

Decidability of Membership Problems for Flat Rational Subsets of $GL(2, \mathbb{Q})$ and Singular Matrices

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

Igor Potapov
Department of Computer Science,
University of Liverpool
Liverpool, United Kingdom
potapov@liverpool.ac.uk

Pavel Semukhin
Department of Computer Science,
University of Oxford
Oxford, United Kingdom
pavel.semukhin@cs.ox.ac.uk

ABSTRACT

This work relates numerical problems on matrices over the rationals to symbolic algorithms on words and finite automata. Using exact algebraic algorithms and symbolic computation, we prove new decidability results for 2×2 matrices over \mathbb{Q} . Namely, we introduce a notion of *flat rational sets*: if M is a monoid and $N \leq M$ is its submonoid, then flat rational sets of M relative to N are finite unions of the form $L_0 g_1 L_1 \cdots g_l L_l$ where all L_i s 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 $GL(2, \mathbb{Q})$ over $GL(2, \mathbb{Z})$ is decidable.

We also show a dichotomy for nontrivial group extension of $GL(2, \mathbb{Z})$ in $GL(2, \mathbb{Q})$: if G is a f.g. group such that $GL(2, \mathbb{Z}) < G \leq GL(2, \mathbb{Q})$, then either $G \cong GL(2, \mathbb{Z}) \times \mathbb{Z}^k$, for some $k \geq 1$, or G contains an extension of the Baumslag-Solitar group $BS(1, q)$, with $q \geq 2$, 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, decidability of the membership problem is open for every such G . 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.

CCS CONCEPTS

• **Theory of computation** → **Formal languages and automata theory**; • **Computing methodologies** → **Symbolic and algebraic algorithms**.

KEYWORDS

membership problem, rational sets, general linear group

Partial support for V. Diekert by the DFG grant DI 435/7, for I. Potapov by the EPSRC grant EP/R018472/1 and for P. Semukhin by the ERC grant AVS-ISS (648701) is greatly acknowledged.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.

ISSAC '20, July 20–23, 2020, Kalamata, Greece

© 2020 Association for Computing Machinery.

ACM ISBN 978-1-4503-7100-1/20/07...\$15.00

<https://doi.org/10.1145/3373207.3404038>

ACM Reference Format:

Volker Diekert, Igor Potapov, and Pavel Semukhin. 2020. Decidability of Membership Problems for Flat Rational Subsets of $GL(2, \mathbb{Q})$ and Singular Matrices. In *International Symposium on Symbolic and Algebraic Computation (ISSAC '20)*, July 20–23, 2020, Kalamata, Greece. ACM, New York, NY, USA, 8 pages. <https://doi.org/10.1145/3373207.3404038>

1 INTRODUCTION

Many problems in 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 these hard questions is the *membership problem* for matrix semigroups: Given $n \times n$ matrices $\{M, M_1, \dots, M_m\}$, determine whether there exist an integer $k \geq 1$ and $i_1, \dots, i_k \in \{1, \dots, m\}$ such that $M = M_{i_1} \cdots M_{i_k}$. In other words, determine whether a matrix belongs to a finitely generated (f.g. for short) semigroup. The membership problem has been intensively studied since 1947 when A. Markov showed in [29] 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* of a monoid. Rational sets are those which can be specified by regular expressions. A special case is the problem above: membership in the semigroup generated by the matrices M_1, \dots, M_m . Another difficult question is to decide the *knapsack problem*: “ $\exists x_1, \dots, x_m \in \mathbb{N} : M_1^{x_1} \cdots M_m^{x_m} = M$?”. Even significantly restricted cases of these problems become undecidable for high dimensional matrices over the integers [6, 26]; and very few cases are known to be decidable, see [3, 7, 12]. The decidability of the membership problem remains open even for 2×2 matrices over integers [11, 14, 21, 25, 33].

Membership in rational subsets of $GL(2, \mathbb{Z})$ (the 2×2 integer matrices with determinant ± 1) is decidable. Indeed, $GL(2, \mathbb{Z})$ has a free subgroup of rank 2 and of index 24 by [32]. Hence it is a f.g. virtually free group, and therefore the family of rational subsets forms an effective Boolean algebra [38, 40]. Two recent results which extended the border of decidability for the membership problem beyond $GL(2, \mathbb{Z})$ were [34, 35]. The first one is in case of the semigroups of 2×2 nonsingular integer matrices, and the second one is in case of $GL(2, \mathbb{Z})$ extended by integer matrices with zero determinant.

This paper pushes the decidability border even further. First of all, we consider membership problems for 2×2 matrices over the rationals whereas [34, 35] deal only with integer matrices. Since decidability of the rational membership problem is known for $GL(2, \mathbb{Z})$, we focus on subgroups G of $GL(2, \mathbb{Q})$ which contain $GL(2, \mathbb{Z})$.

In Sec. 4 we prove a dichotomy result. In the first case of the dichotomy, G is generated by $GL(2, \mathbb{Z})$ and central matrices $\begin{pmatrix} r & 0 \\ 0 & r \end{pmatrix}$.

In that case G is isomorphic to $\text{GL}(2, \mathbb{Z}) \times \mathbb{Z}^k$ 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 the best we can hope for if a group is sitting strictly between $\text{GL}(2, \mathbb{Z})$ and $\text{GL}(2, \mathbb{Q})$, in general.

If such a group G is not isomorphic to $\text{GL}(2, \mathbb{Z}) \times \mathbb{Z}^k$, then our dichotomy states that it contains a Baumslag-Solitar group $\text{BS}(1, q)$ for $q \geq 2$. The Baumslag-Solitar groups $\text{BS}(p, q)$ are defined by two generators a and t with the defining relation $ta^p t^{-1} = a^q$. They were introduced in [4] 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 $pq = 0$ [18]. As a consequence, in both cases of the dichotomy, $\text{GL}(2, \mathbb{Z})$ has infinite index in G . Actually, we prove more, namely, if G contains a matrix of the form $\begin{pmatrix} r_1 & 0 \\ 0 & r_2 \end{pmatrix}$ with $|r_1| \neq |r_2|$ (which is the second case in the dichotomy), then G contains some $\text{BS}(1, q)$ for $q \geq 2$ which has *infinite* index in G . It is wide open whether the membership to rational subsets of G can be decided in that second case. For example, let $p \geq 2$ be a prime, and let G' be generated by $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, and $\begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}$. In this case $\begin{pmatrix} p & 0 \\ 0 & p^{-1} \end{pmatrix}$ also belongs to G' . Due to [5], the matrices $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, and $\begin{pmatrix} p & 0 \\ 0 & p^{-1} \end{pmatrix}$ generate the group $\text{SL}(2, \mathbb{Z}[1/p])$.¹ So G' contains $\text{SL}(2, \mathbb{Z}[1/p])$ as a subgroup. The structure $\text{SL}(2, \mathbb{Z}[1/p])$ is known [39, II.1 Cor. 2] as an amalgam of two copies of $\text{SL}(2, \mathbb{Z})$ over a common subgroup of finite index. It is not even known how to decide subgroup membership in such amalgams. Moreover, $\begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}$ acts by conjugation on $\text{SL}(2, \mathbb{Z}[1/p])$, and since $\begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}$ generates an infinite cyclic group, we have that $G' = \text{SL}(2, \mathbb{Z}[1/p]) \rtimes \mathbb{Z}$. Hence, even if subgroup membership for $\text{SL}(2, \mathbb{Z}[1/p])$ was decidable, then it could still be undecidable in G' . The situation is better for the subgroup $\text{UT}(2, \mathbb{Z}[1/p]) \rtimes \mathbb{Z} \cong \mathbb{Z}[1/p] \rtimes \mathbb{Z} \cong \text{BS}(1, p)$ of G' (which is generated by $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}$) because the subgroup membership is decidable in f.g. metabelian groups [36].²

The complicated structures of simple examples of subgroups in $\text{SL}(2, \mathbb{Q})$ and $\text{GL}(2, \mathbb{Q})$ provide strong reasons to believe that the membership in rational sets becomes undecidable for subgroups of $\text{GL}(2, \mathbb{Q})$, in general. The dichotomy result Thm. 4.1 makes that very concrete. It led us in the direction where we came up with a new, but natural subclass of rational subsets. It is the class of *flat rational sets* $\text{Frat}(M, N)$. The new class satisfies surprisingly good properties. $\text{Frat}(M, N)$ is a relative notion where N is a submonoid of M . It consists of all finite unions of the form $L_0 g_1 L_1 \cdots g_t L_t$, where $g_i \in M$ and $L_i \in \text{Rat}(N)$. Of particular interest in our context is the class $\text{Frat}(G, H)$ where H and G are f.g. groups, $\text{Rat}(H)$ forms a Boolean algebra, and G is the commensurator³ of H . In this case Thm. 3.3 shows that $\text{Frat}(G, H)$ forms a relative Boolean algebra, i.e., it satisfies $L, K \in \text{Frat}(G, H) \implies L \setminus K \in \text{Frat}(G, H)$. Under some mild effectiveness assumptions this means that the

emptiness of finite Boolean combinations of sets in $\text{Frat}(G, H)$ 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 $\text{Rat}(G)$ need not be an effective Boolean algebra. The immediate application in the present paper concerns $\text{Frat}(\text{GL}(2, \mathbb{Q}), \text{GL}(2, \mathbb{Z}))$, see Thm. 3.3 and Cor. 3.4. For example, $\text{GL}(2, \mathbb{Z}) \times \mathbb{Z}$ appears in $\text{GL}(2, \mathbb{Q})$ and $\text{Rat}(\text{GL}(2, \mathbb{Z}) \times \mathbb{Z})$ is not an effective Boolean algebra. Still the smaller class of flat rational sets $\text{Frat}(\text{GL}(2, \mathbb{Z}) \times \mathbb{Z}, \text{GL}(2, \mathbb{Z}))$ is a relative Boolean algebra. In order to apply Thm. 3.3, we need $\text{Rat}(H)$ to be an effective relative Boolean algebra. It happens to be an effective Boolean algebra for virtually free groups and many other groups. This class includes, for example, all f.g. abelian groups, and it is closed under free products.

The power of flat rational sets is even more apparent in the context of the membership problem for rational subsets of $\text{GL}(2, \mathbb{Q})$. Let $P(2, \mathbb{Q})$ denote the monoid $\text{GL}(2, \mathbb{Z}) \cup \{h \in \text{GL}(2, \mathbb{Q}) \mid |\det(h)| > 1\}$; then Thm. 3.6 states that we can solve the membership problem “ $g \in R?$ ” for all $g \in \text{GL}(2, \mathbb{Q})$ and all $R \in \text{Frat}(\text{GL}(2, \mathbb{Q}), P(2, \mathbb{Q}))$. Thm. 3.6 generalizes the main result in [34].

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

We also consider singular matrices and generalize the main result of [35] as follows. Let g be a singular matrix in $M(2, \mathbb{Q})$ and let P be the submonoid generated by $\left\{ \begin{pmatrix} r & 0 \\ 0 & r \end{pmatrix} \mid r \in \mathbb{N} \right\} \cup \text{GL}(2, \mathbb{Z}) \cup \{h \in M(2, \mathbb{Z}) \mid \det(h) = 0\}$. Then we can decide the membership problem “ $g \in R?$ ” for all $R \in \text{Frat}(M(2, \mathbb{Q}), P)$.

Our paper concentrates on decidability. For the complexity of our algorithms with respect to binary encoding of matrices a trivial upper bound is exponential space. This follows, for instance, from [38]. We conjecture that membership for flat rational subsets of $\text{GL}(2, \mathbb{Q})$ over $\text{GL}(2, \mathbb{Z})$ is in NP and that the emptiness problem for Boolean combinations of such sets is in PSPACE.

The following facts about complexities are known: [20] shows that the *subgroup membership problem* is decidable in polynomial time for matrices from the modular group $\text{PSL}(2, \mathbb{Z})$. In [8], Thm. 5.2 says that membership for rational subsets for $\text{PSL}(2, \mathbb{Z})$ is in NP; and Cor. 5.2 states that the problem “ $1 \in \{M_1, \dots, M_n\}^*$ ” is NP-complete for $\text{SL}(2, \mathbb{Z})$.

Note that solving the membership problem for rational sets plays an important role in modern group theory as highlighted for example in [41] and used in [13].

2 PRELIMINARIES

By $M(n, R)$ we denote the ring of $n \times n$ matrices over a commutative ring R , and $\det : M(n, R) \rightarrow R$ is the determinant. By $\text{GL}(n, R)$ we mean the group of invertible matrices, that is, the matrices $g \in M(n, R)$ for which $\det(g)$ is a unit in R . By $\text{SL}(n, R)$ we denote the normal subgroup $\det^{-1}(1)$ of $\text{GL}(n, R)$, called the *special linear group*. Explicit calculation for $\text{SL}(2, \mathbb{Z})$ and for special linear groups over rings of p-adic numbers and function fields are e.g.

¹For the notation $\mathbb{Z}[1/p]$ and some elementary calculations see Sec. 6.

²Decidability of membership for rational subsets in $\text{BS}(1, q)$ for $q \geq 2$ was shown only very recently by Cadilhac, Chistikov, and Zetsche in [10].

³The notion of *commensurator* is a standard concept in group theory which includes many more than matrix groups; the formal definition is given in Sec. 2.1.

in [39]. $BS(p, q)$ denotes the Baumslag-Solitar group $BS(p, q) = \langle a, t \mid ta^p t^{-1} = a^q \rangle$.

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 $MIM \subseteq I$.

2.1 Smith normal forms and commensurators

The standard application for all our results is $GL(2, \mathbb{Q})$, but the results are more general and have the potential to go far beyond. Let $n \in \mathbb{N}$. It is a 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 $r > 0$, $e, f \in SL(n, \mathbb{Z})$, and $q \in \mathbb{Z}$ where $s_q = \begin{pmatrix} 1 & 0 \\ 0 & q \end{pmatrix}$. 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 . It is known that the Smith normal form can be computed in polynomial time [23].

The notion of “commensurator” is well established in 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 . 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 $N = \bigcap \{gHg^{-1} \mid g \in G\}$ is of finite index in G if and only if G/H is finite.

Moreover, if $H \leq H'$ is 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 $H = SL(2, \mathbb{Z})$ and write $g \in GL(2, \mathbb{Q})$ 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 $\begin{pmatrix} a & b/q \\ qc & d \end{pmatrix}$ is in $s_q H s_q^{-1}$ if $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2, \mathbb{Z})$. Thus, the index of $s_q H s_q^{-1} \cap H$ in H is bounded by the size of the finite group $SL(n, \mathbb{Z}/q\mathbb{Z})$. For $n = 2$ this size is in $\mathcal{O}(q^3)$. It follows that $GL(2, \mathbb{Q})$ is the commensurator of $SL(2, \mathbb{Z})$, and hence of $GL(2, \mathbb{Z})$. In fact, it is known that $GL(n, \mathbb{Q})$ is the commensurator of $SL(n, \mathbb{Z})$ for all $n \in \mathbb{N}$, e.g., see [22].

2.2 Rational and recognizable sets

The results in this section are not new. An exception is however Lem. 2.6. We follow the standard notation as in Eilenberg [16]. Let M be any monoid, then $\text{Rat}(M)$ has the following inductive definition using *rational* (aka *regular*) expressions.

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

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 $\text{Rat}(M)$ is intrinsic without 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, $B(L_1 \cup L_2) = B(L_1) \cup B(L_2)$, $B(L_1 \cdot L_2) = B(L_1) \cup B(L_2)$ if both L_1 and L_2 are nonempty, and $B(L_1 \cdot L_2) = \emptyset$ otherwise. Finally, $B(L^*) = B(L) \cup \{1\}$. Since

$B(L)$ is finite, L is a subset of the f.g. submonoid $B(L)^*$. Note that $B(L) = \emptyset \iff L = \emptyset$, hence the emptiness problem is decidable for rational subsets of M if, for example, they are given by rational expressions.

Definition 2.1. Let M be a monoid.⁴ The *membership problem for rational subsets* is defined as follows: given $g \in M$ and $R \in \text{RAT}(M)$, decide whether $g \in R$.

Definition 2.2. Let C be a family of subsets of M . We say that C is a *relative Boolean algebra* if it is closed under finite unions and $K, L \in C$ implies $K \setminus L \in C$. It is an *effective relative Boolean algebra* if first, every $L \in C$ is given by an effective description and second, for $L, K \in C$ the union $L \cup K$ and the relative complement $K \setminus L$ are computable. If additionally, M belongs to C , then C is called an (effective) *Boolean algebra*.

By definition, a relative Boolean algebra is closed under finite unions, it follows that it is closed under finite intersection, too.

Note that $\text{Rat}(\mathbb{Q})$ is a relative Boolean algebra because every finitely generated subgroup is isomorphic to \mathbb{Z} . It is not a Boolean algebra by Prop. 2.4 because $\mathbb{Q} \notin \text{Rat}(\mathbb{Q})$ as $(\mathbb{Q}, +)$ is not f.g.

PROPOSITION 2.3. *The class of monoids M for which $\text{Rat}(M)$ is an effective Boolean algebra satisfies the following properties:*

- (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 [9, 17, 24].*
- (3) *It contains all f.g. virtually free groups [38, 40].*
- (4) *It is closed under the operation of free product. [37].*

We also use the following well-known fact from [2].

PROPOSITION 2.4. *Let G be a group. If a subgroup H is in $\text{Rat}(G)$, then H is finitely generated.*

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

The following assertions are well-known and easy to show [16].

- (1) *Theorem of McKnight [30]: M is finitely generated $\iff \text{Rec}(M) \subseteq \text{Rat}(M)$.*
- (2) *$L, K \in \text{Rat}(M)$ doesn't imply $L \cap K \in \text{Rat}(M)$, in general.*
- (3) *$L \in \text{Rec}(M), K \in \text{Rat}(M) \implies L \cap K \in \text{Rat}(M)$.*
- (4) *Let H be a subgroup of a group G . Then $|G/H| < \infty \iff H \in \text{Rec}(G)$.*

The following (well-known) consequence is easy to show.

COROLLARY 2.5. *Let G be any group and $H \leq G$ be a subgroup of finite index. Then $\{L \cap H \mid L \in \text{Rat}(G)\} = \{L \subseteq H \mid L \in \text{Rat}(G)\}$.*

Cor. 2.5 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 the so-called Howson property: there are f.g. subgroups H, K such that $H \cap K$ is not finitely generated.

The assertion of Lem. 2.6 below is not obvious. It was proved first under the assumption that H has finite index in G , [19, 38, 40]. We show that this assumption is not necessary.⁵

⁴If M is not f.g., then we assume that all elements in M have an effective representation, like in $GL(2, \mathbb{Q})$.

⁵Sénizergues has a proof of Lem. 2.6 using finite transducers, personal communication.

LEMMA 2.6. *Let G be any group and $H \leq G$ be a subgroup. Then*

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

Moreover, suppose (i) that G is a f.g. group with decidable word problem and (ii) that the question “ $g \in H$?” is decidable for $g \in G$. Then for any NFA A with n states and labels in G that accepts $L \subseteq H$, we can effectively construct an NFA A' with n states and labels in H such that A' also accepts L .

PROOF. Let $R \subseteq G$ be such that, first, $1 \in R$ and, second, each right coset $Hr \in H \setminus G$ is represented by exactly one $r \in R$.

Let $L \subseteq H$ and $L = L(A)$ 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 $L \in \text{Rat}(G')$.

Assume we read from some initial state a word u over the alphabet $H' \cup S$ 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 $r = r(p) \in R$. If u' is any word which we can read from the initial state to p , then $u' \in Hr(p)$. Moreover, if p is any initial or final state, then we have $r(p) = 1$.

This will show that we only need the finite subset R' of R . The set R' contains S and all $r \in R$ such that $Hf_p^{-1} = Hr$ where f_p is the label of a shortest path from a state p to a final state. Let $r = r(p) \in R'$ for $p \in Q$. We introduce exactly one new state (p, r) with transitions $p \xrightarrow{r^{-1}} (p, r)$ and $(p, r) \xrightarrow{r} p$. This does not change the language.

Now for each outgoing transition $p \xrightarrow{sa} q$ with $r = r(p)$ and $t = r(q) \in R'$ define $b \in H$ by the equation $b = rsat^{-1}$. Recall if we read u reaching p , then $ur^{-1} \in H$ and $usat^{-1} \in H$. Therefore, $ur^{-1}rsat^{-1} \in H$ and hence $b \in H$. We add a transition

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

This doesn't change the language as $b = rsat^{-1}$ in G and before we added the transition there was a path $(p, r) \xrightarrow{r} p \xrightarrow{sa} q \xrightarrow{t^{-1}} (q, t)$ as can be seen in the following picture:

$$\begin{array}{ccc} (p, r) & \xrightarrow{b} & (q, t) \\ \left. \begin{array}{c} r \downarrow \\ p \end{array} \right\} r^{-1} & & \left. \begin{array}{c} t \downarrow \\ q \end{array} \right\} t^{-1} \\ & \xrightarrow{sa} & \end{array}$$

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 . Indeed, consider any path $p_0 \xrightarrow{s_1 a_1} p_1 \cdots \xrightarrow{s_k a_k} p_k$, where $k \geq 0$ and p_0 is an initial. We claim that the new NFA contains a path labeled by $b_1 \cdots b_k$ with $b_1, \dots, b_k \in H$ from p_0 to $(p_k, r(p_k))$ such that $b_1 \cdots b_k = s_1 a_1 \cdots s_k a_k r(p_k)^{-1}$.

This holds for $k = 0$ because $r(p_0) = 1$ and there is a transition with label 1 from p_0 to $(p_0, 1)$. Let $k \geq 1$. By induction the claim

holds for $k-1$. Inspecting the figure above, where $b = b_k$, $sa = s_k a_k$, $(p, r) = (p_{k-1}, r(p_{k-1}))$ and $(q, t) = (p_k, r(p_k))$, we see that the claim holds for k since $r(p_{k-1})^{-1} b_k = s_k a_k r(p_k)^{-1}$; and so:

$$\begin{aligned} b_1 \cdots b_{k-1} b_k &= s_1 a_1 \cdots s_{k-1} a_{k-1} r(p_{k-1})^{-1} b_k \\ &= s_1 a_1 \cdots s_{k-1} a_{k-1} s_k a_k r(p_k)^{-1}. \end{aligned}$$

We are done, since $r(p_k) = 1$ whenever p_k is final and hence there is a transition with label 1 from $(p_k, 1)$ to p_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). Let us denote the new NFA by A' . Then A' has exactly the same number of states as A .

This shows the non-effective version for all groups G with subgroups H . Finally, in order to make the construction effective it is sufficient that, first, G is f.g. and has a decidable word problem and, second, that the question “ $g \in H$?” is decidable for $g \in G$. \square

PROPOSITION 2.7. *Let H be a subgroup of finite index in a f.g. group G . If the membership problem for rational subsets of H is decidable, then it is decidable for rational subsets of G .*

PROOF. Since H is of finite index, there is a normal subgroup N of finite index in G such that $N \leq H \leq G$, [28]. Using the canonical homomorphism from G to G/N we see that H is recognizable. Hence, “ $g \in H$?” is decidable. We want to decide “ $g \in R$?” for some $R \in \text{Rat}(G)$. Suppose u_1, \dots, u_k are all representatives of right cosets of H in G . Choose i such that $gu_i^{-1} \in H$. Then $g \in R$ if and only if $gu_i^{-1} \in Ru_i^{-1} \cap H$. Since H is recognizable, we have $Ru_i^{-1} \cap H \in \text{Rat}(G)$. By Lem. 2.6, we have $Ru_i^{-1} \cap H \in \text{Rat}(H)$; and hence we can decide whether $g \in R$. \square

3 FLAT RATIONAL SETS

The best situation is when $\text{Rat}(M)$ 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 emptiness of finite Boolean combinations of rational sets or (even weaker) to decide membership in rational sets. Again, in various interesting cases the membership problem in 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 [31], there exists a finitely generated subgroup with undecidable membership problem.

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

Definition 3.1. Let N be a submonoid of M . We say that $L \subseteq M$ is a *flat rational subset* of M relative to N (or over N) if L is a finite union of languages of the form $L_0 g_1 L_1 \cdots g_t L_t$ where all $L_i \in \text{Rat}(N)$ and $g_i \in M$. The family of these sets is denoted by $\text{Frat}(M, N)$.

In our applications we use flat rational sets in the following setting: H is a subgroup of G , and G sits inside a monoid M , where $M \setminus G$ is an ideal (possibly empty). For example, $H = \text{GL}(2, \mathbb{Z}) < G \leq \text{GL}(2, \mathbb{Q})$ and $M \setminus G$ is a (possibly empty) semigroup of singular

matrices. In such a situation there is an equivalent characterization of flat rational sets in M with respect to H . Prop. 3.2 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 3.2. *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 $\text{Frat}(M, H)$ 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 a flat rational set relative to H such that $L \subseteq H$. Recall that L is a finite union of languages $L_0 g_1 L_1 \cdots g_t L_t$, where $\emptyset \neq L_i \in \text{Rat}(H)$ 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 $L \in \text{Rat}(G)$. By Lem. 2.6, L is a rational subset of H , and hence $L^* \in \text{Rat}(H)$. In particular, L^* is flat rational relative to H . \square

THEOREM 3.3. *Let H be a subgroup of a f.g. group G with decidable word problem such that the following conditions hold:*

- $\text{Rat}(H)$ is an effective relative Boolean algebra.⁶
- G is the commensurator of H , and moreover for a given $g \in G$ we can compute the index of H_g in H .
- The membership to H (that is, “ $g \in H$?”) is decidable.

Then $\text{Frat}(G, H)$ 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 proving Thm. 3.3 let us first state a consequence.

COROLLARY 3.4. *Let $B \subseteq \text{GL}(2, \mathbb{Q})$ be a finite Boolean combination of flat rational sets of $\text{GL}(2, \mathbb{Q})$ over $\text{GL}(2, \mathbb{Z})$, then we can decide the emptiness of B .*

PROOF. It is a well-known classical fact that $\text{GL}(2, \mathbb{Z})$ is a finitely generated virtually free group, namely, it contains a free subgroup of rank 2 and index 24. Hence $\text{Rat}(\text{GL}(2, \mathbb{Z}))$ is an effective Boolean algebra by [40]. Let G be a f.g. subgroup of $\text{GL}(2, \mathbb{Q})$ that contains B . Clearly, G has a decidable word problem. It is also well-known that $\text{GL}(2, \mathbb{Q})$ is the commensurator subgroup of $\text{GL}(2, \mathbb{Z})$ in $\text{GL}(2, \mathbb{Q})$. Hence G is the commensurator of $\text{GL}(2, \mathbb{Z})$, too. Thus all hypotheses of Thm. 3.3 are satisfied. \square

A direct consequence of Cor. 3.4 is that we can decide the membership in flat rational subsets of $\text{GL}(2, \mathbb{Q})$ over $\text{GL}(2, \mathbb{Z})$. However in Sec. 4 we explain why we are far away from knowing how to decide the membership for all rational subsets of $\text{GL}(2, \mathbb{Q})$.

For the proof of Thm. 3.3 we need the following observation.

⁶Recall that this does not imply $H \in \text{Rat}(H)$: possibly H is not f.g.

LEMMA 3.5. *Let $L \in \text{Rat}(H)$ and $g \in G$. Recall that*

$$H_g = gHg^{-1} \cap H = \{h \in H \mid g^{-1}hg \in H\}.$$

Then under the assumptions of Thm. 3.3 we can compute an expression for $g^{-1}(L \cap H_g)g \in \text{Rat}(H)$.

PROOF. Since $gHg^{-1} \cap H$ is of finite index in H , we can compute the expression for $L' = L \cap H_g \in \text{Rat}(H_g)$ over a basis $B' \subseteq H_g$ by Lem. 2.6. Now, for any g and $K \in \text{Rat}(H_g)$ we have $g^{-1}K^*g = (g^{-1}Kg)^*$, $g^{-1}(L_1 L_2)g = g^{-1}L_1 g g^{-1}L_2 g$, and $g^{-1}(L_1 \cup L_2)g = g^{-1}L_1 g \cup g^{-1}L_2 g$. 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 . \square

PROOF OF THM. 3.3. Let $g \in G$ and $K \in \text{Rat}(H)$. First, we claim that we can rewrite Kg as $\text{Rat}(G)$ as a finite union of languages $g'K'$ with $g' \in G$ and $K' \in \text{Rat}(H)$.

Note that we can compute a set $U_g \subseteq H$ of left-representatives such that $H = \bigcup \{uH_g \mid u \in U_g\}$. Indeed, by assumption, the membership to H is decidable, and hence the membership to gHg^{-1} and to $H_g = gHg^{-1} \cap H$ is decidable, too. By the second assumption, we can compute the index $k = |H : H_g|$. Thus we can enumerate the elements of H until we find k elements that belong to k different left cosets of H_g . Checking if two elements belong to the same coset is decidable since the membership to H_g can be decided. Thus,

$$\begin{aligned} Kg &= \bigcup \{K \cap uH_g \mid u \in U_g\} g = \bigcup \{ugg^{-1}(u^{-1}K \cap H_g)g \mid u \in U_g\} \\ &= \bigcup \{g'g^{-1}(gg'^{-1}K \cap H_g)g \mid g' \in U_g g\}. \end{aligned}$$

Using Lem. 3.5 we obtain $g^{-1}(gg'^{-1}K \cap H_g)g = K' \in \text{Rat}(H)$. This shows the claim.

Let L be a flat rational subset of G , that is, L is equal to a finite union of languages $L_0 g_1 L_1 \cdots g_t L_t$ where all $L_i \in \text{Rat}(H)$. Using the claim, we can write L as a finite union of languages gK with $g \in G$ and $K \in \text{Rat}(H)$. Since 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 $hK \in \text{Rat}(H)$. Therefore, every flat rational set L can be written as a union $L = \bigcup_{i=1}^n g_i K_i$, where $g_i \in S$ and $K_i \in \text{Rat}(H)$. Since $gK_1 \cup gK_2 = g(K_1 \cup K_2)$, we may assume that all g_i in the expression $L = \bigcup_{i=1}^n g_i K_i$ are different.

Now let L and R be two flat rational sets. By the above argument we may assume that $L = \bigcup_{i=1}^n a_i L_i$ and $R = \bigcup_{j=1}^m b_j R_j$, where $a_i, b_j \in S$ and $L_i, R_j \in \text{Rat}(H)$. Then we have $L \setminus R = \bigcup_{i=1}^n (a_i L_i \setminus \bigcup_{j=1}^m b_j R_j)$. Note that if $a_i \notin \{b_1, \dots, b_m\}$, 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 $\text{Rat}(H)$ is an effective relative 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 $L \setminus R$. \square

Below we give one more application of Thm. 3.3. Let $P(2, \mathbb{Q})$ denote the following submonoid of $\text{GL}(2, \mathbb{Q})$ of matrices:

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

Note that $P(2, \mathbb{Q})$ contains all nonsingular matrices from $M(2, \mathbb{Z})$. So, the next theorem is a generalization of the main result in [34].

THEOREM 3.6. *For any $g \in \text{GL}(2, \mathbb{Q})$ and for any flat rational subset R of $\text{GL}(2, \mathbb{Q})$ relative to $P(2, \mathbb{Q})$, it is decidable whether $g \in R$.*

PROOF. Writing g in Smith normal form, we obtain

$$g = c_r e s_n f = c_r e \begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix} f,$$

where $c_r = \begin{pmatrix} r & 0 \\ 0 & r \end{pmatrix}$ is central, $e, f \in \text{SL}(2, \mathbb{Z})$ 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 $R_i \in \text{Rat}(P(2, \mathbb{Q}))$ and each g_i is of the form $g_i = \begin{pmatrix} r & 0 \\ 0 & r \end{pmatrix}$ with $0 < r < 1$. Multiplying g and R with some appropriate natural number, we can assume that $g = \begin{pmatrix} m & 0 \\ 0 & n \end{pmatrix}$ with $m, n \in \mathbb{N} \setminus \{0\}$ and $R \in \text{Rat}(P(2, \mathbb{Q}))$.

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 $P(2, \mathbb{Q}) \setminus \text{GL}(2, \mathbb{Z})$ 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 $Q \times \{0, \dots, k\}$, initial states $I \times \{0\}$ and final states $F \times \{0, \dots, k\}$. The transitions of \mathcal{B} are defined as follows:

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

The automaton \mathcal{B} defines a flat rational subset $R' \subseteq R$ over $\text{GL}(2, \mathbb{Z})$ such that $g \in R' \iff g \in R$. So, using Thm. 3.3, we can decide whether $g \in R'$ and hence whether $g \in R$. \square

4 DICHOTOMY IN $\text{GL}(2, \mathbb{Q})$

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

THEOREM 4.1. *Let G be a f.g. group such that $\text{GL}(2, \mathbb{Z}) < G \leq \text{GL}(2, \mathbb{Q})$. Then there are two mutually exclusive cases.*

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

PROOF. Let $H = \text{GL}(2, \mathbb{Z})$. 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 $\text{GL}(2, \mathbb{Z}) \leq G$ we see that $Z(G) \leq \left\{ \begin{pmatrix} r & 0 \\ 0 & r \end{pmatrix} \mid r \in \mathbb{Q} \right\}$. Moreover, since $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \in H$, we may assume in the first case that G is generated by H and f.g. subgroup $Z \leq \left\{ \begin{pmatrix} r & 0 \\ 0 & r \end{pmatrix} \mid r \in \mathbb{Q} \wedge r > 0 \right\}$. 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 $e \begin{pmatrix} r & 0 \\ 0 & rq \end{pmatrix} f$. Since $e, f \in \text{GL}(2, \mathbb{Z})$ and $\text{GL}(2, \mathbb{Z}) < G$, without restriction, the generators are either from $\text{GL}(2, \mathbb{Z})$ or they have the form $\begin{pmatrix} r & 0 \\ 0 & rq \end{pmatrix}$ 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 $s = \begin{pmatrix} r & 0 \\ 0 & rq \end{pmatrix}$ where $r > 0$ and $2 \leq q \in \mathbb{N}$.

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

But this is not enough, we need to show that $\text{GL}(2, \mathbb{Z}) \times \mathbb{Z}^k$ cannot contain $\text{BS}(1, q)$, otherwise there is no dichotomy. Actually, we do more: there is no abelian group A such that $\text{BS}(1, q)$ is a subgroup of $\text{GL}(2, \mathbb{Z}) \times A$.

Assume by contradiction that it is. Then there are generators $b = (a, x), t = (s, y) \in \text{GL}(2, \mathbb{Z}) \times A$ such that $tbt^{-1} = b^q$. This implies $(q-1)x = 0$. Since $q \geq 2$, the element x generates a finite subgroup in A . Since b generates an infinite cyclic group, we conclude that $a^m \neq 1$ for all $m \neq 0$. Consider the canonical projection φ of $\text{GL}(2, \mathbb{Z}) \times A$ onto $\text{GL}(2, \mathbb{Z})$ 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 $s^k a^z s^n = 1 \in \text{GL}(2, \mathbb{Z})$; and therefore $a^z = s^{-k-n}$. Hence a^z commutes with s . Hence $a^z = sa^z s^{-1} = a^{qz}$. We conclude $a^{(q-1)z} = 1$. Since $a^m \neq 1$ for all $m \neq 0$ and $q \geq 2$ we have $z = 0$. Hence $g = t^m$ for some $m \in \mathbb{Z}$. Since $\varphi(g) = 1$, we know $s^m = 1$. Therefore, $t^m = (s^m, my)$ acts trivially on b . But in $\text{BS}(1, q)$ this happens for $m = 0$, only. This tells us that φ is injective on $\langle b, t \rangle$, and the claim follows.

The above claim implies that $\text{BS}(1, q)$ appears as a subgroup in $\text{GL}(2, \mathbb{Z})$. However, no virtually free group can contain $\text{BS}(1, q)$ by [18]⁷; and $\text{GL}(2, \mathbb{Z})$ is virtually free. A contradiction. \square

PROPOSITION 4.2. *Let G be isomorphic to $\text{GL}(2, \mathbb{Z}) \times \mathbb{Z}^k$ with $k \geq 1$. Then, the question “ $L = R?$ ” on input $L, R \in \text{Rat}(G)$ is undecidable. However, the question “ $g \in R?$ ” on input $g \in G$ and $R \in \text{Rat}(G)$ is decidable.*

⁷Actually, [18] shows a stronger result. If a Baumslag-Solitar group $\text{BS}(p, q)$ appears in a group G with $pq \neq 0$, then G is not hyperbolic. The result is stronger since all f.g. virtually free groups are hyperbolic.

PROOF. The group $GL(2, \mathbb{Z})$ 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 $L, R \in \text{Rat}(G)$ is undecidable for M [1].

For the decidability we use the fact that $GL(2, \mathbb{Z})$ has a free subgroup F of rank two and index 24. By [27] 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 problem in G is decidable by Prop. 2.7. \square

Remark 1. Let G be a group extension of $GL(2, \mathbb{Z})$ inside $GL(2, \mathbb{Q})$ which is not isomorphic to $GL(2, \mathbb{Z}) \times \mathbb{Z}^k$ for $k \geq 0$. Then, by Thm. 4.1, the group G contains an infinite extension of $BS(1, q)$ for $q \geq 2$. By [10] the membership in rational sets of $BS(1, q)$ is decidable. However, to date it is not clear how to extend this result to infinite extensions of $BS(1, q)$.

5 SINGULAR MATRICES

In this section we show that the membership problem is decidable for flat rational sets containing singular matrices. This extends the results of [35] which considers only integer matrices.

For $H \in GL(2, \mathbb{Z})$ and $a \in \mathbb{Z}$ we let

$$M_{ij}(a) = \left\{ \begin{pmatrix} g_{11} & g_{12} \\ g_{21} & g_{22} \end{pmatrix} \in H \mid g_{ij} = a \right\} \subseteq M(2, \mathbb{Z}).$$

Throughout we will use Lem. 5.1; for a proof see [15, 35].

LEMMA 5.1. *The sets $M_{ij}(a)$ are rational for all i, j and $a \in \mathbb{Z}$.*

THEOREM 5.2. *Let P be the submonoid of $M(2, \mathbb{Q})$ which is generated by $GL(2, \mathbb{Z})$, all central matrices $\begin{pmatrix} r & 0 \\ 0 & r \end{pmatrix}$ with $r \in \mathbb{N}$, 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 “ $g \in R$?” is decidable for singular matrices $g \in M(2, \mathbb{Q})$.*

PROOF. Without restriction, R is given by a trim NFA \mathcal{A} over a f.g. submonoid M of $M(2, \mathbb{Q})$ such that transitions are labeled with elements of H or with matrices rs_q where $q \in \mathbb{N}$ 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 $GL(2, \mathbb{Z})$ or by a central matrix $\begin{pmatrix} r & 0 \\ 0 & r \end{pmatrix}$ or by $s_0 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$.

Since $\det(g) = 0$, the label s_0 must be used at least once. 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 $L_i \in \text{Rat}(M)$. 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 $a, b, c, d \in \mathbb{Z}$:

$$s_0 r \begin{pmatrix} a & b \\ c & d \end{pmatrix} s_0 = s_0 \begin{pmatrix} ra & 0 \\ 0 & 0 \end{pmatrix} s_0 = s_0 r a s_0 = r a s_0. \quad (1)$$

Now, we perform a Benois-type (cf. [9]) of “flooding-the-NFA”.

First Round. 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 $L(p, q) \in \text{Rat}(H)$.
- (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 $1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is the identity matrix, replace $L(p, q)$ by $L(p, q) \setminus \{1\}$ and add a new transition $p \xrightarrow{1} q$.

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

$$p_1 \xrightarrow{L_1} q_1 \xrightarrow{r_1 s_0} p_2 \xrightarrow{L_2} \dots \xrightarrow{r_k s_0} p_k \xrightarrow{L_k} q_k \quad (2)$$

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 without restriction that 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 are labeled by rational subsets of H and which lead to q -states; and q -states where outgoing transitions are 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 a constant ρ depending on R such that each accepting path as in (2) uses a transition labeled by $r = \begin{pmatrix} r & 0 \\ 0 & r \end{pmatrix}$ 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

$$q_0 \xrightarrow{r} p_1 \xrightarrow{L_1} q_1 \xrightarrow{r_1 s_0} p_2 \xrightarrow{L_2} \dots \xrightarrow{r_k s_0} p_k \xrightarrow{L_k} q_k \quad (3)$$

where the $r \in \mathbb{Q}$, $r \neq 0$, $r_i \in \mathbb{N} \setminus \{0\}$, and $0, 1 \notin L_i \in \text{Rat}(M)$. 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 $g \in M(2, \mathbb{Z})$. So, we can assume that, too.

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

Let $g = \begin{pmatrix} g_{11} & g_{12} \\ g_{21} & g_{22} \end{pmatrix}$. 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 $q \xrightarrow{r s_0}$ appears in \mathcal{A} , then r divides t .

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

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

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 $z r z r'$ 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: $p_1 \xrightarrow{L_1} q_1 \xrightarrow{r s_0} p_2 \xrightarrow{L_2} q_2$. By guessing such a

sequence of length three, we may assume that the NFA is equal to that path 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 $f_k \in L_k \in \text{Rat}(H)$ for $k = 1, 2$. We can write $f_1 r s_0 = r \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}$ and $s_0 f_2 = \begin{pmatrix} c & d \\ 0 & 0 \end{pmatrix}$ where the a, b, c, d depend on the pair (f_1, f_2) . Hence, $m = r f s_0 h = r f s_0 s_0 h = r \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \begin{pmatrix} c & d \\ 0 & 0 \end{pmatrix} = r \begin{pmatrix} ac & ad \\ bc & bd \end{pmatrix}$. 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 “ $0 \in M_{ij}(0) \cap L_k = \emptyset$?”. Now, it is enough to consider 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 $g \in R$. \square

THEOREM 5.3. *Let P' be the submonoid of $M(2, \mathbb{Q})$ which is generated by $\text{GL}(2, \mathbb{Z})$, all central matrices $\begin{pmatrix} r & 0 \\ 0 & r \end{pmatrix}$ with $r \in \mathbb{Q}$, 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 $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in R$.*

Note that $P' = P \cdot \left\{ \begin{pmatrix} r & 0 \\ 0 & r \end{pmatrix} \mid r \in \mathbb{Q} \right\}$ where P is from Thm. 5.2. The proof of Thm. 5.3 is straightforward, details are in [15].

6 GENERATORS OF $\text{SL}(2, \mathbb{Z}[1/p])$

As usual, $\mathbb{Z}[1/p]$ denotes the ring $\{p^n r \in \mathbb{Q} \mid n, r \in \mathbb{Z}\}$. We give a simple proof for the well-known fact that $\text{SL}(2, \mathbb{Z}[1/p])$ is generated by $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, and $\begin{pmatrix} p & 0 \\ 0 & p^{-1} \end{pmatrix}$. We use the following notation: let $\alpha, \beta, \gamma, \delta$ denote elements in $\mathbb{Z}[1/p]$, and a, b, c, d denote elements in \mathbb{Z} . Starting with a matrix $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ we do the following:

- (1) Multiply by $\begin{pmatrix} p^{-1} & 0 \\ 0 & p \end{pmatrix}$ on the left until we reach $\begin{pmatrix} \alpha & \beta \\ c & d \end{pmatrix}$.
- (2) Multiply by $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, $\begin{pmatrix} 1 & \pm 1 \\ 0 & 1 \end{pmatrix}$, and $\begin{pmatrix} 1 & 0 \\ \pm 1 & 1 \end{pmatrix}$ until we reach $\begin{pmatrix} \alpha & \beta \\ 0 & d \end{pmatrix}$.
This is trivial for $|c| = |d|$. In the other case we may assume $|c| > |d|$. Next, transform $\begin{pmatrix} \alpha & \beta \\ c & d \end{pmatrix}$ into a matrix of type $\begin{pmatrix} \alpha & \beta \\ c \pm d & d \end{pmatrix}$ such that $|c \pm d| < |c|$. Use induction on $|c| + |d|$.
- (3) Multiply by $\begin{pmatrix} p & 0 \\ 0 & p^{-1} \end{pmatrix}$ on the left until we reach $\begin{pmatrix} \alpha & \beta \\ 0 & \delta \end{pmatrix}$.
- (4) Now, $\alpha\delta = 1$. Hence $\alpha = p^m a$ and $\delta = p^n d$ where $\gcd(a, p) = \gcd(d, p) = 1$. Since p is a prime, $m + n = 0$ and $ad = 1$.
- (5) WLOG $a = d = 1$ and $m \geq 1$ and hence, $\begin{pmatrix} \alpha & \beta \\ 0 & \delta \end{pmatrix} = \begin{pmatrix} p^m & b \\ 0 & p^{-m} \end{pmatrix}$.
- (6) Using $\begin{pmatrix} 1 & \pm 1 \\ 0 & 1 \end{pmatrix}$ we can add or subtract the lower row $p^m |b|$ times to the upper row. Since $m \geq 1$ we obtain $\begin{pmatrix} p & 0 \\ 0 & p^{-1} \end{pmatrix}^m$.

REFERENCES

- [1] I.J. Aalbersberg and H.J. Hoogeboom. 1989. Characterizations of the Decidability of Some Problems for Regular Trace Languages. *Math. Syst. Th.* 22 (1989), 1–19.
- [2] Anatolij V. Anisimov and Franz D. Seifert. 1975. Zur algebraischen Charakteristik der durch kontext-freie Sprachen definierten Gruppen. *Elektron. Inf.-Verarbeit. Kybernetik* 11 (1975), 695–702.
- [3] László Babai, Robert Beals, Jin-yi Cai, Gábor Ivanyos, and Eugene M. Luks. 1996. Multiplicative Equations over Commuting Matrices. In *Proc. 7th SODA*. 498–507.
- [4] Gilbert Baumslag and Donald Solitar. 1962. Some two-generator one-relator non-Hopfian groups. *Bull. Amer. Math. Soc.* 68 (1962), 199–201.
- [5] H. Behr and J. Mennicke. 1968. A presentation of the groups $\text{PSL}(2, p)$. *Canadian Journal of Mathematics* 20 (1968), 1432–1438.
- [6] P. Bell, V. Halava, T. Harju, J. Karhumäki, and I. Potapov. 2008. Matrix Equations and Hilbert’s Tenth Problem. *Int. J. Algebra Comp.* 18 (2008), 1231–1241.
- [7] P. Bell, I. Potapov, and P. Semukhin. 2019. On the Mortality Problem: From Multiplicative Matrix Equations to Linear Recurrence Sequences and Beyond. In *Proc. 44th MFCS (LIPIcs)*. 83:1–83:15. <https://doi.org/10.4230/LIPIcs.MFCS.2019.83>
- [8] P. C. Bell, M. Hirvensalo, and I. Potapov. 2017. The identity problem for matrix semigroups in $\text{SL}_2(\mathbb{Z})$ is NP-complete. In *Proc. SODA’17*. SIAM, 187–206.
- [9] Michèle Benoist. 1969. Parties rationnelles du groupe libre. *C. R. Acad. Sci. Paris, Sér. A* 269 (1969), 1188–1190.
- [10] Michaël Cadilhac, Dmitry Chistikov, and Georg Zetsche. 2020. Rational subsets of Baumslag-Solitar groups. To appear: *Proc. of the 47th ICALP 2020 in LIPIcs*.
- [11] J. Cassaigne, V. Halava, T. Harju, and F. Nicolas. 2014. Tighter Undecidability Bounds for Matrix Mortality, Zero-in-the-Corner Problems, and More. *arXiv eprints abs/1404.0644* (2014).
- [12] Émilie Charlier and Juha Honkala. 2014. The freeness problem over matrix semigroups and bounded languages. *Inf. Comp.* 237 (2014), 243–256.
- [13] Laura Ciobanu and Murray Elder. 2019. Solutions Sets to Systems of Equations in Hyperbolic Groups Are EDT0L in PSPACE. In *Proc. 46th ICALP (LIPIcs, Vol. 132)*. 110:1–110:15. <https://doi.org/10.4230/LIPIcs.ICALP.2019.110>
- [14] T. Colcombet, J. Ouaknine, P. Semukhin, and J. Worrell. 2019. On Reachability Problems for Low-Dimensional Matrix Semigroups. In *Proc. 46th ICALP (LIPIcs)*. 44:1–44:15. <https://doi.org/10.4230/LIPIcs.ICALP.2019.44>
- [15] Volker Diekert, Igor Potapov, and Pavel Semukhin. 2019. Decidability of membership problems for flat rational subsets of $\text{GL}(2, \mathbb{Q})$ and singular matrices. *arXiv eprints abs/1910.02302* (2019).
- [16] S. Eilenberg. 1974. *Automata, Languages, and Machines*. Vol. A. Academic Press.
- [17] Samuel Eilenberg and Marcel-Paul Schützenberger. 1969. Rational sets in commutative monoids. *J. Algebra* 13 (1969), 173–191.
- [18] S. M. Gersten. 1992. Dehn functions and l_1 -norms of finite presentations. In *Algorithms and classification in combinatorial group theory (Berkeley, CA, 1989)*. Math. Sci. Res. Inst. Publ., Vol. 23, 195–224.
- [19] Z. Grunschlag. 1999. *Algorithms in Geometric Group Theory*. Ph.D. Dissertation.
- [20] Yuri Gurevich and Paul Schupp. 2007. Membership problem for the modular group. *SIAM J. Comput.* 37, 2 (2007), 425–459.
- [21] Tero Harju. 2009. Post Correspondence Problem and Small Dimensional Matrices. In *Proc. 13th DLT (LN in Comp. Sci, Vol. 5583)*. 39–46.
- [22] J. Hillman. 2007. Commensurators and deficiency. (2007). <http://www.maths.usyd.edu.au/u/pubs/publist/preprints/2007/hillman-18.pdf>
- [23] R. Kannan and A. Bachem. 1979. Polynomial Algorithms for Computing the Smith and Hermite Normal Forms of an Integer Matrix. *SIAM J. Comput.* 8 (1979), 499–507. <https://doi.org/10.1137/0208040>
- [24] S. Kleene. 1956. Representation of events in nerve nets and finite automata. In *Automata Studies*. Number 34 in Annals of Mathematics Studies. 3–40.
- [25] S. Ko, R. Niskanen, and I. Potapov. 2018. On the Identity Problem for the Special Linear Group and the Heisenberg Group. In *Proc. 45th ICALP (LIPIcs)*. 132:1–132:15. <https://doi.org/10.4230/LIPIcs.ICALP.2018.132>
- [26] Daniel König, Markus Lohrey, and Georg Zetsche. 2015. Knapsack and subset sum problems in nilpotent, polycyclic, and co-context-free groups. *arXiv eprints abs/1507.05145* (2015).
- [27] Markus Lohrey and Benjamin Steinberg. 2008. The submonoid and rational subset membership problems for graph groups. *J. Algebra* 320 (2008), 728–755.
- [28] Roger Lyndon and Paul Schupp. 2001. *Combinatorial Group Theory*. Springer.
- [29] A. Markov. 1947. On certain insoluble problems concerning matrices. *Dok. Akad. Nauk SSSR* 57 (1947), 539–542.
- [30] J. D. McKnight. 1964. Kleene quotient theorem. *Pac. J. Math.* (1964), 1343–1352.
- [31] K. A. Mikhailova. 1958. The occurrence problem for direct products of groups. *Dokl. Akad. Nauk SSSR* 119 (1958), 1103–1105. English translation in: *Math. USSR Sbornik*, 70: 241–251, 1966.
- [32] Morris Newman. 1962. The structure of some subgroups of the modular group. *Illinois J. Math.* 6 (1962), 480–487.
- [33] Igor Potapov. 2019. Reachability Problems in Matrix Semigroups. *Dagstuhl Reports* 9 (2019), 95–98. <https://doi.org/10.4230/DagRep.9.3.83>
- [34] Igor Potapov and Pavel Semukhin. 2017. Decidability of the Membership Problem for 2×2 integer matrices. In *Proc. 28th SODA*. 170–186.
- [35] Igor Potapov and Pavel Semukhin. 2017. Membership Problem in $\text{GL}(2, \mathbb{Z})$ Extended by Singular Matrices. In *Proc. 42nd MFCS*. 44:1–44:13.
- [36] Nikolay S. Romanovskii. 1974. Some algorithmic problems for solvable groups. *Algebra i Logika* 13 (1974), 26–34, 121.
- [37] Jacques Sakarovitch. 1992. The “last” decision problem for rational trace languages. In *Proc. LATIN’92 (LN in Comp. Sci, Vol. 583)*, I. Simon (Ed.), 460–473.
- [38] Gérard Sénizergues. 1996. On the rational subsets of the free group. *Acta Inf.* 33 (1996), 281–296.
- [39] Jean-Pierre Serre. 1980. *Trees*. Springer.
- [40] Pedro V. Silva. 2002. Recognizable subsets of a group: finite extensions and the abelian case. *Bulletin EATCS* 77 (2002), 195–215.
- [41] P. V. Silva. 2017. An Automata-Theoretic Approach to the Study of Fixed Points of Endomorphisms. In *Algorithmic and Geometric Topics Around Free Groups and Automorphisms*, J. González-Meneses, M. Lustig, and E. Ventura (Eds.). Birkhäuser.