OWP 2022 - 07

ALLA DETINKO, DANE FLANNERY AND ALEXANDER HULPKE

Deciding Non-Freeness of Rational Möbius Groups

Mathematisches Forschungsinstitut Oberwolfach gGmbH
Oberwolfach Preprints (OWP) ISSN 1864-7596

Oberwolfach Preprints (OWP)

Imprint:

Mathematisches Forschungsinstitut Oberwolfach gGmbH (MFO)
Schwarzwaldstrasse 9-11
77709 Oberwolfach-Walke
Germany

Tel	+49 7834 979 50
Fax	+49 7834 979 55
Email	admin@mfo.de
URL	www.mfo.de

The Oberwolfach Preprints (OWP, ISSN 1864-7596) are published by the MFO.

DOI	10.14760/OWP-2022-07

DECIDING NON-FREENESS OF RATIONAL MÖBIUS GROUPS

A. S. DETINKO, D. L. FLANNERY, AND A. HULPKE

ABSTRACT. We explore a new computational approach to a classical problem: certifying non-freeness of (2-generator, parabolic) Möbius subgroups of $\mathrm{SL}(2, \mathbb{Q})$. The main tools used are algorithms for Zariski dense groups and algorithms to compute a presentation of $\mathrm{SL}(2, R)$ for a localization $R = \mathbb{Z}[\frac{1}{b}]$ of $\mathbb{Z}$. We prove that a Möbius subgroup G is not free by showing that it has finite index in the relevant $\mathrm{SL}(2, R)$. Further information about the structure of G is obtained; for example, we compute the minimal subgroup of finite index in $\mathrm{SL}(2, R)$ that contains G.

1. INTRODUCTION

For $x \in \mathbb{C}$, define

$$A(x) = \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}, \quad B(x) = A(x)^{\top}.$$

Let $G(x)$ be the subgroup of $\mathrm{SL}(2, \mathbb{C})$ generated by $A(x)$ and $B(x)$, commonly called a (*parabolic*) *Möbius group*. Testing freeness of Möbius groups is a well-studied problem; see, e.g., [1, 3, 12, 15, 17]. Sanov [22] proved that $G(2)$ is free, while Brenner [2] proved that $G(x)$ is free (of rank 2) for all x such that $|x| \geq 2$. Hence, if x is algebraic and $|\bar{x}| \geq 2$ for some algebraic conjugate $\bar{x}$ of x, then $G(x)$ is free [17, p. 1388]. Also, $G(x)$ is free if x is transcendental [27, pp. 30–31].

It is unknown whether there exist rational $x \in (0, 2)$ for which $G(x)$ is free. Overall, testing freeness of matrix groups is difficult. The problem may even be undecidable; note that testing freeness of matrix semigroups is undecidable [4]. However, we can effectively decide virtual solvability [10], and so by the Tits alternative we can decide in practice whether a given finitely generated linear group contains a non-abelian free subgroup (without producing one).

On the other hand, non-freeness of $G(x)$ has been justified for infinitely many rationals in $(0, 2)$, and there is a set of irrational algebraic x that is dense in $(-2, 2)$ and for which $G(x)$ is non-free [1, p. 528].

We take a different approach to certifying non-freeness of Möbius groups in $\mathrm{SL}(2, \mathbb{Q})$, that applies recently developed methods to compute with Zariski dense matrix groups [8, 9].

2010 Mathematics Subject Classification: 20-04, 20G15, 20H25, 68W30.

Keywords: free group, Möbius group, arithmetic group, algorithm, software.

The following notation is used. For an integer $b > 1$, let R be the localization $\mathbb{Z}[\frac{1}{b}] = \{r/b^i \,|\, r \in \mathbb{Z},\, i \geq 0\}$ of $\mathbb{Z}$. We denote $\mathrm{SL}(2, R)$ by Γ. If I is a non-zero proper ideal of R, then there is a unique integer $t > 1$ coprime to b such that $I = tR$. Let $\varphi_I \colon \Gamma \to \mathrm{SL}(2, R/I)$ be the associated congruence homomorphism. The kernel Γ_I of φ_I is a *principal congruence subgroup* (PCS) of Γ. We say that the *level* of Γ_I is t, and write φ_t, Γ_t for φ_I, Γ_I, respectively. The $r \times r$ identity matrix is denoted 1_r, $\mathbb{Z}_k := \mathbb{Z}/k\mathbb{Z}$, and $\mathbb{F}_p$ is the field of size p.

Let S be the set of reciprocals of the primes dividing b. A finite index subgroup of Γ is said to be *S-arithmetic*. By [19, 24], Γ has the *congruence subgroup property* (CSP): each S-arithmetic subgroup H of Γ contains a PCS. The *level* of H is defined to be the level of the maximal PCS in H (the PCS in H with smallest possible level).

Throughout, unless stated otherwise, $m = \frac{a}{b} \in \mathbb{Q}$ where a is a positive integer coprime to b. (Note that $G(\frac{1}{b}) = \Gamma$.) The subgroup $G(m)$ of Γ is Zariski dense in $\mathrm{SL}(2)$. We define its level to be the level of the intersection of all S-arithmetic subgroups of Γ that contain $G(m)$. This intersection, called the *arithmetic closure* of $G(m)$ and denoted $\mathrm{cl}(G(m))$, is S-arithmetic [8, 9].

If $G(m)$ is S-arithmetic then it is not free (see Section 2). Since Γ is finitely presented (see Section 4.1), one can attempt to prove S-arithmeticity of $G(m)$ by coset enumeration. This necessitates determining a presentation of Γ. Algorithms for that task are developed in Section 4.1. Then in Section 4.2 we report on computer experiments carried out using our GAP [14] implementation of the algorithms. There we exhibit S-arithmeticity (hence non-freeness) of $G(m)$ for a range of rational $m \in (0, 2)$. Although non-freeness of some such $G(m)$ was already known, our experiments exemplify the connection between arithmeticity and non-freeness.

Moreover, we provide essential information about the structure and properties of $G(m)$, covering also the case that $G(m)$ is a *thin matrix group* [23], i.e., has infinite index in Γ. Specifically, we prove that $G(m)$ has level a^2 (Theorem 3.7). Hence, if $G(m)$ is S-arithmetic, then we can name the maximal PCS in $G(m)$, and so readily test whether an element of Γ is in $G(m)$. The membership testing problem continues to attract attention; see, e.g., [6, 11]. If $G(m)$ is potentially thin, then one might work instead with $\mathrm{cl}(G(m))$.

We are not aware of any rational $m \in (0, 2)$ such that $G(m)$ is thin; if there are none, then this would explain the lack of free $G(m)$ for these m. Conversely, can a thin $G(m)$ be non-free? Within $\mathrm{SL}(2, \mathbb{Z})$, the situation is more settled: $G(2)$ is a free subgroup of finite index, whereas if $m \geq 3$ then $G(m) \leq \mathrm{SL}(2, \mathbb{Z})$ is free and thin [6, Theorem 3] (indeed, for integers $m > 5$, the normal closure of $G(m)$ in $\mathrm{SL}(2, \mathbb{Z})$ is thin [18, p. 31]). Famously, $\mathrm{SL}(2, \mathbb{Z})$ does *not* have the CSP. We remark that $|\Gamma : G(m)| = \infty$ for any integer $m \geq 1$.

2. Non-freeness criteria for Möbius groups

Set $A = A(m)$, $B = B(m)$, and $G = G(m)$. Each element of G is a word $W_n = A^{\alpha_1}B^{\beta_1}\cdots A^{\alpha_n}B^{\beta_n}$ where $n \geq 1$ and the α_i, β_j are integers, all of which are non-zero except possibly α_1, β_n. If G is not freely generated by A and B, then G is not free [17, p. 1394]. Moreover, G is free and freely generated by A, B if and only if $W_n \neq 1_2$ for each W_n with all exponents α_i, β_j non-zero [21, p. 158].

Non-freeness testing of G by a number of authors (e.g., see [1, 15, 17]) depends on finding words of special form in G. The following is a criterion of such type.

Lemma 2.1. *If $N_G(\langle A\rangle)$ is non-cyclic then G is not free.*

Proof. The elements of the normalizer are upper triangular with constant diagonal ± 1. □

Since $G \leq G(\frac{m}{n})$, non-freeness (respectively, S-arithmeticity) of G implies that of $G(m/n)$. So in searching for $m \in (0, 2)$ such that G is non-free, we can restrict to $m \in (1, 2)$ if we wish.

Detecting non-identity elements of finite order is another way to prove non-freeness [5, 12]. In [5], it is shown that $G(r)$ for $r \in \mathbb{Q}$ has a non-identity element of finite order if and only if $\frac{1}{r} \in \mathbb{Z}$. One direction is simple: $\mathrm{SL}(2, \mathbb{Z}) \subseteq G(\frac{1}{b})$, so, e.g., $-1_2 \in G(\frac{1}{b})$. An elementary proof of the converse is given below.

Proposition 2.2. *For $m = \frac{a}{b}$ where $a > 1$, $G = G(m)$ is torsion-free.*

Proof. If $h \in G$ has prime order, then h is conjugate to an element of $\mathrm{SL}(2, \mathbb{Z})$. The finite order elements of $\mathrm{SL}(2, \mathbb{Z})$ are known by a result of Minkowski [21, p. 179]; of these, only -1_2 is possibly in $G \leq \Gamma_a$. Hence $m = \frac{2}{b}$, b odd. But this cannot be. For an element of G looks like

$$\begin{bmatrix} 1 + m^2 f_1(m) & m f_2(m) \\ m f_3(m) & 1 + m^2 f_4(m) \end{bmatrix}$$

where $f_i(m) \in \mathbb{Z}[m]$, $1 \leq i \leq 4$ ([5, p. 747]), and after clearing out denominators in the equation $2f_1(m) = -b^2$, we get a contradiction against b odd. □

Our preferred criterion for non-freeness testing follows.

Proposition 2.3. *Suppose that G is S-arithmetic. Then G is not free.*

Proof. Since Γ has the CSP, $\Gamma_c \leq G$ for some $c \geq 2$. In turn, Γ_c contains $\langle A(cR)\rangle = \{A(cx) \mid x \in R\}$. The latter is isomorphic to the additive group $(cR)^+$ of the ideal $cR \subseteq R$, and $(cR)^+$ is non-cyclic. □

So, our non-freeness test for Möbius subgroups is really a spinoff from attempts to prove S-arithmeticity in Γ.

3. Exploiting Zariski density of Möbius groups

In this section we establish properties of $G = G(m)$ that derive from Zariski density of G and the fact that Γ has the CSP. In particular, we find a generating set for $\mathrm{cl}(G)$.

Denote the set of prime divisors of $k \in \mathbb{Z}$ by $\pi(k)$. Let $\Pi(H)$ be the (finite) set of all primes p modulo which dense $H \leq \Gamma$ does not surject onto $\mathrm{SL}(2, p)$, i.e.,

$$\Pi(H) = \{p \in \mathbb{Z} \mid p \text{ prime}, \, \gcd(p, b) = 1, \, \varphi_p(H) \neq \mathrm{SL}(2, p)\}.$$

Lemma 3.1. $\Pi(G) = \pi(a)$.

Proof. If $p \,|\, a$ then $G \leq \Gamma_p$; so $\pi(a) \subseteq \Pi(G)$. If $p \nmid a$ then $\varphi_p(G) = \mathrm{SL}(2, p)$, because $\mathrm{SL}(2, p) = \langle A(k), B(k)\rangle$ for any $k \in \mathbb{F}_p \setminus \{0\}$. □

Let l be the level of G. Results from [9] imply that $\Pi(G) \setminus \{2, 3, 5\} = \pi(l) \setminus \{2, 3, 5\}$. We will see that $l = a^2$ (Theorem 3.7); so $\Pi(G) = \pi(a) = \pi(l)$ without exception.

Remark 3.2. If G surjects onto $\mathrm{SL}(2, p)$ modulo the prime p, then G surjects onto $\mathrm{SL}(2, \mathbb{Z}_{p^k})$ modulo p^k for all $k \geq 1$.

Lemma 3.3. *Let $a = p^e c$ where p is a prime, $e \geq 1$, and $\gcd(p, bc) = 1$. Then*

$$\Gamma_{p^{2e}} \leq G\Gamma_{p^f}$$

for any $f \geq 0$, but

$$\Gamma_{p^{2e-1}} \not\leq G\Gamma_{p^f}$$

if $f \geq 2e + 1$.

Proof. The lemma is trivially true if $f \leq 2e$. Suppose that $f > 2e$. Then $\Gamma_{p^f} \leq \Gamma_{p^{2e+1}} \leq \Gamma_{p^{2e}}$.

Since $\gcd(p, bc) = 1$, there is a positive integer i such that $i \cdot \frac{c}{b} \equiv 1 \bmod p^f$, so

$$A(m)^i \equiv A(p^e) \quad \text{and} \quad B(m)^i \equiv B(p^e) \quad \bmod p^f.$$

Hence $\varphi_{p^f}(G) = \varphi_{p^f}(G(p^e))$. We therefore prove the two assertions with $G(p^e)$ in place of G.

Setting $A(p^e) = x$ and $B(p^e) = y$, we have

$$[x, y] = \begin{bmatrix} 1 + p^{2e} + p^{4e} & p^{3e} \\ -p^{3e} & 1 - p^{2e} \end{bmatrix} \equiv \begin{bmatrix} 1 + p^{2e} & 0 \\ 0 & 1 - p^{2e} \end{bmatrix} \quad \bmod p^{2e+1}.$$

It follows that $U := \varphi_{p^{2e}}(G(p^e))$ is abelian, consisting of the p^{2e} distinct images

$$\varphi_{p^{2e}}\Big(\begin{bmatrix} 1 & sp^e \\ tp^e & 1 \end{bmatrix} \Big)$$

for $0 \leq s, t < p^e$. But then U does not contain

$$\varphi_{p^{2e}}\Big(\begin{bmatrix} 1+p^{2e-1} & p^{2e-1} \\ -p^{2e-1} & 1-p^{2e-1} \end{bmatrix}\Big).$$

Thus $\varphi_{p^{2e}}(\Gamma_{p^{2e-1}}) \not\leq U$.

It remains to prove the first assertion, and this we do by induction on f. For the base step $f = 2e+1$, note that the images of $[x, y]$, x^{p^e}, y^{p^e} under $\varphi_{p^{2e+1}}$ are

$$\begin{bmatrix} 1+p^{2e} & 0 \\ 0 & 1-p^{2e} \end{bmatrix}, \quad \begin{bmatrix} 1 & p^{2e} \\ 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 \\ p^{2e} & 1 \end{bmatrix}.$$

Together these generate the elementary abelian group $\varphi_{p^{2e+1}}(\Gamma_{p^{2e}})$, whose elements are of the form $1_2 + p^{2e}u$ where u has entries in $\{0, \ldots, p-1\}$ and $\mathrm{trace}(u) \equiv 0 \bmod p$.

Assume now that the statement is true for $f = k \geq 2e+1$. Then $\varphi_{p^k}(\Gamma_{p^{k-1}}) \leq \varphi_{p^k}(G(p^e))$. Thus, for each $1_2 + p^{k-1}u \in \varphi_{p^k}(\Gamma_{p^{k-1}})$ where u is a $\{0, \ldots, p-1\}$-matrix with zero trace modulo p, there exist $v \in G(p^e)$ and some w such that $v = 1_2 + p^{k-1}u + p^k w$. Then $v^p \equiv 1_2 + p^k u \bmod p^{k+1}$, which implies that $\varphi_{p^{k+1}}(\Gamma_{p^k}) \leq \varphi_{p^{k+1}}(G(p^e))$. Hence $\Gamma_{p^{2e}} \leq \langle G(p^e), \Gamma_{p^{k+1}} \rangle$ by the inductive hypothesis. □

Remark 3.4. Lemma 3.3 is valid for $b = 1$.

Lemma 3.5. *In the notation of Lemma* 3.3*, $\varphi_{p^{2e}}(G) \cong C_{p^e} \times C_{p^e}$. Hence*

$$|\mathrm{SL}(2, \mathbb{Z}_{p^{2e}}) : \varphi_{p^{2e}}(G)| = p^{4e} - p^{4e-2} = p^e|\mathrm{SL}(2, \mathbb{Z}_{p^e})|.$$

Proof. We observed that $\varphi_{p^{2e}}(G) = \varphi_{p^{2e}}(G(p^e)) \cong C_{p^e} \times C_{p^e}$ in the proof of Lemma 3.3. Also, $|\mathrm{SL}(n, \mathbb{Z}_{p^k})| = p^{(n^2-1)(k-1)}|\mathrm{SL}(n, p)|$. □

We gather together various observations about the structure of $\mathrm{SL}(2, \mathbb{Z}_{p^e})$, p prime, that are used in the subsequent proof.

Lemma 3.6.

(i) *Each proper normal subgroup of* $\mathrm{SL}(2, \mathbb{Z}_{p^e})$ *has index divisible by p.*

(ii) *Let $l > 1$ be an integer with prime factorization $l = p_1^{e_1} \cdots p_k^{e_k}$. Let K be a subgroup of* $\mathrm{SL}(2, \mathbb{Z}_l)$ *such that $\varphi_{p_i^{e_i}}(K) = \mathrm{SL}(2, \mathbb{Z}_{p^{e_i}})$ for all i, $1 \leq i \leq k$. Then $K = \mathrm{SL}(2, \mathbb{Z}_l)$.*

Proof. (i) A counterexample would arise from a proper normal subgroup of the quotient $\mathrm{PSL}(2, p)$. Hence the statement is clear for $p \geq 5$, and it follows for $p \in \{2, 3\}$ by inspection.

(ii) We proceed by induction on k, the base step being trivial. Write $l = rp^e$ where p is the largest prime divisor of l and $\gcd(p, r) = 1$. Then $\mathrm{SL}(2, \mathbb{Z}_l) \cong \mathrm{SL}(2, \mathbb{Z}_{p^e}) \times \mathrm{SL}(2, \mathbb{Z}_r)$; so K is a subdirect product of $\varphi_r(K)$ and $\varphi_{p^e}(K) = \mathrm{SL}(2, \mathbb{Z}_{p^e})$. The inductive hypothesis gives $\varphi_r(K) = \mathrm{SL}(2, \mathbb{Z}_r)$. Since, for any prime q, the largest prime divisor of $|\mathrm{SL}(2, q)|$ is q, we see that p cannot divide $|\mathrm{SL}(2, \mathbb{Z}_r)|$. Then (i) forces G to be the full direct product $\mathrm{SL}(2, \mathbb{Z}_{p^e}) \times \mathrm{SL}(2, \mathbb{Z}_r)$. This completes the proof by induction. □

The next theorem is the main result of this section, and it facilitates our experiments in the final section.

Theorem 3.7.

(i) $\mathrm{cl}(G) = G\Gamma_{a^2}$ *has level* a^2.
(ii) $|\Gamma : \mathrm{cl}(G)| = a \cdot |\mathrm{SL}(2, \mathbb{Z}_a)|$.

Proof. (i) Let l be the level of G. If $p^e > 1$ is the largest power of the prime p dividing a, then $G\Gamma_{p^{2e}}$ has level p^{2e} by Lemma 3.3. Since $H := \mathrm{cl}(G) = G\Gamma_l \le G\Gamma_{p^{2e}}$ and therefore $\Gamma_l \le \Gamma_{p^{2e}}$, we see that l is divisible by p^{2e}. Thus a^2 divides l.

Next we will prove $\pi(l) \subseteq \pi(a)$, i.e., $\pi(l) = \pi(a)$. To this end, suppose that $l = rk$ where $r > 1$, $\pi(k) = \pi(a)$, and $\gcd(r, a) = 1$. By Lemma 3.1, Remark 3.2, and Lemma 3.6, $\varphi_r(G) = \mathrm{SL}(2, \mathbb{Z}_r)$. Since $\mathrm{SL}(2, \mathbb{Z}_l) \cong \mathrm{SL}(2, \mathbb{Z}_r) \times \mathrm{SL}(2, \mathbb{Z}_k)$, it follows that $\varphi_l(H) = \varphi_l(G)$ is a subdirect product of $\mathrm{SL}(2, \mathbb{Z}_r)$ and $\varphi_k(H)$. Each proper quotient of $\mathrm{SL}(2, \mathbb{Z}_r)$ has order divisible by a prime in $\pi(r)$, whereas $\varphi_k(H)$ has order divisible only by the primes in $\pi(a)$. Thus $\varphi_l(H) \cong \mathrm{SL}(2, \mathbb{Z}_r) \times \varphi_k(H)$, and as a consequence $\Gamma_k \le H$; but Γ_l is the PCS of least level in H.

We have now proved that $\pi(l) = \pi(a)$. Therefore $\varphi_l(H)$ is a direct product of p-groups $\varphi_{p^f}(H)$ for p ranging over $\pi(a)$. Suppose that $l > a^2$; say p^f divides l where $f > 2e$ and p^e is the largest power of p dividing a. We infer from $\Gamma_{p^{2e}} \le G\Gamma_{p^f}$ that $\varphi_l(\Gamma_{l/p^{f-2e}}) \le \varphi_l(H)$, so $\Gamma_{l/p^{f-2e}} \le H$: contradiction. Hence $l = a^2$.

(ii) This follows from Lemma 3.5. □

Corollary 3.8. $\mathrm{cl}(G)/\Gamma_{a^2} \cong C_a \times C_a$.

The proof of Theorem 3.7 is independent of the denominator b, so additionally we have proved that $G(a) \le \mathrm{SL}(2, \mathbb{Z})$ has level a^2. Cf. [7, Proposition 1.12]: for $n \ge 3$, the 'elementary group' in $\mathrm{SL}(n, \mathbb{Z})$ generated by all matrices $1_n + me_{ij}$ with $i \ne j$ (e_{ij} has 1 in position (i, j) and zeros elsewhere) contains the PCS of level m^2.

In line with [26] (and cf. [7, Proposition 1.10]), one can show that Γ_{a^2} is generated by

$$A(am),\ B(am),\ B(am)^x,\ \text{where } x = \begin{bmatrix} -1 & 1 \\ 0 & 1 \end{bmatrix}.$$

Also, at least when b is prime, Γ_{a^2} is the normal closure $\langle A(am)\rangle^\Gamma = \langle B(am)\rangle^\Gamma$ of $G(am)$ in Γ (this implies the CSP; see [19]). Thus, we get an explicit generating set of $\mathrm{cl}(G)$.

Theorem 3.7 and Corollary 3.8 afford further insights. Lifting from a presentation of $\varphi_{a^2}(G) \cong C_a \times C_a$ by the 'normal generators method' (see, e.g., [10, §3.2]) yields that

$G \cap \Gamma_{a^2}$ is the normal closure in G of

$$\langle A(am), B(am), [A(m), B(m)] \rangle.$$

In summary, using the notation $\leq_{\mathrm{f}}$, $<_{\infty}$ to denote a subgroup of finite or infinite index, respectively:

1. if G is thin then $G(am) \leq G <_{\infty} \mathrm{cl}(G) \leq_{\mathrm{f}} \Gamma_a$;
2. if G is S-arithmetic then $G(am) \leq \Gamma_{a^2} \leq_{\mathrm{f}} G \leq_{\mathrm{f}} \Gamma_a$;
3. G is S-arithmetic if and only if $\langle A(am) \rangle^{\Gamma} \leq G$.

When G is S-arithmetic, an extra benefit of Theorem 3.7 is that it enables us to test membership of $g \in \Gamma$ in G. The idea is obvious: $g \in G$ if and only if $\varphi_{a^2}(g) \in \varphi_{a^2}(G)$. More generally, we could get a negative answer to the question of whether g is in G by testing membership of g in $\mathrm{cl}(G)$.

4. Experimentation

4.1. Computing presentations of $\mathrm{SL}(2, R)$.

A key requirement for the experiments, which feature Todd–Coxeter coset enumeration, is a presentation of Γ. Our algorithm to construct one is based on the next theorem, due to Ihara [25, Corollary 2, p. 80].

Theorem 4.1. *For any prime p,*

$$\mathrm{SL}(2, \mathbb{Z}[1/p]) \cong \mathrm{SL}(2, \mathbb{Z}) *_{\Gamma_0(p)} \mathrm{SL}(2, \mathbb{Z}),$$

the free product with amalgamation $\Gamma_0(p)$, where $\Gamma_0(p)$ comprises all matrices in $\mathrm{SL}(2, \mathbb{Z})$ that are upper triangular modulo p.

Theorem 4.1 can be expanded by iteration to $\mathrm{SL}(2, \mathbb{Z}[1/b])$ for composite b [25, p. 80]. If k is an integer not divisible by p, then $\mathrm{SL}(2, \mathbb{Z}[1/pk])$ is the amalgamated free product of two copies of $\mathrm{SL}(2, \mathbb{Z}[1/k])$, with the amalgamated subgroup as before comprising all mod-p upper triangular matrices.

Theorem 4.1 is applied in a standard way to obtain a presentation of $\mathrm{SL}(2, \mathbb{Z}[1/p])$; see, e.g., [25, pp. 80–81]. We use the presentations

$$\langle s, t \mid s^4 = 1, (st)^3 = s^2 \rangle \quad \text{and} \quad \langle x_p, y_p \mid x_p^4 = 1, (x_p y_p)^3 = x_p^2 \rangle$$

of $\mathrm{SL}(2, \mathbb{Z})$, where

$$s = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \quad t = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}, \quad x_p = \begin{bmatrix} 0 & \frac{1}{p} \\ -p & 0 \end{bmatrix}, \quad y_p = \begin{bmatrix} 1 & -\frac{1}{p} \\ 0 & 1 \end{bmatrix}.$$

We construct a generating set for $\Gamma_0(p)$ whose elements are Schreier generators for the stabilizer of the subspace $\langle (1,0)^{\top} \rangle \subseteq \mathbb{F}_p^2$ under the natural action of $\mathrm{SL}(2, \mathbb{Z})$ modulo p. It is easily seen that $|\mathrm{SL}(2, \mathbb{Z}) : \Gamma_0(p)| = p + 1$. Suppose that $\Gamma_0(p)$ is given by a generating set of matrices $w_i = w_i(x, y)$ that are words in $x = x_p$ and $y = y_p$. We express each

w_i (utilizing the GAP package ModularGroup [16]) as a word $w_i'(s,t)$ in s and t. Then $\mathrm{SL}(2,\mathbb{Z}[1/p])$ has presentation

$$\langle s,t,x,y \mid s^4=1,(st)^3=s^2,x^4=1,(xy)^3=x^2, \\ w_1(x,y)=w_1'(s,t),\ldots,w_k(x,y)=w_k'(s,t)\rangle$$

for some $k \leq p+2$; of course, this may simplify. However, eliminating redundancy is usually not worthwhile, because it comes at the cost of longer words.

Some examples are below.

- Let $p=5$. Then $\Gamma_0(p)$ is generated by

$$x^{-2},\, xyx^{-1},\, y^5,\, y^2xy^{-2},\, yx^{-1}y.$$

Actually, the fifth listed generator is redundant. Now

$$x^{-2}=\begin{bmatrix}-1 & 0\\ 0 & -1\end{bmatrix},\quad xyx^{-1}=\begin{bmatrix}1 & 0\\ 5 & 1\end{bmatrix},\quad y^5=\begin{bmatrix}1 & -1\\ 0 & 1\end{bmatrix},\quad y^2xy^{-2}=\begin{bmatrix}2 & 1\\ -5 & -2\end{bmatrix}.$$

The corresponding words w' are $s^{-2}, t^5, (tst)^{-1}, t^{-2}st^2$. Hence

$$\langle s,\, t,\, x,\, y \mid x^4,\, xyxyxyx^{-2},\, s^4,\,ststst s^{-2},\, x^{-2}s^2,\, xyx^{-1}t^{-5},\, y^5tst,\, y^2xy^{-2}t^{-2}s^{-1}t^2\rangle$$

is a presentation of $\mathrm{SL}(2,\mathbb{Z}[1/5])$.

- We similarly calculate that $\mathrm{SL}(2,\mathbb{Z}[1/7])$ has presentation

$$\langle s,t,x,y \mid s^4,\, stststs^{-2},\, x^4,\, xyxyxyx^{-2},\, x^{-2}s^2,\, xyx^{-1}t^{-7}, \\ y^3x^{-1}y^{-2}t^{-3}st^2,\, y^{-3}x^{-1}y^2t^3st^{-2}\rangle.$$

The generating set in this example is redundant.

- The results for $p=5$ and $p=7$ combine to give

$$\mathrm{SL}(2,\mathbb{Z}[\tfrac{1}{35}])=\langle s,t,x,y,c,d \mid s^4,\, stststs^{-2},\, x^4,\, xyxyxyx^{-2},\, x^{-2}s^2,\, xyx^{-1}t^{-5}, \\ y^5tst,\, y^2xy^{-2}t^{-2}s^{-1}t^2,\, c^4,\, cdcdcdc^{-2},\, c^{-2}s^2, \\ cdc^{-1}t^{-7},\, d^{-3}c^{-1}d^2t^3st^{-2},\, d^3c^{-1}d^{-2}t^{-3}st^2\rangle$$

where $x=x_5$, $y=y_5$, $c=x_7$, and $d=y_7$.

We implemented the above approach as a GAP procedure. It accepts an integer $b>1$ and returns a presentation of $\Gamma=G(1/b)$ on $2+2|\pi(b)|$ generators. In our experience, this procedure completed rapidly for prime $b\approx 2000$. For composite b, the cost is basically just that of the prime factors, since the amalgamation is straightforward. For larger a, we find short word expressions by systematically enumerating all words by increasing length.

4.2. S**-arithmeticity of** $G(m)$**.** In this section we justify S-arithmeticity (and thereby non-freeness) of $G(m)$ for a range of rational m between 0 and 2.

First, we express the generators $A = A(m)$ and $B = B(m)$ of $G = G(m)$ as words in the generators of Γ. When $m = a/p$ for a prime p, this is easy: $A(a/p) = A(1/p)^a = y^{-a}$ and $B(a/p) = sy^a s^{-1}$. For larger a, we try to find short word expressions by random search. Then we take the subgroup of Γ defined by the two words for A and B and carry out Todd–Coxeter coset enumeration (within the GAP package ACE [13]). If the enumeration terminates, then rewriting using the modified Todd–Coxeter algorithm of [20] finds relators in A and B. Unless a is small, these relators tend to be long; e.g., the shortest relator discovered for $m = 4/11$ is $A^{121}BA^{-11}B^2A^{-121}B^{-1}A^{11}B^{-2}$. Relator length typically increases with the index of G in Γ (ruled by a; Theorem 3.7 (ii)). This suggests that searching for short relators with particular patterns (cf. [1]) has limited chance of proving non-freeness. Also recall that if G is S-arithmetic, then it contains upper unitriangular elements u and v such that $\langle u, v\rangle$ is non-cyclic. Once we express $uvu^{-1}v^{-1}$ as a word in A and B, we have a non-trivial relator in G.

Stages in the coset enumeration may entail significantly (and unboundedly) more cosets than $|\Gamma : G|$, so that coset enumeration for G in Γ may fail to terminate within reasonable time or the available memory, even if the index is small. We emphasize that failure to terminate is *not* a proof that G is thin.

If finite, the index $a|\mathrm{SL}(2, \mathbb{Z}_a)|$ of $G(a/b)$ in Γ is greater than 10^6, 10^7, 10^8, for $a = 33$, $a = 59$, $a = 101$, respectively. With four generators, and ignoring overhead, each row in the coset table requires at least $4 \cdot 2 \cdot 8 = 64$ bytes of memory. This means that 1GB of memory can store no more than 10^7 cosets. By this reckoning, we expect that coset enumeration becomes difficult when a is between 40 and 50. If the index is finite, then we would expect that enumeration succeeds if $a \leq 25$.

Returning to an earlier point: S-arithmeticity of $G(a/b)$ implies S-arithmeticity of $G(a/kb)$ for every integer $k > 0$, so we could restrict experimentation to groups $G(a/p)$ where p is prime. However, the practicality of an attempt to prove S-arithmeticity of $G(a/b)$ is affected by the size of a. Thus, we investigated $G(m)$ with $m = a/b < 2$ where $b = p^k$, $p \leq 23$ prime. For each fixed denominator b, we found an integer $a_{\max}$ such that $G(a/b)$ is S-arithmetic whenever $a \leq a_{\max}$; see Table 1. We also managed to prove that $G(m)$ is S-arithmetic for the following $m = a/b$ where a exceeds $a_{\max}$ for the given b: $63/64, 65/64, 44/125, 51/125, 57/125, 29/49$.

Unsuccessful enumerations were re-attempted for comparatively small a. Here we tried strategies such as increased memory, simplifying the presentation, or use of intermediate subgroups. None of these helped, leading us to suspect that the maximum numerator values up to 30 or so are likely to be correct.

$a_{\max}$	3	7	13	23	37	45	57	5	14	31	41	9	28	39	11	25
b	2	4	8	16	32	64	128	3	9	27	81	5	25	125	7	49

$a_{\max}$	12	23	15	14	14	14
b	11	121	13	17	19	23

TABLE 1. Values of $a_{\max}$ and b such that $G(m)$ is S-arithmetic for all $m = \frac{a}{b}$, where $a \leq a_{\max}$

Our experiments show that many $G(m)$ previously known to be non-free are S-arithmetic (see, e.g., [1, 12, 17]). As a single complementary example, we proved that $G(11/19)$ is not free, whereas freeness of $G(11/19)$ was unresolved in [1].

As further illustration, Figure 1 plots $a_{\max}$ against the denominators $b = p^k$ for the primes $p \leq 11$ considered in Table 1. The results for small b hint that $G(a/b)$ is thin if $a/b > 9/5$.

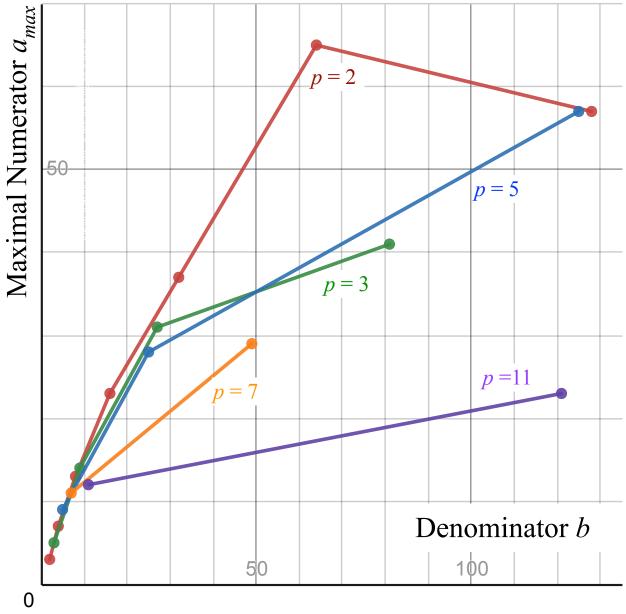

FIGURE 1. S-arithmeticity of $G(a_{\max}/b)$

GAP code to accompany this section is posted at `https://github.com/hulpke/arithmetic`.

Acknowledgments. We thank Vladimir Shpilrain for helpful conversations. This research was supported through the Oberwolfach Research Fellows programme of the Mathematisches Forschungsinstitut Oberwolfach in 2021. The third author's work was supported also by NSF Grant DMS-1720146 and Simons Foundation Grant 852063, which are gratefully acknowledged.

References

1. A. F. Beardon, *Pell's equation and two generator free Möbius groups*, Bull. London Math. Soc. **25** (1993), no. 6, 527–532.
2. J. L. Brenner, *Quelques groupes libres de matrices*, C. R. Acad. Sci. Paris **241** (1955), 1689–1691.
3. J. L. Brenner, R. A. Macleod, and D. D. Olesky, *Non-free groups generated by two* 2×2 *matrices*, Canadian J. Math. **27** (1975), 237–245.
4. J. Cassaigne, T. Harju, and J. Karhumäki, *On the undecidability of freeness of matrix semigroups*, Internat. J. Algebra Comput., **9** (1999), no.s 3-4, 295–305.
5. A. Charnow, *A note on torsion free groups generated by pairs of matrices*, Canad. Math. Bull. **17** (1974/75), no. 5, 747–748.
6. A. Chorna, K. Geller, and V. Shpilrain, *On two-generator subgroups in* $SL_2(\mathbb{Z})$, $SL_2(\mathbb{Q})$, *and* $SL_2(\mathbb{R})$, J. Algebra **478** (2017), 367–381.
7. A. S. Detinko, D. L. Flannery, and A. Hulpke, *Algorithms for arithmetic groups with the congruence subgroup property*, J. Algebra **421** (2015), 234–259.
8. A. S. Detinko, D. L. Flannery, and A. Hulpke, *Zariski density and computing in arithmetic groups*, Math. Comp. **87** (2018), no. 310, 967–986.
9. A. S. Detinko, D. L. Flannery, and A. Hulpke, *Zariski density and computing with* S*-integral groups*, preprint (2021).
10. A. S. Detinko, D. L. Flannery, and E. A. O'Brien, *Algorithms for the Tits alternative and related problems*, J. Algebra **344** (2011), 397–406.
11. H.-A. Esbelin and M. Gutan, *Solving the membership problem for parabolic Möbius monoids*, Semigroup Forum **98** (2019), no. 3, 556–570.
12. S. P. Farbman, *Non-free two-generator subgroups of* $\mathrm{SL}_2(\mathbf{Q})$, Publ. Mat. **39** (1995), no. 2, 379–391.
13. G. Gamble, A. Hulpke, G. Havas, and C. Ramsay, The GAP package ACE (Advanced Coset Enumerator). https://www.gap-system.org/Packages/ace.html
14. The GAP Group, *GAP – Groups, Algorithms, and Programming*. http://www.gapsystem.org
15. M. Gutan, *Diophantine equations and the freeness of Möbius groups*, Applied Mathematics **5** (2014), 1400–1411. http://dx.doi.org/10.4236/am.2014.510132
16. L. L. Junk and G. Weitze-Schmithüsen The GAP package ModularGroup, https://github.com/AG-Weitze-Schmithusen/ModularGroup
17. R. C. Lyndon and J. L. Ullman, *Groups generated by two parabolic linear fractional transformations*, Canadian J. Math. **21** (1969), 1388–1403.
18. J. Mennicke, *Finite factor groups of the unimodular group*, Ann. of Math. (2) **81** (1965), no. 1, 31–37.
19. J. Mennicke, *On Ihara's modular group*, Invent. Math. **4** (1967), 202–228.
20. J. Neubüser, *An elementary introduction to coset table methods in computational group theory*, Groups—St. Andrews 1981 (St. Andrews, 1981), London Math. Soc. Lecture Note Ser., vol. 71, Cambridge Univ. Press, Cambridge-New York, 1982, pp. 1–45.
21. M. Newman, *Integral matrices*, Academic Press, New York-London, 1972.
22. I. N. Sanov, *A property of a representation of a free group*, Doklady Akad. Nauk SSSR (N. S.) **57** (1947), 657–659.

23. P. Sarnak, *Notes on thin matrix groups*, Thin groups and superstrong approximation, 343–362, Math. Sci. Res. Inst. Publ. **61**, Cambridge Univ. Press, Cambridge, 2014.
24. J.-P. Serre, *Le problème des groupes de congruence pour* **SL2**, Ann. of Math. (2) **92** (1970), 489–527.
25. J.-P. Serre, *Trees*, Springer-Verlag, Berlin-New York, 1980.
26. B. Sury and T. N. Venkataramana, *Generators for all principal congruence subgroups of* $\mathrm{SL}(n, Z)$ *with* $n \geq 3$, Proc. Amer. Math. Soc. **122** (1994), no. 2, 355–358.
27. B. A. F. Wehrfritz, *Infinite linear groups*, Springer-Verlag, New York-Heidelberg, 1973.

DEPARTMENT OF COMPUTER SCIENCE, SCHOOL OF COMPUTING AND ENGINEERING, UNIVERSITY OF HUDDERSFIELD, HUDDERSFIELD HD13DH, UK

E-mail address: detinko.alla@gmail.com

SCHOOL OF MATHEMATICAL AND STATISTICAL SCIENCES, NATIONAL UNIVERSITY OF IRELAND GALWAY, GALWAY H91TK33, IRELAND

E-mail address: dane.flannery@nuigalway.ie

DEPARTMENT OF MATHEMATICS, COLORADO STATE UNIVERSITY, FORT COLLINS, CO 80523-1874, USA

E-mail address: Alexander.Hulpke@colostate.edu