Non-freeness of groups generated by two parabolic elements

SANG-HYUN KIM AND THOMAS KOBERDA

Abstract. Let $q \in \mathbb{C}$, let

$$a = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \quad b_q = \begin{pmatrix} 1 & q \\ 0 & 1 \end{pmatrix},$$

and let $G_q < \mathrm{SL}_2(\mathbb{C})$ be the group generated by a and b_q. In this paper, we study the problem of determining when the group G_q is not free for $|q| < 4$ rational. We give a robust computational criterion which allows us to prove that if $q = s/r$ for $|s| \leqslant 27$ then G_q is non-free, with the possible exception of $s = 24$. In this latter case, we prove that the set of denominators $r \in \mathbb{N}$ for which $G_{24/r}$ is non-free has natural density 1. For a general numerator $s > 27$, we prove that the lower density of denominators $r \in \mathbb{N}$ for which $G_{s/r}$ is non-free has a lower bound

$$1 - \left(1 - \frac{11}{s}\right) \prod_{n=1}^{\infty} \left(1 - \frac{4}{s^{2^n - 1}}\right).$$

Finally, we show that for a fixed s, there are arbitrarily long sequences of consecutive denominators r such that $G_{s/r}$ is non-free. The proofs of some of the results are computer assisted, and Mathematica code has been provided together with suitable documentation.

1. Introduction

For each $q \in \mathbb{C}$, let us write

$$a = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \quad b_q = \begin{pmatrix} 1 & q \\ 0 & 1 \end{pmatrix},$$

and write G_q for the subgroup of $\mathrm{SL}_2(\mathbb{C})$ generated by a and b_q.

The group G_q is not infinite cyclic unless $q = 0$. It is proved by Sanov [20] and Brenner [5] that the group G_q is free for all $q \in \mathbb{R} \backslash (-4, 4)$; more strongly, the group G_q is discrete and free for all q in the *Riley slice* of the complex plane [13].

In this paper, we study the following conjecture:

Main Conjecture. *For each nonzero rational number $q = s/r$ in $(-4, 4)$, the group*

$$G_q := \langle a, b_q \rangle \leqslant \mathrm{SL}_2(\mathbb{C})$$

2010 *Mathematics Subject Classification.* Primary: 30F35, 30F40; Secondary: 20E05, 11J70.
Key words and phrases. Fuchsian groups, Kleinian groups.

is not free.

Lyndon and Ullman asked this conjecture (as a question) in [17]. This problem has a long history, and the reader is directed to [9] and to Section 1.2 below for the state of the art prior to this writing.

Slightly different normalizations have also been considered in the literature. We may define

$$H_q = \left\langle \begin{pmatrix} 1 & 0 \\ q & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & q \\ 0 & 1 \end{pmatrix} \right\rangle.$$

The corresponding question for H_q is attributed to Merzlyakov in the Kourovka Notebook [12, Problem 15.83]. It is noted in [6] that $H_q \cong G_{q^2}$. In some other papers such as [6, 9], the group G_{2q} is considered.

Remark 1.1. Under the hypothesis that q is rational and belongs to $(-4, 4)$, the group G_q is discrete only if $|q| \in \{0, 1, 2, 3\}$; see [16].

1.1. **Main results.** As mentioned above, G_q is free whenever $q \in \mathbb{R}\backslash(-4, 4)$. It is easy to see that G_q is free if q is transcendental. However, being algebraic is not sufficient to guarantee non-freeness. As noted in [7], Galois conjugation yields an isomorphism

$$G_{4-\sqrt{2}} \cong G_{4+\sqrt{2}},$$

the latter of which is indeed free by the result of Sanov and Brenner.

Definition 1.2. We will say $q \in \mathbb{C}$ is a *relation number* if G_q is not a rank–two free group.

A good summary of known results about *rational* relation numbers can be found in Theorem 7.7 of [9]. Before stating the results of this paper, we introduce some terminology. Let $F = \langle x, y\rangle$ be a free group of rank two. A complex number q is called an *ℓ–step relation number* if there exists a nontrivial word of the form

$$w = y^{m_1} x^{m_2} \cdots y^{m_{2k+1}} \in F$$

for some $k \in [0, \ell]$ and $m_i \in \mathbb{Z}\backslash\{0\}$ such that $w(a, b_q)$ is a lower–triangular matrix in $\mathrm{SL}_2(\mathbb{C})$.

It turns out then every relation number is an ℓ–step relation number for some $\ell \geqslant 0$, and vice versa (Lemma 2.2). Actually, if q is an ℓ–step relation number, then there exists a word $v = v(x, y) \in F$ of syllable length at most $8(\ell + 1)$ such that $v(a, b_q) = 1$; see Remark 2.3.

Let $X \subset \mathbb{Z}$ be a subset. The *(right) upper density* of X is given by

$$\overline{d}(X) = \limsup_N \frac{X \cap [1, N]}{N}.$$

The *(right) lower density* of X is similarly given by

$$\underline{d}(X) = \liminf_{N} \frac{X \cap [1, N]}{N}.$$

If these limits coincide, they are called the *(right) natural density* of X. Note we allow X to have negative integers.

Remark 1.3. One may also consider a *symmetric (lower or upper) density*, which is a limit (superior or inferior) of $(X \cap [-N, N])/(2N + 1)$. For the integer sets concerned in this paper, all right densities will coincide with symmetric densities, whence we will simply refer to upper and lower densities when no confusion can arise. Note in particular that if s/r is an ℓ–step relation number then so is $s/(-r)$.

Our main results are towards resolving the Main Conjecture. Precisely, we prove the following:

Theorem 1.4. *Let s be a positive integer.*

(1) Suppose $s \leqslant 27$ and $s \neq 24$. Then for all but finitely many nonzero integers r, the number s/r is a 2–step relation number. Moreover, for all nonzero integer r satisfying $s/r \in (-4, 4)$, the number s/r is a relation number.
(2) If $s = 24$, then s/r is a 2–step relation number for all r in some natural density–one subset of $\mathbb{N}$.

By our previous discussion, the above theorem resolves the Main Conjecture for all r if $s \in [1, 27]\backslash\{24\}$, and for almost all r if $s = 24$. It even asserts that for a given $s \leqslant 27$ and for almost all $r \in \mathbb{N}$, there exists a nontrivial word of syllable length at most 24 in G_q that becomes trivial. We note that some parts of the proof are computer assisted, and we have provided code and documentation in the appendices below.

For a general $s \in \mathbb{N}$, we have the following result which finds a very large number of relation numbers with a given numerator:

Theorem 1.5. *Let s be an integer greater than* 27*. If we set*

$$A_s^{(2)} := \{r \in \mathbb{Z}\backslash\{0\} \mid s/r \text{ is a 2–step relation number}\},$$

then we have

$$\underline{d}\left(A_s^{(2)}\right) \geqslant 1 - \left(1 - \frac{11}{s}\right) \prod_{n=1}^{\infty} \left(1 - \frac{4}{s^{2^n - 1}}\right).$$

It is natural to wonder if $d\left(A_s^{(2)}\right) = 1$. Unfortunately, the sequence $\{s^{2^n-1}\}_{i \in \mathbb{N}}$ grows much too quickly, and generally the infinite product in Theorem 1.5 will converge to real number strictly less than 1 (see Section 6 below). Of course, the choices of such a sequence can be modified, but it is not clear to the authors that the methods given here avail themselves to a suitable choice that witnesses $d\left(A_s^{(2)}\right) = 1$.

Question 1.6. *For an integer $s > 27$, is it true that $d\left(A_s^{(2)}\right) = 1$?*

We are able to prove one further result which strongly suggests that the answer to Question 1.6 is yes, without quite establishing it definitively.

Theorem 1.7. *(see Corollary 3.9) Let $s, r, N \in \mathbb{N}$. Then there exists an $M = M(s, r, N) \in \mathbb{N}$ such that*

$$\frac{s}{r + i + sMj}$$

is a 2–step relation number for all integers $0 \leqslant i < N$ and $j \neq 0$.

In particular, for a fixed s there are arbitrarily long sequences of consecutive denominators which give rise to relation numbers of the form s/r. However, such sequences may possibly be spaced very sparsely within $\mathbb{N}$.

1.2. **Notes and references.** As noted above, the extent to which Sanov's result holds or fails for $q \in (-4, 4)$ has a long history. Some of the earliest examples of non-integral rational relation numbers of q were found by Ree [18]. On the other hand, many conditions for freeness of G_q were found by Chang–Jennings–Ree [6]. Many more examples of relation numbers were found in [4, 10, 11, 17, 2]. Connections to diophantine problems, and especially solutions to Pell's Equation, were studied in [8, 22, 3]. Discreteness of G_q for a complex parameter $q \in \mathbb{C}$ has been extensively studied; see [1, 9] and the references therein. For related discreteness questions in $\mathrm{PSL}_2(\mathbb{R})$, see [15], for instance.

A dynamical interpretation of relation numbers was suggested first by Tan–Tan [22], and these ideas have been developed in [2, 19, 21].

One may compare the results of this paper to the results outlined in Theorem 7.7 of [9]. We are primarily concerned with groups of the form G_q for $|q| < 1$ rational, whereas the results there are given for groups of the form H_q where q may be non-rational algebraic. One notes immediately from Theorem 1.4 that we have produced many new examples of rational relation values of q, and in view of Theorems 1.5 and 1.7, many new infinite families of relation values which do not fall under the purview of previously known results.

The freeness and non-freeness of the groups G_q has applications to group–based cryptography and theoretical computer science. See for instance [7].

Finally, a remark about normalizations. We consider the groups $\{G_q\}_{q\in\mathbb{Q}}$ over the groups $\{H_q\}_{q\in\mathbb{Q}}$, in spite of the break in symmetry, because the groups $\{G_q\}_{q\in\mathbb{Q}}$ encompass a larger class of subgroups of $\mathrm{SL}_2(\mathbb{Q})$ and hence give rise to an *a priori* richer theory.

2. Notation and terminology

Recall the following definition from Introduction.

Definition 2.1. A complex number q is called an *ℓ–step relation number* if there exist integers $k \in [0, \ell]$ and $m_1, \ldots, m_k \in \mathbb{Z}\backslash\{0\}$ such that for the word

$$w = y^{m_1} x^{m_2} \cdots y^{m_{2k+1}} \in F$$

the matrix $w(a, b_q)$ is a lower–triangular matrix in $\mathrm{SL}_2(\mathbb{C})$.

The number $q = 0$ is the unique 0–step relation number. The following lemma (due to Lyndon and Ullman) describes the relationship between the Main Conjecture and ℓ–step relation numbers.

Lemma 2.2 ([17])**.** *A complex number q is a relation number if and only if it is an ℓ–step relation number for some $\ell \geqslant 0$.*

Proof. The forward direction is obvious from the fact that the identity matrix is lower–triangular. For the converse, let $w = w(x, y)$ be as in Definition 2.1. Then the matrix

$$w(a, b_q) \cdot a \cdot w(a, b_q)^{-1}$$

is lower triangular such that the diagonal entries are 1. It follows that the reduced word $[wxw^{-1}, x]$ becomes the identity in $\mathrm{SL}_2(\mathbb{C})$ after setting $x = a$ and $y = b_q$. □

Remark 2.3. The *syllable length* of a nontrivial element $g \in F$ is the smallest integer $\ell \geqslant 0$ such that

$$g = w_1 \cdots w_\ell$$

for some $w_i \in \langle x\rangle \cup \langle y\rangle$. The above proof shows that if q is an ℓ–step relation number then there exists a nontrivial word $v(x, y) = [wxw^{-1}, x]$ of syllable length at most $8(\ell + 1)$ such that $v(a, b_q) = 1$.

From Lemma 2.2, we see that the Main Conjecture has the following diophantine-type formulation.

Conjecture 2.4. *Every rational number is an ℓ–step relation number for some $\ell \geqslant 0$.*

Let us describe a notation that will be used often throughout this paper. Let $q \in \mathbb{C}$, and let $m_1, m_2, \ldots$ be a sequence of nonzero integers. We define complex vectors $v_1, v_2, \ldots$ by setting $v_1 = (1, 0)$ and

$$v_{i+1} = (1, 0) b_q^{m_1} a^{m_2} \cdots (b_q \text{ or } a)^{m_i}.$$

Note that q is an ℓ–step relation number if and only if one can find a sequence $\{m_i\} \subseteq \mathbb{Z}\backslash\{0\}$ such that $v_{2k+2} \in \mathbb{C} \times \{0\}$ for some $k \leqslant \ell$.

As we are only interested in whether or not the second coordinate of v_i becoming zero, we may regard v_i as a point in the projective space $\mathbb{C}P^1$. In particular, we will identify (x, y) and (nx, ny) for $x, y \in \mathbb{Z}$ and $n \in \mathbb{Z}\setminus\{0\}$. We will then use the notation

$$(*) \qquad v_1 := (1,0) \overset{m_1}{\twoheadrightarrow} v_2 \overset{m_2}{\to} v_3 \overset{m_3}{\twoheadrightarrow} \cdots \overset{m_{2i}}{\to} v_{2i+1} \twoheadrightarrow \cdots .$$

The nonzero exponents $m_1, m_2, \ldots$ will often be suppressed as well.

Example 2.5. For $q = 1$ or $q = 2$, we have a sequence

$$(1,0) \twoheadrightarrow (1,2) \to (-1,2) \twoheadrightarrow (-1,0) = (1,0).$$

For $q = 3$, we see

$$(1,0) \overset{1}{\twoheadrightarrow} (1,3) \overset{-1}{\to} (-2,3) \overset{1}{\twoheadrightarrow} (-2,-3) \overset{-1}{\to} (1,-3) \overset{1}{\twoheadrightarrow} (1,0).$$

It follows that all integers in the interval $[-3, 3]$ are relation numbers.

The Main Conjecture can be reformulated in terms of generalized continued fractions. Suppose we have an orbit as above in $(*)$. Write $Q = 1/q$ and $v_i = (x_i, y_i)$. Assuming $x_i y_i \neq 0$, we define

$$q_i := Q y_i / x_i = y_i / (q x_i).$$

Then we have that

$$q_{i+1} = \begin{cases} Q(y_i + q m_i x_i)/x_i = m_i + q_i & \text{if } 2 \nmid i, \\ Q y_i / (x_i + m_i y_i) = Q/(m_i + Q/q_i) & \text{if } 2 \mid i. \end{cases}$$

On the other hand, it is obvious that q is a relation number if $x_i y_i = 0$ for some i, or if

$$(x_i, y_i) = (x_j, y_j) \in \mathbb{C}P^1$$

for some $i < j$. In summary, we have the following.

Proposition 2.6. *Let $Q \in \mathbb{C}\setminus\{0\}$. Then $1/Q$ is a relation number if and only if there exists a finite sequence of non-zero integers*

$$m_1, \ldots, m_\ell$$

such that the sequence

$$a_k := m_k + \cfrac{Q}{m_{k-1} + \cfrac{Q}{\cdots + \cfrac{Q}{m_2 + \cfrac{Q}{m_1}}}}$$

either terminates with $a_\ell = 0$ for some $\ell \geqslant 2$, or satisfies $a_\ell = a_{\ell'}$ for some $\ell > \ell' \geqslant 2$.

The Main Conjecture asserts that one has a sequence $\{m_i\}$ as above whenever $Q \in \mathbb{Q}\backslash[-1/4, 1/4]$.

3. Families of rational relation numbers

In this section, we develop a foundation for producing large collections of rational relation numbers in the sequel.

Let us define

$$R_{\mathbb{Q}} := \{q \in \mathbb{Q} \mid q \text{ is a relation number}\};$$
$$R_{\mathbb{Q}}^{(\ell)} := \{q \in \mathbb{Q} \mid q \text{ is an } \ell\text{–step relation number}\};$$
$$A_s^{(\ell)} := \{r \in \mathbb{Z}\backslash\{0\} \mid s/r \text{ is an } \ell\text{–step relation number}\}.$$

We also let $A_s := \bigcup_{\ell \geqslant 0} A_s^{(\ell)}$. *Throughout this section, we fix an integer $s > 1$.*

3.1. On 1–step relation numbers.

Lemma 3.1. *The following hold.*

1. *For positive integers ℓ and n, if $q \in R_{\mathbb{Q}}^{(\ell)}$, then $\pm q/n \in R_{\mathbb{Q}}^{(\ell)}$.*
2. *For all nonzero integers r, s, t, we have $(r + t)/(rst) \in R_{\mathbb{Q}}^{(1)}$.*
3. *For each $n \in \mathbb{Z}\backslash\{0\}$, we have that*

$$1/n,\ 2/n, 1 - 1/n \in R_{\mathbb{Q}}^{(1)}.$$

Proof. Part (1) is immediate from $b_q = (b_{q/n})^n$. For part (2), we let $q = (r+t)/(rst)$ and compute

$$(1, 0) \xrightarrow{r} \left(1, \tfrac{r+t}{st}\right) \xrightarrow{-s} \left(-\tfrac{r}{t}, \tfrac{r+t}{st}\right) \xrightarrow{t} \left(-\tfrac{r}{t}, 0\right).$$

Let us prove part (3). Combining Example 2.5 with part (1) we see that $1/n$ and $2/n$ are 1–step relation numbers. By substituting $(r, s, t) = (n, 1, -1)$, we see from part (2) that

$$1 - 1/n = -(r + t)/(rst)$$

is a 1–step relation number. □

3.2. On 2–step relation numbers.

The notation $x \mid y \pm z$ means x is a divisor of either $y + z$ or $y - z$. It will be convenient for us to use the notation

$$(x_1, x_2, \ldots, x_k\,; y) = \bigcup_{1 \leqslant i \leqslant k} (x_i + y\mathbb{Z}).$$

For instance, we have $(5\,; 12) = 5 + 12\mathbb{Z}$, and $(\pm 5\,; 12) = (5 + 12\mathbb{Z}) \cup (-5 + 12\mathbb{Z})$.

The followingl tool is crucial for this paper.

Lemma 3.2. *Suppose there exist nonzero integers w, m, y such that*

$$y \mid m, \quad \text{and} \quad w \mid smy \pm 1.$$

Then for all $r \in (w\,;sm)\backslash\{0, \pm 1, w\}$ we have $s/r \in R_{\mathbb{Q}}^{(2)}$.

In particular, it follows that $s/r \in (-4, 4)$ for such an r.

Proof of Lemma 3.2. We will assume that $w \mid smy - 1$, as the other case follows similarly. For some $u \neq 0$ we have

$$1 = wu + smy.$$

Let us write $r = w + smt$ for some $t \neq 0$, and put $v := m(y - ut)$. Then

$$1 = (w + smt)u + sm(y - ut) = ru + sv.$$

Since $|r| > 1$ and $u \neq 0$, we see that $v \neq 0$.

After setting $q := s/r$, we have an orbit of $\langle a, b_q\rangle$ as follows.

$$(1,0) \xrightarrow{\ ry\ } (1, sy) \xrightarrow{\ -v/y\ } (ru, sy) \xrightarrow{\ -t\ } (ru, s(y - ut))$$

$$\xrightarrow{\ m\ } (1, s(y - ut)) \xrightarrow{-r(y-ut)} (1,0).$$

From $rvt \neq 0$, it follows that $s/r \in R_s^{(2)}$. ☐

Definition 3.3. Let s, w, m be nonzero integers such that $s > 1$, and let

$$D := \gcd(w, sm), d := \gcd(w, s).$$

We say the set

$$(w\,; sm) \subseteq \mathbb{Z}$$

is an *s–good coset* if there is an integer y satisfying the following two conditions:

- $yD \mid md$;
- $w \mid smy \pm D$.

In this case, w is called a *good representative* of $(w\,; sm)$.

Example 3.4. (1) The coset $(0\,; s) = (s\,; s)$ is s–good. Indeed, if we set $w = s$ and $m = y = 1$, then

$$w \mid sm - \gcd(w, sm) = 0.$$

Moreover, $(0\,; sn) = n(0\,; s)$ is also s–good for $n \neq 0$.

(2) If w is a divisor of $s \pm 1$, then $(w\,; s)$ is s–good. In particular, $\pm(1\,; s)$ is s–good.

(3) More generally, if w, m, y satisfy the hypothesis of Lemma 3.2, then $(w\,; sm)$ is s–good. In this case, we have that $\gcd(w, sm) = \gcd(w, s) = 1$.

(4) Let $s = 25$. If we set $w = 9$ and $m = y = 2$, then we have

$$w = 9 \mid 99 = smy - \gcd(w, sm).$$

Hence, $(9\,;50)$ is 25–good.

Recall we have fixed $s > 1$ in this section. We see that all but at most four integers in an s–good coset belong to $A_s^{(2)}$, which generalizes Lemma 3.2.

Lemma 3.5. *If $(w\,;sm)$ is s–good with a good representative w, then we have that*

$$(w\,;sm)\backslash\{0, w, \pm\gcd(w, sm)\} \subseteq A_s^{(2)}.$$

Proof of Lemma 3.5. Let D and d be as in Definition 3.3. Set $w' = w/D, s' = s/d$ and $m' = md/D$. Suppose we have an integer t such that

$$r := w + smt \notin \{0, w, \pm D\}.$$

Put $r' := r/D = w' + s'm't$. By the s–good hypothesis, some $y \in \mathbb{Z}$ satisfies

$$y \mid m', \text{ and } w' \mid s'm'y \pm 1.$$

Moreover, $r' \notin \{0, \pm 1, w'\}$. Lemma 3.2 implies that $s'/r' \in R_{\mathbb{Q}}^{(2)}$. It follows that

$$\frac{s}{w + smt} = \frac{s'}{r'} \cdot \frac{1}{D/d} \in R_{\mathbb{Q}}^{(2)}. \qquad \square$$

Let us note one further consequence of Lemma 3.2

Lemma 3.6. *Suppose nonzero integers w, m, y satisfy that*

$$y \mid m, \quad \text{and} \quad w \mid smy \pm \gcd(w, s).$$

Then we have that $(w\,;sm)$ is s–good and that

$$(w\,;sm)\backslash\{0, w, \pm\gcd(w, s)\} \subseteq A_s^{(2)}.$$

Proof. As in Lemma 3.5, we let $D = \gcd(w, sm)$ and $d = \gcd(w, s)$. From $D \mid w$ and from the hypothesis, we have $D \mid d$. So, $D = d$ and $(w\,;sm)$ is s–good. $\square$

We note that $z(\{x_i\}\,;y) = \bigcup_i x_i z + yz\mathbb{Z}$. We also record the following.

Lemma 3.7. *If C is an s–good coset, then so is nC for all $n \in \mathbb{Z}\backslash\{0\}$.*

Proof. Let $C = (w\,;sm)$ with a good representative w. Then $nC = (nw\,;snm)$ is also s–good; this follows from $\gcd(nw, snm) = |n| \cdot \gcd(w, sm)$. $\square$

Proposition 3.8. *Suppose that for each $n \in \mathbb{N}$ we can find a collection of $f(n)$–many s–good cosets whose union contains $\{1, 2, \dots, n\}$. Then we have that*

$$\underline{d}\left(A_s^{(2)}\right) \geqslant 1 - 2\limsup_n f(n)/n.$$

Proof. By Lemma 3.5, all positive integers in each s–good coset are in $A_s^{(2)} \cap \mathbb{N}$, with at most two exceptions. Hence, we have that

$$\#(A_s^{(2)} \cap [1, n])/n \geqslant (n - 2f(n))/n. \qquad \square$$

Theorem 1.7 is an immediate consequence of this corollary.

Corollary 3.9. *For each finite set $Q \subseteq \mathbb{Z}$, there is a nonzero integer M such that*

$$Q + sM\,(\mathbb{Z}\backslash\{0\}) \subseteq A_s^{(2)}.$$

Proof. For each $a \in Q$, there exists some $m_a \in \mathbb{Z}\backslash\{0\}$ such that

$$sm_a \equiv \gcd(a, s) \pmod{a}.$$

By Lemma 3.6 we have that $(a\,;sm_a)$ is s–good and that

$$a + sm_a\,(\mathbb{Z}\backslash\{0\}) \subseteq A_s^{(2)} \cup \{0, \pm\gcd(a, s)\}.$$

So, for $M_0 = \mathrm{lcm}\{m_a \mid a \in Q\}$ we have that

$$Q + sM_0\,(\mathbb{Z}\backslash\{0\}) \subseteq A_s^{(2)} \cup \{0\} \cup \{d \in \mathbb{Z} \mid d \text{ divides } s\}.$$

By setting M to be a sufficiently large multiple of M_0, we obtain the desired conclusion. $\square$

Corollary 3.10. *For an integer w in $[-4, 4] \cup \{\pm 6\}$, the following hold.*

(1) The coset $(w; s)$ is s–good.

(2) If an integer t satisfies $s/(w + st) \in (-4, 4)$, then $s/(w + st) \in R_{\mathbb{Q}}$.

Proof. (1) By Example 3.4, we may only look at the case that $w \neq 0$. It suffices to show that w divides $s \pm \gcd(w, s)$. We may assume $w \nmid s$ and $w \nmid s \pm 1$, for otherwise the proof is trivial. Then it only remains to consider the case $|w| \geqslant 4$.

If $|w| = 4$, then our assumption implies that $s \equiv 2 \pmod 4$. Then we see that

$$s - \gcd(w, s) = s - 2 \equiv 0 \pmod{w}.$$

Suppose $|w| = 6$. Our assumption implies that $s \equiv \pm 2$ or $s \equiv 3$ modulo 6. Then $\gcd(w, s) = 2$ or $\gcd(w, s) = 3$, and we obtain the desired conclusion.

(2) We may assume $w \neq 0$. Then the above proof implies that w is a good representative of $(w\,; s)$. By Lemma 3.5, we have that either

$$s/(w + st) \in R_{\mathbb{Q}}^{(2)},$$

or

$$w + st \in \{w, \pm\gcd(w, s)\} \subseteq [-6, 6].$$

It is a simple computational verification that for all nonzero integer $u \in [-6, 6]$ and for all integer $s \in (-4|u|, 4|u|)$ the number s/u is a relation number; see Proposition A.2 in Appendix A. This completes the proof that $s/(w + st) \in R_{\mathbb{Q}}$. $\square$

Example 3.11. The above corollary implies that $s/(4+st)$ is a 2–step relation number for all $t \in \mathbb{Z}$ satisfying $4 + st \neq 0$ and $-4 < s/(4 + st) < 4$.

The following extends Lemma 3.1 (3).

Corollary 3.12. *For each nonzero integer n, we have the following:*

$$3/n,\ 1-2/n,\ 1-3/n,\ 1-4/n,\ 1-6/n,\ 2-1/n \in R_{\mathbb{Q}} \cup \mathbb{Z}.$$

Proof. Let $n \in \mathbb{Z}\backslash\{0\}$ be arbitrary. We may assume $|n| > 6$, for otherwise the proof is trivial from direct computations; see also Proposition A.2. Since 3 is a relation number, so is $3/n$.

In the case when $|w| \leqslant 4$ or $|w| = 6$, we see from Corollary 3.10 that $1 - w/n = (n - w)/(w + (n - w))$ is a relation number.

Let $w = 1 - n$ and $s = 2n - 1$. Since $w \mid s - 1$, Lemma 3.2 implies that

$$2 - 1/n = s/(w + s) \in R_{\mathbb{Q}}. \qquad \square$$

4. Fixed numerators

In this section, we establish the Main Conjecture for rational numbers with numerators less than 28 and that are not 24.

Theorem 4.1. *Let r, s be nonzero integers such that $|s| \leqslant 27$ and $|s| \neq 24$. If $q = s/r \in (-4, 4)$, then q is a relation number.*

We prove Theorem 4.1 for the rest of this section by establishing several claims. *We adopt the convention that variables are always integer–valued unless specified otherwise.*

Lemma 4.2. *For each integer $s \in [1, 11] \cup \{14, 15\}$, we have that*

$$\{w \in \mathbb{Z} \mid \gcd(w, s) = 1\} = \bigcup \{(w\,; s) \mid w \text{ divides } s \pm 1\}.$$

Proof. If $s = 7$ then we see that

$$\{w \in \mathbb{Z} \mid \gcd(w, 7) = 1\} = (\pm1, \pm2, \pm3\,; 7) = \bigcup \{(w\,; s) \mid w \text{ divides } 6\}.$$

For another example, if $s = 11$, then we have

$$(\pm1, \pm2, \pm3, \pm4, \pm5\,; 11) = \bigcup \{(w\,; 11) \in \mathbb{Z} \mid w \text{ divides } 10 \text{ or } 12\}.$$

The other values of s can be treated similarly, so we omit the details. $\square$

Lemma 4.3. *Suppose an integer s satisfies $2 \leqslant s \leqslant 27$ and $s \neq 24$.*

(1) Then there exists a finite collection of s–good cosets

$$\{(w_i\,; sm_i)\}$$

whose union contains all integers that are relatively prime to s; moreover, we can require that $m_i \mid 60$.

(2) In part (1), we can further require that

$$\bigcup_i \{w_i, \pm\gcd(w_i, sm_i)\} \subseteq A_s \cup [-s/4, s/4].$$

Sketch of the proof. This lemma is a consequence of Proposition B.1 (1) in Appendix. For illustration, we will give more hands-on explanation here and leave the computational details to Appendix.

Let us set

$$X_s := \{r \in \mathbb{Z} \mid \gcd(r, s) = 1 \text{ and } r \not\equiv w \pmod{s} \text{ for all divisor } w \text{ of } s \pm 1\}.$$

For part (1), it suffices to find a finite collection of s–good cosets whose union contains X_s; for, once such a collection is found then we can additionally include $(w\ ; s)$ for all divisor w of $s \pm 1$. By Lemma 4.2, we may assume $s > 11$ and $s \notin \{14, 15\}$.

In each case, we will find a list of pairs $((w\ ; sm), y)$ that satisfy the conditions of Definition 3.3; we may say y is the "certificate" for the s–goodness of $(w\ ; sm)$. We only illustrate the proof for $s = 12$ and $s = 21$.

Case $s = 12$: Note $X_s = (\pm 5\ ; 12) = (\pm 5, \pm 7\ ; 24)$. Then the following is the desired list of pairs $((w\ ; sm), y)$:

$$((\pm 5\ ; 24), 1), ((\pm 7\ ; 24), 2).$$

This notation is actually an abbreviation of the list

$$((5\ ; 24), 1), ((-5\ ; 24), 1), ((7\ ; 24), 2), ((-7\ ; 24), 2).$$

Case $s = 21$: We have $X_s = (\pm 8\ ; 21)$. We compute as follows.

$$\begin{aligned}
(\pm 8\ ; 21) &= (\pm 8, \pm 29, \pm 13\ ; 63), \\
(\pm 29\ ; 63) &= (\pm 29, \pm 34\ ; 126) = (\pm 29\ ; 126) \cup 2(\pm 17\ ; 63), \\
(\pm 13\ ; 63) &= (\pm 13, \pm 50\ ; 126) = (\pm 13\ ; 126) \cup 2(\pm 25\ ; 63), \\
X_s &= (\pm 8\ ; 63) \cup (\pm 13, \pm 29\ ; 126) \cup 2(\pm 17, \pm 25\ ; 63) \\
&\subseteq (\pm 8\ ; 63) \cup (\pm 13, \pm 29\ ; 126) \cup 2(\pm 4\ ; 21)
\end{aligned}$$

Since $(\pm 4\ ; 21)$ is s–good, so is $2(\pm 4\ ; 21)$; see Lemma 3.7. The following is the desired list of pairs:

$$(2(\pm 4\ ; s), 1), ((\pm 8\ ; 3s), 1), ((\pm 13\ ; 6s), 3), ((\pm 29\ ; 6s), 3).$$

See Proposition B.1 for other cases of s and for more details.

For part (2), recall that an s–good coset $(w\ ; sm)$ contains at most three nonzero integers

$$w,\ \gcd(w, sm),\ -\gcd(w, sm)$$

that are possibly not in $A_s^{(2)}$. We collect such possible exceptions and individually verify that each one belongs to A_s as long as $|s/r| < 4$. This is also done in the proof of Proposition B.1. □

Proof of Theorem 4.1. We may assume that $s > 0$. If $\gcd(r, s) = 1$, then Lemmas 3.5 and 4.3 imply that $r \in A_s$.

Let us now assume $d := \gcd(r, s) > 1$. Put $r' = r/d$ and

$$s' = s/d \leqslant s/2 \leqslant 27/2.$$

Since $\gcd(r', s') = 1$ and $s' \leqslant 13$, we see from the previous paragraph that $s/r = s'/r'$ is a relation number. □

5. The case $s = 24$

In this section, we will deduce Theorem 1.4 (2) by proving the following.

Theorem 5.1. *Let $s = 24$. Then there exists a sequence of pairs of integers*

$$\{(a_i, b_i)\}_{i\geqslant 0}$$

such that for each $i \geqslant 0$ and for $M_i = 1680 \cdot 3^i$, every integer x satisfies at least one of the following:

(A) We have $(x\,; sM_i) \subseteq (\pm a_i, \pm b_i\,; sM_i)$;
(B) We have $(x\,; sm)$ is an s–good coset for some m dividing M_i.

Proof of Theorem 1.4 (2) from Theorem 5.1. Let $s = 24$, and let $i \geqslant 0$. Recall from Lemma 3.5 that all but at most four integers in each s–good coset belong to $A_s^{(2)}$. Hence, Theorem 5.1 implies that

$$\overline{d}\left(\mathbb{Z}\backslash A_s^{(2)}\right) \leqslant \overline{d}\left((\pm a_i, \pm b_i\,; sM_i)\backslash A_s^{(2)}\right) \leqslant d(\pm a_i, \pm b_i\,; sM_i) \leqslant 4/(sM_i).$$

By sending $i \to \infty$, we see that $\mathbb{Z}\backslash A_s^{(2)}$ has density zero. □

In the remainder of this section, we prove Theorem 5.1. For this, let us consider integer sequences $\{z_i\}$ and $\{\delta_i\}$ determined by the following conditions.

- $z_0 = 1$;
- $z_i \equiv \delta_i \pmod 3$ and $\delta_i \in \{-1, 0, 1\}$ for each $i \geqslant 0$;
- $z_{i+1} = (z_i + 32\delta_i)/3$.

Lemma 5.2. *For each $i \geqslant 0$ and for each $\delta \in \{-1, 0, 1\}\backslash\{\delta_i\}$, we have that*

$$z_i + 32\delta \subseteq (\pm 1, \pm 5\,; 12).$$

Proof. By the nature of the given recursion, the sequences $\{z_i\}$ and $\{\delta_i\}$ must be periodic. So, one can verify the lemma by brute force. Actually, those sequences have period eight; see Table 1. □

i	δ_i	$z_i, z_i + 32, z_i - 32$	$z_i + 32\delta_i$	i	δ_i	$z_i, z_i + 32, z_i - 32$	$z_i + 32\delta_i$
0	1	1,33,-31	33	4	0	-15,17,-47	-15
1	-1	11,53,-21	-21	5	1	-5,27,-37	27
2	-1	-7,25,-39	-39	6	0	9,41,-23	9
3	-1	-13,19,-45	-45	7	0	3,35,-29	3

TABLE 1. Proof of Lemma 5.2

We can now define the desired sequences $\{a_i, b_i\}_{i\geqslant 0}$ as follows.

$$a_i = 1 + 1260 \cdot 3^i z_i,$$
$$b_i = 1 + 1260 \cdot 3^i z_{i+5}.$$

The key step of the proof is the following lemma.

Lemma 5.3. *For each $i \geqslant 0$, the following hold.*

(1) $a_{i+1} = a_i + \delta_i sM_i$ and $b_{i+1} = b_i + \delta_{i+5} sM_i$

(2) If

$$\delta \in \{-1, 0, 1\} \backslash \{\delta_i\}$$

then there exists a divisor m of M_{i+1} such that

$$(a_i + \delta sM_i \; ; sm)$$

is s–good.

(3) If

$$\delta \in \{-1, 0, 1\} \backslash \{\delta_{i+5}\}$$

then there exists a divisor m of M_{i+1} such that

$$(b_i + \delta sM_i \; ; sm)$$

is s–good.

Proof. (1) Note that

$$1260 = 35 \cdot 36, \quad 1680s = 35 \cdot 36 \cdot 32.$$

We see from Lemma 5.2 that

$$a_i + \delta_i sM_i - a_{i+1} = 1260 \cdot 3^i z_i + 1680s \cdot 3^i \delta_i - 1260 \cdot 3^{i+1} z_{i+1}$$
$$= 35 \cdot 36 \cdot 3^i (z_i + 32\delta_i - 3z_{i+1}) = 0.$$
$$b_i + \delta_{i+5} sM_i - b_{i+1} = 1260 \cdot 3^i z_{i+5} + 1680s \cdot 3^i \delta_{i+5} - 1260 \cdot 3^{i+1} z_{i+6} = 0.$$

(2) We saw in Lemma 5.2 that

$$z_i + 32\delta = 12p + c$$

for some $p \in \mathbb{Z}$ and $c \in \{\pm 1, \pm 5\}$. Put $m = 18c \cdot 3^i$, so that $m \mid M_{i+1}$. Then

$$(a_i + \delta s M_i - 1 + 2m)/(sm) = 3^i(1260z_i + 1680s\delta + 36c)/(3^i \cdot 36 \cdot 12c)$$
$$= (35(z_i + 32\delta) + c)/(12c) = (35 \cdot (12p + c) + c)/(12c) = (35/c)p + 3 \in \mathbb{Z}.$$

So, we have that

$$a_i + \delta s M_i \equiv 1 - 2m \pmod{sm}.$$

Note that

$$1 - 2m \mid 4m^2 - 1 = s \cdot m \cdot (m/6) - 1.$$

By setting $y = m/6$ in Definition 3.3 (or, Example 3.4 (3)), we see that

$$(a_i + \delta s M_i\,;sm) = (1 - 2m\,;sm)$$

is an s–good coset.

(3) The proof is essentially the same, after replacing (a_i, δ_i) by (b_i, δ_{i+5}). □

Proof of Theorem 5.1. We use induction. The base case $i = 0$ is a consequence of Proposition B.1 in Appendix, where a computer–assisted proof is given. Namely, we may set

$$a_0 = 1261, \quad b_0 = -6299.$$

Let us now assume the conclusion for some $i \geqslant 0$. This means that if $x \in \mathbb{Z}$ satisfies

$$(x\,;sM_i) \nsubseteq (\pm a_i, \pm b_i\,;sM_i),$$

then $(x\,;sm)$ is s–good for some $m \mid M_i$.

We note that

$$(a_i\,;sM_i) = (a_i - sM_i, a_i, a_i + sM_i\,;sM_{i+1}).$$

By Lemma 5.3, one of the above three cosets on the right-hand side coincides with

$$(a_i + \delta_i s M_i\,;sM_{i+1}) = (a_{i+1}\,;sM_{i+1}).$$

The same lemma implies that every integer contained in the other two cosets satisfies the alternative (B) of the conclusion.

By applying the same argument to the cosets

$$-(a_i\,;sM_i),\ (b_i\,;sM_i),\ -(a_i\,;sM_i)$$

we obtain the desired conclusion for $i + 1$. □

We end this section by extracting the strategy of Theorem 5.1 to obtain the following lemma. The proof is essentially identical to the one we have already given.

Lemma 5.4. *Let s, a, M_0, t be nonzero integers. Suppose there exist integers*

$$f, \ell, u, v_0, w, z_0, \delta_0$$

such that all of the following conditions hold.

- *$s = uf^2$ and $fM_0 = \ell v_0 w$;*
- *uf divides $\gcd(tw, \ell + 1)$;*
- *$a = 1 + f\ell u v_0 z_0$;*
- *for all $\delta \in \mathbb{Z}\backslash(\delta_0 \,; t)$, the set $(z_0 + \delta w \,; uf)$ contains a divisor of ℓ.*

Then the following hold.

(1) *For each $j \in \{1, \ldots, t-1\}$, there is a divisor $m = m(j)$ of $M_0 t$ such that*

$$(a + (\delta_0 + j)sM_0 \,; sm)$$

is s–good.

(2) *We have that*

$$\overline{d}\left((a \,; sM_0)\backslash A_s^{(2)}\right) = \overline{d}\left((a + \delta_0 sM_0 \,; sM_0 t)\backslash A_s^{(2)}\right).$$

(3) *Assume further that there exist integer sequences $\{z_i\}, \{\delta_i\}$ starting with z_0, δ_0 satisfying the following for each $i \geqslant 0$.*
   - *$z_i + w\delta_i = tz_{i+1}$;*
   - *for each $\delta \notin (\delta_i \,; t)$, the set $(z_i + w\delta \,; uf)$ contains a divisor of ℓ.*

   If $t > 1$, then we have that

$$d\left((a \,; sM_0)\backslash A_s^{(2)}\right) = 0.$$

Example 5.5. (1) The parameters that we have considered in this section are

$$s = 24, M_0 = 1680, t = 3, f = 2, u = 6, v_0 = 3, \ell = 35, w = 32.$$

(2) Lemma 5.4 is robust enough to be used for certain other choices of numerators. For instance, we may pick arbitrary $k, v_1 \in \mathbb{Z}$ and let

$$s = 144,\ u = 1,\ f = 12,\ v_0 = 3v_1,\ \ell = 5(12k - 5),\ w = 32,\ t = 3.$$

As in Lemma 5.2, we can use the same

$$\{z_i\}, \{\delta_i\}.$$

Setting

$$a = 1 + 180v_1(12k - 5),\ M_0 = 40v_1(12k - 5),$$

we can verify that all the conditions are satisfied. We conclude that

$$d\left((a \,; sM_0)\backslash A_s^{(2)}\right) = d\left((1 + 180v_1(12k - 5) \,; 5760v_1(12k - 5))\backslash A_{144}^{(2)}\right) = 0.$$

If we plug in $k = v_1 = 2$, then we see

$$d\left((a \,; sM_0)\backslash A_s^{(2)}\right) = d\left((6841 \,; 218880))\backslash A_{144}^{(2)}\right) = 0.$$

6. General density estimates

In this section we establish Theorem 1.5, which we do by an averaging argument. Let us fix $s \geqslant 28$. We will recursively construct an increasing sequence $\{m_n\}_{n\geqslant 0}$ such that the set

$$B_n := \{(w\,;sm_n) | (w\,;sm_n) \text{ is not contained in an } s\text{–good coset}\}$$

has a small density. Then, we apply Lemma 3.5 to see that

$$\underline{d}\left(A_s^{(2)}\right) \geqslant 1 - \#B_n/(sm_n).$$

For the base case $n = 0$, we set $m_0 = 1$. By Corollary 3.10, we see that

$$(w\,;s) \notin B_0$$

for $|w| \leqslant 4$ or $|w| = 6$. In particular,

$$\#B_0/(sm_0) \leqslant 1 - 11/s.$$

Suppose we have constructed $m_n \in \mathbb{N}$. For brevity, let us write

$$m := m_n,\ B_n = \{(w_1\,;sm), \dots, (w_\ell\,;sm)\},\ v_i := \gcd(w_i, sm).$$

We may choose w_i in the set $(-sm/2, sm/2]$ such that

$$w_i \notin \{0, \pm 1, \pm 2, \pm 3, \pm 4, \pm 6\}.$$

We define

$$Z := \{(i, x) \mid i \in [1, \ell] \text{ and } x \in [1, sm] \text{ such that } smx \equiv \pm v_i \pmod{w_i}\}.$$

Let $Y_i := Z \cap (\{i\} \times \mathbb{Z})$. We begin by establishing the following.

Claim 1. *The following hold.*

1. *For each $(i, x) \in Z$ the coset $(w_i\,;smx)$ is s–good.*
2. *If (i, x) and (j, x) are distinct elements of Z, then the cosets $(w_i\,;smx)$ and $(w_j\,;smx)$ are distinct as well.*
3. *For each $i \in [1, \ell]$, the cardinality of Y_i is at least four.*

Proof of Claim 1. (1) If $(i, x) \in Z$, then $\gcd(w_i, smx) = v_i$. It follows from definition that $(w_i\,;smx)$ is s–good.

(2) This is becase $w_i \not\equiv w_j \pmod{sm}$.

(3) Suppose first that $w_i \nmid 2v_i$. Then the modular arithmetic equation

$$smx \equiv v_i \pmod{w_i}$$

has a unique solution modulo w_i/v_i. Similarly, $smx \equiv -v_i$ has a unique solution as well. Since $v_i \not\equiv -v_i \pmod{w_i}$, we have that

$$\#Y_i \geqslant 2\left\lfloor \frac{sm}{|w_i/v_i|} \right\rfloor \geqslant 2\left\lfloor \frac{sm}{sm/2} \right\rfloor = 4.$$

If $w_i \mid 2v_i$, then $w_i/v_i = \pm 2$ or ± 1. So, we have

$$\#Y_i \geqslant \left\lfloor \frac{sm}{2} \right\rfloor \geqslant \frac{28}{2} > 4. \qquad \square$$

By applying Claim 1 and averaging x over $[1, \ell]$, we can find some $X \in [1, sm]$ such that the number of distinct s–good cosets in the set

$$\{(w_i\, ; smX)\}_{i \in [1,\ell]}$$

is at least

$$\#Z/sm \geqslant \sum_i \#Y_i/sm \geqslant 4\ell/sm.$$

To make the recursion deterministic, we pick the smallest such X.

We now define $x_n := X$ and $m_{n+1} = m_n x_n$. The set B_{n+1} is contained in the set

$$\{(w_i + smk\, ; smX) \mid i \in [1, \ell] \text{ and } k \in [0, X)\}.$$

In the set above, at least $4\ell/sm$ cosets are s–good. It follows that

$$\frac{\#B_{n+1}}{sm_{n+1}} \leqslant \frac{1}{smX}\left(\ell X - \frac{4\ell}{sm}\right) = \frac{\#B_n}{sm_n}\left(1 - \frac{4}{sm_{n+1}}\right)$$

Summing up, we have that

$$\bar{d}\left(\mathbb{Z}\backslash A_s^{(2)}\right) \leqslant \liminf_{n\to\infty} \frac{\#B_n}{sm_n} \leqslant \left(1 - \frac{11}{s}\right) \prod_{n=1}^{\infty} \left(1 - \frac{4}{sm_n}\right).$$

From the inequality $x_{n-1} \leqslant sm_{n-1}$, we have that

$$m_n = sm_{n-1}x_{n-1} \leqslant s^2 m_{n-1}^2 \leqslant \cdots \leqslant s^{2+4+\cdots+2^n} m_0^{2^n} = s^{2^n - 2}.$$

Hence, the theorem follows. $\square$

As remarked in the introduction, Theorem 1.5 does not quite show that $A_s^{(2)}$ has natural density 1, but the infinite product does give a significant improvement to the density estimate. As a particular example, we consider the case $s = 28$. We have that

$$\left(1 - \frac{11}{28}\right) = \frac{17}{28} \approx 0.6071428571.$$

The infinite product converges very quickly, and multiplying it out up to $n = 4$ yields

$$\left(1 - \frac{11}{28}\right)\left(1 - \frac{4}{28}\right)\left(1 - \frac{4}{28^3}\right)\left(1 - \frac{4}{28^7}\right)\left(1 - \frac{4}{28^{15}}\right) \approx 0.5203133366.$$

Similarly, for $s = 29$ we obtain the estimates 0.6206896552 and 0.5349895317, respectively. For $s = 30$, we obtain the estimates 0.6333333333 and 0.5488075719, respectively.

APPENDIX A. CERTIFYING s/r IS A RELATION NUMBER

In this appendix, we give a detailed description of the algorithms used in the paper and provide the full Mathematica code implementing such algorithms. We include relevant outputs of those code as well; the full output is available for download as an ancillary file (`relnum-v1.pdf`) with the arXiv version of this paper [14] and also on the authors' respective websites.

Let $x, y \in \mathbb{Z}\backslash\{0\}$. Setting $t = x - y\lfloor x/y \rfloor$, we define a *shifted remainder* of x by y as

$$\mathrm{SR}(x,y) := \begin{cases} t, & \text{if } t = x + y, \\ t, & \text{if } t \neq x \text{ and } |t| \leqslant |y|/2, \\ t - y, & \text{otherwise} \end{cases}$$

Note that $t \equiv x \pmod{y}$. We also let

$$\mathrm{sign}(x) := \begin{cases} 1, & \text{if } x \geqslant 0, \\ -1, & \text{otherwise.} \end{cases}$$

An algorithm to compute a function $\textsc{RelNum}(s, r, M)$ is given in Algorithm 1, and is inspired by [17, 22]. This algorithm begins with the moves

$$\begin{aligned}(1,0) = (r,0) &\overset{1}{\twoheadrightarrow} (r,s) \to (\mathrm{SR}(r,s),s) = (r\mathrm{SR}(r,s), rs) \\ &\overset{-1}{\twoheadrightarrow} (r\mathrm{SR}(r,s), s(r - \mathrm{SR}(r,s)) =: (x_0, sy_0).\end{aligned}$$

Then, we define

$$\begin{aligned}&(x_i, sy_i) \to (\mathrm{SR}(x_i, sy_i), sy_i) = (x', sy_i) = (rx', rsy_i) \twoheadrightarrow (rx', s \cdot \mathrm{SR}(ry_i, x')) \\ &= (x'', sy') = (x''\sigma/d, sy'\sigma/d) = (x_{i+1}, y_{i+1}).\end{aligned}$$

The function $\textsc{RelNum}(s, r, M)$ returns `True` if the orbits $\{(x_i, y_i)\}$ becomes periodic (up to changing the sign of y_i), or if $x_i y_i (x_i - 1) = 0$ for some $i \leqslant M$.

In this case, we see that s/r is a relation number; see Proposition 2.6. Otherwise, the algorithm returns `False`, and is inconclusive.

Let us now consider a (typically slower) variation of Algorithm 1. For nonzero integers a, b, c satisfying $a, c > 0$ and $a \nmid b$, we write

$$(u, v) = \textsc{Min}_3(a, b, c),$$

where u and v are nonzero integers minimizing the value

$$|(au + b)v + c|.$$

We consider an arbitrary choice if such a pair (u, v) is not unique. Then Algorithm 2 attempts to find an orbit coming from the moves

$$(x, sy) = (rx, rsy) \twoheadrightarrow (rx, s(ry + ux)) \to (rx + s(ry + ux)v, s(ry + ux)) = (x', sy'),$$

Algorithm 1 Certifying $q = s/r \in R_{\mathbb{Q}}$ by shifted remainders

function RelNum(s, r, M)
  if $|s/r| \geqslant 4$ or $\gcd(s,r) \neq 1$ or $r \in \mathbb{Z}$ **then**
    Print("known cases") and **return** `Null`
  $i \leftarrow 0, \quad x_0 \leftarrow r, \quad y_0 \leftarrow (r - \mathrm{SR}(r,s))/s,$ flag $\leftarrow$ `False`
  if $y_0 = 0$ **then** flag$\leftarrow$ `True`
  while $i < M$ and flag=`False` **do**
    $x \leftarrow x_i$ and $y \leftarrow y_i$
    $x' \leftarrow \mathrm{SR}(x, sy)$
    $y' \leftarrow \mathrm{SR}(ry, x')$ and $x'' \leftarrow rx'$
    $d \leftarrow \gcd(x'', y')$ and $\sigma = \mathrm{sign}(x'')$
    if d$\neq 0$ **then**
      $x \leftarrow x''\sigma/d$ and $y \leftarrow y'\sigma/d$
    else
      $x \leftarrow x''\sigma$ and $y \leftarrow y'\sigma$
    if $xy(x-1) = 0$ or $(x,y) = (x_j, \pm y_j)$ for $\exists j < i$ **then**
      flag$\leftarrow$`True`
    $i \leftarrow i + 1$
    $x_i \leftarrow x$ and $y_i \leftarrow y$
  return flag

while minimizing the value of $|x'|$ in each step.

The following conjecture would imply the Main Conjecture.

Conjecture A.1. *For all $s, r \in \mathbb{N}$ satisfying $s/r < 4$, there exists $M > 0$ such that* RelNum$(s, r, M) =$ `True` *or* RelNumMin$(s, r, M) =$ `True`*.*

We will list the Mathematica code (Version 11.3) implementing algorithms of this appendix in Section C. Using this code, we prove the following.

Proposition A.2. *Let s and r be positive integers such that $s/r < 4$.*

(1) If $r \leqslant 8$, then s/r is a relation number.
(2) If $s \leqslant 30$ and $s/r \geqslant 1/10$, then s/r is a relation number.

Proof. By induction, it suffices to consider the case when $\gcd(s, r) = 1$.

For part (1), we use the Mathematica code (functions) given in Section C, along with the following code.

```
excp={};
For[r = 2, r <= 10, r++, For[s = 2, s <= 4 r - 1, s++,
 If[!RelNum[s, r, 5000], excp=Append[excp, {s, r}]];]];
Print["Unresolved cases are :", excp, ": END"];
```

Algorithm 2 Certifying $q = s/r \in R_{\mathbb{Q}}$ by minimizing coordinates

function RelNumMin(s, r, M)
  if $|s/r| \geqslant 4$ or $\gcd(s, r) \neq 1$ or $r \in \mathbb{Z}$ **then**
    Print("known cases") and **return** `Null`
  $i \leftarrow 0$, $x \leftarrow \mathrm{SR}(r, s)$, $y \leftarrow (r - \mathrm{SR}(r, s))/s$, flag $\leftarrow$ `False`
  if $y_0 = 0$ **then** flag$\leftarrow$ `True`
  $x_0 \leftarrow \mathrm{sign}(x)x$ and $y_0 \leftarrow \mathrm{sign}(x)y$
  while $i < M$ and flag=`False` **do**
    $x \leftarrow x_i$ and $y \leftarrow y_i$
    $(u, v) \leftarrow \mathrm{Min}_3(sx, sry, rx)$
    $x' \leftarrow rx + s(ry + ux)v$ and $y' \leftarrow ry + ux$
    $d \leftarrow \gcd(x', y')$ and $\sigma = \mathrm{sign}(x')$
    if d$\neq 0$ **then**
      $x \leftarrow x'\sigma/d$ and $y \leftarrow y'\sigma/d$
    else
      $x \leftarrow x'\sigma$ and $y \leftarrow y'\sigma$
    if $xy(x - 1) = 0$ or $(x, y) = (x_j, \pm y_j)$ for $\exists j < i$ **then**
      flag$\leftarrow$`True`
    $i \leftarrow i + 1$
    $x_i \leftarrow x$ and $y_i \leftarrow y$
  return flag

The final output of the above code is as follows.

```
Unresolved cases are :{{35,9},{39,10}}: END
```

This verifies part (1). We remark that our algorithm does not determine whether or not the following are relation numbers in 5000 steps:

$$35/9,\ 39/10.$$

For part (2), we use:

```
excp={};
For[s = 2, s <= 30, s++, For[r = 2, r <= 10 s, r++,
 If[GCD[s, r] == 1 && !RelNum[s, r, 5000],
  excp=Append[excp, {s, r}]];]];
Print["Unresolved cases are :", excp, ": END"];
```

The final output is:

```
Unresolved cases are :{{28,17},{29,17}}: END
```

The output says that the algorithm is inconclusive for the numbers

$$28/17, 29/17,$$

for which we apply Algorithm 2. With the input

```
RelNumMin[28, 17, 10];
RelNumMin[29, 17, 10];
```

we have the output

```
28/17 is a relation number with a list {{11,-28},{19,-168},
{13,-336},{3,-112},{5,-28},{1,84}}
29/17 is a relation number with a list {{12,-29},{1,203}}
```

So, we are done. □

Appendix B. Certifying $\mathbb{Z}$ is a finite union of s–good cosets

Proposition B.1. *Let s be a positive integer in $[2, 27]$.*

(1) If $s \neq 24$, then there exists a finite collection of s–good cosets

$$\{(w_i\,;sm_i)\}_{1\leqslant i\leqslant k}$$

whose union is $\mathbb{Z}$, such that

$$(**)\qquad \bigcup_{1\leqslant i\leqslant k}\{w_i, \pm\gcd(w_i, sm_i)\} \subseteq A_s \cup [-s/4, s/4].$$

Moreover, we can require that $m_i \mid 60$.

(2) If $s = 24$, then every integer x satisfies at least one of the following.

(A) we have that $(x\,;1680s) \subseteq (\pm1261, \pm6299\,;1680s)$;

(B) we have that $(x\,;sm)$ is an s–good coset for some m dividing 1680.

Proof. (1) By induction, it suffices to find a finite collection $\mathscr{F}_s = \{(w_i\,;sm_i)\}_i$ of s–good cosets containing

$$Y_s = \{x \in \mathbb{N} \mid \gcd(x, s) = 1\}$$

such that (**) holds.

If $s \leqslant 11$, then we simply choose the collection

$$\mathscr{F}_s = \{(x\,;s) \mid \gcd(x, s) = 1 \text{ and } 1 \leqslant x < s\}.$$

From Lemma 4.2, each coset in the above collection is s–good. Moreover, whenever $1 \leqslant x < s$ we have that $x \in A_s$ by Proposition A.2. This completes the proof for $s \leqslant 11$.

Let $s \geqslant 12$. Let us list a specific sequence $t_{12}, t_{13}, \ldots$ as follows.

$$t_{12} = 2, 2, 2, 2, 2, 3, 6, 2, 4, 6, 12, 12, 1680, 6, 60, t_{27} = 60.$$

In particular, $t_{24} = 1680$.

Claim 1. *Let $s \in [12, 27]$ and $s \neq 24$. Then for each $w \in [1, st_s)$ satisfying $\gcd(w, s) = 1$, there exist integers w', m, y such that the following hold:*

(i) $y \mid m$ and $m \mid t_s$;

(ii) $w' \equiv \pm w \pmod{sm}$*;*
(iii) $smy \equiv \pm \gcd(w', sm) \pmod{w'}$*;*
(iv) $w', \gcd(w', sm) \in A_s \cup [-s/4, s/4]$.

This claim obviously implies part (1). We prove the claim by brute force, using the function VERIFYLIST in Section C and the following Mathematica code:

```
listgood = {};
excp = {}; excp2 = {}; T = {2, 2, 2, 2, 2, 3, 6, 2, 4, 6, 12, 12,
  1680, 6, 60, 60};
For[s = 12, s <= 27, s++,
  l0 = VerifyList[s, T[[s - 11]]]; l = l0[[2]]; flag = l0[[1]];
  If[flag, listgood = Append[listgood, s];
   Print[s, "/r is a relation number for almost all r;"];
   Print["this is certified by the list of s-good cosets ", l];
   excp = Union[excp, l0[[3]]];];];
Print["The list of s such that s/r is a relation number
  for almost all r:"];
Print[listgood];
Print["Pairs of (s,r) that require individual verifications:", excp];
For[i = 1, i <= Length[excp], i++, s = excp[[i, 1]];
  r = excp[[i, 2]];
  If[! RelNum[s, Abs[r], 5000],
   Print["No answer found for s/r = ", s/r];
   excp2 = Append[excp2, {s, r}]]];
If[excp2 == {}, Print["Individual verification is complete."]];
```

Among the output of the above code is the following line

```
The list of s such that s/r is a relation number
for almost all r:
{12,13,14,15,16,17,18,19,20,21,22,23,25,26,27}
```

This verifies parts (i) through (iii) of the claim for each s in the above list.

Recall that if r is an element of an s–good coset $(w\,;sm)$, then either $r \in A_s^{(2)}$ or r coincides with one of the following four exceptions:

$$0, w, \pm \gcd(w, sm).$$

The above Mathematica code collects all such possible exceptions and individually verify that each integer is in $A_s \cup [-s/4, s/4]$. So, part (iv) of the claim follows from the final output below:

```
Individual verification is complete.
```

(2) The outputs of the above code includes:

```
For s = 24, the following remainders are not eliminated:
{1261,6299,34021,39059} modulo 1680 * s
```

This implies part (2) as well. ◻

Appendix C. Mathematica (Version 11) code

In this section, we includes Mathematica code for the following functions

$\mathrm{SR}(x,y)$, $\textsc{RelNum}(x,y)$, $\textsc{Min}_3(x,y)$, $\textsc{RelNumMin}(x,y)$, $\textsc{VerifyList}(x,y)$,

which were introduced in this Appendix.

```
SR[x_Integer, y_Integer] := Module[{t}, t = x - y Floor[x/y];
   Return[
    If[t == x + y || (t != x && Abs[t] <= Abs[y]/2), t, t - y]];];

RelNum[s_Integer, r_Integer, M_Integer] :=

  Module[{flag, i, d, sg, S, x, y, Stemp},
   If[s/r >= 4 || IntegerQ[s/r] || GCD[r, s] != 1,
    Print["known cases"]; Return[]];
   x = r; y = (r - SR[r, s])/s; S = {{x, s y}}; i = 1; flag = False;
   While[i < M && ! flag, x = S[[i, 1]]; y = S[[i, 2]]/s;
    x = SR[x, s y];
    y = SR[r y, x]; x = r x;
    d = GCD[x, y]; sg = If[x >= 0, 1, -1];
    If[d != 0, x = x sg/d; y = y sg/d, x = x sg; y = y sg];
    Stemp = S;
    S = Append[S, {x, s y}];
    If[x y (Abs[x] - 1) == 0 || MemberQ[Stemp, {x, s y}]
      || MemberQ[Stemp, {x, -s y}],
     Print[s/r, " is a relation number with a list ", S];
     flag = True]; i++;];
   If[! flag,
    Print["No answers up to ", M, " iterations for ", s/r]];
   Return[flag];];

Min3[a_Integer, b_Integer, c_Integer] :=

  Module[{ybound, y, t, x, xr, yr, min, minTemp},
   If[a b c == 0 || a < 0 || c < 0, Return[False]];
   If[Mod[b, a] == 0, Return[{-b/a, 1, c}]];
   ybound = Min[a - 2, c + Abs[c - Abs[a - Abs[b]]]];
   xr = 1; yr = 1; min = Abs[a + b + c];
   For[y = -ybound, y <= ybound, y++, If[y == 0, Continue[]];
    t = -(c/y + b)/a; x = Floor[t];
    If[x == 0 || (x != -1 && t - x > 1/2), x += 1];
    minTemp = Abs[(a x + b) y + c];
```

```
    If[minTemp < min, xr = x; yr = y; min = minTemp];];
   Return[{xr, yr, (a xr + b) yr + c}];];

RelNumMin[s_Integer, r_Integer, M_Integer] :=

  Module[{flag, i, d, sg, S, x, y, temp, u, v, xp, yp, Stemp},
   If[s/r >= 4 || IntegerQ[s/r] || GCD[r, s] != 1, Return[]];
   x = SR[r, s]; y = (r - SR[r, s])/s; sg = If[x >= 0, 1, -1];
   x = sg x; y = sg y; S = {{x, s y}}; i = 1; flag = False;
   If[y == 0, flag = True];
   While[i < M && ! flag, x = S[[i, 1]]; y = S[[i, 2]]/s;
    temp = Min3[s x, s r y, r x];
    u = temp[[1]]; v = temp[[2]]; xp = temp[[3]];
    yp = r y + u x;
    d = GCD[xp, yp]; sg = If[xp >= 0, 1, -1];
    If[d != 0, x = xp sg/d; y = yp sg/d, x = xp sg; y = yp sg];
    Stemp = S; S = Append[S, {x, s y}];
    If[x y (Abs[x] - 1) == 0 || MemberQ[Stemp, {x, s y}]
      || MemberQ[Stemp, {x, -s y}],
     Print[s/r, " is a relation number with a list ", S];
     flag = True]; i++;];
   If[! flag,
    Print["No answers up to ", M, " iterations for ", s/r]];
   Return[flag];];

VerifyList[s_Integer, M_Integer] :=

  Module[{mList, mList2, lt, i, j, j2, lp, ltmp, w, flag, m, wp, d,
    DD, y, result, exc},
   exc = {}; result = {}; lp = {}; mList = Divisors[M];
   For[i = 2, i <= s - 2, i++,
    If[GCD[s, i] != 1, Continue[]];
    If[Mod[s + 1, i] == 0 || Mod[s - 1, i] == 0 ||
      Mod[s + 1, s - i] == 0 || Mod[s - 1, s - i] == 0, Continue[]];
    lp = Append[lp, i];];
   lt = lp; ltmp = {};
   For[i = 1, i < M, i++, lt = Union[lt, lp + s i];];
   For[i = 1, i <= Length[lt], i++,
    w = lt[[i]]; flag = False;
    If[Mod[w, s] == 0, flag = True;
     result = Append[result, {w, 1, 1}]; Continue[]];
    For[j = 1, j <= Length[mList] && ! flag, j++,
     m = mList[[j]];
```

```
    wp = Mod[w, s m]; d = GCD[s, wp]; DD = GCD[s m, wp];
    mList2 = Divisors[m d / DD];
    For[j2 = 1, j2 <= Length[mList2] && ! flag, j2++,
     y = mList2[[j2]];
     If[Mod[s m y + DD, wp] == 0 || Mod[s m y - DD, wp] == 0 ||
       Mod[s m y + DD, s m - wp] == 0 ||
       Mod[s m y - DD, s m - wp] == 0, flag = True;
      result = Append[result, {w, m, y}];
      exc = Union[
        exc, {{s, wp}, {s, s m - wp}, {s, DD}, {s, -DD}}]]]];
   If[! flag, ltmp = Append[ltmp, i]];];
  lt = Mod[lt[[ltmp]], s M];
  If[Length[lt] == 0,
   Return[{True, result, exc}];];
  Print["For s = ", s,
   ", the following remainders are not eliminated: ", lt,
   " modulo ", M, " * s "];
  Return[{False, lt}];];
```


Acknowledgements

The authors thank V. Shpilrain for pointing out the Main Conjecture to them. The authors also thank T. Tsuboi for suggesting a connection to generalized continued fractions. The first author is supported by Samsung Science and Technology Foundation (SSTF-BA3301-06). The second author is partially supported by an Alfred P. Sloan Foundation Research Fellowship and NSF Grant DMS-1711488.

References

[1] Hirotaka Akiyoshi, Makoto Sakuma, Masaaki Wada, and Yasushi Yamashita, *Punctured torus groups and 2-bridge knot groups. I*, Lecture Notes in Mathematics, vol. 1909, Springer, Berlin, 2007. MR2330319

[2] John Bamberg, *Non-free points for groups generated by a pair of* 2×2 *matrices*, J. London Math. Soc. (2) **62** (2000), no. 3, 795–801. MR1794285

[3] A. F. Beardon, *Pell's equation and two generator free Möbius groups*, Bull. London Math. Soc. **25** (1993), no. 6, 527–532. MR1245077

[4] J. L. Brenner, R. A. MacLeod, and D. D. Olesky, *Non-free groups generated by two* 2×2 *matrices*, Canad. J. Math. **27** (1975), 237–245. MR0372042

[5] Joël Lee Brenner, *Quelques groupes libres de matrices*, C. R. Acad. Sci. Paris **241** (1955), 1689–1691. MR0075952

[6] Bomshik Chang, S. A. Jennings, and Rimhak Ree, *On certain pairs of matrices which generate free groups*, Canad. J. Math. **10** (1958), 279–284. MR0094388

[7] Anastasiia Chorna, Katherine Geller, and Vladimir 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. MR3621679

[8] S. Peter Farbman, *Non-free two-generator subgroups of* $\mathrm{SL}_2(\mathbf{Q})$, Publ. Mat. **39** (1995), no. 2, 379–391. MR1370894

[9] Jane Gilman, *The structure of two-parabolic space: parabolic dust and iteration*, Geom. Dedicata **131** (2008), 27–48. MR2369190

[10] Yu. A. Ignatov, *Rational nonfree points of the complex plane*, Algorithmic problems in the theory of groups and semigroups (Russian), Tul′sk. Gos. Ped. Inst., Tula, 1986, pp. 72–80, 127. MR932273

[11] ———, *Rational nonfree points of the complex plane. II*, Algorithmic problems in the theory of groups and semigroups (Russian), Tul′sk. Gos. Ped. Inst., Tula, 1990, pp. 53–59. MR1240515

[12] E. I. Khukhro and V. D. Mazurov (eds.), *The Kourovka Notebook*, 19th ed., Russian Academy of Sciences, Siberian Branch, Sobolev Institute of Mathematics, Novosibirsk, 2018.

[13] Linda Keen and Caroline Series, *The Riley slice of Schottky space*, Proc. London Math. Soc. (3) **69** (1994), no. 1, 72–90. MR1272421

[14] S. Kim and T. Koberda, Ancillary file with the arXiv paper 1901.06375, https://arxiv.org/abs/1901.06375

[15] S. Kim, T. Koberda, and M. Mj, *Flexibility of group actions on the circle*, Springer Lecture Notes in Mathematics, Volume 2231, to appear.

[16] A. W. Knapp, *Doubly generated Fuchsian groups*, Michigan Math. J. **15** (1969), 289–304. MR0248231

[17] R. C. Lyndon and J. L. Ullman, *Groups generated by two parabolic linear fractional transformations*, Canad. J. Math. **21** (1969), 1388–1403. MR0258975

[18] Rimhak Ree, *On certain pairs of matrices which do not generate a free group*, Canad. Math. Bull. **4** (1961), 49–52. MR0142612

[19] Dan Romik, *The dynamics of Pythagorean triples*, Trans. Amer. Math. Soc. **360** (2008), no. 11, 6045–6064. MR2425702

[20] I. N. Sanov, *A property of a representation of a free group*, Doklady Akad. Nauk SSSR (N. S.) **57** (1947), 657–659. MR0022557

[21] Piotr Słanina, *On some Möbius transformations generating free semigroup*, Monograph on the occasion of 100th birthday anniversary of Zygmunt Zahorski, Wydaw. Politech. Śl., Gliwice, 2015, pp. 313–323. MR3330412

[22] Eng-Chye Tan and Ser-Peow Tan, *Quadratic Diophantine equations and two generator Möbius groups*, J. Austral. Math. Soc. Ser. A **61** (1996), no. 3, 360–368. MR1420342

School of Mathematics, Korea Institute for Advanced Study (KIAS), Seoul, 02455, Korea
E-mail address: `skim.math@gmail.com`
URL: `http://cayley.kr`

Department of Mathematics, University of Virginia, Charlottesville, VA 22904-4137, USA
E-mail address: `thomas.koberda@gmail.com`
URL: `http://faculty.virginia.edu/Koberda`