Decidability of membership problems for flat rational subsets of $\mathrm{GL}(2, \mathbb{Q})$ and singular matrices

Volker Diekert
Formale Methoden der Informatik, Universität Stuttgart, Germany
diekert@fmi.uni-stuttgart.de

Igor Potapov
Department of Computer Science, Ashton Building, Ashton Street, University of Liverpool, Liverpool, L69-3BX, UK
potapov@liverpool.ac.uk

Pavel Semukhin
Department of Computer Science, University of Oxford, Wolfson Building, Parks Road, Oxford, OX1 3QD, UK
pavel.semukhin@cs.ox.ac.uk

Abstract

In this work we extend previously known decidability results for 2×2 matrices over $\mathbb{Q}$. Namely, we introduce a notion of *flat rational sets*: if M is a monoid and $N \le M$ is its submonoid, then flat rational sets of M relative to N are finite unions of the form $L_0 g_1 L_1 \cdots g_t L_t$ where all L_is are rational subsets of N and $g_i \in M$. We give quite general sufficient conditions under which flat rational sets form an effective relative Boolean algebra. As a corollary, we obtain that the emptiness problem for Boolean combinations of flat rational subsets of $\mathrm{GL}(2, \mathbb{Q})$ over $\mathrm{GL}(2, \mathbb{Z})$ is decidable.

We also show a dichotomy for nontrivial group extension of $\mathrm{GL}(2, \mathbb{Z})$ in $\mathrm{GL}(2, \mathbb{Q})$: if G is a f.g. group such that $\mathrm{GL}(2, \mathbb{Z}) < G \le \mathrm{GL}(2, \mathbb{Q})$, then either $G \cong \mathrm{GL}(2, \mathbb{Z}) \times \mathbb{Z}^k$, for some $k \ge 1$, or G contains an extension of the Baumslag-Solitar group $\mathrm{BS}(1, q)$, with $q \ge 2$, of infinite index. It turns out that in the first case the membership problem for G is decidable but the equality problem for rational subsets of G is undecidable. In the second case, the membership problem for G is an open problem as it is open for $\mathrm{BS}(1, q)$.

In the last section we prove new decidability results for flat rational sets that contain singular matrices. In particular, we show that the membership problem is decidable for flat rational subsets of $M(2, \mathbb{Q})$ relative to the submonoid that is generated by the matrices from $M(2, \mathbb{Z})$ with determinants $0, \pm 1$ and the central rational matrices.

2012 ACM Subject Classification Theory of computation → Formal languages and automata theory; Computing methodologies → Symbolic and algebraic algorithms

Keywords and phrases Membership problem, rational sets, general linear group

1 Introduction

Many problems for the analysis of matrix products are inherently difficult to solve even in dimension two, and most of such problems become undecidable in general starting from dimension three or four. One of the such hard questions is the *Membership problem* for matrix semigroups: Given a finite set of $n \times n$ matrices $\{M_1, \dots, M_m\}$ and a matrix M, determine whether there exist an integer $k \ge 1$ $i_1, \dots, i_k \in \{1, \dots, m\}$ s.t.

$$M_{i_1} \cdots M_{i_k} = M.$$

In other words, determine whether a matrix M belongs to a given finitely generated (f.g. for short) semigroup. The membership problem was intensively studied since 1947 when A. Markov showed in [22] that this problem is undecidable for matrices in $\mathbb{Z}^{6\times 6}$. A natural and important generalization is the *Membership problem in rational subsets*. Rational sets in a monoid are those which can be specified by regular expressions. For example, the problem above is the same as to decide membership in $(M_1 \cup \cdots \cup M_m)^+$: that is, the semigroup generated by the matrices $M_1, \ldots, M_m$. Another difficult question is to ask membership in the rational submonoid $M_1^* \cdots\ M_m^*$. That is to decide: "$\exists x_1, \ldots, x_m \in \mathbb{N}$: $M_1^{x_1} \cdots M_m^{x_m} = M$?" (also known as Knapsack problem). However, even in significantly restricted cases these problems become undecidable for high dimensional matrices over the integers, [3, 20]; and a very few cases are known to be decidable, see [5, 8]. The decidability of the membership problem remains open even for 2×2 matrices over integers [7, 10, 15, 19, 24]

On the other hand, it is classical that membership in rational subsets of $\mathrm{GL}(2, \mathbb{Z})$ (the 2×2 integer matrices with determinant ± 1) is decidable. Indeed, $\mathrm{GL}(2, \mathbb{Z})$ is a f.g. virtually free group, and therefore the family of rational subsets forms an effective Boolean algebra, [28]. A group is virtually free if it has a free subgroup of finite index. $\mathrm{GL}(2, \mathbb{Z})$ has a free subgroup of rank 2 and of index 24. Note that solving the membership problem for rational sets plays an important role in modern group theory as highlighted for example in [31] or used in [9].

Two recent results that significantly extended the border of decidability for the membership problem moving beyond $\mathrm{GL}(2, \mathbb{Z})$ were [25, 26], the first one in case of the semigroups of 2×2 nonsingular integer matrices and and the second one in case of $\mathrm{GL}(2, \mathbb{Z})$ extended by integer matrices with determinants $0, \pm 1$.

This paper pushes the decidability border even further. First of all we consider membership problems for 2×2 matrices over the rationals whereas [25, 26] deal with integer matrices. Since everything is fine for $\mathrm{GL}(2, \mathbb{Z})$, our interest is in subgroups G of $\mathrm{GL}(2, \mathbb{Q})$ which strictly contain $\mathrm{GL}(2, \mathbb{Z})$. In Section 4 we prove a dichotomy result which, to the best of our knowledge, has not been stated or shown elsewhere. In the first case G is generated by $\mathrm{GL}(2, \mathbb{Z})$ and central matrices $\left(\begin{smallmatrix} r & 0 \\ 0 & r \end{smallmatrix}\right)$. In that case G is isomorphic to $\mathrm{GL}(2, \mathbb{Z}) \times \mathbb{Z}^k$ for $k \geq 1$. It can be derived from known results in the literature about free partially commutative monoids and groups that equality test for rational sets in G is undecidable, but the membership problem in rational subsets is still decidable. So, this is best we can hope for groups sitting strictly between $\mathrm{GL}(2, \mathbb{Z})$ and $\mathrm{GL}(2, \mathbb{Q})$, in general. If such a group G is not isomorphic to $\mathrm{GL}(2, \mathbb{Z}) \times \mathbb{Z}^k$, then our dichotomy states that it contains a Baumslag-Solitar group $\mathrm{BS}(1, q)$ for $q \geq 2$. The Baumslag-Solitar groups $\mathrm{BS}(1, q)$ are defined by two generators a and t with a single defining relation $ta^p t^{-1} = a^q$. They were introduced in [2] and widely studied since then. It is fairly easy to see (much more is known) that they have no free subgroup of finite index unless $pq = 0$. As a consequence, in both cases of the dichotomy, $\mathrm{GL}(2, \mathbb{Z})$ has infinite index in G. Actually, we prove more, we show that if G contains a matrix of the form $\left(\begin{smallmatrix} r_1 & 0 \\ 0 & r_2 \end{smallmatrix}\right)$ with $|r_1| \neq |r_2|$ (which is the second case in dichotomy), then G contains some $\mathrm{BS}(1, q)$ for $q \geq 2$ which has infinite index in G. It is wide open whether the membership in rational sets of G can be decided in that second case. For example, as soon as G contains a matrix $\left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right)$ where p is prime, a semi-direct product $\mathrm{SL}(2, \mathbb{Z}[1/p]) \rtimes \mathbb{Z}$ appears in G. This provide reasons for the hardness of deciding the membership for arbitrary rational subsets of $\mathrm{GL}(2, \mathbb{Q})$ in the form of that dichotomy result. Actually, it is tempting to believe that the membership in rational sets becomes undecidable for subgroups of $\mathrm{GL}(2, \mathbb{Q})$ in general.

Let's take the dichotomy as a preamble. It lead us in the direction where we came up with a new, but natural subclass of rational subsets. The new class satisfies surprisingly good properties.

Let us introduce to you the class of *flat rational sets* $\mathrm{Frat}(M, N)$. It is a relative notion where N is a submonoid of M. It contains all finite unions of the form $g_0 L_1 g_1 \cdots L_m g_m$ where

$g_i \in M$ and $L_i \in \mathrm{Rat}(N)$. Of particular interest in our context is the class $\mathrm{Frat}(G, H)$ where H and G are f.g. groups, $\mathrm{Rat}(H)$ forms a Boolean algebra, and G is the commensurator of H. The notion of *commensurator* is a standard concept in geometric group theory which includes many more than matrix groups, the formal definition is given in Section 2.1. Theorem 10 shows that in this case, $\mathrm{Frat}(G, H)$ forms a relative Boolean algebra. That is: $L, K \in \mathrm{Frat}(G, H) \implies L \setminus K \in \mathrm{Frat}(G, H)$. Under some mild effectiveness assumptions this means that the emptiness of finite Boolean combinations of sets in $\mathrm{Frat}(G, H)$ can be decided. Thus, we have an abstract general condition to decide such questions for a natural subclass of all rational sets in G where the whole class $\mathrm{Rat}(G)$ need not to be an effective Boolean algebra. The immediate application in the present paper concerns $\mathrm{Frat}(\mathrm{GL}(2, \mathbb{Q}), \mathrm{GL}(2, \mathbb{Z}))$, see Theorem 10 and Corollary 11. For example, $\mathrm{GL}(2, \mathbb{Z}) \times \mathbb{Z}$ appears in $\mathrm{GL}(2, \mathbb{Q})$ and $\mathrm{Rat}(\mathrm{GL}(2, \mathbb{Z}) \times \mathbb{Z})$ is not an effective Boolean algebra. Still the smaller class of flat rational sets $\mathrm{Frat}(\mathrm{GL}(2, \mathbb{Z}) \times \mathbb{Z}, \mathrm{GL}(2, \mathbb{Z}))$ is a relative Boolean algebra. In order to apply Theorem 10 we need that $\mathrm{Rat}(H)$ forms an effective Boolean algebra. This is actually true for many other groups than virtually free groups. It includes for example all f.g. abelian groups and it is closed under free products.

The power of flat rational sets is even better visible in the context of membership problems for rational subsets of $\mathrm{GL}(2, \mathbb{Q})$. Let $P(2, \mathbb{Q})$ denote the monoid $\mathrm{GL}(2, \mathbb{Z}) \cup \{h \in \mathrm{GL}(2, \mathbb{Q}) \mid |\det(h)| > 1\}$. Then Theorem 13 states that we can solve the membership problem "$g \in R$?" for all $g \in \mathrm{GL}(2, \mathbb{Q})$ and all $R \in \mathrm{Frat}(\mathrm{GL}(2, \mathbb{Q}), P(2, \mathbb{Q}))$. Theorem 13 generalizes the main result in [4].

Let us summarize the statements about groups G sitting between $\mathrm{SL}(2, \mathbb{Z})$ and $\mathrm{GL}(2, \mathbb{Q})$. Our current knowledge is as follows. There is some evidence that the membership in rational subsets of G is decidable if and only if G doesn't possess any $\left(\begin{smallmatrix} r_1 & 0 \\ 0 & r_2 \end{smallmatrix}\right)$ where $|r_1| \neq |r_2|$. However, we always can decide the membership problem for all $L \in \mathrm{Frat}(\mathrm{GL}(2, \mathbb{Q}), P(2, \mathbb{Q}))$. Moreover, it might be that such a positive result is close to the border of decidability.

We also consider singular matrices. As a matter of fact, the membership problem becomes simpler in the following sense. Let g be a singular matrix in $M(2, \mathbb{Q})$ and let P be the submonoid generated by $\{\left(\begin{smallmatrix} r & 0 \\ 0 & r \end{smallmatrix}\right) \mid r \in \mathbb{N}\} \cup \mathrm{GL}(2, \mathbb{Z}) \cup \{h \in M(2, \mathbb{Z}) \mid \det(h) = 0\}$. Then can decide the membership problem "$g \in R$?" for all $R \in \mathrm{Frat}(M(2, \mathbb{Q}), P)$.

2 Preliminaries

By $M(n, R)$ we denote the ring of $n \times n$ matrices over a commutative ring R, and $\det : M(n, R) \to R$ is the determinant. By $\mathrm{GL}(n, R)$ we mean the group of invertible matrices. These are those matrices $g \in M(n, R)$ for which $\det(g)$ is a unit in R. By $\mathrm{SL}(n, R)$ we denote its normal subgroup $\det^{-1}(1)$, called the *special linear group*. Interesting results and explicit calculation for $\mathrm{SL}(2, \mathbb{Z})$ and for special linear groups over other rings of integers for number fields and function fields are in [30]. $\mathrm{BS}(p, q)$ denotes the Baumslag-Solitar group $\mathrm{BS}(p, q) = \langle a, t \mid ta^p t^{-1} = a^q \rangle$.

For groups (and more generally for monoids) we write $N \leq M$ if N is a submonoid of M and $N < M$ if $N \leq M$ but $N \neq M$. If M is a monoid, then $Z(M)$ denotes the center of M, that is, the submonoid of elements which commute with all elements in M. A subsemigroup I of a monoid M is an *ideal* if $M\, I\, M \subseteq I$.

2.1 Smith normal forms and commensurators

The standard application for all our results is the general linear group $\mathrm{GL}(2, \mathbb{Q})$, but the results are more general and have the potential to go far beyond. Let $n \in \mathbb{N}$. It is classical fact from linear algebra that each nonzero matrix $g \in M(n,\mathbb{Q})$ admits a *Smith normal form*. This is a factorization

$$g = r\, e\, s_q\, f$$

such that $r \in \mathbb{Q}^*$ with $r > 0$, $e, f \in \mathrm{SL}(n,\mathbb{Z})$, and $q \in \mathbb{Z}$ where s_q denotes the matrix

$$s_q = \left(\begin{smallmatrix} 1 & 0 \\ 0 & q \end{smallmatrix}\right).$$

The matrices e and f in the factorization are not unique, but both the numbers r and q are. The existence and uniqueness of r and s_q are easy to see by the corresponding statement for integer matrices. Clearly, $r^2 q = \det(g)$. So, for $g \neq 0$, the sign of $\det(g)$ is determined by the sign of q.

The notion of "commensurator" is well established in geometric group theory. Let H be a subgroup in G, then the *commensurator* of H in G is the set of all $g \in G$ such that $gHg^{-1} \cap H$ has finite index in H (note that this also implies that $gHg^{-1} \cap H$ has finite index in gHg^{-1}, too). If H has finite index in G, then G is always a commensurator of H because the normal subgroup $N = \bigcap \left\{ gHg^{-1} \,\middle|\, g \in G \right\}$ is of finite index in G if and only if G/H is finite.

Moreover, if $H \leq H'$ be of finite index and $H' \leq G' \leq G$ such that G is a commensurator of H, then G' is a commensurator of H'. The notion of a commensurator pops up naturally in our context. Indeed, let $H = \mathrm{SL}(2,\mathbb{Z})$ and write $g \in \mathrm{GL}(2,\mathbb{Q})$ in its Smith normal form $g = r\, e\, s_q\, f$. Then the index of $gHg^{-1} \cap H$ in H is the same as the index of $s_q H s_q^{-1} \cap H$ in H; and every matrix of the form $\left(\begin{smallmatrix} a & b/q \\ qc & d \end{smallmatrix}\right)$ is in $s_q H s_q^{-1}$ if $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}(2,\mathbb{Z})$. Thus, the index of $s_q H s_q^{-1} \cap H$ in H is bounded by the size of the finite group $\mathrm{SL}(n,\mathbb{Z}/q\mathbb{Z})$. For $n = 2$ the size $\mathrm{SL}(n,\mathbb{Z}/q\mathbb{Z})$ is in $\mathcal{O}(q^3)$. It follows that $\mathrm{GL}(2,\mathbb{Q})$ is the commensurator of $\mathrm{SL}(2,\mathbb{Z})$, and hence of $\mathrm{GL}(2,\mathbb{Z})$. In fact, it is known that $\mathrm{GL}(n,\mathbb{Q})$ is the commensurator of $\mathrm{SL}(n,\mathbb{Z})$ for all $n \in \mathbb{N}$, e.g., see [16].

2.2 Rational and recognizable sets

The results in this section are the basis for the following sections and not new. An exception is however Lemma 5. The corresponding result in the literature is stated only for H and G where the index of the subgroup H is finite in G. We use the our stronger version in the proof of Proposition 9. We follow the standard notation as Eilenberg [11]. Let M be any monoid, then $\mathrm{Rat}(M)$ has the following inductive definition using *rational* (aka *regular*) expressions.

1. $L < \infty, L \subseteq M \implies L \in \mathrm{Rat}(M)$.
2. $L_1, L_2 \in \mathrm{Rat}(M) \implies L_1 \cup L_2, L_1 \cdot L_2, L_1^* \in \mathrm{Rat}(M)$.

For $L \subseteq M$ the set L^* denotes the submonoid of M which is generated by L. The submonoid L^* is also called the *Kleene-star* of L. Note that the definition of $\mathrm{Rat}(M)$ is intrinsic without any reference to any generating set. It is convenient to define simultaneously a *basis* $B(L)$ for L (more precisely for a given rational expression): If $L < \infty$, then $B(L) = L$. Moreover, $B(L^*) = B(L)$ and $B(L_1 \cup L_2) = B(L_1) \cup B(L_2)$. Finally, $B(L_1 \cdot L_2) = B(L_1) \cup B(L_2)$ if $B(L_1) \neq \emptyset$ and $B(L_2) \neq \emptyset$, and $B(L_1 \cdot L_2) = \emptyset$, otherwise. Every rational set is contained in a f.g. submonoid of M, namely, $L \subseteq B(L)^*$. We will also use the fact that the emptiness problem is decidable for rational subsets of M since $L \neq \emptyset \iff B(L) \neq \emptyset$.

▶ **Definition 1.** *Let $\mathcal{C}$ be a family of subsets of M which is closed under finite union. We say that $\mathcal{C}$ is an* effective relative Boolean algebra *if first, every $L \in \mathcal{C}$ is given by an effective description and second, if on an input $K, L \in \mathcal{C}$ the relative complement $K \setminus L$ is an effectively computable set in $\mathcal{C}$. If in addition, M belongs to $\mathcal{C}$, then $\mathcal{C}$ is is called* effective Boolean algebra

We note that since by the above definition a relative Boolean algebra is closed under finite unions, it follows that it is closed under finite intersection, too.

The following proposition gives examples when $\mathrm{Rat}(M)$ is an effective Boolean algebra.

▶ **Proposition 2.** *The class of monoids M where* $\mathrm{Rat}(M)$ *is an effective Boolean algebra satisfies the following:*

1. *It contains only f.g. monoids. (Trivial.)*
2. *It contains all f.g. free monoids, f.g. free groups, and f.g. abelian monoids [18, 6, 12].*
3. *It contains all f.g. virtually free groups [32].*
4. *It is closed under free product [27].*

We also use the following well-known fact from [1].

▶ **Proposition 3.** *Let G a group. If a subgroup H is in* $\mathrm{Rat}(G)$*, then H is finitely generated.*

The family of *recognizable* subsets $\mathrm{Rec}(M)$ is defined as follows. We have $L \in \mathrm{Rec}(M)$ if and only if there is a homomorphism $\varphi\colon M \to N$ such that $|N| < \infty$ and $\varphi^{-1}\varphi(L) = L$.

The following assertions are well-known and easy to show, see for example [11].

1. McKnight: M is finitely generated $\iff$ $\mathrm{Rec}(M) \subseteq \mathrm{Rat}(M)$.
2. $L, K \in \mathrm{Rat}(M)$ doesn't imply $L \cap K \in \mathrm{Rat}(M)$, in general.
3. $L \in \mathrm{Rec}(M), K \in \mathrm{Rat}(M) \implies L \cap K \in \mathrm{Rat}(M)$.
4. Let H be a subgroup of a group G. Then $|G/H| < \infty \iff H \in \mathrm{Rec}(G)$.

Lemma 4 is well-known and an easy corollary of the above properties.

▶ **Lemma 4.** *Let G any group and $H \leq G$ be a subgroup of finite index. Then*

$$\{L \cap H \mid L \in \mathrm{Rat}(G)\} = \{L \subseteq H \mid L \in \mathrm{Rat}(G)\}\,.$$

Lemma 4 doesn't hold if H has infinite index in G. For example it fails for $F_2 \times \mathbb{Z} = F(a, b) \times F(c)$ which does not have Howson property: there are f.g. subgroups H, K such that $H \cap K$ is not finitely generated.

The assertion of Lemma 5 below is not obvious and was proved first under the assumption that H has finite index in G by [14, 28, 32]. The proof in [28] states the result for f.g. virtually free groups, only. Our proof is conceptually simple. It just uses elementary transformations on NFAs. What is new is that there is no hypothesis that H has finite index in G. This turns out to be useful later.

▶ **Lemma 5.** *Let G be any group and $H \leq G$ be a subgroup. Then*

$$\{L \subseteq H \mid L \in \mathrm{Rat}(G)\} = \mathrm{Rat}(H).$$

Proof. Let $R \subseteq G$ such that first, $1 \in R$ and second, R is in bijection with $H \setminus G$ via $r \mapsto Hr$. Thus, R is coset representation.

Let $L = L(A)$ for an NFA A with state set Q. Since $G = \langle H \cup R\rangle$ as a monoid and since $1 \in R$ and $1 \in H$ we may assume that all transition are labeled by elements from G having the form sa with $s \in R$ and $a \in H$. Moreover, we may assume that every state p is on some accepting path. Since there are only finitely many transitions there are finite subsets $H' \subseteq H$ and $S \subseteq R$ such that if sa with $s \in R$ labels a transition, then $s \in S$ and $a \in H'$. Moreover, $G' = \langle H \cup S \rangle$ is a f.g. subgroup $G' \leq G$ such that $L \in \mathrm{Rat}(G')$.

We obtain the first invariant. Assume we read from the initial state a word u over the $H' \cup S$ such that reading that word leads to the state p with $u \in Hr$ for $r \in R$. Then there is some $f \in G$ which leads us to a final state. Thus, $uf \in L(A) \subseteq H$, and therefore $u \in Hf^{-1}$. This means $Hf^{-1} = Hr$ and therefore r doesn't depend on u. It depends on p only: each state $p \in Q$ "knows" its value $r(p) \in R$.

This will show that we only need the finite subset R' of R. The set R' contains the $s \in R$ appearing on transitions in the NFA and the $r \in R$ such that $Hf^{-1} = Hr$ where f_q is the label of a shortest path from a state q to a final state. For simplicity $R = R'$.

Let $r = r(p) \in R$ for $p \in Q$. We introduce exactly one new state (p, r) with transitions $p \xrightarrow{r} (p, r)$ and $(p, r) \xrightarrow{r^{-1}} p$. This does not change the language.

Now for each outgoing transition $p \xrightarrow{sa} q$ define $b \in H$ and $t \in R$ by the equation $r^{-1}sa = bt$. Recall if we read u reaching p, then $u \in Hr$. Thus, $usa \in Ht$; and we can add a transition

$$(p, r) \xrightarrow{b^{-1}} (q, t^{-1}).$$

This doesn't change the language as $b = r^{-1}sat^{-1} = b$ in G.

Now, the larger NFA still accepts L, but the crucial point is that for $u \in L(A)$ we can accept the same element in G by reading just labels from H. This is easy to see by induction on k.

Now we can remove all original states since they are good for nothing anymore by making $(p, 1)$ initial (resp. final) if and only if p was initial (resp. final). So, the last modifications do not enlarge the size of the NFA. At the end the new NFA has exactly the same size the one for the set $L \cap H \in \mathrm{Rat}(G)$. ◀

▶ Remark 6. Another proof leaning on finite transducers was given by Sénizergues [29].

As a first corollary of Lemma 5 we state another well-known fact.

▶ **Proposition 7.** *Let H be a subgroup of finite index in G. If the membership problem is decidable for* $\mathrm{Rat}(H)$*, then it is decidable for* $\mathrm{Rat}(G)$*.*

Proof. Let $R \subseteq G$ be a rational subset and $g \in G$. We want to decide "$g \in R$?". Suppose $u_1, \ldots, u_k$ are all representatives of right cosets of H in G. Choose i such that $g \in Hu_i$. Then $gu_i^{-1} \in H$, and $g \in R$ if and only if $gu_i^{-1} \in Ru_i^{-1} \cap H$. Since H has finite index in G, it is recognizable, and hence $Ru_i^{-1} \cap H \in \mathrm{Rat}(G)$. By Lemma 5, we have $Ru_i^{-1} \cap H \in \mathrm{Rat}(H)$. Since the membership for $\mathrm{Rat}(H)$ is decidable, we can decide whether $g \in R$. ◀

3 Flat rational sets

The best situation is when $\mathrm{Rat}(M)$ is an effective Boolean algebra because in this case all decision problems we are studying here are decidable. However, our focus is on matrices over the rational or integer numbers, in which case such a strong assertion is either wrong or not known to be true. Our goal is to search for weaker conditions under which it becomes possible to decide the emptiness of finite Boolean combinations of rational sets or (even weaker) to decide the membership in rational sets. Again, in various interesting cases the membership to rational subsets is either undecidable or not known to be decidable. The most prominent example is the direct product $F_2 \times F_2$ of two free groups of rank 2 in which, due to the construction of Mihailova [23], there exists a finitely generated subgroup with undecidable membership problem.

In this work we introduce a notion of *flatness* for rational sets and show that the membership problem and (even stronger) the emptiness problem for Boolean combinations of flat rational sets are decidable in $\mathrm{GL}(2, \mathbb{Q})$.

▶ **Definition 8.** *Let N be a submonoid of M. We say that $L \subseteq M$ is flat rational subset of M relative to N (or over N) if L is a finite union of languages of type $L_0 g_1 L_1 \cdots g_t L_t$ where all $L_i \in \mathrm{Rat}(N)$ and $g_i \in M$. The family of these sets is denoted by* $\mathrm{Frat}(M, N)$.

In our applications we use flat rational sets in the following setting of a group G with a subgroup H and G sits inside a monoid M, where $M \setminus G$ is ideal (possibly empty). For example, $H = \mathrm{GL}(2, \mathbb{Z}) < G \leq \mathrm{GL}(2, \mathbb{Q})$ and $M \setminus G$ is a (possibly empty) semigroup of singular matrices. In such a situation there is an equivalent characterization of flat rational set in M with respect to H. Proposition 9 shows it can be defined as the family of rational sets when the Kleene-star is restricted to subsets which belong to the submonoid H.

▶ **Proposition 9.** *Let H be a subgroup of G and G be a subgroup of a monoid M such that $M \setminus G$ is an ideal. Then the family* $\mathrm{Frat}(M, H)$ *is the smallest family $\mathcal{R}$ of subsets of M such that the following holds.*

- *$\mathcal{R}$ contains all finite subsets of M,*
- *$\mathcal{R}$ is closed under finite union and concatenation,*
- *$\mathcal{R}$ is closed under taking the Kleene-star over subsets of H which belong to $\mathcal{R}$.*

Proof. Clearly, all flat rational sets relative to H are contained in $\mathcal{R}$. To prove inclusion in the other direction, we need to show that the family of flat rational subsets of M relative to H (i) contains all finite subsets of M, (ii) is closed under finite union and concatenation, and (iii) is closed under taking the Kleene-star over subsets of H. The first two conditions are obvious. To show (iii), let L be flat rational set relative to H such that $L \subseteq H$. Recall that L is a finite union of the form $L_0 g_1 L_1 \cdots g_t L_t$, where $\emptyset \neq L_i \in \mathrm{Rat}(H)$ and $g_i \in M$. If $g_i \in M \setminus G$ for some i, then we have $L_0 g_1 L_1 \cdots g_t L_t \setminus G \neq \emptyset$ because $M \setminus G$ is an ideal, and hence $L \not\subseteq H$.

So if $L \subseteq H$, then all $g_i \in G$ and $L \in \mathrm{Rat}(G)$. By Lemma 5, L is a rational subset of H, and hence $L^* \in \mathrm{Rat}(H)$. In particular, L^* is flat rational relative to H. ◀

▶ **Theorem 10.** *Let H and G be f.g. groups with $H \leq G$ such that the following holds.*

- $\mathrm{Rat}(H)$ *is an effective Boolean algebra.*
- *G is the commensurator of H.*
- *The membership to H (that is, the question "$g \in H$?") is decidable.*
- *Given $g \in G$ we can compute a set of left coset representatives of $H_g = gHg^{-1} \cap H$ in H. (Note that this set is finite by the above assumption.)*

Then $\mathrm{Frat}(G, H)$ *forms an effective relative Boolean algebra. In particular, given a finite Boolean combination B of flat rational sets of G over H, we can decide the emptiness of B.*

Before giving the proof Theorem 10 let us state its consequence for $\mathrm{GL}(2, \mathbb{Q})$.

▶ **Corollary 11.** *Let $B \subseteq \mathrm{GL}(2, \mathbb{Q})$ be a finite Boolean combination of flat rational sets of* $\mathrm{GL}(2, \mathbb{Q})$ *over* $\mathrm{GL}(2, \mathbb{Z})$*, then we can decide the emptiness of B.*

Proof. It is a well-known classical fact that $\mathrm{GL}(2,\mathbb{Z})$ is a finitely generated virtually free group, namely, it contains a free subgroup of rank 2 and index 24. Hence $\mathrm{Rat}(\mathrm{GL}(2,\mathbb{Z}))$ is an effective Boolean algebra by [32]. It is also well-knows that $\mathrm{GL}(2,\mathbb{Q})$ is the commensurator subgroup of $\mathrm{GL}(2,\mathbb{Z})$ in $\mathrm{GL}(2,\mathbb{Q})$. Thus, all hypotheses of Theorem 10 are satisfied. ◀

A direct consequence of Corollary 11 is that we can decide the membership for flat rational sets of $\mathrm{GL}(2,\mathbb{Q})$ over $\mathrm{GL}(2,\mathbb{Z})$. However in Section 4 we explain why we are far away from knowing how to decide the membership for all rational subsets of $\mathrm{GL}(2,\mathbb{Q})$.

For the proof of Theorem 10 we need the following observation.

▶ **Lemma 12.** *Let $L \in \mathrm{Rat}(H)$ and $g \in G$. As above, let*

$$H_g = gHg^{-1} \cap H = \left\{h \in H \,\middle|\, g^{-1}hg \in H\right\}.$$

Then we can compute an expression for $g^{-1}(L \cap H_g)g \in \mathrm{Rat}(H)$.

Proof. Since $gHg^{-1} \cap H$ is of finite index in H, we can compute the expression for $L' = L \cap H_g \in \mathrm{Rat}(H_g)$ over a basis $B' \subseteq H_g$ by Lemma 5. Now, for any g and $K \in \mathrm{Rat}(H_g)$ we have $g^{-1}K^*g = (g^{-1}Kg)^*$, $g^{-1}(L_1L_2)g = g^{-1}L_1gg^{-1}L_2g$, and $g^{-1}(L_1 \cup L_2)g = g^{-1}L_1g \cup g^{-1}L_2g$. Hence, we simply replace the basis $B' \subseteq H_g$ by $g^{-1}B'g \subseteq H$. This gives a rational expression for $g^{-1}(L \cap H_g)g$ over H. ◀

Proof of Theorem 10. Let $g \in G$ and $K \in \mathrm{Rat}(H)$. First, we claim that we can rewrite $Kg \in \mathrm{Rat}(G)$ as a finite union of languages $g'K'$ with $g' \in G$ and $K' \in \mathrm{Rat}(H)$.

Indeed, by assumption we can compute a set $U_g \subseteq H$ of left-representatives such that $H = \bigcup \{uH_g \mid u \in U_g\}$. Thus,

$$\begin{aligned} Kg &= \bigcup \{K \cap uH_g \mid u \in U_g\}\, g = \bigcup \left\{ug\, g^{-1}(u^{-1}K \cap H_g)g \,\middle|\, u \in U_g\right\} \\ &= \bigcup \left\{g'g^{-1}(u^{-1}K \cap H_g)g \,\middle|\, g' \in U_g g\right\}. \end{aligned}$$

Using Lemma 12 we obtain $g^{-1}(u^{-1}K \cap H_g)g = K' \in \mathrm{Rat}(H)$. This shows the claim.

Let L be a flat rational subset G, that is, L is equal to a finite union of languages $L_0g_1L_1 \cdots g_tL_t$ where all $L_i \in \mathrm{Rat}(H)$. Using the claim, we can write L as a finite union of languages gK with $g \in G$ and $K \in \mathrm{Rat}(H)$. Since the membership in H is decidable, we can computably enumerate a set S of all distinct representatives of the right cosets of H, and moreover for each $g \in G$ find a representative $g' \in S$ such that $g \in g'H$. Since $g = g'h$ for some $h \in H$, we can write $gK = g'(hK)$, where $hK \in \mathrm{Rat}(H)$. Therefore, every flat rational set L can be written as a union $L = \bigcup_{i=1}^{n} g_iK_i$, where $g_i \in S$ and $K_i \in \mathrm{Rat}(H)$. Since $gK_1 \cup gK_2 = g(K_1 \cup K_2)$, we may assume that all g_i in the expression $L = \bigcup_{i=1}^{n} g_iK_i$ are different.

Now let L and R be two flat rational sets. By the above argument we may assume that

$$L = \bigcup_{i=1}^{n} a_iL_i \quad \text{and} \quad R = \bigcup_{j=1}^{m} b_jR_j,$$

where $a_i, b_j \in S$ and $L_i, R_j \in \mathrm{Rat}(H)$. Then we have

$$L \setminus R = \bigcup_{i=1}^{n} \big(a_iL_i \setminus \bigcup_{j=1}^{m} b_jR_j\big).$$

Note that if $a_i \notin \{b_1, \ldots, b_m\}$, then $a_i L_i \setminus \bigcup_{j=1}^m b_j R_j = a_i L_i$, but if $a_i = b_j$ for some j then $a_i L_i \setminus \bigcup_{j=1}^m b_j R_j = a_i(L_i \setminus R_j)$. Since $\mathrm{Rat}(H)$ is an effective Boolean algebra, we can compute the rational expression for $L_i \setminus R_j$ in H. Hence we can compute the flat rational expression for $L \setminus R$. ◀

Below we give one more application of Theorem 10. Let $P(2,\mathbb{Q})$ we denote the following submonoid of $\mathrm{GL}(2,\mathbb{Q})$ of matrices:

$$P(2,\mathbb{Q}) = \{h \in \mathrm{GL}(2,\mathbb{Q}) \mid |\det(h)| > 1\} \cup \mathrm{GL}(2,\mathbb{Z}).$$

Note that $P(2,\mathbb{Q})$ contains all nonsingular matrices from $M(2,\mathbb{Z})$. So, the following theorem is a generalization of the main result in [25].

▶ **Theorem 13.** *Let $g \in \mathrm{GL}(2,\mathbb{Q})$ and R be a flat rational subset of $\mathrm{GL}(2,\mathbb{Q})$ with respect to $P(2,\mathbb{Q})$. Then we can decide $g \in R$.*

Proof. Smith normal forms tells us that

$$g = c_r e s_n f = c_r e \left(\begin{smallmatrix} 1 & 0 \\ 0 & n \end{smallmatrix}\right) f,$$

where $c_r = \left(\begin{smallmatrix} r & 0 \\ 0 & r \end{smallmatrix}\right)$ is central, $e, f \in \mathrm{SL}(2,\mathbb{Z})$ and $r \in \mathbb{Q}$. Replacing R by $r^{-1}e^{-1}Rf^{-1}$, we may assume that $g = s_n$ with $0 \neq n \in \mathbb{Z}$. Moreover, by making guesses we may assume that

$$R = R_0 g_1 R_1 \cdots g_t R_t$$

where $R_i \in \mathrm{Rat}(P(2,\mathbb{Q}))$ and each g_i is of the form $g_i = \left(\begin{smallmatrix} r & 0 \\ 0 & r \end{smallmatrix}\right)$ with $0 < r < 1$. Multiplying g and R with some appropriate natural number, we can assume that $g = \left(\begin{smallmatrix} m & 0 \\ 0 & n \end{smallmatrix}\right)$ with $m, n \in \mathbb{N} \setminus \{0\}$ and $R \in \mathrm{Rat}(P(2,\mathbb{Q}))$.

Without restriction we may assume that R is given by a trim NFA $\mathcal{A}$ with state space Q, initial states I and final states F. (Trim means that every state is on some accepting path.) Note that a path in $\mathcal{A}$ accepting g can use transitions with labels from $P(2,\mathbb{Q}) \setminus \mathrm{GL}(2,\mathbb{Z})$ at most $k = \left\lfloor \frac{\log(mn)}{\log t} \right\rfloor$ many times, where

$$t = \min\{\, |\det(h)| \;:\; |\det(h)| > 1 \text{ and } h \text{ appears as a label of a transition in } \mathcal{A}\,\}.$$

Consider a new automaton $\mathcal{B}$ with state space $Q \times \{0, \ldots, k\}$, initial states $I \times \{0\}$ and final states $F \times \{0, \ldots, k\}$. The transitions of $\mathcal{B}$ are defined as follows:

- for every transition $p \xrightarrow{g} q$ in $\mathcal{A}$ with $g \in \mathrm{GL}(2,\mathbb{Z})$, there is a transition $(p,i) \xrightarrow{g} (q,i)$ in $\mathcal{B}$ for every $i = 0, \ldots, k$;
- for every transition $p \xrightarrow{g} q$ in $\mathcal{A}$ with $g \in P(2,\mathbb{Q}) \setminus \mathrm{GL}(2,\mathbb{Z})$, there is a transition $(p,i) \xrightarrow{g} (q,i+1)$ in $\mathcal{B}$ for every $i = 0, \ldots, k-1$.

The automaton $\mathcal{B}$ defines a flat rational subset $R' \subseteq R$ over $\mathrm{GL}(2,\mathbb{Z})$ such that $g \in R' \iff g \in R$. So, using Theorem 10, we can decide whether $g \in R'$ and hence whether $g \in R$. ◀

4 Dichotomy in $\mathrm{GL}(2,\mathbb{Q})$

In the following we show a dichotomy result. To the best of the authors the result has not been stated elsewhere. The dichotomy shows that extending our decidability results beyond flat rational sets over $\mathrm{GL}(2,\mathbb{Z})$ seems to be quite demanding.

▶ **Theorem 14.** *Let G be a f.g. group such that $\mathrm{GL}(2,\mathbb{Z}) < G \leq \mathrm{GL}(2,\mathbb{Q})$. Then there are two mutually exclusive cases.*

1. *G is isomorphic to* $\mathrm{GL}(2,\mathbb{Z}) \times \mathbb{Z}^k$*, with $k \geq 1$, and does not contain a copy of the Baumslag-Solitar group* $\mathrm{BS}(1,q)$ *for any $q \geq 2$.*
2. *G contains a subgroup which is an extension of* $\mathrm{BS}(1,q)$*, for some $q \geq 2$, of infinite index.*

Proof. Let $H = \mathrm{GL}(2,\mathbb{Z})$. There are two cases. In the first case some finite generating set for G contains only elements from H and from the center $Z(G)$. Since $\mathrm{GL}(2,\mathbb{Z}) \leq G$ we see that $Z(G) \leq \{\left(\begin{smallmatrix} r & 0 \\ 0 & r \end{smallmatrix}\right) \mid r \in \mathbb{Q}\}$. Moreover, since $\left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right) \in H$, we may assume in the fist case that G is generated by H and f.g. subgroup $Z \leq \{\left(\begin{smallmatrix} r & 0 \\ 0 & r \end{smallmatrix}\right) \mid r \in \mathbb{Q} \wedge r > 0\}$. The homomorphism $g \mapsto |\det(g)|$ embeds Z into the torsion free group $\{r \in \mathbb{Q}^* \mid r > 0\}$. Hence, Z is isomorphic to $\mathbb{Z}^k$ for some $k \geq 1$. Since $Z \cap H = \{1\}$, the canonical surjective homomorphism from $Z \times H$ onto G is an isomorphism.

In the second case we start with any generating set and we write the generators in Smith normal form $e \left(\begin{smallmatrix} r & 0 \\ 0 & rq \end{smallmatrix}\right) f$. Since $e, f \in \mathrm{GL}(2,\mathbb{Z})$ and $\mathrm{GL}(2,\mathbb{Z}) < G$, without restriction, the generators are either from $\mathrm{GL}(2,\mathbb{Z})$ or they have the form $\left(\begin{smallmatrix} r & 0 \\ 0 & rq \end{smallmatrix}\right)$ with $r > 0$ and $0 \neq q \in \mathbb{N}$. So, if we are not in the first case, there is at least one generator $s = \left(\begin{smallmatrix} r & 0 \\ 0 & rq \end{smallmatrix}\right)$ where $r > 0$ and $2 \leq q \in \mathbb{N}$.

Let BS be the subgroup of G which is generated by $\left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$ and s and $\mathrm{BS}(1,q)$ be the Baumslag-Solitar group with generators b and t such that $tbt^{-1} = b^q$. We have $s \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right) s^{-1} = \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)^q$. Hence there is surjective homomorphism $\varphi : \mathrm{BS}(1,q) \to G$ such that $\varphi(t) = s$ and $\varphi(b) = \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$. Let us show that φ is an isomorphism. Every element $g \in \mathrm{BS}(1,q)$ can be written the form $t^k b^x t^n$ where k, x, n are integers. Suppose $\varphi(t^k b^x t^n) = 1$. Then $\left(\begin{smallmatrix} 1 & 0 \\ x & 1 \end{smallmatrix}\right) = \varphi(b^x) = \varphi(t^{-k-n}) = \left(\begin{smallmatrix} r & 0 \\ 0 & rq \end{smallmatrix}\right)^{-k-n}$ is a diagonal matrix. This implies $x = 0$. But then $g = t^m$ and $\varphi(g) = s^m = 1$ implies $m = 0$. Hence, φ is an isomorphism and BS is the group $\mathrm{BS}(1,q)$. Moreover, consider any $g \in \mathrm{BS} \cap \mathrm{SL}(2,\mathbb{Z})$. As above $g = s^k \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)^x s^m$ with $x, k, m \in \mathbb{Z}$. Since by assumption $\det(g) = 1$ we obtain $m = -k$ and hence $g = \left(\begin{smallmatrix} 1 & 0 \\ xk & 1 \end{smallmatrix}\right) \in \langle\left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)\rangle$. Therefore $\mathrm{SL}(2,\mathbb{Z}) \cap \mathrm{BS}$ is the infinite cyclic group $\langle\left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)\rangle = \mathbb{Z}$, which has infinite index in $\mathrm{SL}(2,\mathbb{Z})$. It follows that G contains an extension of $\mathrm{BS}(1,q)$ of infinite index.

But this is not enough, we need to show that $\mathrm{GL}(2,\mathbb{Z}) \times \mathbb{Z}^k$ cannot contain $\mathrm{BS}(1,q)$, otherwise there is no dichotomy. Actually, we do a little bit more: $\mathrm{BS}(1,q)$ is not a subgroup in $\mathrm{GL}(2,\mathbb{Z}) \times A$ for all abelian groups A. Assume by contradiction that it is. Then there are generators $b = (a,x), t = (s,y) \in \mathrm{GL}(2,\mathbb{Z}) \times A$ such that $tbt^{-1} = b^q$. As $q \geq 2$ this implies $x = 0$. Thus, $b = (a,0)$. Consider the canonical projection φ of $\mathrm{GL}(2,\mathbb{Z}) \times A$ onto $\mathrm{GL}(2,\mathbb{Z})$ such that $\varphi(b) = a$ and $\varphi(t) = s$. We claim that the restriction of φ to $\langle b, t\rangle$ is injective.

Let $\varphi(g) = 1$ for $g \in \langle b, t\rangle$. As above we write $g = t^k b^z t^n$ with $z, k, n \in \mathbb{Z}$. Then we have $s^k a^z s^n = 1 \in \mathrm{GL}(2,\mathbb{Z})$; and therefore $a^z = s^{-k-n}$. Hence a^z commutes with s, but since $sas^{-1} = a^q$ for $q \geq 2$, this is possible only if $z = 0$. Hence $g = t^m$ for some $m \in \mathbb{Z}$. Since $\varphi(g) = 1$, we know $s^m = 1$ and hence $m = 0$. This tells us that φ is injective on $\langle b, t\rangle$, and the claim follows.

The above claim implies that $\mathrm{BS}(1,q)$ appears as a subgroup in $\mathrm{GL}(2,\mathbb{Z})$. However, no virtually free group can contain $\mathrm{BS}(1,q)$ by [13]; and $\mathrm{GL}(2,\mathbb{Z})$ is virtually free. A contradiction.

Actually, [13] shows a stronger result. If a Baumslag-Solitar group $\mathrm{BS}(p,q)$ appears in a group G with $pq \neq 0$, then G is not hyperbolic. On the other hand, f.g. virtually free groups are basic examples of hyperbolic groups. ◀

▶ **Proposition 15.** *Let G be isomorphic to* $\mathrm{GL}(2,\mathbb{Z}) \times \mathbb{Z}^k$ *with $k \geq 1$. Then, the question "$L = R$?" on input $L, R \in \mathrm{Rat}(G)$ is undecidable. However, the question "$g \in R$?" on input $g \in G$ and $R \in \mathrm{Rat}(G)$ is decidable.*

Proof. The group $\mathrm{GL}(2,\mathbb{Z})$ contains a free monoid $\{a,b\}^*$ of rank 2. Thus, under the conditions above, G contains the free partially commutative monoid $M = \{a,b\}^* \times \{c\}^*$. It is known that the question "$L = R$?" on input $L, R \in \mathrm{Rat}(G)$ is undecidable for M, see [17].

For the decidability we use the fact that $\mathrm{SL}(2,\mathbb{Z})$ has a free subgroup F of rank two and index 12. Thus, the index of F in $\mathrm{GL}(2,\mathbb{Z})$ is 24 and therefore finite. By [21] the question "$g \in R$?" is decidable in $F \times \mathbb{Z}^k$. Since $F \times \mathbb{Z}^k$ is of finite index (actually 24) in G, the membership in G is decidable by Proposition 7. ◀

▶ Remark 16. Let G be a group extension of $\mathrm{GL}(2,\mathbb{Z})$ inside $\mathrm{GL}(2,\mathbb{Q})$ which is not isomorphic to $\mathrm{GL}(2,\mathbb{Z}) \times \mathbb{Z}^k$ for $k \geq 0$. Then, by Theorem 14, the group G contains an infinite extension of $\mathrm{BS}(1,q)$ for $q \geq 2$. To date (when this text was written) it is still open whether the membership in rational sets of $\mathrm{BS}(1,q)$ is decidable. However, even if it was decidable, it is by far not clear how to extend these results to infinite extensions of $\mathrm{BS}(1,q)$.

5 Singular matrices

5.1 Membership for the zero matrix

The membership problem for the zero matrix is decidable with respect to the largest class of flat rational sets we are considering in our paper.

▶ **Theorem 17.** *Let P the submonoid of $M(2,\mathbb{Q})$ which is generated by all central matrices $\left(\begin{smallmatrix} r & 0 \\ 0 & r \end{smallmatrix}\right)$, all matrices in $\mathrm{GL}(2,\mathbb{Z})$ and all matrices $h \in M(2,\mathbb{Z})$ with $\det(h) = 0$. If $R \subseteq M(2,\mathbb{Q})$ is flat rational over P, then we can decide $\left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right) \in R$.*

Proof. We may assume that R is given by a trim NFA over a f.g. submonoid M of $\mathrm{M}(2,\mathbb{Q})$. If any transition is labeled by 0, then we have $0 \in R$ since the NFA is trim. Thus, we may assume that all transitions labeled by a central matrix are invertible. However, invertible central matrices have no effect for accepting 0. Thus, we can assume that all transitions labeled by a central matrix are the identity matrix. These transitions can be removed by standard techniques. Thus, we can assume that R is flat rational over $\mathrm{GL}^0(2,\mathbb{Z}) = \mathrm{GL}(2,\mathbb{Z}) \cup \{g \in \mathrm{M}(2,\mathbb{Z}) \mid \det(g) = 0\}$. Replacing R by $R' = \left(\begin{smallmatrix} k & 0 \\ 0 & k \end{smallmatrix}\right) \cdot R$ where $k \in \mathbb{N}$ is large enough, we may eventually assume that $R \subseteq \mathrm{M}(2,\mathbb{Z})$ is flat rational over $\mathrm{GL}^0(2,\mathbb{Z})$. The result follows from Theorem 18. ◀

5.2 Membership for the singular matrices

Throughout this section, H denotes $\mathrm{GL}(2,\mathbb{Z})$; and for $a \in \mathbb{Z}$ we let

$$M_{ij}(a) = \{\left(\begin{smallmatrix} g_{11} & g_{12} \\ g_{21} & g_{22} \end{smallmatrix}\right) \in H \mid g_{ij} = a\}\,.$$

The monoid P' mentioned in Theorem 18 is a proper submonoid of monoid P mentioned in Theorem 17. The difference is that P allows all central matrices whereas P' allows only those matrices $\left(\begin{smallmatrix} r & 0 \\ 0 & r \end{smallmatrix}\right)$ where r is a natural number.

▶ **Theorem 18.** *Let P' the submonoid of $M(2,\mathbb{Q})$ which is generated by all central matrices $\left(\begin{smallmatrix} r & 0 \\ 0 & r \end{smallmatrix}\right)$ with $r \in \mathbb{N}$, all matrices in $\mathrm{GL}(2,\mathbb{Z})$ and all matrices $h \in M(2,\mathbb{Z})$ with $\det(h) = 0$. If $R \subseteq M(2,\mathbb{Q})$ is flat rational over P', then we can decide $g \in R$ for all singular matrices g in $M(2,\mathbb{Q})$.*

The proof of Theorem 18 covers the rest of Section 5.2. The following lemma was originally shown in [26], but we include its proof here for completeness.

▶ **Lemma 19.** *The sets $M_{ij}(a) \subseteq M(2,\mathbb{Z})$ are rational for all i, j and $a \in \mathbb{Z}$.*

Proof. For $a = 0$ we see that $M_{21}(0) = \pm \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)^{\mathbb{Z}}$ is rational. From that we can easily deduce that $M_{ij}(0) \in \mathrm{Rat}(H)$ for all i, j.

Therefore let $a \neq 0$. Let us show that $M_{ij}(a) \in \mathrm{Rat}(H)$ for al i, j. We content ourselves to show it for $M_{11}(a)$. Indeed, then we have $g \in M_{11}(a)$ if and only if $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = \left(\begin{smallmatrix} a & b_0+ma \\ c_0+na & d \end{smallmatrix}\right)$ where $m, n \in \mathbb{Z}$ and $0 \leq b_0, c_0 < |a|$. Moreover.

$$\left(\begin{smallmatrix} a & b_0+ma \\ c_0+na & d \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 0 \\ n & 1 \end{smallmatrix}\right) \left(\begin{smallmatrix} a & b_0 \\ c_0 & d' \end{smallmatrix}\right) \left(\begin{smallmatrix} 1 & m \\ 0 & 1 \end{smallmatrix}\right)$$

where $d' = \frac{1+b_0c_0}{a} \in \mathbb{Z}$ and $0 \leq d' \leq |a|$. Hence, $M_{11}(a) \in \mathrm{Rat}(H)$ because $M(a)$ is a finite union of languages of type

$$\left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)^{\mathbb{Z}} \left(\begin{smallmatrix} a & b_0 \\ c_0 & d' \end{smallmatrix}\right) \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)^{\mathbb{Z}}.$$

The assertion of Lemma 19 follows. ◀

We may assume that R is given by a trim NFA $\mathcal{A}$ over a f.g. submonoid M of $\mathrm{M}(2,\mathbb{Q})$. Without restriction, all transitions are labeled with elements of H or rs_q for $q \in \mathbb{N}$ or $r \geq 0$. If $g = 0$ and there is one transition labeled by 0, then we know $g \in R$. For $g \neq 0$ we cannot use any transition labeled by 0. Hence without restriction, if a transition is labeled by a rational number r, then $r > 0$. Using Smith normal form and writing rs_q as a product, in the beginning all transitions are labeled either by a matrix in $\mathrm{GL}(2,\mathbb{Z})$ or by a central matrix $\left(\begin{smallmatrix} r & 0 \\ 0 & r \end{smallmatrix}\right)$ or by $s_0 = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right)$.

Since $\det(g) = 0$, such a transition must be used at least once. So, by writing R as a finite union $R_1 \cup R_m$ and guessing the correct j we may assume without restriction that $g \in R_j = R = L_1 s_0 L_2$ where $L_i \in \mathrm{Rat}(M)$. Note that the L_i are just rational, and not assumed to be flat rational. Throughout we use the following equation for $r \in \mathbb{Q}$ and $a, b, c, d \in \mathbb{Z}$:

$$s_0 r \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) s_0 = s_0 \left(\begin{smallmatrix} ra & 0 \\ 0 & 0 \end{smallmatrix}\right) s_0 = s_0 ras_0 = ras_0. \tag{1}$$

Now, we perform a first round of "flooding-the-NFA" with more transitions without changing the state set.

1. For all states p, q of $\mathcal{A}$ consider the subautomaton $\mathcal{B}$ where p is the unique initial and q is the unique final state and where all transitions are labeled by $h \in H$ (all other are removed from $\mathcal{A}$). This defines a rational language $L(p,q) \in \mathrm{Rat}(H)$.
2. Introduce for all states p, q of $\mathcal{A}$ an additional new transition labeled by $L(p,q)$.
3. If $g = 0$ and $0 \in L(p,q)$, then accept $g \in R$. After that replace all $L(p,q)$ by $L(p,q) \setminus \{0\}$.
4. If $1 \in L(p,q)$ where $1 = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ is the identity matrix, replace $L(p,q)$ by $L(p,q) \setminus \{1\}$ and introduce a new transition $p \xrightarrow{1} q$.

After that we may assume that all accepting paths of $\mathcal{A}$ are as follows:

$$p_1 \xrightarrow{L_1} q_1 \xrightarrow{r_1 s_0} p_2 \xrightarrow{L_2} \cdots \xrightarrow{r_k s_0} p_k \xrightarrow{L_k} q_k \tag{2}$$

where $r_i \in \mathbb{Q}$, $r_i > 0$, and $0, 1 \notin L_i$ for all $1 \leq i \leq k$. We may assume the transition $p_1 \xrightarrow{L_1} q_1$ is the only transition leaving a unique initial state p_1.

It is convenient to assume that the states are divided into two sets: p-states where outgoing transitions labeled by rational subsets of H and which lead to q-states; and q-states where outgoing transitions labeled by rs_0 and lead to p-states. In particular, $p_i \neq q_j$ for all i, j.

Since R is flat over P', there is constant ρ depending on R such that each accepting path as in (2) uses a transition labeled by $r = \left(\begin{smallmatrix} r & 0 \\ 0 & r \end{smallmatrix}\right)$ with $r \notin \mathbb{N}$ at most ρ times. Splitting R again into a finite union we may assume that all accepting paths have the form

$$q_0 \xrightarrow{r} p_1 \xrightarrow{L_1} q_1 \xrightarrow{r_1 s_0} p_2 \xrightarrow{L_2} \cdots \xrightarrow{r_k s_0} p_k \xrightarrow{L_k} q_k \tag{3}$$

where the $r \in \mathbb{Q}$, $r \neq 0$, $r_i \in \mathbb{N} \setminus \{0\}$, and $0, 1 \notin L_i \in \mathrm{Rat}(M)$. Here, q_0 is a new unique initial state. We choose some $z \in \mathbb{Z}$ such that $rz \in \mathbb{N}$; and we aim to decide $zg \in zR$. The NFA for zR is obtained by making the unique p_1-state initial again, to remove q_0, and to replace all outgoing transitions $q_1 \xrightarrow{r_1 s_0} p_2$ by $q_1 \xrightarrow{z r_1 s_0} p_2$. After that little excursion we are back at a situation as in (2). The difference is that all r_i are positive natural numbers. In order to have $g \in R$, we must have $g \in \mathrm{M}(2, \mathbb{Z})$. So, we can assume that, too.

Phrased differently, without restriction from the very beginning $g \in \mathrm{M}(2, \mathbb{Z})$, $\det(g) = 0$, and $\mathcal{A}$ accepts R such that all accepting paths are as in (2) where all $r_i \in \mathbb{N} \setminus \{0\}$.

Let $g = \left(\begin{smallmatrix} g_{11} & g_{12} \\ g_{21} & g_{22} \end{smallmatrix}\right)$. We define a *target* value $t \in \mathbb{N}$ by the greatest common divisor of the numbers in $\{g_{11}, g_{12}, g_{21}, g_{22}\}$.

We keep the following assertion as an invariant. If a transition $q \xrightarrow{rs_0}$ appears in $\mathcal{A}$, then r divides t. This leads to second "flooding" with transitions.

Second flooding. As long as possible, do the following.

- Choose a sequence of transitions $q' \xrightarrow{rs_0} p \xrightarrow{L} q \xrightarrow{r's_0} p'$ and an integer $z \in \mathbb{Z}$ such that:
  1. $z = 0 \iff g = 0$,
  2. the integer rzr' divides t,
  3. we have $L \cap M_{11}(z) \neq \emptyset$,
  4. there is no transition $q' \xrightarrow{rzr'} p'$.
- Introduce an additional transition $q' \xrightarrow{rzr'} p'$.

It is clear that the procedure terminates since for $g \neq 0$ the target t has only finitely many divisors. So, the number of integers r, z, r' such that rzr' divides t is finite for $g \neq 0$. For $g = 0$ we have $z = 0$ and 0 divides the target 0. The accepted language of $\mathcal{A}$ was not changed. But now, every accepting path for g can take short cuts. As a consequence, we may assume that all accepting paths for g have length three:

$$p_1 \xrightarrow{L_1} q_1 \xrightarrow{rs_0} p_2 \xrightarrow{L_2} q_2. \tag{4}$$

By guessing such a sequence of length three, we may assume that the NFA is exactly that path in (4) with those four states and where r divides t.

We are ready to check whether $g \in L(\mathcal{A})$. Indeed, we know that each matrix $m \in L(\mathcal{A})$ can be written as

$$m = f_1 r s_0 f_2$$

with $f_k \in L_k \in \mathrm{Rat}(H)$ for $k = 1, 2$. We can write $f_1 r s_0 = r \left(\begin{smallmatrix} a & 0 \\ b & 0 \end{smallmatrix}\right)$ and $s_0 f_2 = \left(\begin{smallmatrix} c & d \\ 0 & 0 \end{smallmatrix}\right)$ where the a, b, c, d depend on the pair (f_1, f_2). Hence

$$m = rfs_0h = rfs_0s_0h = r \left(\begin{smallmatrix} a & 0 \\ b & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} c & d \\ 0 & 0 \end{smallmatrix}\right) = r \left(\begin{smallmatrix} ac & ad \\ bc & bd \end{smallmatrix}\right).$$

Remember that $0 \neq r \in \mathbb{Z}$. We make the final tests. We have $g \in R$ if and only if r, L_1, and L_2 allow to have the four values rac, rad, rbc, rbd to be the corresponding g_{ij}. To see this we start with eight tests "$0 \in M_{ij}(0) \ \cap L_k = \emptyset$?". After that it is enough to consider those entries g_{ij} where $g_{ij} \neq 0$. But then each g_{ij}/r has finitely many divisors $e \in \mathbb{Z}$, only. Thus, a few tests "$M_{ij}(e) \ \cap L_k = \emptyset$?" suffice to decide $g \in R$. We are done.

References

1 A. V. Anisimow and F. D. Seifert. Zur algebraischen Charakteristik der durch kontext-freie Sprachen definierten Gruppen. *Elektron. Informationsverarbeit. Kybernetik*, 11(10–12):695–702, 1975.

2 G. Baumslag and D. Solitar. Some two-generator one-relator non-Hopfian groups. *Bull. Amer. Math. Soc.*, 68:199–201, 1962.

3 P. Bell, V. Halava, T. Harju, J. Karhumäki, and I. Potapov. Matrix equations and Hilbert's tenth problem. *IJAC*, 18(8):1231–1241, 2008.

4 P. C. Bell, M. Hirvensalo, and I. Potapov. The identity problem for matrix semigroups in $\mathrm{SL}_2(\mathbb{Z})$ is NP-complete. In *Proceedings of the Annual ACM-SIAM Symposium on Discrete Algorithms (SODA'17)*, pages 187–206, 2017.

5 P. C. Bell, I. Potapov, and P. Semukhin. On the mortality problem: From multiplicative matrix equations to linear recurrence sequences and beyond. In *44th International Symposium on Mathematical Foundations of Computer Science, MFCS 2019, August 26-30, 2019, Aachen, Germany.*, pages 83:1–83:15, 2019.

6 M. Benois. Parties rationelles du groupe libre. *C. R. Acad. Sci. Paris, Sér. A*, 269:1188–1190, 1969.

7 J. Cassaigne, V. Halava, T. Harju, and F. Nicolas. Tighter undecidability bounds for matrix mortality, zero-in-the-corner problems, and more. *CoRR*, abs/1404.0644, 2014.

8 E. Charlier and J. Honkala. The freeness problem over matrix semigroups and bounded languages. *Information and Computation*, 237:243–256, 2014.

9 L. Ciobanu and M. Elder. Solutions sets to systems of equations in hyperbolic groups are EDT0L in PSPACE. In C. Baier, I. Chatzigiannakis, P. Flocchini, and S. Leonardi, editors, *46th International Colloquium on Automata, Languages, and Programming (ICALP 2019)*, volume 132 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 110:1–110:15, Dagstuhl, Germany, 2019. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik.

10 T. Colcombet, J. Ouaknine, P. Semukhin, and J. Worrell. On reachability problems for low-dimensional matrix semigroups. In *46th International Colloquium on Automata, Languages, and Programming, ICALP 2019, July 9-12, 2019, Patras, Greece.*, pages 44:1–44:15, 2019.

11 S. Eilenberg. *Automata, Languages, and Machines*, volume A. Academic Press, New York and London, 1974.

12 S. Eilenberg and M.-P. Schützenberger. Rational sets in commutative monoids. *Journal of Algebra*, 13:173–191, 1969.

13 S. M. Gersten. Dehn functions and l_1-norms of finite presentations. In *Algorithms and classification in combinatorial group theory (Berkeley, CA, 1989)*, volume 23 of *Math. Sci. Res. Inst. Publ.*, pages 195–224. Springer, New York, 1992.

14 Z. Grunschlag. *Algorithms in Geometric Group Theory.* PhD thesis, University of California, 1999. AAI9931252.

15 T. Harju. Post correspondence problem and small dimensional matrices. In *Developments in Language Theory, 13th International Conference, DLT 2009, Stuttgart, Germany, June 30 - July 3, 2009. Proceedings*, pages 39–46, 2009.

16 J. Hillman. Commensurators and deficiency. Preprint available at `http://www.maths.usyd.edu.au/u/pubs/publist/preprints/2007/hillman-18.pdf`.

17 IJsbrand Jan Aalbersberg and H. J. Hoogeboom. Characterizations of the decidability of some problems for regular trace languages. *Mathematical Systems Theory*, 22:1–19, 1989.

18 S. C. Kleene. Representation of events in nerve nets and finite automata. In C. E. Shannon and J. McCarthy, editors, *Automata Studies*, number 34 in Annals of Mathematics Studies, pages 3–40. Princeton University Press, 1956.

19 S. Ko, R. Niskanen, and I. Potapov. On the identity problem for the special linear group and the heisenberg group. In *45th International Colloquium on Automata, Languages, and Programming, ICALP 2018, July 9-13, 2018, Prague, Czech Republic*, pages 132:1–132:15, 2018.

20 D. König, M. Lohrey, and G. Zetzsche. Knapsack and subset sum problems in nilpotent, polycyclic, and co-context-free groups. *CoRR*, abs/1507.05145, 2015.

21 M. Lohrey and B. Steinberg. The submonoid and rational subset membership problems for graph groups. *Journal of Algebra*, 320(2):728–755, 2008.

22 A. Markov. On certain insoluble problems concerning matrices. *Doklady Akad. Nauk SSSR*, 57(6):539–542, June 1947.

23 K. A. Mihailova. The occurrence problem for direct products of groups. *Dokl. Akad. Nauk SSSR*, 119:1103–1105, 1958. English translation in: Math. USSR Sbornik, 70: 241–251, 1966.

24 I. Potapov. Reachability problems in matrix semigroups. *Dagstuhl Reports*, 9(3):95–98, 2019.

25 I. Potapov and P. Semukhin. Decidability of the membership problem for 2×2 integer matrices. In *Proceedings of the Twenty-Eighth Annual ACM-SIAM Symposium on Discrete Algorithms, SODA*, pages 170–186, 2017.

26 I. Potapov and P. Semukhin. Membership problem in $\mathrm{GL}(2, \mathbb{Z})$ extended by singular matrices. In *42nd International Symposium on Mathematical Foundations of Computer Science, MFCS 2017, August 21-25, 2017 - Aalborg, Denmark*, pages 44:1–44:13, 2017.

27 J. Sakarovitch. The “last” decision problem for rational trace languages. In I. Simon, editor, *Proc. 1st Latin American Symposium on Theoretical Informatics (LATIN’92)*, volume 583 of *Lecture Notes in Computer Science*, pages 460–473, Heidelberg, 1992. Springer-Verlag.

28 G. Sénizergues. On the rational subsets of the free group. *Acta Informatica*, 33:281–296, 1996.

29 G. Sénizergues. Personal communication, 2019.

30 J.-P. Serre. *Trees*. Springer, 1980. French original 1977.

31 P. Silva. An automata-theoretic approach to the study of fixed points of endomorphisms. In J. González-Meneses, M. Lustig, and E. Ventura, editors, *Algorithmic and Geometric Topics Around Free Groups and Automorphisms*, Advanced Courses in Mathematics - CRM Barcelona. Birkhäuser, Basel, Switzerland, 2017.

32 P. V. Silva. Recognizable subsets of a group: finite extensions and the abelian case. *Bulletin of the EATCS*, 77:195–215, 2002.