J. Austral. Math. Soc. (*Series A*) **67** (1999), 380–398

ALGORITHMIC QUESTIONS IN RINGS OF RATIONAL MATRICES

CHARLES C. SIMS

Dedicated to Mike (M. F.) Newman on the occasion of his 65th birthday

(Received 12 July 1999; revised 7 August 1999)

Communicated by E. A. O'Brien

Abstract

This paper discusses several algorithmic problems related to rings of rational matrices. It provides solutions to these problems in the commutative case and points out some of the difficulties to be overcome in the general case. A connection with attempts to construct Gröbner bases for ideals in free rings is also illustrated.

1991 *Mathematics subject classification* (*Amer. Math. Soc.*): primary 16S50; secondary 16–04, 16S36, 68Q40.
Keywords and phrases: rings of matrices, free rings, noncommutative Gröbner bases, algorithms.

1. Introduction

This paper discusses several algorithmic questions related to rings of rational matrices. Some questions about Gröbner bases of ideals in free rings are also mentioned. The number of answers given is considerably smaller than the number of questions raised. It is hoped that others will find these questions interesting and be able to make progress on them.

Throughout this paper, all rings and algebras are associative and are assumed to have multiplicative identities. All ideals are two-sided unless there is an explicit statement to the contrary.

The investigations reported on here began with the following observation. Let n be a positive integer, let $\mathrm{Mat}(n, \mathbb{Q})$ be the algebra of all rational n-by-n matrices, and

let $GL(n, \mathbb{Q})$ denote the group of invertible elements of $Mat(n, \mathbb{Q})$. If U is a finite subset of $Mat(n, \mathbb{Q})$ and v is an element of $Mat(n, \mathbb{Q})$, then there are three natural algorithmic questions that can be asked:

(1) Is v in the $\mathbb{Q}$-subalgebra of $Mat(n, \mathbb{Q})$ generated by U?

(2) Is v in the subring of $Mat(n, \mathbb{Q})$ generated by U?

(3) Assuming v and the elements of U are invertible, is v in the subgroup of $GL(n, \mathbb{Q})$ generated by U?

These problems will be referred to as the *membership problems* for finitely generated algebras, rings, and groups of rational matrices, respectively.

The membership problem for algebras of rational matrices is easily solved using only elementary linear algebra. We initialize a set B to consist of the identity matrix and then carry out the following step:

> Let C be a basis for the $\mathbb{Q}$-subspace of $Mat(n, \mathbb{Q})$ spanned by the union of B and the set of elements of the form bu with b in B and u in U. If $|C| = |B|$, then stop. Otherwise, replace B by C and repeat.

This step clearly terminates and when it does, the subspace spanned by B is the $\mathbb{Q}$-algebra $\mathscr{A}$ generated by U. At this point it is immediate to decide whether or not v is in $\mathscr{A}$.

As first observed in [5], the membership problem for groups of rational matrices is undecidable, at least when $n \geq 4$. For any group G there is a one-to-one correspondence between the set of normal subgroups of G and the subgroups of $G \times G$ that contain the diagonal. This implies that the word problem for finitely presented groups, which is known to be undecidable, is equivalent to the membership problem for finitely generated subgroups H of $F \times F$, where F is a free group of finite rank and H contains the diagonal. The group $GL(2, \mathbb{Q})$ is known to contain subgroups that are free of any finite or countable rank. Therefore, all the groups $F \times F$ with F free of finite rank can be found as subgroups of $GL(2, \mathbb{Q}) \times GL(2, \mathbb{Q})$, which is obviously a subgroup of $GL(4, \mathbb{Q})$.

Thus the membership problem for finitely generated rings of rational matrices is in some sense intermediate between an easy problem and an impossible one. No general solution of the ring membership problem is known to me.

The ring membership problem has a simple solution when $n = 1$. A subring $\mathscr{R}$ of $\mathbb{Q}$ is completely determined by the set of primes that are units in $\mathscr{R}$. Thus if $n = 1$, then v is in the subring generated by U if and only if each prime occurring in the denominator of the entry of v occurs in the denominator of the entry of at least one of the elements of U.

When $n > 1$, the lattice of subrings of $Mat(n, \mathbb{Q})$ is much more complicated. We do have the following straight-forward result, although it is not much help in our situation.

PROPOSITION 1. *The subrings of* $\mathrm{Mat}(n, \mathbb{Q})$ *that contain* $\mathrm{Mat}(n, \mathbb{Z})$ *are in one-to-one correspondence with the subsets of primes.*

2. The commutative case

In this section a solution of the membership problem for finitely generated rings of rational matrices is given for the case in which the ring $\mathscr{R}$ generated by the finite set U of matrices is commutative. The solution uses Gröbner basis methods.

The ring $\mathscr{R}$ is commutative if and only if any two elements of U commute. In this case, for v to be in $\mathscr{R}$ each element of U must commute with v. Let us assume that all elements of $U \cup \{v\}$ commute.

Let $r = |U|$ and let $\mathbb{Z}[X] = \mathbb{Z}[x_1, \ldots, x_{r+1}]$ be the ring of integer polynomials in $r + 1$ (commuting) indeterminates. In the context of polynomial rings, a *term* is a product of the form $x_1^{e_1} \cdots x_{r+1}^{e_{r+1}}$, where the exponents e_i are nonnegative integers. Set $\mathscr{R}^*$ equal to the ring generated by $U \cup \{v\}$. There is a ring homomorphism f from $\mathbb{Z}[X]$ to $\mathscr{R}^*$ that for $1 \leq i \leq r$ takes x_i to the i-th element of U and takes x_{r+1} to v. Let K be the kernel of f.

If we can find a finite generating set W for the ideal K, then we can decide whether or not v is in $\mathscr{R}$. We choose a term ordering on the terms in the x_i such that x_{r+1} is larger than any term not involving x_{r+1}. Then, starting with W, we compute a Gröbner basis B for K as an ideal of $\mathbb{Z}[X]$ with respect to this ordering. The matrix v is in $\mathscr{R}$ if and only if B contains an element of the form $x_{r+1} - g$, where g is a polynomial that does not involve x_{r+1}.

Thus it remains to show that we can find a presentation as a commutative ring for the ring $\mathscr{R}$ generated by a finite set U of commuting rational matrices. Let $r = |U|$, let X denote the set of indeterminates $x_1, \ldots, x_r$, let f be the homomorphism from $\mathbb{Z}[X]$ to $\mathscr{R}$ taking x_i to the i-th element of U, and let K be the kernel of f.

To find a finite generating set for K, we start by finding an algebra presentation for the $\mathbb{Q}$-algebra $\mathscr{A}$ generated by U. Since $\mathbb{Z}[X]$ is a subring of $\mathbb{Q}[X]$ and $\mathscr{R}$ is a subring of $\mathscr{A}$, we can extend f to be a $\mathbb{Q}$-algebra homomorphism of $\mathbb{Q}[X]$ onto $\mathscr{A}$. Let L be the kernel of f considered as a map from $\mathbb{Q}[X]$ to $\mathscr{A}$.

Let $1 = z_1, z_2, \ldots$ be the terms in the x_i listed in order of total degree and then lexicographically, and let d be the dimension of $\mathscr{A}$. The images of the z_i under f span $\mathscr{A}$. Let J be the set of positive integers j such that $f(z_j)$ is not a linear combination of the $f(z_i)$ with $i < j$. Then $|J| = d$ and the matrices $f(z_j)$ with j in J form a basis for $\mathscr{A}$. For each positive integer k not in J there is an equation in $\mathscr{A}$ of the form

$$f(z_k) - \sum_{j \in J} a_{kj} f(z_j) = 0,$$

https://doi.org/10.1017/S144678870000207X Published online by Cambridge University Press

where the a_{kj} are rational numbers. The polynomials

$$z_k - \sum_{j \in J} a_{kj} z_j$$

for which the degree of z_k does not exceed by more than 1 the degree of any of the z_j with j in J constitute a set of generators for L.

Now $K = L \cap \mathbb{Z}[X]$. Finding a generating set for K can be accomplished with Gröbner basis methods. Let B be a Gröbner basis (over $\mathbb{Q}$) for L. The term ordering is not important, but let us choose the total degree plus lexicographic order used above. By clearing denominators, we may assume that for each b in B the coefficients of b are integers that are relatively prime and the leading coefficient of b is positive. Clearly the ideal K_0 of $\mathbb{Z}[X]$ generated by B is contained in K. Let q be the least common multiple of the head coefficients of the elements of B.

PROPOSITION 2. *In this situation* $K_0 = K$ *if and only*

$$\frac{1}{q}(K_0 \cap q\mathbb{Z}[X]) \subseteq K_0.$$

PROOF. If g is an element of K all of whose coefficients are divisible by q, then g/q is in L and is in $\mathbb{Z}[X]$. Therefore g/q is in K.

Now suppose that

$$\frac{1}{q}(K_0 \cap q\mathbb{Z}[X]) \subseteq K_0$$

but that $K_0 \neq K$. Choose an element g of K that is not in K_0 such that the head term z of g is as small as possible. Since g is in L and B is a Gröbner basis for L, there is an element b of B such that the head term of b divides the head term of g. Since the head coefficient of b divides q, there is an integer a and a term z' such that the head terms of g and $(a/q)z'b$ are equal. Thus $h = g - (a/q)z'b$ is in L and either $h = 0$ or the head term of h is less than that of g. Now qh has integer coefficients and thus is in K. By the minimality of g, we know that qh is in K_0. Therefore

$$qg = qh + az'b$$

is in K_0. But qg is in $q\mathbb{Z}[X]$ and hence by assumption g is in K_0. □

Given the generating set B for K_0, we can compute a generating set C for

$$K_0 \cap q\mathbb{Z}[X]$$

using standard Gröbner basis techniques. See Section 6.2 of [2] for example. If g/q is in K_0 for each g in C, then we know that B generates K. If some $h = g/q$ is not in K_0, then we add h to B, compute a new Gröbner basis, and repeat the test. Since the ascending chain condition holds for ideals of $\mathbb{Z}[X]$, this process eventually terminates and gives us a presentation for $\mathscr{R}$.

https://doi.org/10.1017/S144678870000207X Published online by Cambridge University Press

3. The general case

The solution of the membership problem for finitely generated commutative rings of rational matrices given in Section 2 depends on being able to get presentations for such rings and on being able to perform Gröbner basis computations in finitely generated free commutative rings, that is, polynomial rings.

As we consider the general case, it is natural to ask whether we can find finite presentations for arbitrary finitely generated rings of rational matrices and perform Gröbner basis computations in the ideals of free rings that arise. The answers are disappointing.

A literature search on the finite presentability of finitely generated matrix rings did not locate any reference on the subject. However, it is known that finitely generated groups of rational matrices need not have finite group presentations. Example 4.22 of [10] can be easily modified to prove the following.

PROPOSITION 3. *There exists a finitely generated subring of* Mat(4, $\mathbb{Q}$) *that is not finitely presentable.*

PROOF. We start with a subring of Mat(3, $\mathbb{Q}$). Let $\mathscr{R}$ be the ring generated by the matrices

$$a = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \qquad b = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}, \qquad t = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1/2 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Let I be the identity matrix. If $u = a - I$ and $v = b - I$, then

$$t^i u = \begin{bmatrix} 0 & 0 & 0 \\ 1/2^i & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \qquad vt^i = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1/2^i & 0 \end{bmatrix},$$

and

$$t^i ub - bt^i u = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1/2^i & 0 & 0 \end{bmatrix}.$$

It follows that $\mathscr{R}$ consists of all matrices

$$\begin{bmatrix} \alpha & 0 & 0 \\ \gamma & \beta & 0 \\ \delta & \epsilon & \alpha \end{bmatrix},$$

https://doi.org/10.1017/S144678870000207X Published online by Cambridge University Press

where α is in $\mathbb{Z}$ and β, γ, δ, and ϵ are in $\mathbb{Z}[\frac{1}{2}]$.

Let M be the set of elements in $\mathscr{R}$ of the form

$$\begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ \delta & 0 & 0 \end{bmatrix}.$$

It is easy to check that M is an ideal of $\mathscr{R}$ and that left and right multiplication by a, b, and t act as the identity on M. Thus any additive subgroup of M is an ideal of $\mathscr{R}$. Since the additive group of $\mathbb{Z}[\frac{1}{2}]$ is not finitely generated, M is not finitely generated as an ideal of $\mathscr{R}$.

Let f be the map from $\mathscr{R}$ to Mat(4, $\mathbb{Q}$) defined by

$$f : \begin{bmatrix} \alpha & 0 & 0 \\ \gamma & \beta & 0 \\ \delta & \epsilon & \alpha \end{bmatrix} \longmapsto \begin{bmatrix} \alpha & 0 & 0 & 0 \\ \gamma & \beta & 0 & 0 \\ 0 & 0 & \beta & 0 \\ 0 & 0 & \epsilon & \alpha \end{bmatrix}.$$

It is easy to check that f is a ring homomorphism with kernel M. If the image $\mathscr{R}_1$ of f were finitely presented, then M would be finitely generated as an ideal. Since this is not the case, $\mathscr{R}_1$ is not finitely presented. □

Let X be a finite set of (noncommuting) indeterminates. We may consider the free ring $\mathbb{Z}\langle X\rangle$ generated by X to be a subring of the free $\mathbb{Q}$-algebra $\mathbb{Q}\langle X\rangle$ generated by X. An alternative statement of Proposition 3 is: Let I be an ideal of $\mathbb{Q}\langle X\rangle$ with finite vector space codimension. Then I is easily seen to be finitely generated. It is even finitely generated as a right ideal. Let $J = I \cap \mathbb{Z}\langle X\rangle$. Then J need not be finitely generated as an ideal of $\mathbb{Z}\langle X\rangle$.

Since ideals in $\mathbb{Q}\langle X\rangle$ and $\mathbb{Z}\langle X\rangle$ need not be finitely generated, these ideals certainly need not have finite Gröbner bases. In $\mathbb{Q}\langle X\rangle$ it is at least possible to decide when a given finite set of elements forms a Gröbner basis for the ideal it generates, see [8]. For $\mathbb{Z}\langle X\rangle$ I am not aware of any algorithm that determines whether or not a finite set of elements forms a Gröbner basis.

Gröbner bases in free algebras over fields have been considered in [4, 7, 8]. A discussion of Gröbner bases in free algebras over (commutative) polynomial rings is presented in [6], which has an extensive bibliography. For the special case of $\mathbb{Z}\langle X\rangle$, one can make relatively simple changes in the exposition in [2, Chapter 5 and Section 10.1]. The approach adopted here draws on [2, 6]. Because few new ideas are involved, proofs will frequently be sketched or omitted completely.

An element of $\mathbb{Z}\langle X\rangle$ is an integer linear combination of elements of the free monoid X^* generated by X. Often elements of X^* are called *words*, but in the context of free rings elements of X^* are usually called *terms*. We start by fixing a *term order* $<$ on X^*.

https://doi.org/10.1017/S144678870000207X Published online by Cambridge University Press

This is a well ordering such that for all terms s, t, u, and v, if $s < t$, then $usv < utv$. A *monomial* is a product of a nonzero integer and a term.

An element f of $\mathbb{Z}\langle X\rangle$ can be written uniquely in the form

$$a_1u_1 + a_2u_2 + \cdots + a_ru_r,$$

where the a_i are nonzero integers and the u_i are terms with $u_1 > u_2 > \cdots > u_r$. (If $f = 0$, then $r = 0$.) If f is not 0, then the *head monomial* of f is $\mathrm{HM}(f) = a_1u_1$, the *head term* of f is $\mathrm{HT}(f) = u_1$, and the *head coefficient* of f is $\mathrm{HC}(f) = a_1$. We shall abuse language and refer to elements of $\mathbb{Z}\langle X\rangle$ as (noncommutative) polynomials.

A monomial au *divides* a monomial bv if a divides b and u is a substring of v, or equivalently, if there exist an integer c and terms s and t such that $b = ca$ and $v = sut$. A finite subset B of $\mathbb{Z}\langle X\rangle$ is a *Gröbner basis* if 0 is not in B and for every nonzero element f of the ideal generated by B, there exists an element g of B such that $\mathrm{HM}(g)$ divides $\mathrm{HM}(f)$.

Given any finite subset B of $\mathbb{Z}\langle X\rangle$ and an element f of $\mathbb{Z}\langle X\rangle$, we can reduce f with respect to B by repeating the following:

While $f \neq 0$ and there exists an element g of B such that $\mathrm{HM}(g)$ divides $\mathrm{HM}(f)$ do
  Let $\mathrm{HM}(f) = au\,\mathrm{HM}(g)v$, where a is an integer and u and v are terms.
  Let $f = f - augv$.
od.

If B is a Gröbner basis, then a polynomial f is in the ideal generated by B if and only if f reduces to 0 with respect to B. We say the f is *top reducible* with respect to B if either $f = 0$ or the reduction loop is executed at least once. That is, $\mathrm{HM}(f)$ is divisible by the head monomial of some element of B.

In the commutative case, any two terms have a well-defined least common multiple, which divides any common multiple. When indeterminates do not commute, the situation is much more complicated. Let t_1 and t_2 be elements of X^*. A *minimal common multiple* of t_1 and t_2 is a quintuple of terms (w, u_1, v_1, u_2, v_2) such that $w = u_1t_1v_1 = u_2t_2v_2$, either u_1 or u_2 is empty, and either v_1 or v_2 is empty. If this holds, then the term w is clearly a common multiple of t_1 and t_2. The condition on the u_i and v_i ensures that the occurrences of t_1 and t_2 in w are not both part of some proper substring of w.

For $1 \leq i \leq 2$ let g_i be a nonzero polynomial. Let $a_i = \mathrm{HC}(g_i)$ and $t_i = \mathrm{HT}(g_i)$. Set $a = \mathrm{lcm}(a_1, a_2)$ and $d = \gcd(a_1, a_2)$. There are integers b_i and c_i such that

$$a = b_ia_i, \quad \text{and} \quad d = c_1a_1 + c_2a_2.$$

For each minimal common multiple $m = (w, u_1, v_1, u_2, v_2)$ of t_1 and t_2 we have the *S-polynomial* and the *G-polynomial* of g_1 and g_2 defined by

$$\mathrm{spol}(g_1, g_2, m) = b_1u_1g_1v_1 - b_2u_2g_2v_2$$

https://doi.org/10.1017/S144678870000207X Published online by Cambridge University Press

and

$$\text{gpol}(g_1, g_2, m) = c_1 u_1 g_1 v_1 + c_2 u_2 g_2 v_2.$$

Note that the head monomials of the two summands cancel in the definition of $\text{spol}(g_1, g_2, m)$. The definition given for $\text{gpol}(g_1, g_2, m)$ depends on c_1 and c_2. As explained in [2, Section 10.1], for each pair of integers (a_1, a_2) one can fix a pair (c_1, c_2) and always use these multipliers.

PROPOSITION 4. *A finite subset B of $\mathbb{Z}\langle X\rangle$ not containing 0 is a Gröbner basis if and only if for all g_1 and g_2 in B and all minimal common multiples $m = (w, u_1, v_1, u_2, v_2)$ of $\text{HT}(g_1)$ and $\text{HT}(g_2)$ the element $\text{spol}(g_1, g_2, m)$ can be reduced to 0 with respect to B and $\text{gpol}(g_1, g_2, m)$ is top reducible with respect to B.*

As is shown below, following [8], the criterion in Proposition 4 reduces to a finite test when the elements of B are monic. However, in general it appears that infinitely many S- and G-polynomials must be considered. It seems appropriate to call attention to this fact by stating the following.

PROBLEM. Is it possible to decide whether a finite subset of $\mathbb{Z}\langle X\rangle$ is a Gröbner basis?

Another form of the criterion for a finite set B of polynomials to be a Gröbner basis can be stated using the notion of a t-representation. Let f be an element of the ideal generated by B and let t be a term. A *t-representation* of f with respect to B is an expression of f as a sum

$$f = \sum_{i=1}^{r} a_i u_i g_i v_i,$$

where the a_i are nonzero integers, the u_i and v_i are terms, the g_i are in B, and for all i we have $\text{HT}(a_i u_i g_i v_i) < t$. As before, the empty sum is considered a t-representation of 0. (Note that this is a slight modification of the definition given in [2].)

PROPOSITION 5. *Let B be a finite subset of $\mathbb{Z}\langle X\rangle$ not containing 0. Suppose for each pair of elements g_1 and g_2 in B and for each minimal common multiple $m = (w, u_1, v_1, u_2, v_2)$ of $\text{HT}(g_1)$ and $\text{HT}(g_2)$ that $\text{spol}(g_1, g_2, m)$ has a $\text{HT}(u_1 g_1 v_1)$-representation with respect to B and $\text{gpol}(g_1, g_2, m)$ is top reducible with respect to B. Then B is a Gröbner basis.*

I close this section with an example that shows in one specific case that it is possible to decide whether a given set of polynomials is a Gröbner basis, even if some of the polynomials in the set are not monic. At this point I cannot say whether this example is typical.

https://doi.org/10.1017/S144678870000207X Published online by Cambridge University Press

The following example was studied as part of an effort to gain some insight into the structure of finitely generated rings of rational matrices. Let x and y be the following elements of Mat(2, $\mathbb{Q}$).

$$x = \begin{bmatrix} -1 & 0 \\ -5/2 & 2 \end{bmatrix}, \qquad y = \begin{bmatrix} 4 & -2 \\ 1 & 9/2 \end{bmatrix}.$$

The $\mathbb{Q}$-algebra generated by x and y has a basis consisting of the matrices $1, x, y,$ and xy and is defined by the following $\mathbb{Q}$-algebra relations:

$$x^2 - x - 2 = 0,$$
$$yx + xy - y - 17x/2 - 3/2 = 0,$$
$$y^2 - 17y/2 + 20 = 0.$$

The left sides of these relations form a Gröbner basis for the ideal of $\mathbb{Q}\langle x, y\rangle$ they generate. Here the ordering on terms is first by length and then lexicographic with $x < y$.

By clearing denominators in the $\mathbb{Q}$-algebra relations, we obtain the following ring relations:

$$x^2 - x - 2 = 0, \qquad 2yx + 2xy - 2y - 17x - 3 = 0, \qquad 2y^2 - 17y + 40 = 0.$$

Using *ad hoc* methods, it was determined that these relations imply that

$$2xyx + 4y - 20x - 34 = 0.$$

Dividing this relation by 2, we get the new ring relation

$$xyx + 2y - 10x - 17 = 0.$$

A prototype Maple implementation of the test in Proposition 4 has been written. This program investigates a specified finite set of S-polynomials and G-polynomials. This program was run with the input

$$x^2 - x - 2,$$
$$2yx + 2xy - 2y - 17x - 3,$$
$$2y^2 - 17y + 40,$$
$$xyx + 2y - 10x - 17.$$

The output from the program consisted of the following five polynomials.

$$h_1 = x^2 - x - 2,$$

https://doi.org/10.1017/S144678870000207X Published online by Cambridge University Press

$$h_2 = 2yx + 2xy - 2y - 17x - 3,$$
$$h_3 = 2y^2 - 17y + 40,$$
$$h_4 = xyx + 2y - 10x - 17,$$
$$h_5 = yxy - 10y - 20x + 20.$$

Enough S-polynomials and G-polynomials had been considered that it was plausible that this set B of five polynomials formed a Gröbner basis.

As the following result shows, it is easy to see that all G-polynomials obtained from elements of B are top reducible.

PROPOSITION 6. *Suppose that g_1 and g_2 are nonzero elements of $\mathbb{Z}\langle X\rangle$ such that* $\mathrm{HC}(g_1)$ *divides* $\mathrm{HC}(g_2)$. *Then for any minimal common multiple* $m = (w, u_1, v_1, u_2, v_2)$ *of* $\mathrm{HT}(g_1)$ *and* $\mathrm{HT}(g_2)$ *the corresponding* G*-polynomial is top reducible with respect to* $\{g_1\}$.

PROOF. We may take $\mathrm{gpol}(g_1, g_2, m)$ to be $u_1 g_1 v_1$. □

It is not clear that all the S-polynomials obtained from elements g_1 and g_2 of B can be reduced to 0. Let $m = (w, u_1, v_1, u_2, v_2)$ be a minimal common multiple of $\mathrm{HT}(g_1)$ and $\mathrm{HT}(g_2)$. There are only finitely many cases in which the occurrences of $\mathrm{HT}(g_1)$ and $\mathrm{HT}(g_2)$ in w overlap. These can be considered individually and in all cases the S-polynomials reduce to 0.

As we consider the minimal common multiples in which $t_1 = \mathrm{HT}(g_1)$ and $t_2 = \mathrm{HT}(g_2)$ do not overlap, it suffices to assume that t_1 is a prefix of w and t_2 is a suffix of w. Thus there is a term v such that $w = t_1 v t_2$, $u_1 = v_2 = \varepsilon$, $v_1 = v t_2$ and $u_2 = t_1 v$. Let us denote the corresponding S-polynomial as $S(g_1, g_2, v)$.

The following general result eliminates many cases.

PROPOSITION 7. *Suppose g_1 and g_2 are nonzero elements of $\mathbb{Z}\langle X\rangle$ such that* $\mathrm{HC}(g_1)$ *and* $\mathrm{HC}(g_2)$ *are relatively prime. Then for any term v the polynomial $S(g_1, g_2, v)$ has a t-representation with respect to $\{g_1, g_2\}$, where* $t = \mathrm{HT}(g_1) v\, \mathrm{HT}(g_2)$.

PROOF. Under the given assumptions,

$$\begin{aligned} S(g_1, g_2, v) &= g_1 v\, \mathrm{HM}(g_2) - \mathrm{HM}(g_1) v g_2 \\ &= [g_1 - \mathrm{HM}(g_1)] v g_2 - g_1 v [g_2 - \mathrm{HM}(g_2)]. \end{aligned}$$

The polynomials $[g_1 - \mathrm{HM}(g_1)]vg_2$ and $g_1 v[g_2 - \mathrm{HM}(g_2)]$ are either 0 or have head terms less than $\mathrm{HT}(g_1) v\, \mathrm{HT}(g_2)$. Thus the last expression is a t-representation of $S(g_1, g_2, v)$, where $t = \mathrm{HT}(g_1) v\, \mathrm{HT}(g_2)$. □

https://doi.org/10.1017/S144678870000207X Published online by Cambridge University Press

Putting Proposition 6 and Proposition 7 together, we see that there is a finite test to decide whether a finite set of monic polynomials in $\mathbb{Z}\langle X\rangle$ is a Gröbner basis.

In our example, the finitely many S-polynomials that are not of the form $S(g_1, g_2, v)$ can be checked individually and shown to have appropriate t-representations. There are four cases $S(g_1, g_2, v)$ that are not covered by Proposition 7. They are $S(h_2, h_2, v)$, $S(h_2, h_3, v)$, $S(h_3, h_2, v)$, and $S(h_3, h_3, v)$. Let us examine each one in turn. Let

$$\begin{aligned} T_1(v) &= S(h_2, h_2, v) + h_2v[xy - y - 8x - 1] + [-xy + y + 9x + 2]vh_2 \\ &= yxvx + xvyx + xvxy + xyvx + vyx + vxy - yvx + yxv \\ &\quad - xvy - 17xvx + xyv - vy - 10vx - yv - 10xv - 3v. \end{aligned}$$

Let $W_1(v) = yxvyx = \mathrm{HT}(h_2vyx) = \mathrm{HT}(yxvh_2)$. To show that $S(h_2, h_2, v)$ has $W_1(v)$-representation, it suffices to show that $T_1(v)$ has a $W_1(v)$-representation.

To show that $S(h_2, h_3, v)$ has the appropriate representation, it suffices to show that

$$\begin{aligned} T_2(v) &= S(h_2, h_3, v) + [-xy + y + 9x + 2]vh_3 + h_2v[8y + 20] \\ &= yxvy + xvyy + xyvy + vyy - yvy - 17xvy - 10vy + 20xv + 20v \end{aligned}$$

has a $W_2(v)$-representation, where $W_2(v) = yxvyy$.

To show that $S(h_3, h_2, v)$ and $S(h_3, h_3, v)$ have the appropriate representations, it suffices to show that $T_3(v)$ has a $W_3(v)$-representation and $T_4(v)$ has a $W_4(v)$-representation, where

$$\begin{aligned} T_3(v) &= S(h_3, h_2, v) + h_3v[xy - y - 8x - 1] + [9y - 20]vh_2 \\ &= yvyx + yvxy + yyvx - yvy - 17yvx + yyv + 20vx - 10yv + 20v, \\ T_4(v) &= S(h_3, h_3, v) + [9y - 20]vh_3 + h_3v[-8y + 20] \\ &= yvyy + yyvy - 17yvy + 20vy + 20yv, \\ W_3(v) &= yyvyx, \quad \text{and} \quad W_4(v) = yyvyy. \end{aligned}$$

PROPOSITION 8. *For $1 \leq i \leq 4$, and for all terms v, there is a $W_i(v)$-representation of $T_i(v)$.*

PROOF. We proceed by induction on $|v|$. The case $v = \varepsilon$ is easily checked. Now assume that $v = xu$ for some term u. Straightforward computation shows that

$$T_1(xu) = yh_1[ux + u] + xT_1(u) - h_1y[ux + u].$$

Now, no matter what u is, $\mathrm{HT}(yh_1ux) = yxxux < W_1(ux) = yxxuyx$. Similarly, $\mathrm{HT}(h_1yux)$ is less than $W_1(ux)$. By induction, $T_1(u)$ has a $W_1(u)$-representation. It follows easily that $xT_1(u)$ has a $xW_1(u)$-representation and $xW_1(u) = xyxuyx < W_1(ux)$. Therefore, $T_1(ux)$ has the desired $W_1(ux)$-representation.

https://doi.org/10.1017/S144678870000207X Published online by Cambridge University Press

Additional computation shows that

$$T_2(xu) = yh_1uy + xT_2(u) - h_1yuy,$$
$$T_3(xu) = yT_1(u) - h_5u[x+1] - T_3(u) + h_3u[x+1],$$
$$T_4(xu) = yT_2(u) - h_5uy - T_4(u) + h_3uy,$$

and the same kind of argument shows that each of the polynomials $T_i(xu)$ has a $W_i(xu)$-representation for $2 \leq i \leq 4$.

It remains to consider the case $v = yu$ for some term u. Here we have

$$T_1(yu) = h_5u[x+1] + [x+1]T_3(u) - h_3u[x+1], \qquad T_3(yu) = yT_3(u),$$
$$T_2(yu) = h_5uy + [x+1]T_4(u) - h_3uy, \qquad T_4(yu) = yT_4(u).$$

Again the induction assumption for $T_i(u)$ makes it possible to conclude that $T_i(yu)$ has a $W_i(yu)$-representation. □

The idea behind the proof of Proposition 8 can be automated. However, it is not clear whether a failure of the induction step always produces a polynomial that must be added to the current basis. Thus more work is needed before this procedure can be claimed to give a finite test for being a Gröbner basis.

4. Related problems

There are several problems related to the membership problem for finitely generated rings of rational matrices that should be mentioned.

We begin by pointing out that it is possible to determine the intersection of a subspace V of $\mathbb{Q}^m$ with $\mathbb{Z}^m$. In fact this is similar to and easier than finding the intersection of an ideal in $\mathbb{Q}[X]$ with $\mathbb{Z}[X]$, where X is a set of commuting indeterminates. The solution sketched here is in the spirit of the solution sketched above for the ideal intersection problem.

If the dimension of V is r, then $W = V \cap \mathbb{Z}^m$ is a free Abelian group of rank r. Let B be a basis for V. By clearing denominators, we may assume that the elements of B are in $\mathbb{Z}^m$. Let W_0 be the subgroup of $\mathbb{Z}^m$ generated by B. Then $|W : W_0|$ is finite and W is the set of elements a in $\mathbb{Z}^m$ such that some positive integer multiple of a is in W_0. Let M be the r-by-m matrix whose rows are the elements of B. We may assume that M is in row-Hermite normal form, see [9]. The order of $|W : W_0|$ divides the product n of the 'corner entries' in M.

PROPOSITION 9. *In this situation, $W = W_0$ if and only for each prime p dividing n we have*

$$\frac{1}{p}(W_0 \cap p\mathbb{Z}^m) \subseteq W_0.$$

https://doi.org/10.1017/S144678870000207X Published online by Cambridge University Press

PROOF. If $W = W_0$ and w is an element of $(1/p)(W \cap p\mathbb{Z}^m)$, then w is in V and also in $\mathbb{Z}^m$. Therefore w is in $W = W_0$.

Now suppose that

$$\frac{1}{p}(W_0 \cap p\mathbb{Z}^m) \subseteq W_0$$

for all primes p dividing n but $W_0 \neq W$. Then there exists an element w in W such that w is not in W_0 but pw is in W_0 for some prime p and p divides $|W : W_0|$, which divides n. But then pw is in $W_0 \cap p\mathbb{Z}^m$ and by our assumption $w = (pw)/p$ is in W_0 after all. □

Given the generating set B for W_0, we can construct a generating set for $W_0 \cap p\mathbb{Z}^m$ as follows: Let $a = (a_1, \ldots, a_r)$ be a variable vector in $\mathbb{Z}^r$. Find a set A of elements of $\mathbb{Z}^r$ that maps to a basis modulo p for the solutions of the linear system $aM \equiv 0 \pmod{p}$. Then $W_0 \cap p\mathbb{Z}^m$ is generated by the elements pb with b in B together with the elements aM with a in A. Thus to check whether

$$\frac{1}{p}(W_0 \cap p\mathbb{Z}^m) \subseteq W_0,$$

we have only to test whether $(aM)/p$ is in W_0 for all a in A.

For any element u of $\mathrm{Mat}(n, \mathbb{Q})$ let $\mathrm{denom}(u)$ denote the smallest positive integer d such that du has integer entries and let $\mathrm{num}(u)$ denote $\mathrm{denom}(u)u$. If U is a nonempty, finite subset of $\mathrm{Mat}(n, \mathbb{Q})$, let $\mathrm{denom}(U)$ be the least common multiple of the numbers $\mathrm{denom}(u)$ with u in U.

Let U be our finite subset of $\mathrm{Mat}(n, \mathbb{Q})$, let $\mathscr{A}$ be the $\mathbb{Q}$-algebra generated by U, and let $\mathscr{R}$ be the ring generated by U. We can consider the following problems:

(1) The ring $\mathscr{R}_1 = \mathscr{R} \cap \mathrm{Mat}(n, \mathbb{Z})$ is finitely generated as an Abelian group. Find a basis for this ring.

(2) More generally, for a given positive integer d find a basis for the Abelian group $\mathscr{R}_d = d\mathscr{R} \cap \mathrm{Mat}(n, \mathbb{Z})$.

(3) Determine the ring $\mathscr{S}$ of scalar matrices contained in $\mathscr{R}$.

(4) Decide whether $\mathscr{R}$ is conjugate in $\mathrm{Mat}(n, \mathbb{Q})$ to a subring of $\mathrm{Mat}(n, \mathbb{Z})$, that is, whether there is an element w of $\mathrm{GL}(n, \mathbb{Q})$ such that $w^{-1}\mathscr{R}w$ is contained in $\mathrm{Mat}(n, \mathbb{Z})$.

We can find a vector space basis for $\mathscr{A}$ and thus, by the above argument, a basis as a free Abelian group for the ring $\mathscr{T}_1 = \mathscr{A} \cap \mathrm{Mat}(n, \mathbb{Z})$. We can also determine a basis for the ring $\mathscr{T}_0$ generated by the elements $\mathrm{num}(u)$ with u in U. Then

$$\mathscr{T}_0 \subseteq \mathscr{R}_1 \subseteq \mathscr{T}_1$$

https://doi.org/10.1017/S144678870000207X Published online by Cambridge University Press

and the index (as an additive subgroup) of $\mathscr{T}_0$ in $\mathscr{T}_1$ is finite. If we can decide membership in $\mathscr{R}$, then we can choose coset representatives for $\mathscr{T}_0$ in $\mathscr{T}_1$ and use them to determine $\mathscr{R}_1$.

Our element v is in $\mathscr{R}$ if and only if $\text{num}(v)$ is in $d\mathscr{R} \cap \text{Mat}(n, \mathbb{Z})$, where $d = \text{denom}(v)$. Thus being able to solve the second problem makes it possible to decide membership in $\mathscr{R}$. Since $d\mathscr{R} \cap \text{Mat}(n, \mathbb{Z})$ contains $d\mathscr{T}_0$ as a subgroup of finite index, the argument of the previous paragraph shows that the second problem is equivalent to deciding membership in $\mathscr{R}$.

The ring of scalar matrices in $\text{Mat}(n, \mathbb{Q})$ is isomorphic to $\mathbb{Q}$. In the following, we identify these two rings. In particular, we write 1 for the n-by-n identity matrix. To solve the third problem it suffices to decide for which primes p is $1/p$ in $\mathscr{R}$. Any such prime must divide the denominator of some element of U and hence there are only finitely many candidates for p. Therefore, if we can decide membership in $\mathscr{R}$, then we can solve the third problem.

We can determine the ring of scalar matrices in $\mathscr{R}$ when $\mathscr{R}$ is commutative. A prime p is a unit in $\mathscr{R}$ if and only if the ideal N of $\mathscr{R}$ generated by p is all of $\mathscr{R}$. If we have an ideal generating set R for an ideal K of $\mathbb{Z}[X]$ such that $\mathscr{R}$ is isomorphic to $\mathbb{Z}[X]/K$, then $\mathscr{R}/N$ is isomorphic to $Z[X]/H$, where H is the ideal generated by $R \cup \{p\}$. Gröbner basis methods allow us to decide whether or not $H = \mathbb{Z}[X]$. If it does, then we can express 1 in terms of the elements of $R \cup \{p\}$. That is, we can find polynomials $f_0, f_1, \ldots, f_s$, and $g_1, \ldots, g_s$ such that the g_i are in R and

$$1 = pf_0 + f_1g_1 + \cdots + f_sg_s.$$

The image of f_0 in $\mathscr{R}$ is $1/p$.

An alternative approach to deciding whether $1/p$ is in $\mathscr{R}$ is to consider the ideal M of $\mathbb{Z}_p[X]$ generated by the image of R, since p is invertible in $\mathscr{R}$ if and only if $M = \mathbb{Z}_p[X]$. Gröbner basis techniques in $\mathbb{Z}_p[X]$ suffice for this.

Somewhat surprisingly, the fourth problem can be solved. In [1], it is shown that given a finite subset U of $\text{GL}(n, \mathbb{Q})$, it is possible to determine whether the group G generated by U is conjugate in $\text{GL}(n, \mathbb{Q})$ to a subgroup of $\text{GL}(n, \mathbb{Z})$. Now G is conjugate to a subgroup of $\text{GL}(n, \mathbb{Z})$ if and only if the ring $\mathscr{S}$ generated by G is conjugate to a subring of $\text{Mat}(n, \mathbb{Z})$ and $\mathscr{S}$ is generated by $U \cup U^{-1}$. If one assumes that $U = U^{-1}$, then the proof in [1] does not depend in any significant way on the fact that the elements of U are invertible. Thus the approach in [1] can be easily modified to give a solution to problem (4). Here is a brief sketch of that solution.

PROPOSITION 10. *Let $\mathscr{R}$ be a subring of* $\text{Mat}(n, \mathbb{Q})$. *The following are equivalent*:

(i) *$\mathscr{R}$ is conjugate to a subring of* $\text{Mat}(n, \mathbb{Z})$.

(ii) *$\mathscr{R}$ is finitely generated as an Abelian group.*

https://doi.org/10.1017/S144678870000207X Published online by Cambridge University Press

(iii) *There is a positive integer d such that $d\mathscr{R} \subseteq \mathrm{Mat}(n, \mathbb{Z})$.*

(iv) *$\mathscr{R}\mathbb{Z}^n$ is contained in a lattice.*

PROOF. A subring $\mathscr{S}$ of $\mathrm{Mat}(n, \mathbb{Z})$ is finitely generated as an Abelian group and hence any subring of $\mathrm{Mat}(n, \mathbb{Q})$ conjugate to $\mathscr{S}$ has the same property. Thus (i) implies (ii).

Suppose that $v_1, \ldots, v_r$ is a basis for $\mathscr{R}$ as an Abelian group. Let d be $\mathrm{denom}(\{v_1, \ldots, v_r\})$. Then $d\mathscr{R} \subseteq \mathrm{Mat}(n, \mathbb{Z})$. Thus (ii) implies (iii).

Suppose that $d\mathscr{R} \subseteq \mathrm{Mat}(n, \mathbb{Z})$. Then $\mathscr{R}\mathbb{Z}^n \subseteq (1/d)\mathbb{Z}^n$ and $(1/d)\mathbb{Z}^n$ is a lattice. Thus (iii) implies (iv).

Suppose that $\mathscr{R}\mathbb{Z}^n \subseteq V$, where V is a lattice in $\mathbb{Q}^n$. We may assume that V is the additive subgroup generated by $\mathscr{R}\mathbb{Z}^n$. Thus $\mathscr{R}V = V$. Since $\mathscr{R}$ contains the identity, V has rank n. Let $v_1, \ldots, v_n$ be a basis for V as an Abelian group. Then the v_i form a vector space basis for $\mathbb{Q}^n$ and the matrices for elements of $\mathscr{R}$ with respect to this basis have integer entries. If w is the matrix with the v_i as columns, then $w^{-1}\mathscr{R}w \subseteq \mathrm{Mat}(n, \mathbb{Z})$. Thus (iv) implies (i). □

Let $\mathscr{R}$ be a subring of $\mathrm{Mat}(n, \mathbb{Q})$. The $\mathbb{Q}$-subalgebra generated by $\mathscr{R}$ is called the *enveloping algebra* of $\mathscr{R}$ and denoted $\mathrm{env}(\mathscr{R})$. Let $u_1, \ldots, u_r$ be a basis for $\mathrm{env}(\mathscr{R})$. (The u_i may be chosen to be elements of $\mathscr{R}$.) Let T be the r-by-r matrix whose ij-th entry is $\mathrm{Tr}(u_i u_j)$, where Tr denotes the trace. The following is Lemma 2.1 of [1], which is quoted from [3, page 106].

PROPOSITION 11. *Under the stated assumptions, T is nonsingular if and only if* $\mathrm{env}(\mathscr{R})$ *is semisimple. In fact, the radical of* $\mathrm{env}(\mathscr{R})$ *consists of those elements*

$$\sum_{i=1}^{r} \alpha_i u_i$$

such that $T\alpha = 0$.

Since elements of $\mathrm{Mat}(n, \mathbb{Z})$ have integer traces and conjugate matrices have the same trace, a necessary condition for a subring $\mathscr{R}$ of $\mathrm{Mat}(n, \mathbb{Q})$ to be conjugate to a subring of $\mathrm{Mat}(n, \mathbb{Z})$ is that all elements of $\mathscr{R}$ have integer traces. The following is essentially part (b) of Theorem 2.4 of [1].

PROPOSITION 12. *Let $\mathscr{R}$ be a subring of* $\mathrm{Mat}(n, \mathbb{Q})$ *such that all elements of $\mathscr{R}$ have integer traces. If* $\mathrm{env}(\mathscr{R})$ *is semisimple, then $\mathscr{R}$ is conjugate to a subring of* $\mathrm{Mat}(n, \mathbb{Z})$.

PROOF. Let $r, u_1, \ldots, u_r$, and T be as in the previous proposition, with the u_i chosen to be in $\mathscr{R}$. Then T is a nonsingular integer matrix. Let $d_1 = \mathrm{denom}(\{u_1, \ldots, u_r\})$

and $d_2 = |\det(T)|$. By Cramer's rule, $d_2 T^{-1}$ is an integer matrix. Set $d = d_1 d_2$. Let u be in $\mathscr{R}$. Then

$$u = \sum_{i=1}^{r} \alpha_i u_i,$$

where the α_i are rational numbers. For $1 \leq i \leq r$, let $\tau_i = \mathrm{Tr}(uu_i)$, which by assumption is an integer. Then $\tau = T\alpha$ and hence $\alpha = T^{-1}\tau$. It follows that $d\alpha_i u_i = (d_2 T^{-1}\tau)_i d_1 u_i$ is an integer matrix and therefore so is du. Hence $d\mathscr{R} \subseteq \mathrm{Mat}(n, \mathbb{Z})$. □

PROPOSITION 13. *Let $\mathscr{R}$ be a finitely generated subring of* $\mathrm{Mat}(n, \mathbb{Q})$. *Suppose that V is an $\mathscr{R}$-submodule of $\mathbb{Q}^n$ such that the ring of linear transformations induced by $\mathscr{R}$ on $V \oplus (\mathbb{Q}^n / V)$ is finitely generated as an Abelian group. Then $\mathscr{R}$ is finitely generated as an Abelian group.*

PROOF. Let $\mathscr{S}$ be the ring of linear transformations induced by $\mathscr{R}$ on $V \oplus (\mathbb{Q}^n / V)$. The rings of linear transformations induced by $\mathscr{R}$ on V and on $\mathbb{Q}^n / V$ are quotient rings of $\mathscr{S}$ and hence also finitely generated as Abelian groups. Let m be the dimension of V. By Proposition 10, we may chose a basis $v_1, \ldots, v_n$ of $\mathbb{Q}^n$ such that $v_1, \ldots, v_m$ is a basis for V and with respect to the v_i the matrices for elements of $\mathscr{R}$ have the block form

$$\begin{bmatrix} A & B \\ 0 & C \end{bmatrix},$$

where A and C are integer matrices. Suppose we have two such matrices

$$u_i = \begin{bmatrix} A_i & B_i \\ 0 & C_i \end{bmatrix}.$$

for $i = 1, 2$. Then $u_1 u_2$ is

$$\begin{bmatrix} A_1 A_2 & A_1 B_2 + B_1 C_2 \\ 0 & C_1 C_2 \end{bmatrix},$$

It follows that if d is a positive integer such that du_1 and du_2 are both integer matrices, then $du_1 u_2$ is also an integer matrix. By assumption, $\mathscr{R}$ is generated by a finite set U. If $d = \mathrm{denom}(U)$, then $d\mathscr{R} \subseteq \mathrm{Mat}(n, \mathbb{Z})$. By Proposition 10, $\mathscr{R}$ is finitely generated as an Abelian group. □

PROPOSITION 14. *Let $\mathscr{R}$ be a finitely generated subring of* $\mathrm{Mat}(n, \mathbb{Q})$ *such that the trace of every element of $\mathscr{R}$ is an integer. Then $\mathscr{R}$ is conjugate to a subring of* $\mathrm{Mat}(n, \mathbb{Z})$.

https://doi.org/10.1017/S144678870000207X Published online by Cambridge University Press

PROOF. We proceed by induction on the dimension m of env($\mathscr{R}$). If env($\mathscr{R}$) is semisimple (in particular, if $m = 1$), then the result follows from Proposition 12. Let N be the radical of $\mathscr{R}$ and assume that $N \neq 0$. Let k be the smallest positive integer such that $N^k = 0$ and set $V = N\mathbb{Q}^n$, which is a proper, nontrivial env($\mathscr{R}$)-submodule of $\mathbb{Q}^n$. Let $\mathscr{S}$ be the ring of linear transformations induced on $V \oplus (\mathbb{Q}^n / V)$ by $\mathscr{R}$. Note that env($\mathscr{S}$) is the image of env($\mathscr{R}$). Elements of N map $\mathbb{Q}^n / V$ to 0 and elements of N^{k-1} map V to 0. Thus N^{k-1} is in the kernel of the homomorphism f from env($\mathscr{R}$) to env($\mathscr{S}$). Thus the dimension of env($\mathscr{S}$) is less than m. The map f preserves traces. Thus the trace of every element of $\mathscr{S}$ is an integer. The image under f of the finite generating set for $\mathscr{R}$ is a generating set for $\mathscr{S}$. Thus by induction, $\mathscr{S}$ is conjugate to a subring of Mat(n, $\mathbb{Z}$). By Proposition 13, $\mathscr{R}$ is conjugate to a subring of Mat(n, $\mathbb{Z}$). □

If we are given a finite subset U of Mat(n, $\mathbb{Q}$), then it is not immediately apparent whether the trace of every element of the ring $\mathscr{R}$ generated by U is an integer. We can form a few 'random' elements of $\mathscr{R}$. If we find any with nonintegral traces, then we know that $\mathscr{R}$ is not conjugate to a subring of Mat(n, $\mathbb{Q}$).

The proof of Proposition 14 contains an algorithm for determining an integer d such that $d\mathscr{R} \subseteq$ Mat(n, $\mathbb{Z}$). The algorithm is only guaranteed to work if the trace of every element of $\mathscr{R}$ is an integer. However, we can apply the algorithm any way. If any of the traces that are computed in executing the algorithm turn out not to be integers, then we abandon the computation. If this does not happen then we obtain a positive integer d such that either $d\mathscr{R} \subseteq$ Mat(n, $\mathbb{Z}$) or for no integer $e > 0$ is $e\mathscr{R} \subseteq$ Mat(n, $\mathbb{Z}$). We can decide whether $d\mathscr{R} \subseteq$ Mat(n, $\mathbb{Z}$) as follows:

(1) Let $L = d\mathbb{Z}^n$.
(2) If L is not contained in $\mathbb{Z}^n$, then return false.
(3) If $uL \subseteq L$ for all u in U, then return true.
(4) Let u be an element of U such that $uL \not\subseteq L$.
(5) Replace L by $L + uL$ and go to 2.

The running time analysis in [1] carries over and we find that one can decide whether the subring generated by a given set of rational matrices is conjugate to a ring of integer matrices in time polynomial in the size of the input.

5. A single generator

The ring $\mathscr{R}$ is commutative when the generating set U consists of a single element. In this case, we can give concise answers to many of the questions about the ring generated by U. We start with the following result.

PROPOSITION 15. *Let u be an element of* Mat(n, $\mathbb{Q}$). *The following are equiva-*

https://doi.org/10.1017/S144678870000207X Published online by Cambridge University Press

lent:

(1) *The characteristic polynomial of u has integer coefficients.*

(2) *The monic minimal polynomial of u has integer coefficients.*

(3) *The subring of* $\mathrm{Mat}(n, \mathbb{Q})$ *generated by u is finitely generated as an Abelian group.*

PROOF. If there is a monic integer polynomial g such that $g(u) = 0$, then the ring $\mathscr{R}$ generated by u is generated as an Abelian group by $1, u, \ldots, u^{r-1}$, where r is the degree of g. Thus (1) or (2) implies (3). If (3) holds, then, as noted above, $\mathscr{R}$ is conjugate to a subring of $\mathrm{Mat}(n, \mathbb{Z})$. In particular u is similar to an integer matrix and hence (1) holds. The monic minimal polynomial divides the characteristic polynomial and it is an easy consequence of Gauss' Lemma that (2) must also hold. □

Let x be a single indeterminate. The monic minimal polynomial g in $\mathbb{Z}[x]$ of an element u of $\mathrm{Mat}(n, \mathbb{Q})$ has in general coefficients that are not integers. However, there is a unique rational multiple h of g that is a primitive polynomial in $\mathbb{Z}[x]$ with positive head coefficient. Let us call h the *primitive minimal polynomial* of u.

PROPOSITION 16. *Let h be the primitive minimal polynomial of an element u of* $\mathrm{Mat}(n, \mathbb{Q})$ *and let M be the ideal of* $\mathbb{Z}[x]$ *generated by h. Then the ring generated by u is isomorphic to* $\mathbb{Z}[x]/M$.

PROOF. Let $\mathscr{R}$ be the ring generated by u and let N be the ideal of $\mathbb{Q}[X]$ generated by h. Then $\mathscr{R}$ is isomorphic to $\mathbb{Z}[X]/N \cap \mathbb{Z}[X]$. Let g be an element of $\mathbb{Z}[X]$ divisible by h in $\mathbb{Q}[X]$. Since h is primitive, Gauss' Lemma implies that h divides g in $\mathbb{Z}[X]$. □

We can now determine the scalar matrices in the ring generated by u.

PROPOSITION 17. *Let u be an element of* $\mathrm{Mat}(n, \mathbb{Q})$ *with primitive minimal polynomial* $h = a_r x^r + a_{r-1}x^{r-1} + \cdots + a_0$. *If* $\mathscr{R}$ *is the ring generated by u, then the ring* $\mathscr{S}$ *of scalar matrices contained in* $\mathscr{R}$ *is generated by* $1/q$, *where* $q = \gcd(a_r, \ldots, a_1)$.

PROOF. We have to determine for which primes p the ideal of $\mathbb{Z}_p[x]$ generated by the image $\overline{h}$ of h contains 1. Since h is primitive, $\overline{h}$ is not 0. Since $\mathbb{Z}_p$ is a field, 1 is divisible in $\mathbb{Z}_p[x]$ by $\overline{h}$ if and only if $\overline{h}$ is a nonzero scalar, or equivalently, p divides $a_1, \ldots, a_r$. □

References

[1] L. Babai, R. Beals and D. Rockmore, 'Deciding finiteness of matrix groups in deterministic polynomial time', in: *Proceedings of ISSAC 93* (ACM, New York, 1993) pp. 117–126.

[2] T. Becker and V. Weispfenning, *Gröbner bases* (Springer, New York, 1993).
[3] L. E. Dickson, *Algebras and their arithmetics* (University of Chicago Press, Chicago, 1923).
[4] E. Green, T. Mora and V. Ufnarovski, 'The non-commutative Gröbner freaks', in: *Symbolic rewriting techniques (Ascona 1995)*, Progr. Comput. Sci. Appl. Logic 15 (Birkhäuser, Basel, 1998) pp. 93–104.
[5] K. A. Mihailova, 'The occurrence problem for direct products of groups', *Dokl. Akad. Nauk SSSR* **119** (1958), 1103–1105, in Russian.
[6] A. Mikhalev and A. Zolotykh, 'Standard Grobner-Shirshov bases of free algebras over rings, I. Free associative algebras', *Internat. J. Algebra Comput.* **8** (1998), 689–726.
[7] T. Mora, 'Groebner bases in noncommutative algebras', in: *Symbolic and algebraic computation (Rome, 1998)*, Lecture Notes in Comput. Sci. 358 (Springer, Berlin, 1989) pp. 150–161.
[8] ———, 'An introduction to commutative and noncommutative Gröbner bases', in: *Second International Colloquium on Words, Languages, and Combinatorics (Kyoto, 1992)*, Theoret. Comput. Sci. 134 (Elsevier, Amsterdam, 1994) pp. 131–173.
[9] C. C. Sims, *Computation with finitely presented groups* (Cambridge University Press, Cambridge, 1994).
[10] B. A. F. Wehrfritz, *Infinite linear groups* (Springer, New York, 1973).

Mathematics Department
Rutgers University
New Brunswick NJ 08903
USA
e-mail: sims@math.rutgers.edu