks of G_ρ^x are abelian. Treating each diagonal block of G^x separately, assume that G_ρ is abelian. Let $M = \{h_1, \ldots, h_t\} = \mathtt{NormalGenerators}(G_\rho)$; i.e, $G_\rho = \langle M \rangle^G$. With a subscript '$u$' denoting unipotent part from a Jordan decomposition, $H = \langle (h_1)_u, \ldots, (h_t)_u \rangle = \langle M \rangle_u \leq (G_\rho)_u$. Set $U = \mathrm{Fix}((G_\rho)_u)$ and $W = \mathrm{Fix}(H)$. Since G normalizes $(G_\rho)_u$, we see that U is a G-module. We find U as follows.

(1) $\bar{W} := W$.
(2) While $\exists\, g_i \in \mathcal{S}$ such that $g_i \bar{W} \neq \bar{W}$
  $\bar{W} := g_i \bar{W} \cap \bar{W}$.
(3) Return $\bar{W}$.

Clearly $U \subseteq \bar{W}$. Let $v \in \bar{W}$ and $g \in G$; then $(h_i)_u^g v = g^{-1}(h_i)_u.gv = g^{-1}gv$ (because $gv \in \bar{W} \subseteq W$) $= v$. This shows that $\bar{W} = U$. By [20, Theorem 5, p. 172], U is completely reducible as a G_ρ-module. Therefore, if $\operatorname{char} \mathbb{F}$ does not divide $|G : G_\rho|$, then U is a completely reducible G-module by [20, Theorem 1, p. 122]. Repeat the previous computation after replacing the current underlying space V for G by V/U. Continuing in this fashion, we eventually produce a flag $V = V_1 \supset V_2 \supset \cdots \supset V_l \supset \{0\}$ of G-modules with each quotient V_i/V_{i+1} completely reducible.

We adopt the following notation in our pseudocode. For a matrix group H in block upper triangular form, μ denotes the projection of H onto its block diagonal, and μ_i is the projection onto its ith diagonal block. When all diagonal blocks are completely reducible, $\ker \mu = U(H)$ and $\mu(H)$ is a 'completely reducible part' of H.

$\mathtt{CompletelyReduciblePart}(G)$

Input: a finite subset $\mathcal{S}$ of $\mathrm{GL}(n, \mathbb{F})$ such that $\operatorname{char} \mathbb{F}$ does not divide $|G : G_\rho|$ and $G = \langle \mathcal{S} \rangle$ is SF.

Output: a generating set for a completely reducible part of G.

(1) Replace G by G^x in block upper triangular form with k diagonal blocks, where $\mu(G_\rho^x)$ is abelian.
(2) $M := \mathtt{NormalGenerators}(G_\rho)$.
(3) For $i = 1$ to k, determine x_i such that $\mu_i(G)^{x_i}$ is block upper triangular with completely reducible diagonal blocks, by the recursive calculation of fixed point spaces for $\langle \mu_i(M) \rangle_u$.
(4) Return $\mu(\mathcal{S}^y)$ where $y = x \cdot \mathrm{diag}(x_1, \ldots, x_k)$.

Remark 4.1. If G is nilpotent-by-finite then we can take $k = 1$, $\mu_1 = \mathrm{id}$, and omit Step (1).

We need one other procedure for completely reducible $G \leq \mathrm{GL}(n, \mathbb{P})$: $\mathtt{PresentationCR}(G)$ returns a presentation of G. This combines a presentation of $\varphi_\rho(G)$, computed using the machinery of [3], with $\mathtt{PresentationA}(G_\rho)$.

4.3. **The unipotent radical.** Our next procedure is based on Lemma 3.9 and its proof.

$\texttt{RankOfUnipotentRadical}(G)$

Input: a finite subset $\mathcal{S} = \{g_1, \ldots, g_r\}$ of $\mathrm{GL}(n, \mathbb{P})$ such that $G = \langle \mathcal{S} \rangle$ is SF.
Output: $\mathrm{h}(U(G)) = \mathrm{rk}(U(G))$.

(1) $\tilde{G} := \langle \texttt{CompletelyReduciblePart}(G) \rangle$.
(2) Find $X := \texttt{NormalGenerators}(U(G))$ from $\texttt{PresentationCR}(\tilde{G})$.
(3) While $\texttt{RankU}(\langle x, x^{g_i}, x^{g_i^{-1}} : x \in X, 1 \leq i \leq r \rangle) > \texttt{RankU}(\langle X \rangle)$ do
$X := \{x, x^{g_i}, x^{g_i^{-1}} : x \in X, 1 \leq i \leq r\}$.
(4) Return $\texttt{RankU}(\langle X \rangle)$.

Remark 4.2. The finitely generated subgroup $H = \langle X \rangle$ of $U(G)$ such that $\mathrm{rk}(H) = \mathrm{rk}(U(G))$ found at the end of Step (3) could be valuable in further computations with G.

4.4. **Algorithms for computing ranks, and an application.** Guided by Remark 2.4, we assemble our constituent procedures into the final algorithms.

$\texttt{HirschNumber}(G)$

Input: a finite subset $\mathcal{S}$ of $\mathrm{GL}(n, \mathbb{P})$ such that $G = \langle \mathcal{S} \rangle$ is SF.
Output: $\mathrm{h}(G)$.

Return $\texttt{RankCR}(\langle \texttt{CompletelyReduciblePart}(G) \rangle) + \texttt{RankUnipotentRadical}(G)$.

Then $\texttt{RankBound}(G) := \texttt{HirschNumber}(G) + \mathrm{rk}(\mathrm{GL}(nm, 3))$ is an upper bound on the Prüfer rank of G (see Remark 2.10).

Corollary 3.3 gives us the following.

$\texttt{IsOfFiniteIndex}(G, H)$

Input: finite subsets $\mathcal{S}_1$, $\mathcal{S}_2$ of $\mathrm{GL}(n, \mathbb{P})$ such that $G = \langle \mathcal{S}_1 \rangle$ is SF and $H = \langle \mathcal{S}_2 \rangle \leq G$.
Output: `true` if $|G : H|$ is finite; `false` otherwise.

Return `true` if $\texttt{HirschNumber}(G) = \texttt{HirschNumber}(H)$; else return `false`.

4.5. **The implementation.** We have implemented our algorithms as part of the MAGMA package INFINITE [9]. An algorithm of Biasse and Fieker [4] is used to work with irreducible abelian groups over number fields.

We report on several examples below (these will be available in a future release of INFINITE). Our experiments were performed on a 2GHz machine using MAGMA V2.19-6. The test groups are conjugated to ensure that generators are not sparse and matrix entries are large. Each time has been averaged over three runs. As observed in [7, 8], the single most expensive task is evaluating relators to obtain normal generators for the congruence subgroup.

(1) G_1 is an irreducible non-abelian subgroup of $\mathrm{GL}(2, \mathbb{Q}(i))$, $i = \sqrt{-1}$, and $G_2 \leq \mathrm{GL}(5, \mathbb{Q})$ is a solvable group from the database of maximal finite rational matrix groups [14]. Then $G_3 = G_1 \otimes G_2$ is a 5-generator AF completely reducible subgroup of $\mathrm{GL}(10, \mathbb{Q}(i))$. We compute $\mathrm{h}(G_3) = 3$ in 10s.

(2) $G_4 \leq G_3 \otimes \mathrm{UT}(3, \mathbb{Z})$ is a 15-generator, nilpotent-by-finite (NF), reducible but not completely reducible subgroup of $\mathrm{GL}(30, \mathbb{Q}(i))$. We compute $\mathrm{h}(G_4) = 6$ in 87s.
(3) $G_5 \leq H \otimes T$ where T is an upper triangular subgroup of $\mathrm{GL}(6, \mathbb{Q})$ and $H = \mathrm{diag}(H_1, H_2)$; H_1, H_2 are maximal finite rational matrix groups of degrees 4, 2 respectively. The 8-generator group G_5 is SF and not NF. We compute $\mathrm{h}(G_5) = 7$ in 1104s, and establish that a random 4-generator subgroup has infinite index in 163s.
(4) Let $a \in \mathrm{GL}(6, \mathbb{Q})$ be of the form $\mathrm{diag}(1, 2, \ldots)$ and let $b = \begin{pmatrix} x & y \\ 0 & u \end{pmatrix}$ where $x = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, y is a non-zero 2×4 matrix over $\mathbb{Q}$, and $u \in \mathrm{UT}(4, \mathbb{Z})$. Then $G_6 \leq \mathrm{GL}(6, \mathbb{Q}(\sqrt{5}))$ is conjugate to a group generated by a, b, another diagonal matrix and two other unipotent matrices in $\mathrm{GL}(6, \mathbb{Q})$. Note that G_6 is SF but not PF. We compute $\mathrm{h}(G_6) = 12$ in 18s.
(5) For each of G_3, G_4, G_6 we select random finitely generated non-cyclic subgroups $\hat{G}_j$. To establish that $\hat{G}_j$ has finite index in G_j takes 4s, 53s, and 17s respectively.

Acknowledgments. Detinko and Flannery were supported by Science Foundation Ireland grants 08/RFP/MTH1331 and 11/RFT.1/MTH/3212-STTF11. O'Brien was supported by the Marsden Fund of New Zealand grant UOA 1015. We are very grateful to D.J.S. Robinson for allowing us to include his proof of Theorem 3.1 in the paper.

REFERENCES

1. B. Assmann, *Polycyclic presentations for matrix groups*, Diplom thesis, Technische Universität Braunschweig, 2003.
2. ______, *Computing polycyclic presentations for polycyclic rational matrix groups*, J. Symbolic Comput. **40** (2005), no. 6, 1269–1284.
3. H. Bäärnhielm, D. F. Holt, C. R. Leedham-Green, and E.A. O'Brien, *A practical model for computation with matrix groups*, preprint (2011).
4. J.-F. Biasse and C. Fieker, *Improved techniques for computing the ideal class group and a system of fundamental units in number fields*, Proceedings of the Tenth Algorithmic Number Theory Symposium, University of California, San Diego, 2012 (to appear).
5. W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265.
6. W. A. de Graaf, A. Pavan, *Constructing arithmetic subgroups of unipotent groups*, J. Algebra **322** (2009), 3950–3970.
7. A. S. Detinko, D. L. Flannery, and E. A. O'Brien, *Algorithms for the Tits alternative and related problems*, J. Algebra **344** (2011), 397–406.
8. ______, *Recognizing finite matrix groups over infinite fields*, J. Symbolic Comput. **50** (2013), 100–109.
9. ______, `http://magma.maths.usyd.edu.au/magma/` (2011).
10. J. D. Dixon, *The orbit-stabilizer problem for linear groups*, Canad. J. Math. **37** (1985), no. 2, 238–259.
11. V. M. Kopytov, *Matrix groups*, Algebra i Logika **7** (1968), no. 3, 51–59.
12. L. G. Kovács and G. R. Robinson, *Generating finite completely reducible linear groups*, Proc. Amer. Math. Soc., **112** (1991), no. 2, 357–364.
13. J. C. Lennox and D. J. S. Robinson, *The theory of infinite soluble groups*, Oxford Mathematical Monographs, The Clarendon Press Oxford University Press, Oxford, 2004.
14. G. Nebe and W. Plesken, *Finite rational matrix groups*, Mem. Amer. Math. Soc. **116** (1995), no. 556.
15. L. Pyber, *Asymptotic results for permutation groups*, Groups and computation (New Brunswick, NJ, 1991), DIMACS Ser. Discrete Math. Theoret. Comput. Sci., vol. 11, Amer. Math. Soc., Providence, RI, 1993, pp. 197–219.
16. L. Rónyai, *Computations in associative algebras*, DIMACS Series in Discrete Mathematics, vol. 11, pp. 221–243, 1993.
17. D. Segal, *Polycyclic groups*, Cambridge University Press, Cambridge, 1983.

18. C. C. Sims, *Computation with finitely presented groups*, Encyclopedia of Mathematics and its Applications, vol. 48, Cambridge University Press, Cambridge, 1994.
19. I. N. Stewart and D. O. Tall, *Algebraic number theory*, Chapman and Hall, London, 1987.
20. D. A. Suprunenko, *Matrix groups*, Transl. Math. Monogr., vol. 45, American Mathematical Society, Providence, RI, 1976.
21. B. A. F. Wehrfritz, *Infinite linear groups*, Springer-Verlag, New York, 1973.