Journal of Symbolic Computation 68 (2015) 138–145

Contents lists available at ScienceDirect

Journal of Symbolic Computation

www.elsevier.com/locate/jsc

Integrality and arithmeticity of solvable linear groups ☆

A.S. Detinko [a], D.L. Flannery [a], W.A. de Graaf [b]

[a] Department of Mathematics, National University of Ireland, Galway, Ireland
[b] Department of Mathematics, University of Trento, Italy

ARTICLE INFO

Article history:
Received 25 October 2013
Accepted 10 March 2014
Available online 11 August 2014

Keywords:
Arithmetic group
Algorithm
Algebraic group
Lattice

ABSTRACT

We develop a practical algorithm to decide whether a finitely generated subgroup of a solvable algebraic group G is arithmetic. This incorporates a procedure to compute a generating set of an arithmetic subgroup of G. We also provide a simple new algorithm for integrality testing of finitely generated solvable-by-finite linear groups over the rational field. The algorithms have been implemented in MAGMA.

1. Introduction

For $K \leq \mathrm{GL}(n, \mathbb{C})$ and a subring R of $\mathbb{C}$, denote $K \cap \mathrm{GL}(n, R)$ by K_R. Let G be an algebraic group defined over $\mathbb{Q}$. This paper is concerned with the question:

Given a finitely generated subgroup H of $G_{\mathbb{Q}}$, is H an arithmetic subgroup of G? $(*)$

Recall that $H \leq G_{\mathbb{Q}}$ is an arithmetic subgroup of G if it is commensurable with $G_{\mathbb{Z}}$, i.e., $H \cap G_{\mathbb{Z}} = H_{\mathbb{Z}}$ has finite index in both H and $G_{\mathbb{Z}}$. (More generally, a matrix group is said to be arithmetic if it is an arithmetic subgroup of some algebraic $\mathbb{Q}$-group (Segal, 1983, p. 119).) The significance of $(*)$ is evidenced by, e.g., Sarnak (2012). Decidability of $(*)$ has not been settled. However, it seems to be undecidable, even for $G = \mathrm{SL}(n, \mathbb{C})$ (Miller, 2013). We prove that $(*)$ is decidable *when G is solvable*, by giving a practical algorithm to answer this question.

☆ The authors were supported by Science Foundation Ireland grant 11/RFP.1/MTH3212.
E-mail addresses: alla.detinko@nuigalway.ie (A.S. Detinko), dane.flannery@nuigalway.ie (D.L. Flannery), degraaf@science.unitn.it (W.A. de Graaf).

http://dx.doi.org/10.1016/j.jsc.2014.08.011
0747-7171/

As further motivation for arithmeticity testing we observe that a positive answer enables the use of arithmetic group theory to investigate the group at hand. For example, the automorphism group of a finitely generated nilpotent group is isomorphic to an arithmetic group (Segal, 1983, Corollary 9, p. 122). There are polycyclic groups that are not isomorphic to any arithmetic group (Segal, 1983, Proposition 3, p. 259). Although we can test whether a polycyclic subgroup of $G_{\mathbb{Q}}$ is arithmetic, testing arithmeticity of polycyclic groups in this broader context is still open.

Our approach draws on recent progress (de Graaf and Pavan, 2009; Faccin et al., 2013) in the construction of generating sets of $G_{\mathbb{Z}}$ when G is unipotent or a torus. We combine those to construct a finite index subgroup of $G_{\mathbb{Z}}$ for a solvable algebraic group G—a result of interest in its own right.

We adapt methods for computing with SF (solvable-by-finite) linear groups (Detinko et al., 2011, 2013a, 2013b). To decide whether H is commensurable with $G_{\mathbb{Z}}$, we use an algorithm from Detinko et al. (2013b) to compute the rank of an SF linear group. We also design a simple new algorithm to test whether a finitely generated SF subgroup of $\mathrm{GL}(n,\mathbb{Q})$ is conjugate to a subgroup of $\mathrm{GL}(n,\mathbb{Z})$. Since integrality is an important linear group property (Dixon, 1971, Theorem 3.5, pp. 54–55), this is another useful result of the paper. Integrality testing appears as a component of earlier algorithms to test finiteness (Babai et al., 1993) and polycyclicity (Assmann and Eick, 2007).

The paper is organized as follows. Section 2 gives a procedure to construct a generating set of a finite index subgroup of $G_{\mathbb{Z}}$, where G is solvable algebraic. In Section 3 we consider testing finiteness of $|K : K_{\mathbb{Z}}|$ for $K \leq \mathrm{GL}(n,\mathbb{Q})$. If this index is finite, we explain how to find $K_{\mathbb{Z}}$ and $g \in \mathrm{GL}(n,\mathbb{Q})$ such that $K^g \leq \mathrm{GL}(n,\mathbb{Z})$. Section 4 then describes a new algorithm to test integrality of SF subgroups of $\mathrm{GL}(n,\mathbb{Q})$. Our main algorithm is presented in Section 5. A discussion of experimental results derived from a MAGMA (Bosma et al., 1997) implementation of the algorithms concludes the paper.

2. Computing an arithmetic subgroup of a solvable algebraic group

Let G be a solvable algebraic $\mathbb{Q}$-group. In this section we combine results from de Graaf and Pavan (2009) and Faccin et al. (2013) to construct a generating set of a finite index subgroup of $G_{\mathbb{Z}}$.

The first result is Vinberg et al. (2000, Proposition 7.2(3)).

Proposition 2.1. *Suppose that $G = A \ltimes N$, where both A and N are algebraic subgroups of G, defined over $\mathbb{Q}$. Let Γ_A, Γ_N be arithmetic subgroups of A and N respectively. Then $\Gamma_A \ltimes \Gamma_N$ is an arithmetic subgroup of G.*

From Chevalley (1955, Ch. 5, §3, No. 5, Propositions 20 and 21) we get the following.

Proposition 2.2. *Let G be connected and solvable, with Lie algebra $\mathfrak{g} \subset \mathfrak{gl}(n,\mathbb{C})$. Let $\mathfrak{n}$ be the ideal of $\mathfrak{g}$ consisting of all nilpotent elements of $\mathfrak{g}$. Then there is a subalgebra $\mathfrak{d}$ of $\mathfrak{g}$, consisting of commuting semisimple elements, such that $\mathfrak{g} = \mathfrak{d} \oplus \mathfrak{n}$. Moreover, both $\mathfrak{n}$, $\mathfrak{d}$ are algebraic, and if we let N, D be the corresponding connected subgroups of G, then $G = D \ltimes N$.*

Let G, $\mathfrak{g}$ be as in Proposition 2.2. We suppose that $\mathfrak{g}$ is given by a basis consisting of matrices having entries in $\mathbb{Q}$. In de Graaf (2009), an algorithm that computes bases of subalgebras $\mathfrak{d}$, $\mathfrak{n}$ with the properties of Proposition 2.2 is given. Here we do not go into the details but only briefly recall the basic steps.

1. Compute a Cartan subalgebra $\mathfrak{h}$ of $\mathfrak{g}$.
2. Let $a_1, \ldots, a_r$ be a basis of $\mathfrak{h}$, and let $a_i = s_i + n_i$ be the Jordan decomposition of a_i.
3. Let $\mathfrak{d}$ be the space spanned by $s_1, \ldots, s_r$ and let $\mathfrak{n}$ be the space spanned by $n_1, \ldots, n_r$ along with the Fitting 1-component $\mathfrak{g}_1(\mathfrak{h})$. (The latter is the space $\bigcap_{i\geq 1}[\mathfrak{h}^i, \mathfrak{g}]$, where $[\mathfrak{h}^i, \mathfrak{g}] = [\mathfrak{h}, [\mathfrak{h}, \ldots, [\mathfrak{h}, \mathfrak{g}]\ldots]]$ (i factors $\mathfrak{h}$).)

Starting from the given basis of $\mathfrak{g}$, we compute generators of an arithmetic group in $G_{\mathbb{Z}}$ by the following.

`GeneratingArithmetic`(G)

Input: a basis of the Lie algebra $\mathfrak{g}$ of the solvable algebraic group G.
Output: a generating set for a finite index subgroup of $G_{\mathbb{Z}}$.

1. Compute bases of $\mathfrak{d}$ and $\mathfrak{n}$ as above. Denote by D, N the connected subgroups of G with respective Lie algebras $\mathfrak{d}$, $\mathfrak{n}$.
2. Compute generators of $N_{\mathbb{Z}}$ using the algorithm from de Graaf and Pavan (2009), and generators of $D_{\mathbb{Z}}$ using the algorithm from Faccin et al. (2013). (These algorithms take as input bases of $\mathfrak{d}$ and $\mathfrak{n}$ respectively.)
3. Return the union of the two generating sets obtained in the previous step.

We note that `GeneratingArithmetic` is correct. Indeed, let H be the group generated by its output. Then $H \leq G_{\mathbb{Z}}$. On the other hand, H is an arithmetic subgroup of G by Proposition 2.1. So H has finite index in $G_{\mathbb{Z}}$.

`GeneratingArithmetic`(G) forms a vital part of our main algorithm. Notice that G need not be connected. Indeed, let G° be the connected component of the identity of G. Since $|G_{\mathbb{Z}} : G^\circ_{\mathbb{Z}}|$ is finite, `GeneratingArithmetic`(G°) returns a generating set of an arithmetic subgroup of G.

3. Integrality and GL($n, \mathbb{Z}$)-intercepts

This section and the next depend on some ideas from Babai et al. (1993).

An element or subgroup of $\mathrm{GL}(n, \mathbb{Q})$ that has a conjugate in $\mathrm{GL}(n, \mathbb{Z})$ is said to be *integral*. Let $H \leq \mathrm{GL}(n, \mathbb{Q})$.

Lemma 3.1. *(See Babai et al., 1993, Proposition 2.3.) H is integral if and only if there exists a positive integer d such that $dh \in \mathrm{Mat}(n, \mathbb{Z})$ for all $h \in H$.*

Proof. Suppose that $H^g \leq \mathrm{GL}(n, \mathbb{Z})$ for some $g \in \mathrm{GL}(n, \mathbb{Q})$. Then $m^2 H \subseteq \mathrm{Mat}(n, \mathbb{Z})$ where m is any common multiple of the denominators of the entries in g and g^{-1}.

Suppose that $dH \subseteq \mathrm{Mat}(n, \mathbb{Z})$. Let g be any matrix whose columns comprise a $\mathbb{Z}$-basis of the lattice generated by $dH\mathbb{Z}^n$. Then $g \in \mathrm{GL}(n, \mathbb{Q})$ and $H^g \leq \mathrm{GL}(n, \mathbb{Z})$.

Call $d = d(H)$ as in Lemma 3.1 a *common denominator* for H. As the above proof demonstrates, knowing $d(H)$ is equivalent to knowing $g \in \mathrm{GL}(n, \mathbb{Q})$ such that $H^g \leq \mathrm{GL}(n, \mathbb{Z})$. A method to construct d may be extracted from Babai et al. (1993, Section 2); we give an algorithm that is a modification of this for our purposes in Section 4. If H is finitely generated then we calculate g from d by means of the following (cf. Babai et al., 1993, Section 3).

`BasisLattice`(S, d)

Input: a finite set $S \subseteq \mathrm{GL}(n, \mathbb{Q})$ and $d = d(H)$, $H = \langle S \rangle$.
Output: a basis for the lattice generated by $dH\mathbb{Z}^n$ in $\mathbb{Z}^n$.

1. $\mathcal{L} := d\mathbb{Z}^n$.
2. While $\exists h \in S \cup S^{-1}$ such that $h\mathcal{L} \nsubseteq \mathcal{L}$ do

   $\mathcal{L} :=$ the lattice generated by $\mathcal{L} \cup h\mathcal{L}$.

3. Return a basis of $\mathcal{L}$.

We write $L \leq_f H$ to indicate that the subgroup L has finite index in H.

Lemma 3.2. *Let $H_1 \leq_f H$. Then H is integral if and only if H_1 is integral.*

Proof. Suppose that H_1 is integral. By Lemma 3.1, $d_1 H_1 \subseteq \mathrm{Mat}(n, \mathbb{Z})$ for some $d_1 \in \mathbb{Z}$. Choose a transversal $\{h_1, \ldots, h_r\}$ for the cosets of H_1 in H, and let d_2 be a positive integer such that $d_2 h_i \in \mathrm{Mat}(n, \mathbb{Z})$ for all i. Since $d_1 d_2 H \subseteq \mathrm{Mat}(n, \mathbb{Z})$, H is integral by Lemma 3.1 again.

Lemma 3.3. *Suppose that d is a common denominator for H, and let $\mathcal{L}$ be the lattice generated by $dH\mathbb{Z}^n$.*

(i) $\mathcal{L} \subseteq \mathbb{Z}^n \subseteq \frac{1}{d}\mathcal{L}$.
(ii) *H acts by left multiplication on the (finite) set of lattices lying between $\mathcal{L}$ and $\frac{1}{d}\mathcal{L}$.*
(iii) *$H_{\mathbb{Z}}$ is the stabilizer of $\mathbb{Z}^n$ under the action in* (ii).

Proof. (i) Clear: $dH \subseteq \mathrm{Mat}(n, \mathbb{Z})$ and $d\mathbb{Z}^n \subseteq dH\mathbb{Z}^n \subseteq \mathcal{L}$.
(ii) We have $H\mathcal{L} = \mathcal{L}$. Thus H acts on the set of lattices $\mathcal{L}'$ such that $\mathcal{L} \subseteq \mathcal{L}' \subseteq \frac{1}{d}\mathcal{L}$.
(iii) Let $h \in H$. If $h \in H_{\mathbb{Z}}$ then $\mathbb{Z}^n = h(h^{-1}\mathbb{Z}^n) \subseteq h\mathbb{Z}^n$, so $h\mathbb{Z}^n = \mathbb{Z}^n$. Conversely, if $h\mathbb{Z}^n = \mathbb{Z}^n$ then every entry in h is an integer.

Proposition 3.4. *H is integral if and only if $H_{\mathbb{Z}} \leq_f H$.*

Proof. This is a consequence of Lemmas 3.2 and 3.3.

The following procedure constructs $H_{\mathbb{Z}}$ if H is finitely generated and $d(H)$ is known.

`IntegralIntercept`(S, d)
Input: a finite set $S \subseteq \mathrm{GL}(n, \mathbb{Q})$ and $d = d(H)$, $H = \langle S \rangle$.
Output: a generating set of $H_{\mathbb{Z}}$.

1. $\mathcal{L} :=$ the lattice generated by `BasisLattice`(S, d).
2. $\Lambda :=$ the set of all lattices $\mathcal{L}'$ such that $\mathcal{L} \subseteq \mathcal{L}' \subseteq \frac{1}{d}\mathcal{L}$.
3. Return a generating set for the stabilizer of $\mathbb{Z}^n$ under the action of H on Λ.

Remark 3.5. Step (3) may be carried out using standard algorithms for finite permutation groups to obtain a transversal for $H_{\mathbb{Z}}$ in H, then writing down Schreier generators. More practical approaches are possible in special situations; say for polycyclic H (e.g., arithmetic $H \leq G_{\mathbb{Q}}$ and solvable G). In that case an algorithm can be based on an orbit-stabilizer approach. This is similar to the algorithm described in Laue et al. (1984). Such an algorithm enumerates the orbit of $\mathbb{Z}^n$ under action by H, in the process obtaining generators of the stabilizer. The efficiency of this approach depends heavily on orbit size.

4. Integrality of solvable-by-finite subgroups of GL$(n, \mathbb{Q})$

We next describe how to test integrality of a finitely generated SF subgroup of $\mathrm{GL}(n, \mathbb{Q})$, and compute a common denominator if the group is integral.

Let $H = \langle h_1, \ldots, h_r \rangle \leq \mathrm{GL}(n, \mathbb{Q})$. We have $H \leq \mathrm{GL}(n, R)$ where $R = \frac{1}{b}\mathbb{Z} = \{a/b^i \mid a \in \mathbb{Z},\ i \geq 0\}$ for some positive integer b determined by the entries in the h_i and h_i^{-1}. For any prime $p \in \mathbb{Z}$ not dividing b, reduction modulo p of matrix entries defines a congruence homomorphism $\varphi_p : \mathrm{GL}(n, R) \to \mathrm{GL}(n, p)$. If H is SF and $p \neq 2$ then $H_p = \ker \varphi_p \cap H$ is torsion-free and unipotent-by-abelian (see Dixon, 1985, Lemma 9, or Detinko et al., 2011, Section 2.2.1). Assume that p has been so chosen whenever H is SF.

Denote the unipotent radical of $K \leq \mathrm{GL}(n, \mathbb{Q})$ by $U(K)$. Replace K if necessary by a conjugate in block triangular form with completely reducible diagonal blocks. If π denotes projection of K onto the block diagonal then $U(K) = \ker \pi$.

Lemma 4.1. *The following are equivalent.*

(i) H *is integral.*
(ii) $\pi(H)$ *is integral.*
(iii) $\pi(H_p)$ *is integral.*

Proof. By Babai et al. (1993, Theorem 2.4), a finitely generated subgroup K of $\mathrm{GL}(n,\mathbb{Q})$ is integral if and only if $\{\mathrm{tr}(x) \mid x \in K\} \subseteq \mathbb{Z}$. Thus (i) $\Leftrightarrow$ (ii). Since $|\pi(H) : \pi(H_p)| = |H : H_p U(H)| < \infty$, Lemma 3.2 gives (ii) $\Leftrightarrow$ (iii).

Denote the characteristic polynomial of $h \in \mathrm{GL}(n,\mathbb{C})$ by $\chi_h(X)$.

Proposition 4.2. *(Cf. Lemma 8 and Theorem 9 of Assmann and Eick, 2007.) Suppose that each element of H is equal to $h_1^{m_1} \cdots h_r^{m_r}$ for some $m_i \in \mathbb{Z}$. Then H is integral if and only if each h_i is integral, i.e., $\chi_{h_i}(X) \in \mathbb{Z}[X]$ and $\det(h_i) = \pm 1$ for $1 \le i \le r$.*

Proof. If $\chi_{h_i}(X) \in \mathbb{Z}[X]$ has constant term ± 1 for all i then $\langle h_i \rangle \subseteq \{\sum_{j=0}^{n-1} a_j h_i^j \mid a_j \in \mathbb{Z}\}$. So there exist positive integers d_i, $1 \le i \le r$, such that $d_i \langle h_i \rangle \subseteq \mathrm{Mat}(n,\mathbb{Z})$. Hence $d = d_1 \cdots d_r$ is a common denominator for H.

If H is polycyclic with polycyclic sequence $(h_1, \ldots, h_r)$, then H satisfies the hypothesis of Proposition 4.2. Any generating set of H is similarly suitable when H is abelian.

Lemma 4.3. *Suppose that $H \le K \le \mathrm{GL}(n,\mathbb{Q})$ and the normal closure H^K is finitely generated abelian. Then H^K is integral if and only if each h_i is integral.*

Proof. If the h_i are integral then Proposition 4.2 guarantees that H is integral. Since H^K is finitely generated, there are $x_1, \ldots, x_t \in H$ and $y_1, \ldots, y_t \in K$ such that $H^K = \langle x_i^{y_i} : 1 \le i \le t \rangle$. By Proposition 4.2 again, H^K is integral.

Lemma 4.4. *Suppose that H is SF and Y is a normal generating set for H_p ($p \neq 2$), i.e., $H_p = \langle Y \rangle^H$. Then H is integral if and only if each element of Y is integral.*

Proof. If each element of Y is integral then the same holds for $\pi(Y)$. Hence the finitely generated abelian group $\pi(H_p) = \langle \pi(Y) \rangle^{\pi(H)}$ is integral by Lemma 4.3. The claim now follows from Lemma 4.1.

We compute Y from a presentation $\mathcal{P}$ of $\varphi_p(H) \le \mathrm{GL}(n,p)$ on $\varphi_p(h_1), \ldots, \varphi_p(h_r)$ using the function `NormalGenerators` as in Detinko et al. (2011, Section 3.2): this evaluates the relators of $\mathcal{P}$, replacing $\varphi_p(h_i)$ everywhere by h_i, $1 \le i \le r$. Proposition 4.2 and Lemma 4.4 consequently provide our straightforward procedure to test integrality of H.

`IsIntegralSF`(S)
Input: a finite subset S of $\mathrm{GL}(n,\mathbb{Q})$ such that $H = \langle S \rangle$ is SF.
Output: `true` if H is integral; `false` otherwise.

1. $Y :=$ `NormalGenerators`(S).
2. If every element of Y is integral then return `true`;
   else return `false`.

Remark 4.5. When H is finite we have $H_p = 1$, so `IsIntegralSF` always returns `true` for such input.

A major class of SF groups is PF (polycyclic-by-finite) groups. According to Assmann and Eick (2007, Corollary 10), one may test integrality of a PF subgroup H of $\mathrm{GL}(n,\mathbb{Q})$ after computing a polycyclic sequence and transversal for a finite index polycyclic normal subgroup of H. By contrast, `IsIntegralSF` does not require H to be PF and just tests integrality of several matrices in H_p.

To conjugate an integral SF group H into $\mathrm{GL}(n,\mathbb{Z})$, or to compute generators of its finite index subgroup $H_{\mathbb{Z}}$ via `IntegralIntercept`, we must know $d(H)$. The method below to find this common denominator is a simplification of Babai et al. (1993, p. 120) for SF input.

First determine a block upper triangular conjugate of H with completely reducible diagonal blocks; this may be done as in Detinko et al. (2013b, Section 4.2). Let $\{a_1,\dots,a_m\} \subseteq \pi(H)$ be a basis of the enveloping algebra $\langle \pi(H)\rangle_{\mathbb{Q}}$. If c is a common multiple of the denominators of entries in the a_i then $d_1 := c\det([\mathrm{tr}(a_i a_j)]_{1\le i,j\le n}) = d(\pi(H))$. Define $u_i = h_i - \pi(h_i)$ and $v_i = h_i^{-1} - \pi(h_i^{-1})$. Let $d_2 = e^{n-1}$ where e is a common multiple of denominators of entries in the u_i and v_i. Each element of H is a sum of terms $x = \pi(g_1)w_1\cdots\pi(g_k)w_k$ where $g_j \in H$ and $w_j = 1$ or some u_i or v_i. Since $\pi(h)u_j$ and $\pi(h)v_j$ are nilpotent, if there are at least n occurrences of u_js and v_js in x then $x = 0$. Thus $dH \subseteq \mathrm{Mat}(n,\mathbb{Z})$ where $d = d_1^n d_2$. Note that for completely reducible H (e.g., H is finite), $d(H) = d(\pi(H)) = d_1$.

5. Arithmeticity testing in solvable algebraic groups

In this section we apply results of Detinko et al. (2013b) and the previous sections to test whether a finitely generated subgroup $H \le G_{\mathbb{Q}}$ of a solvable algebraic group G is arithmetic.

Denote the Hirsch number of a group K with finite torsion-free rank by $\mathrm{h}(K)$. Finitely generated SF subgroups of $\mathrm{GL}(n,\mathbb{Q})$ have finite torsion-free rank (Detinko et al., 2013b, Proposition 2.6).

Lemma 5.1. *Let L be a finitely generated SF subgroup of $\mathrm{GL}(n,\mathbb{Q})$, and let $K \le L$. Then $K \le_f L$ if and only if $\mathrm{h}(K) = \mathrm{h}(L)$.*

Proof. This follows from Proposition 2.3 and Corollary 3.3 of Detinko et al. (2013b).

Corollary 5.2. *H is an arithmetic subgroup of G if and only if H is integral and $\mathrm{h}(H) = \mathrm{h}(G_{\mathbb{Z}})$. In particular, $H \le G_{\mathbb{Z}}$ is arithmetic if and only if $\mathrm{h}(H) = \mathrm{h}(G_{\mathbb{Z}})$.*

Proof. This is immediate from Proposition 3.4 and Lemma 5.1, using that $\mathrm{h}(H) = \mathrm{h}(H_{\mathbb{Z}})$ when $H_{\mathbb{Z}} \le_f H$.

Remark 5.3. If G is a unipotent $\mathbb{Q}$-group then we have a more general statement (Detinko et al., 2013b, Lemma 3.7): $H \le G_{\mathbb{Q}}$ is arithmetic in G if and only if $\mathrm{h}(H) = \mathrm{h}(G_{\mathbb{Q}})$, i.e., $\mathrm{h}(H)$ equals the dimension of G. For non-unipotent solvable (even abelian) G this is not true; $G_{\mathbb{Q}}$ need not even have finite rank.

We now state our arithmeticity testing algorithm. This uses the procedure `HirschNumber` from Detinko et al. (2013b, Section 4.4), which returns $\mathrm{h}(K)$ for a finitely generated SF subgroup K of $\mathrm{GL}(n,\mathbb{Q})$.

`IsArithmeticSolvable`(S, G)

Input: a finite subset S of $G_{\mathbb{Q}}$, G a solvable algebraic group.
Output: `true` if $H = \langle S\rangle$ is arithmetic; `false` otherwise.

1. If `IsIntegralSF`$(S) =$ `false` then return `false`.
2. $T :=$ `GeneratingArithmetic`(G).
3. If `HirschNumber`$(S) \ne$ `HirschNumber`(T) then return `false`;
   else return `true`.

Table 1
Running times (in seconds) of the steps in `IsArithmeticSolvable`.

n	$\dim \mathfrak{g}(n)$	$\mathrm{h}(\widetilde{G}(n)_{\mathbb{Z}})$	`IsInt`(S)	$T :=$ `GA`$(\widetilde{G}(n))$	$\mathrm{h}(\langle S\rangle)$	$\mathrm{h}(\langle T\rangle)$
2	6	5	0.12	0.05	0.51	0.68
3	15	14	0.29	0.19	2.10	2.28
4	28	27	0.86	1.12	11.28	12.77

Remark 5.4. Steps (1) and (3) are justified by Corollary 5.2. If G is unipotent then H is integral (Segal, 1983, Lemma 2, p. 111), and step (1) can be omitted.

6. Practical performance

We have implemented our algorithms in Magma. The implementation relies on the package 'Infinite' (Detinko et al., 2013c) and procedures available at de Graaf (2013). Although the main goal has been to establish that arithmeticity is decidable, in this section we show that our algorithms can be applied in practice to nontrivial examples.

One of the main bottlenecks of `GeneratingArithmetic` lies in the computation of the torus part. Let $\mathfrak{g} = \mathfrak{d} \oplus \mathfrak{n}$ and D be as in Proposition 2.2. The first step of the algorithm given in Faccin et al. (2013) for computing generators of $D_{\mathbb{Z}}$ constructs the associative algebra A with unity generated by $\mathfrak{d}$. Subsequently A is written as a direct sum of number fields $\mathbb{Q}(\alpha)$. For each such field, generators of the unit group of $\mathbb{Z}[\alpha]$ are computed. But the algorithm for this task (as implemented in Magma) becomes extremely difficult to apply in practice if the degree of $\mathbb{Q}(\alpha)$ is too large, say 30 or more. On the other hand, if all fields that occur are equal to $\mathbb{Q}$ then the computation of generators of $D_{\mathbb{Z}}$ is trivial. For these reasons we constructed test examples where the field extensions have degree ≤ 2 (and some extensions of degree 2 do occur). This construction works as follows. First we define a Lie algebra $\mathfrak{g}(n) \subset \mathfrak{gl}(2n, \mathbb{C})$, $n \geq 2$. For this we divide the matrices of $\mathfrak{gl}(2n, \mathbb{C})$ into 2×2 blocks. Our Lie algebra $\mathfrak{g}(n)$ is the direct sum $\mathfrak{g}(n) = \mathfrak{t} \oplus \mathfrak{n}$ of two subalgebras. The subalgebra $\mathfrak{t}$ has dimension n, and the ith basis element has on its ith diagonal block the matrix

$$\begin{pmatrix} 0 & 1 \\ 2i-1 & 0 \end{pmatrix}$$

and zeros elsewhere.

Let $e_{i,j}$ be the elementary matrix with 1 in position (i, j) and zeros elsewhere. Then $\mathfrak{n}$ is spanned by the $e_{i,j}$ where (i, j) appears in a block above the diagonal. So $\dim \mathfrak{n} = 4\binom{n}{2}$.

The Lie algebra $\mathfrak{g}(n)$ is algebraic, and we let $G(n) < \mathrm{GL}(2n, \mathbb{C})$ be the connected algebraic group with Lie algebra $\mathfrak{g}(n)$.

Now let m be a $2n \times 2n$ matrix produced by the following randomized construction. The entries of m are randomly and uniformly chosen from $(0, 0, 1)$ (so we make it twice as likely that a 0 is chosen). We continue to produce matrices like this until the determinant is not 0 or ± 1.

Set $\widetilde{G}(n) = mG(n)m^{-1}$. This is an algebraic group with Lie algebra $m\mathfrak{g}(n)m^{-1}$. The Lie algebra has basis B_n consisting of all mum^{-1}, for u in the above constructed basis of $\mathfrak{g}(n)$. Let $g_1, \ldots, g_r$ be generators of an arithmetic subgroup of $G(n)_{\mathbb{Z}}$. For $1 \leq i \leq r$ let k_i be chosen randomly and uniformly from $\{1, 2\}$. Then $S = \{(mg_im^{-1})^{k_i} \mid 1 \leq i \leq r\}$ generates a subgroup of $\widetilde{G}(n)_{\mathbb{Q}}$ (and note that it always is arithmetic). The input on which we tested our implementation of `IsArithmeticSolvable` is the set S, together with the algebraic group $\widetilde{G}(n)$ given by its Lie algebra, in turn given by its basis B_n.

In Table 1 we report on the running times of our algorithm with the input as above for $n = 2, 3, 4$. All experiments were performed on a 3.16 GHz machine running Magma V2.19-9. The first three columns of Table 1 list n, $\dim \mathfrak{g}(n)$, and the Hirsch number of $\widetilde{G}(n)_{\mathbb{Z}}$. The other columns list running times of `IsIntegralSF`(S), $T :=$ `GeneratingArithmetic`$(\widetilde{G}(n))$, `HirschNumber`(S) and `HirschNumber`(T).

From Table 1 we see that our algorithm is efficient enough to handle quite nontrivial examples. Moreover, the bulk of the running time goes into computing Hirsch numbers. Of course, this depends on our particular test example. If we took examples where it is difficult to compute generators of $D_{\mathbb{Z}}$,

then a much larger proportion of the time would go into computing an arithmetic subgroup. However, the current implementation is rather sensitive to randomness of the input. Occasionally it happens that generators in T have coefficients with many digits (up to 10, for example). This then causes problems when computing the Hirsch number. So we have averaged times over 50 runs in order to dampen the effects of randomness of the input.

References

Assmann, B., Eick, B., 2007. Testing polycyclicity of finitely generated rational matrix groups. Math. Comput. 76, 1669–1682.
Babai, L., Beals, R., Rockmore, D.N., 1993. Deciding finiteness of matrix groups in deterministic polynomial time. In: Proc. of International Symposium on Symbolic and Algebraic Computation. ISSAC '93. ACM Press, pp. 117–126.
Bosma, W., Cannon, J., Playoust, C., 1997. The Magma algebra system. I. The user language. J. Symb. Comput. 24 (3–4), 235–265.
Chevalley, C., 1955. Théorie des Groupes de Lie, Tome III. Théorèmes généraux sur les algèbres de Lie. Hermann, Paris.
de Graaf, W., 2009. Constructing algebraic groups from their Lie algebras. J. Symb. Comput. 44, 1223–1233.
de Graaf, W., 2013. http://www.science.unitn.it/~degraaf/arith/arithgrp.m.
de Graaf, W., Pavan, A., 2009. Constructing arithmetic subgroups of unipotent groups. J. Algebra 322, 3950–3970.
Detinko, A.S., Flannery, D.L., O'Brien, E.A., 2011. Algorithms for the Tits alternative and related problems. J. Algebra 344, 397–406.
Detinko, A.S., Flannery, D.L., O'Brien, E.A., 2013a. Recognizing finite matrix groups over infinite fields. J. Symb. Comput. 50, 100–109.
Detinko, A.S., Flannery, D.L., O'Brien, E.A., 2013b. Algorithms for linear groups of finite rank. J. Algebra 393, 187–196.
Detinko, A.S., Flannery, D.L., O'Brien, E.A., 2013c. http://magma.maths.usyd.edu.au/magma/.
Dixon, J.D., 1971. The Structure of Linear Groups. Van Nostrand Reinhold, London.
Dixon, J.D., 1985. The orbit-stabilizer problem for linear groups. Can. J. Math. 37 (2), 238–259.
Faccin, P., de Graaf, W., Plesken, W., 2013. Computing generators of the unit group of an integral abelian group ring. J. Algebra 373, 441–452.
Laue, R., Neubüser, J., Schoenwaelder, U., 1984. Algorithms for finite soluble groups and the SOGOS system. In: Computational Group Theory. Durham, 1982. Academic Press, London, pp. 105–135.
Miller III, C.F., 2013. Personal communication.
Sarnak, P., 2012. Notes on thin matrix groups. http://arxiv.org/abs/1212.3525.
Segal, D., 1983. Polycyclic Groups. Cambridge University Press, Cambridge.
Vinberg, E.B., Gorbatsevich, V.V., Shvartsman, O.V., 2000. Discrete subgroups of Lie groups. In: Lie Groups and Lie Algebras, II. Encycl. Math. Sci., vol. 21. Springer, Berlin, pp. 1–123, 217–223.