The freeness problem in matrix groups and related topics

Georgi Kocharyan

December 22, 2021

Abstract

This report was written at the end of a summer research placement from 26.06.2021-25.08.2021 supervised by Emmanuel Breuillard at the Department of Pure Mathematics and Mathematical Statistics at the University of Cambridge. We summarise known results about natural algorithmic decision problems arising in group theory with a focus on linear groups, and further we are able to prove a few new results about some of them as well as ask new questions.

1 Introduction

The general motive of this article is to discuss known undecidability results about problems concerning semigroups, and to think about how to generalise them to groups. It turns out that this problem, even though it is intuitively similar to the semigroup one, is mostly much, much harder and when a solution is known, it is won through a vastly different approach. We will consider mainly the word problem and the freeness problem as well as other minor problems such as the orbit, conjugacy, order or membership problem and others. We hope to cleanly summarise known results, to provide a few new perspectives on some of them as well as present some new ideas.

2 Notation and definitions

We use the letters Σ and Δ to denote alphabets. The *Kleene star* Σ^* refers to all words we can write using the letters in Σ, including the empty word ϵ. We interpret this as being the free monoid generated by the letters in Σ. For the semigroup (i.e. without the identity) we write Σ^+.If we want to discuss the *group* alphabet using the letters in Σ and there inverses, we denote this as $\langle\Sigma\rangle$, which can be seen as shorthand for $(\Sigma \cup \Sigma^{-1} \cup \{\epsilon\})^*$ or similarly as before, the free group generated by the letters in Σ. In general if we want to speak about a free group of rank n we use the notation F_n.
$\langle\Sigma\rangle$ only contains *freely reduced* words, which means that there is no occurrence of a letter followed by its inverse. A similar notion to this is that of a *cyclically reduced* word, which means that cyclic permutations do not shorten the word, or equivalently that we cannot conjugate the word to a shorter one.
The length of a word w in any semigroup or group is denoted $|w|$.

3 Undecidability and basic undecidable problems

We pick Turing machines as the model for computation that will be used in the rest of the article. We use the standard notions of Turing machine and undecidability laid out for example in Chapter 12 of [33]. We take it as a given that there exists an enumeration of all Turing machines T_i.

Definition 3.1. A subset $S \subseteq \mathbb{N}$ is called *recursively enumerable* (r.e.) or *listable* if there exists a Turing machine which will print out only numbers of S and $\forall s \in S$, it will eventually print out s.

Definition 3.2. A subset $S \subseteq \mathbb{N}$ is called *computable* or *recursive* if there exists a Turing machine which, given an $n \in N$ will correctly determine whether or not $n \in S$.

Theorem 3.3. $S \subseteq \mathbb{N}$ is computable if and only if S and $\mathbb{N}\backslash S$ are recursive.

Proof. The implication is clear. For the converse, consider a $n \in N$. Run the listing algorithms for S and $N\backslash S$ in parallel. Since either $n \in S$ or $n \notin S$, one will halt in finite time, giving a correct answer. □

The *halting problem*, i.e., is it possible to find a Turing machine which will correctly predict if a given Turing machine on a given input will halt, was the first problem to be shown to be undecidable by Turing in 1938[36]. We sketch a proof given in [33].

Theorem 3.4. The halting problem is undecidable.

Proof. By contradiction. If it were decidable, then $S = \{n \in N |\ T_n \text{ halts on input } n\}$ is computable. By Theorem 3.3, $S' = \mathbb{N} \backslash S$ would be listable. Take a Turing machine T' listing this set, i.e. one which will halt if it gets an input in S' and not if not. Since $T' = T_m$ for some $m \in \mathbb{N}$, we have that if T' halts on m, then $m \notin S$, so it doesn't, but if it doesn't halt on m, then $m \in S$ and T' would have had to halt on m, a contradiction. □

Obviously, the halting problem is not a very natural setting for most combinatorial and algebraic decision problems. A helpful other undecidable problem is the so called *word problem* for an algebraic structure.

Definition 3.5. A solution to the *word problem* for a semigroup $S = \langle s_1, \ldots, s_n |\ u_1 = v_1, \ldots, u_m = v_m \rangle$ is an algorithm that, given any two words w_1, w_2 in the generators, will correctly determine if they are equivalent in S or not.

Turing was also able to show the following in [37].

Theorem 3.6. There exists a finitely presented semigroup with unsolvable word problem.

A more modern and accessible proof can be found in Theorem 12.5 of [33]. Obviously, we can ask the same question for *groups*. This turns out to be much more difficult, but still true.

Definition 3.7. A solution to the *word problem* for a group $G = \langle g_1, \ldots, g_n |\ r_1, \ldots, r_m \rangle$ is an algorithm that, given any w in the generators, will correctly determine if $w = e_S$ in S or not.

Theorem 3.8 (Novikov-Boone Theorem)**.** There exists a finitely presented group with unsolvable word problem.[33]

Remark 3.9. The reason why we require the (semi)group to be finitely presented is that it turns out to be quite easy to construct an infinitely presented group with unsolvable word problem. If K is any non-recursive subset of the naturals, then

$$G = \langle a, b | b^{-k} a b^k, k \in K \rangle$$

has unsolvable word problem.

In fact, in light of the following theorem the Novikov-Boone Theorem becomes an easy corollary by embedding G in the given group:

Theorem 3.10 (Higman's embedding theorem)**.** Any finitely generated and recursively presented group embeds in a finitely presented group.

We will use the unsolvability of the semigroup word problem to prove the undecidability of the *Post correspondence problem* (PCP), which is the undecidable problem we will reduce most results in this report to. For now we will only consider the PCP over a free *semigroup*.
We can picture an instance of the PCP as a finite set of dominoes, with each of them having (different) words in a finite alphabet Δ written on the top and the bottom. Provided an infinite supply of these dominoes, the PCP asks for an algorithm which will determine if there exists a string of dominoes which, laid out next to each other, spell out the same word on the top and the bottom. More formally:

Definition 3.11 (Post correspondence problem)**.** Let Σ and Δ be two finite alphabets. A solution to the PCP is an algorithm, that given two morphisms $h, g : \Sigma \to \Delta$ decides whether or not there exists a $w \in \Sigma^*$ with $h(w) = g(w)$.

Remark 3.12. PCP over a free semigroup means that the letters do not cancel and we do not allow inverses. If we mention the PCP without mentioning any algebraic structure, we mean the PCP over a free semigroup. We will discuss variants in more detail later.

In general we can prove the undecidability of a problem by reducing it to a known undecidable problem, i.e. we show that if the problem were decidable, we could use the algorithm to construct an algorithm solving an undecidable problem.

Theorem 3.13. The PCP is undecidable.

The original proof is given by Post in [30]. Another proof is in [34]. The proof recounted here is the simplest we could find, in [24]

Proof. Assume an algorithm for PCP exists, and we want to decide if $x = y$ in $S = \langle x_1, \dots, x_n | u_1 = v_1, \dots, u_m = v_m \rangle$. We use the notation given in the definition of the PCP.
Pick $\Delta = \{x_1, \dots, x_n, x'_1, \dots, x'_n, I\}$ with $2n+1$ letters, and have $\Sigma = \{a_1, \dots, a_n, b_1, \dots, b_n, c_1, \dots c_m, s, e\}$ have $2 + 2n + m$ letters.
Now define the morphisms h and g as follows:

$$\begin{array}{rl} h : \Sigma^* \to \Delta^* & g : \Sigma^* \to \Delta^* \\ a_i \mapsto x_i & a_i \mapsto x'_i \\ b_i \mapsto x'_i & b_i \mapsto x_i \\ c_i \mapsto v'_i & c_i \mapsto u_i \\ s \mapsto Ix & s \mapsto I \\ e \mapsto I & e \mapsto yI \end{array}$$

We imagine s and e as the starting and ending letters - we see that any word with $h(w) = g(w)$ must start with s. But $h(s)$ is longer than $g(s)$, so we must fill up the word with letters of the form a_i, b_i, c_i to get a word spelt out in the image of g that is equal to x in S, where we might have used relations via the c_i. But then we have a copy of this word, primed, in the image of h. If the PCP has a solution, continuing like this, since we have to end with the letter e, gives a series of reductions from x to y and vice versa. □

Note

The 'vice versa' at the end of the proof is crucial. If this were not true, it could be that our algorithm for the PCP outputs 'no', but there still exists a solution to the semigroup word problem.

Remark 3.14. An easy restriction to the PCP is to ask about the number of letters we allow in Σ and Δ. The meaning of this in the domino interpretation is that $n = |\Sigma|$ is the amount of dominoes while $m = |\Delta|$ is the amount of letters we can use when writing on them. We will soon see that it is easy to fix $m = 2$ without changing the argument (obviously the problem becomes decidable for $m = 1$.)
As for n, it has been shown that the PCP remains undecidable for $n \geq 5$ [27] but becomes decidable for $n \leq 2$ [11]. The values in between remain open problems.

Definition 3.15. The *generalised PCP* (GPCP) is the question whether or not, given in addition to (h, g) 4 words a_1, b_1, a_2, b_2 whether or not there exists $w \in \Sigma^+$ with $a_1 h(w) b_1 = a_2 g(w) b_2$.

Obviously the GPCP remains undecidable as it reduces to the PCP by setting $a_1 = b_1 = a_2 = b_2 = 1$.

4 Freeness problems

This is one of the main decision problems we will consider in the report. A very good reference is [8], which we will be quoting frequently.

Definition 4.1. A solution to the *freeness problem* on a (semi)group G is an algorithm, that, given a set of k elements $S \subseteq G$ correctly decides whether or not they generate a free (semi)group of rank k.

4.1 Basic freeness problems on free structures

We are especially interested in the freeness problem on matrix (semi)groups. Before we think about these, we will summarise a few known important results. We will see that it is possible to embed direct products of free semigroups and groups into certain matrix groups, which obviously preserves the solvability of many decision problems - so it is clear that it might be interesting to first investigate the freeness problem on free (semi)groups.

Firstly, notice that we can always assume that we are speaking about the free (semi)group on two generators. This is because there exist embeddings of this group into the free (semi)group on $n \geq 2$ generators and vice versa.

Lemma 4.2. We can embed the free semigroup on $n \geq 2$ generators into the one on two generators, say $\{a, b\}^*$.

Proof. For any $k \in \mathbb{N}$ we have that for $S = \{a^i b, 1 \leq i \leq k\}$ that S^+ is a free semigroup of rank k. (it is what we call a *prefix code*, see Remark 4.5 - given a word, we can immediately uniquely tell which element of S it started with since no element is a prefix of another) □

Lemma 4.3. We can embed the free group F_n for $n \geq 2$ into F_2.

Proof. Remembering Remark 3.9 we are done since

$$G_k = \langle b^{-i} a b^i, 1 \leq i \leq k \rangle$$

generates a free group. □

Note that in both cases we can also get the free group on countably infinitely many generators as a subgroup.

Theorem 4.4 (Sardinas-Patterson algorithm, 1953)**.** The freeness problem on free semigroups is decidable.

This is one of the main results of Chapter 4 in [35]. After a definition we recount the algorithm, but we will not provide the proof of its correctness.

Remark 4.5. A set of k elements of a free semigroup Σ^+ spanning a free semigroup of rank k is usually called a *code*. This is because an alternative definition is the following: $S \subseteq \Sigma^+$ is a code if for any $x_i \in S$, we have

$$x_{i_1} x_{i_2} \dots x_{i_n} = x_{j_1} x_{j_2} \dots x_{j_m} \Leftrightarrow n = m, x_{i_k} = x_{j_k}.$$

In particular this means that given a word in Σ^+, we can uniquely 'decode' it into the elements of S which formed it. The classical reference for code theory is [3], from where the bottom examples come from.

Example

(i) $\{aa, ba, baa\}$ is a code (check this!).

(ii) $\{a, ab, ba\}$ is not a code since $(a)(ba) = (ab)(a)$.

The Sardinas-Patterson algorithm operates by transforming the given set of words iteratively, namely by forming the new set of words that are suffix of a word x in the previous set formed by this suffix and a word in the original set y or vice versa. Concisely, if we want to investigate whether or not S is a code, we form the sets

$$S_0 = S$$
$$S_{i+1} = \{w |\ xw = y \vee yw = x, x \in S, y \in S_{i+1}\}$$

Since the length of the words in the sets is bounded by the length of the words in S, the S_i have to start looping at some point - if every $S_i \cap S$ is empty, then S is a code, and if not, then not. As said, a proof can be found in [35].
So we have solved the freeness problem for semigroups.
The problem for free groups is also solvable, but this time via a completely different, almost topological approach. Firstly the following theorem must be mentioned.

Theorem 4.6 (Nielsen-Schreier)**.** Any subgroup of a free group is free.

The following ideas all stem from [15].
We can associate any finitely generated subgroup of a free group $\langle H \rangle \leq F_n$ with a finite labeled directed graph X_H that is *folded*, by this we mean that no vertex has two edges with the same label that are either both heading outwards from or towards the vertex. We get this graph by following the following procedure:

1. Add a base vertex v.
2. For each generating word $w = a_1 \cdot a_n \in H$, add a wedge with an edge heading outwards to a new vertex labelled with each standard generating element a_i of F_n and inwards for an inverse element (but still labelled with the corresponding positive element), looping back around to v.
3. Fold the graph by 'pushing' together two vertices that are connected to the same vertex via an edge that is labelled the same and points in the same direction. Repeat until it is folded.

This is a very intuitive and informal explanation. For details see [15], from which also the following illustration is taken.

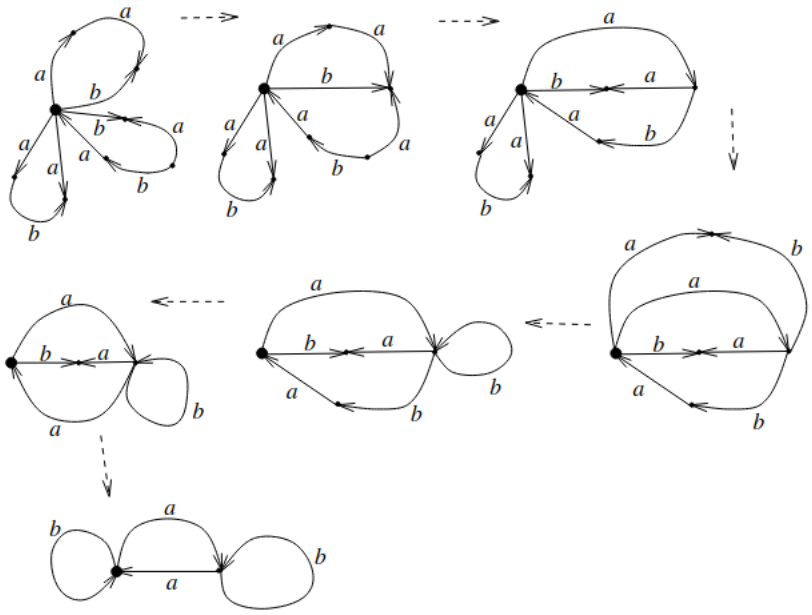

Figure 1: The above procedure applied to $H = \langle a^b, ba^{-1}ba, a^{-1}ba \rangle \leq F_2$.

The subgroup H can be found in its original directed graph as the group of paths beginning and ending at v, but these words are not necessarily freely reduced. We can check (again see [15] for details) that a folded graph has the following properties:

- The group of paths beginning and ending at v remains the same as it was in the original directed graph.
- The words spelt out are freely reduced.
- it is the union of all reduced paths (i.e. we never use the same edge forwards and backwards consecutively) from v to v.

In the light of these we see how the algorithm must work. We generate this folded graph from the given generators of H, and then try to calculate the rank of the group of paths beginning and ending at v. The latter part works by finding a spanning tree of the folded graph and then counting the amount of 'loops', i.e. edges which are outside of it.

Claim 4.7. The set of shortest paths from v to v using the edges not in the spanning tree (in a positive sense, i.e. traversing them in the direction they point) outside of the graph freely generates H.

Proof. Obviously we must prove this in two parts - first we show that they generate H, then that they admit no relation in between them. We start with the first part.
We claim first that H is generated by all paths p_e for every edge e, where p_e is precisely the path going from v to v via the quickest route using (in a positive sense) the edge e. Pick $h \in H$, which is a path which can be written as a sequence of edges beginning and ending at v, and traversing the vertices $v, v_1, v_2, \ldots, v_n, v$. Now notice that if e_0 is the edge between v and v_1, and e_1 the edge between v_1 and v_2 and so on, we can write

the path as $p_{e_0} \cdots p_{e_n}$.
Now we show that these paths are independent, i.e. that no nontrivial combination of them and their inverses that is freely reduced can give the identity.. Let $h = p_{e_1} \cdots p_{e_n}$, where the e_i are edges outside of the tree and h is not trivially freely unreduced, i.e. $e_i \neq e_{i+1}$. We can freely reduce this to the path going to the origin of e_1, then over e_1 to the target vertex, then via the tree to the origin of e_2 and so on. We claim that this word is already completely freely reduced - this is because if not, since the graph is folded, we would have that we traversed an edge forwards and backwards consecutively, a contradiction to $e_i \neq e_{i+1}$. So we have a nontrivial reduced path and thus a nontrivial reduced word in H. □

So the amount of these edges is the rank of H. Equivalently, since every finite graph has a spanning tree, we can just calculate the Euler characteristic χ of the folded graph to calculate the rank of H – it would just be $1 - \chi$.

4.2 Matrix semigroup freeness

When trying to prove results about matrices the method that is mostly used is a clever embedding attributed to Paterson [12]. If $\Sigma = \{a_1, \cdots a_n\}$ is a finite alphabet, we can consider the reverse $n-$ary representation of a word in Σ^+ :

$$\sigma(a_{i_1} \cdots a_{i_k}) = \sum_{j=1}^{k} i_j n^{k-j}$$

Then it is easy to check that

$$\begin{aligned} \gamma : \Sigma^+ \times \Sigma^+ &\to \mathbb{N}^{3\times 3} \\ (u, v) &\mapsto \begin{pmatrix} n^{|u|} & 0 & 0 \\ 0 & n^{|v|} & 0 \\ \sigma(u) & \sigma(v) & 1 \end{pmatrix} \end{aligned}$$

is an injective homomorphism. Given this tool many decision questions about matrix semigroups reduce to problems over the direct product of two free semigroups – such as the freeness problem. In the following we will prove that the freeness problem for this direct product is *undecidable*. Our observations at the beginning of this chapter show that it is equivalent whether or not we regard the free (semigroup) on 2 generators or more. A first attempt to prove this leads to an interesting variant of the PCP. In the following write $\mathbb{W}$ as the free semigroup on the two generators a and b.
Our target is to reduce the freeness problem on $\mathbb{W} \times \mathbb{W}$ to the PCP on n letters. Given an instance $h, g : \Sigma^+ \to \Delta^+$, regard the subset S of $\Sigma^+ \times \Sigma^+$ given by

$$S := \{(a, h(a))|\ a \in \Sigma\} \cup \{(a, g(a))|\ a \in \Sigma\}. \tag{†}$$

It turns out that this is not quite enough (yet), since a relation in S implies that there exists a word $w = a_1 \cdots a_n \in \Sigma^+$ with the property that there exist $h_i, g_i, 1 \leq i \leq n$ with not all $h_i = g_i$ so that

$$h_1(a_1) \cdots h_n(a_n) = g_1(a_1) \cdots g_n(a_n).$$

We call deciding exactly this the *Mixed Modification* of the PCP, or MMPCP for short.
Now follows exactly the theorem that we would expect.

Theorem 4.8. MMPCP is undecidable. [8] [7]

Proof. This proof will fall into more or less two parts. In the first part we define so called *Claus instances*, which are a specific constraint on a regular instance of the PCP and show that the PCP and the MMPCP are equivalent on these instances. After this, we can show that if the PCP is decidable on Claus instances, it is decidable everywhere, hence showing that MMPCP is undecidable on Claus instances and hence also everywhere.
The definition of the Claus instances is quite unintuitive, though we will try to explain every step. These instances are defined based on a given instance (h, g) of the PCP with morphisms $h, g : \Sigma^+ \to \Delta^+$ on two more letters, which we call d and e in addition to the letters in Σ.

Pick a letter $a \in \Sigma$. The morphisms $h_a, g_a : (\Sigma \cup \{d, e\})^+ \to (\Delta \cup \{c, d, e\})^+$ are called the corresponding $a-$*Claus instances* to h, g if

$$\begin{aligned} h_a(x) &= l(h(x)) & g_a(x) &= r(g(x)), x \in \Sigma \\ h_a(d) &= cl(h(a)) & g_a(d) &= cdr(g(a)) \\ h_a(e) &= de & g_a(e) &= e \end{aligned}$$

The morphisms l and r plant the letter d in between every letter and to the left or to the right of the word, respectively (i.e. $r(aba) = adbdbd, l(aa) = dada$). For intuition: The reason for this is so that given a word with a d between every letter that is cut off at a certain place, we can uniquely determine if the letter that follows must be mapped to by h_a or by g_a. The details will become clear in due course. c and e are to be regarded as starting and ending a shortest solution – concisely:

Claim. The shortest solution (to be understood as it is locally shortest, i.e. any solution can be shortened to one of this form and no further) to the MMPCP on Claus instances is of the form dwe where $w \in \Sigma^+$.

Proof. Notice that w does not contain d or e. Assume w is a shortest solution and $w = a_1 a_2 \dots a_k$ where $a_i = e$.

$$h_1(a_1) \cdots h_k(a_k) = g_1(a_1) \cdots g_k(a_k) \tag{4.1}$$

from the condition. Now since the h and g preserve the amount of e's in a word and the equivalence above gives $h_1(a_1) \cdots h_i(a_i) \subseteq g_1(a_1) \cdots g_i(a_i)$ or vice versa but both words end in e, we see that we must in fact have $h_1(a_1) \cdots h_i(a_i) = g_1(a_1) \cdots g_i(a_i)$. This is a shorter solution, hence a contradiction unless $i = k$. We can give exactly the same argument with d at the beginning and c instead of e. □

Claim. If $dwe, w \in \Sigma^+$ is a shortest solution to the MMPCP on a Claus instance, then w is a solution to the PCP on the same Claus instance (and obviously vice versa).

Proof. We claim that we can always set $h_i = h$ and $g_i = g$ for all i. W.l.o.g. assume that $h_1 \neq g_1$. Also w.l.o.g. assume that $h_1 = h$ and $g_1 = g$. To see the claim we pick the minimum $i + 1$ so that $h_{i+1} \neq h_1$ and the minimum $j + 1$ so that $g_{j+1} \neq g_1$. Now because of (4.1) we see that $h(a_1 \cdots a_i) \subseteq g(a_1 \cdots a_j)$ or vice versa. We can assume that the latter is a strict subsequence since else we would have to have $a_i = a_j = e$ and thus $i = j = k$.
This is where our comment about the morphisms l and r comes in. $g(w)$ has the property that there is a d between any two letters. $h(w)$ never ends in a d though, so since $h(a_1 \cdots a_i) \subseteq g(a_1 \cdots a_j)$ it must continue with a d, i.e. $h_{i+1}(a_{i+1})$ must start with a d. This is only possible though if $h_{i+1} = h$, which is in contradiction to our conditions - so in fact all h_i are h and all g_i are g, and dwe solves the PCP.´ □

What we have shown so far is that if the MMPCP were decidable, the PCP would be decidable on Claus instances. But this already finishes off the problem since the latter implies the decidability of the PCP in general. This is because if a solution exists, then a shortest solution dwe exists and we see that

$$\begin{aligned} & h_a(dwe) = g_a(dwe) \\ \Leftrightarrow\ & cl(h(a))l(h(w))de = cdr(g(a))r(g(x))e \\ \Leftrightarrow\ & l(h(aw))d = dr(g(aw)) \\ \Leftrightarrow\ & h(aw) = g(aw) \end{aligned}$$

so if MMPCP was decidable, we could decide PCP by checking for a solution on every a-Claus instance of (h, g) for every letter $a \in \Sigma$. □

Given our remark before Theorem 4.8, we get following corollary.

Corollary 4.9. The freeness problem is undecidable for 3×3 matrix semigroups generated by sets of 10 elements.

Proof. Looking at the encoding in (†), we require $2n$ elements for undecidability where n is the amount of letters that the PCP is undecidable on. □

Remark 4.10. A clever trick is employed in Theorem 7.18. of [8] to get this number down to $2n-1$, i.e. in our case 9 matrices. Note that in this paper the result of undecidability of PCP on 5 letters was not yet known.

For 2×2-matrices the problem is open. We will now consider a special case which has been open for a very long time. [16]

4.3 The Lyndon-Ullman problem

Definition 4.11. The *Lyndon-Ullman-problem* asks for which $r \in \mathbb{C}$ the matrices

$$\begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ r & 1 \end{pmatrix}$$

generate a free (semi)group.

The original question asks for the group they generate, but no complete results are known for either. We will concentrate on this version. It is easy to see that we can only regard algebraic numbers since transcendental numbers will always generate free structures as any relation will give a polynomial equation in r. We can show that for $|r| \geq 2$, we also always get a free group. Call the set of r giving a free group Λ.

Theorem 4.12 (Ping-pong lemma)**.** Let $\{h_1, \ldots, h_k\} \subseteq H$ for a group H acting on a set X. If X has disjoint subsets $X_1, \ldots, X_k$ for which h_i^m maps X_i into other X_j with $i \neq j$ $\forall m \neq 0$, then $\langle h_1, \ldots, h_k \rangle \cong F_k$. [9]

The intuition behind this is that (picking for instance $k = 2$) we will have two sets that our two group elements send set elements between (hence the name). This ensures that no word written in them can fix an element in one of the sets and so cannot be the identity.

Proof. Given a freely reduced word $h_{i_1}^{a_{i_1}} h_{i_2}^{a_{i_2}} \cdots h_{i_n}^{a_{i_n}} \in \langle h_1, \ldots, h_k \rangle$, we write it as $h_{i_1}^{a_{i_1}} h_{i_2}^{a_{i_2}} \cdots h_{i_n} h_{i_1}^{a}$, where a can also be 0. Now if this is the identity, we can conjugate it and it will still remain the identity. Conjugate by a power of h_{i_1} so that both a_{i_1} and a are nonzero. Then this cannot be the identity though, since any element in X_{i_1} will be mapped between the X_i until the last element, namely a power of h_{i_1}, maps it outside of X_{i_1}. So the group elements acts on an element of X nontrivially, hence cannot be the identity. □

Theorem 4.13. If $|r| \geq 2$, then $r \in \Lambda$.

Proof. Use the ping-pong lemma. Can check that picking the sets

$$X_1 = \{\begin{pmatrix} x \\ y \end{pmatrix} \mid |x| < |y|\}, \qquad X_2 = \{\begin{pmatrix} x \\ y \end{pmatrix} \mid |x| > |y|\}$$

fulfills the conditions for $h_1 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, h_2 = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$. □

Also an interesting result is the following.

Theorem 4.14. $\Lambda \cap A$ lies dense in the plane, where A is the set of algebraic complex numbers.

Proof. This is clear for $|r| \geq 2$. Now notice that if r has an algebraic conjugate (i.e. a root of its minimal polynomial) which has a modulus ≥ 2, then $r \in \Lambda$ since if there was a relation the other number would fulfill it too. The following claim makes the proposition clear.

Claim 4.15. Let S be an open subset of the plane. The set of all numbers with an algebraic conjugate $\in S$ is dense in the plane. [25]

Proof. Pick a point $z \in \mathbb{C}$. We want to show that it is possible to find an irreducible polynomial with a root arbitrarily close to z as well as a root $s \in S$. Pick a rational close to z and a rational in S. Let $\alpha = \alpha_0 + \alpha_1 z + \ldots + \alpha_n z^n$ be a rational polynomial with these roots. For every prime p with $p \nmid \alpha_n$, we have that $p\alpha + 1$ is irreducible. Indeed, if it was reducible, then changing the variable to $x := \frac{1}{z}$ gives the equation

$$(p\alpha_0 + 1)x^n + p\alpha_1 x^{n-1} + \ldots + p\alpha_n = 0$$

which is irreducible by Eisenstein's criterion.
Now we see that we can pick p large enough so that, by continuity, the zeroes of $p\alpha + 1$ are arbitrarily close to s and to z, so we can also pick them large enough so that the latter is in S. □

Now simply pick any open subset of the plane which is outside of the circle of radius 2 centered at the origin, and we are done. □

Remark 4.16. The Lyndon-Ullman problem for semigroups is also open, and in this case it turns out that the ping pong argument works for $|r| \geq 1$.

Actually, if we could solve the Lyndon-Ullman problem, we could solve the freeness problem for any two *linear fractional parabolic transformations*, that is, Möbius maps with determinant 1 and trace 2. We can identify these transformations with matrices in $\mathrm{SL}_2(\mathbb{C})$ with trace 2. This follows from the following lemma.

Lemma 4.17. Denote conjugacy by $\sim$. Given $A, B, A', B' \in \mathrm{SL}_2(\mathbb{C})$. If $A \sim A'$, $B \sim B'$ and $AB \sim A'B'$, then all these conjugacies are via the same matrix, i.e. $\exists P \in \mathrm{SL}_2(\mathbb{C})$ with $P^{-1}AP = A', P^{-1}BP = B'$.

Proof. First we begin by noticing that we can w.l.o.g. assume that $A = A'$. This is because of the following: Assume that $QAQ^{-1} = S$. Then we can replace A by S in

$$\begin{aligned} A &\sim A' \\ B &\sim B' \\ AB &\sim A'B' \end{aligned}$$

by changing the statements to

$$\begin{aligned} S &\sim A' \\ QBQ^{-1} &\sim B' \\ SQBQ^{-1} &\sim A'B' \end{aligned}$$

The last one is true since

$$Q^{-1}(SQBQ^{-1})Q = Q^{-1}SQB = AB \sim A'B'.$$

So now replace A with A', since they are conjugate, to get the statement.
It is well known that two matrices in $\mathrm{SL}_2(\mathbb{C})$ are conjugate iff they have the same trace. We use this in the following.

- Case 1: $A = A'$ is diagonalisable.
  In this case we can, as outlined above, assume that

  $$A = A' = \begin{pmatrix} u & 0 \\ 0 & u^{-1} \end{pmatrix}$$

  Given that $B = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, B' = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$ we get that $AB = \begin{pmatrix} au & bu \\ cu^{-1} & du^{-1} \end{pmatrix}$, so equating traces and using the third conjugacy gives that

  $$\begin{aligned} au + du^{-1} &= a'u + d'u^{-1} \\ (a - a')u &= (d' - d)u^{-1} \end{aligned}$$

  Now if $u^2 \neq 1$, we have that $a = a'$ and $d = d'$. This actually is enough for the conclusion since the centraliser of $A = A'$ are other diagonal matrices, which can be tweaked so to conjugate B to B'. If $br = b'$, pick $P = \begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix}$ with $x^2 = r$ to get $PBP^{-1} = B'$.
  If $u^2 = 1$, then $A = A' = \pm I$ and we can pick any matrix we want that conjugates B to B'.

- Case 2: $A = A' = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Now we can check that

  $$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \in C_{\mathrm{SL}_2(\mathbb{C})}(A),$$

i.e. we can pick any x and the matrix $\begin{pmatrix}1 & x\\ 0 & 1\end{pmatrix}$ will conjugate A to A', or said differently, leave A fixed. In this case the trace of B also has to be 2, or else we can swap their roles and use Case 1. Using the relation $AB \sim A'B'$ gives that

$$\begin{pmatrix}a+c & b+d\\ c & d\end{pmatrix} \sim \begin{pmatrix}a'+c' & b'+d'\\ c' & d'\end{pmatrix}$$
$$\Leftrightarrow a+c+d = a'+c'+d'$$
$$\Leftrightarrow c = c'$$

It is left to the reader to check that

$$\begin{pmatrix}1 & x\\ 0 & 1\end{pmatrix}\begin{pmatrix}a & b\\ c & 2-a\end{pmatrix}\begin{pmatrix}1 & -x\\ 0 & 1\end{pmatrix} = \begin{pmatrix}a' & b'\\ c & 2-a'\end{pmatrix}$$

for $x = \frac{a'-a}{c}$, so the same matrix will conjugate A to A' and B to B' and we are done.

□

Now how do we use this to get statements about groups generated by two parabolic Möbius maps? Since

$$\operatorname{tr}\begin{pmatrix}1 & r\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & 0\\ r & 1\end{pmatrix} = 2+r^2,$$

if we name the invariant $\tau = \operatorname{tr} AB - 2$ for two parabolic Möbius maps A, B we see:

Corollary 4.18. If two parabolic Möbius maps A, B have invariant τ and $r^2 = \tau$, then

$$\langle A, B\rangle \cong \langle \begin{pmatrix}1 & r\\ 0 & 1\end{pmatrix}, \begin{pmatrix}1 & 0\\ r & 1\end{pmatrix}\rangle$$

Proof. Taking the canonical matrices in $\mathrm{SL}_2(\mathbb{C})$ corresponding to A and B, using the previous lemma we see that $A \sim \begin{pmatrix}1 & r\\ 0 & 1\end{pmatrix}, B \sim \begin{pmatrix}1 & 0\\ r & 1\end{pmatrix}$ and the condition on τ gives that their products are also conjugate, so in fact the map $\phi : A \mapsto PAP^{-1}$ where P is given by the lemma is an isomorphism, i.e. the groups are even conjugate. □

4.4 Matrix group freeness

What about matrix groups?
Though the Lyndon-Ullman problem shows that little can yet be said for 2x2-matrices, maybe again we have results for larger ones. But it turns out that here almost nothing is known. We will show now that the freeness problem for matrix groups is decidable on 2×2 *integer* matrices, but the rest are open problems.

Note

If A is a group property, then a group G is *virtually* A if it has a finite index subgroup that is A.

Lemma 4.19. $\mathrm{SL}_2(\mathbb{Z})$ is virtually free.

Proof. We can show that $\langle \begin{pmatrix}1 & 2\\ 0 & 1\end{pmatrix}, \begin{pmatrix}1 & 0\\ 2 & 1\end{pmatrix}\rangle$ has index 12 in $\mathrm{SL}_2(\mathbb{Z})$. Sanov showed (exercise) that these matrices are precisely those of the form $\begin{pmatrix}2k & 4l+1\\ 4m+1 & 2n\end{pmatrix}$. Obviously this has index 2 in the congruence subgroup $\Gamma(2)$ which has index 6 in $\mathrm{SL}_2(\mathbb{C})$, and is free by Theorem 4.13. □

Theorem 4.20. The freeness problem is decidable for virtually free groups.

Proof. □

Corollary 4.21. The freeness problem is decidable for invertible 2x2 integer matrices.

We will summarise a few results about what we can say at this stage, but we will mention this problem many more times later in this report.
An idea would be that we could again find an embedding of the direct product of free groups into a matrix group. This actually works!

Lemma 4.22. There exists an embedding of $F_2 \times F_2$ into $GL_4(\mathbb{Z})$.

Proof. Recall the Lyndon-Ullman problem and that $\begin{pmatrix}1&2\\0&1\end{pmatrix}, \begin{pmatrix}1&0\\2&0\end{pmatrix}$ generate a free group. Using this knowledge we see that

$$\phi : F_2 \times F_2 \to GL_4(\mathbb{Z})$$

$$(a,a) \mapsto \begin{pmatrix}1&2&0&0\\0&1&0&0\\0&0&1&2\\0&0&0&1\end{pmatrix} \qquad (b,a) \mapsto \begin{pmatrix}1&0&0&0\\2&1&0&0\\0&0&1&2\\0&0&0&1\end{pmatrix}$$

$$(a,b) \mapsto \begin{pmatrix}1&2&0&0\\0&1&0&0\\0&0&1&0\\0&0&2&1\end{pmatrix} \qquad (b,b) \mapsto \begin{pmatrix}1&0&0&0\\2&1&0&0\\0&0&1&0\\0&0&2&1\end{pmatrix}$$

is a valid embedding. □

So now we have gotten our hopes up - if we can show that the freeness problem is undecidable on $F_2 \times F_2$, we are done. But this is not even an open problem, it is simply wrong, so we see that this route will be of no help.

Theorem 4.23. If the groups G_1 and G_2 have decidable freeness problem, then $G_1 \times G_2$ also does.

Proof. Let $K \subseteq G_1 \times G_2$, and $K_1 \subseteq G_1, K_2 \subseteq G_2$ be the respective projections. It is easy to see that if either of K_1 or K_2 are free then K is free. If neither are free, then look at the canonical induced homomorphisms $\phi_1 : F \to K_1$, $\phi_2 : F \to K_2$ where F is a sufficiently large free group. Then neither ϕ_1 nor ϕ_2 are injective, so their kernels are nontrivial. But this is enough to imply that their intersection (i.e. the kernel of the induced mapping of the free group into $\langle K \rangle \leq G$) is nontrivial since if it wasn't, the kernels would be commuting normal subgroups, so we could find a copy of $\mathbb{Z}^2$ in F. □

Corollary 4.24. The freeness problem is decidable for $F_2 \times F_2$.

Note the interesting discrepancy between this case for semigroups and this case for groups.
So this idea cannot work. In fact we would have encountered difficulties even if it did, since in the proof for semigroups we used that the PCP is undecidable on free semigroups. Here we would need it for groups.

Definition 4.25 (Post correspondence problem on free groups.)**.** Let Σ and Δ be two finite alphabets. A solution to the PCP on free groups is an algorithm, that given two morphisms $h, g : \langle \Sigma \rangle \to \langle \Delta \rangle$ decides whether or not there exists a nontrivial $w \in \langle \Sigma \rangle$ with $h(w) = g(w)$.

Note

The PCP on free groups is an open problem, but the GPCP is known to be undecidable. [26]

Our previous theorems spark an idea though: We proved that if MMPCP on free semigroups was decidable, then the PCP would be as well. MMPCP was undecidable because (or this was equivalent to saying that) the freeness problem on $\mathbb{W} \times \mathbb{W}$ was undecidable. So can we use the decidability of the freeness problem on $F_2 \times F_2$ to engineer a group version of MMPCP that is decidable, and use this to prove that the PCP is?

Definition 4.26. We call the *MMPCP on free groups* the problem of deciding whether or not, given two morphisms $h, g : \langle \Sigma \rangle \to \langle \Delta \rangle$, there exist words $w = a_1 \cdots a_n, w' = b_1 \cdots b_m \in \langle \Sigma \rangle$ with the property that there exist $h_i, g_i, 1 \leq i \leq n$ with not all $h_i = g_i$ so that

$$h_1(a_1) \cdots h_n(a_n) = g_1(b_1) \cdots g_m(b_m),$$

and $w = w' \neq 1$ in the free group, i.e. they freely reduce to the same word.

Theorem 4.27. The MMPCP on free groups is decidable.

Proof. Using exactly the same encoding as in Corollary 4.9 gives the result, but this time $F_2 \times F_2$ has decidable freeness problem. □

We cannot just directly transfer the original definition since then the decidability of $F_2 \times F_2$ will not imply anything about it - we just get that $w = w'$ in the free group and not that they spell out exactly the same word.

Open problem. If we define the MMPCP with $w = w'$ as words, is it still decidable?

Now we can try to use our definition of the MMPCP to prove the decidability of the PCP. We have found no working strategy, and the following details why blindly copying the idea with the Claus instances will not work.
An important step in Theorem 4.8 was to prove that MMPCP and PCP were equivalent on Claus instances. It even went so far as to show they would have the same solution! We now provide a counterexample to this in the free groups case.

Proposition 4.28. There exists a Claus instance (h_a, g_a) so that the PCP with (h, g) has no solution but the MMPCP with (h_a, g_a) does.

Proof. We by no means claim this is a minimal example - it is simply the first we found.
Define the morphisms as follows:

$$\begin{aligned} h, g : \langle a, b, c\rangle &\to \langle a, b, x\rangle \\ h(a) = x \qquad & g(a) = xa \\ h(b) = ab \qquad & g(b) = b^{-1}a^{-1} \\ h(c) = a^{-1}b^{-1} \qquad & g(c) = b \end{aligned}$$

Remark that by the encodings we saw before we could take the target alphabet to be binary. Now we can check that the PCP has no solution here. If there was a solution w, then w^{-1} would also be a solution, so we can assume that the first letter of the freely reduced w is not an inverse. The letters are picked so that the x is 'uninvertible', i.e. if w is freely reduced and contains an $a(a^{-1})$, then the $x(x^{-1})$ corresponding to that a in $h(w)$ or $g(w)$ will not be cancelled (check this!).

- Now if a solution w starts with an a, we can easily check it must continue with b.

  $$\begin{aligned} x|&\ ab \\ xa|&b^{-1}a^{-1} \end{aligned}$$

  But this is already a contradiction since we cannot get the bottom row to invert away the false b^{-1} without using an uninvertible x or breaking the rule that w is freely reduced.

- If a solution starts with b, we immediately get a contradiction since none of these are invertible.

  $$\begin{aligned} ab&| \\ b^{-1}a^{-1}&| \end{aligned}$$

- If a solution starts with c, then the second letter must be b, again leading to a contradiction.

  $$\begin{aligned} a^{-1}b^{-1}|&\ ab \\ b|&b^{-1}a^{-1} \end{aligned}$$

So the PCP has no solution, but we can check that (if h_a, g_a are the corresponding Claus instances)

$$h_a(d)h_a(b)g_a(b^{-1})h_a(e) = g_a(d)h_a(c^{-1})g_a(c)g_a(e)$$

so our definition of the group MMPCP *does* have a solution.

□

This ultimtely means that Claus instances are unsuitable for handling the group case.

Open problem. Does there exist a transformation of group morphisms h, g to say, *alternative Claus instances* (A.C.I.), so that

- the decidability of the free group PCP on A.C.I. implies the decidability of the PCP in general, and
- the free group MMPCP and free group PCP are equivalent on A.C.I.?

5 The word problem and other general group problems

We have already discussed the word problem for groups and semigroups in general. Obviously an algorithm can freely reduce, so it is decidable for free (semi)groups. But what happens for matrix groups?

Theorem 5.1. A residually finite and finitely presented group G has decidable word problem. [21]

Proof. Take $w \in G$. If it is the identity, we will eventually reach it by trying out all of the consquences of the relators. In parallel run an algorithm enumerating the homomorphisms of G into finite groups (i.e. by looking at subgroups of symmetric groups which fulfill the relations). If $w \neq 1$, then one of these must map w to a non identity element, in which case we also halt. □

Theorem 5.2. Finitely presented matrix groups are residually finite. [28]

So we see that we can indeed solve the word problem in these groups. We now define a type of group which will come in handy. The following definitions and examples are from [5].

Definition 5.3. We say that a finitely generated group $G = \langle S|R\rangle$, where R is symmetrised, i.e. is closed under cyclic reduction and inverses, has *small cancellation* $\lambda \in [0, 1]$, denoted by $C'(\lambda)$ if $\forall r_1, r_2 \in R$ with $r_1 \neq r_2^{-1}$ the part of r_1 that is absorbed in the product $r_1 r_2$ is of length $< \lambda \cdot \min(|r_1|, |r_2|)$ and vice versa.

Definition 5.4. Groups which admit a presentation that has cancellation $\frac{1}{6}$ are called *sixth groups*.

Proposition 5.5. Every finitely presented group has a presentation with $C'(\frac{1}{5})$. [29]

Example

(i) $\mathbb{Z}^2$ is not a sixth group.

(ii) $\langle a, b, c|\ a^l, b^m, c^n\rangle$. has small cancellation λ for any $\lambda > 0$.

For example, following is known.

Theorem 5.6. Sixth groups are linear. [2]

So they have solvable word problem. Also clearly the following question would answer the freeness problem for matrix groups in a negative sense.

Open problem. Does there exist a sixth group with unsolvable freeness problem?

These questions provoke investigating the relationship between the freeness problem and the word problem. Is one in some sense 'stronger' than the other? First notice that in any torsion-free group with undecidable word problem (we simply take the existence of these for granted), the freeness problem must be undecidable. This is because deciding if $\langle w\rangle$ is free is the same question as deciding whether or not $w = 1$. We can answer the converse fairly well by producing a group that has solvable word problem but undecidable freeness problem.

Lemma 5.7. There exists a computable function $f : \mathbb{N} \to \mathbb{N}$ with a non-recursive image.

Proof. Encode Turing machines into natural numbers. Now define

$$\phi : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$$
$$(a, b) \mapsto \begin{cases} a \text{ if a halts after b steps} \\ 0 \text{ else} \end{cases}$$

Now obviously $a \in \mathrm{Im}(\phi)$ iff a halts, so we could solve the halting problem if the image were computable. Now since we can biject $\mathbb{N} \times \mathbb{N}$ with $\mathbb{N}$, i.e. by $f(a, b) = 2^a(2b + 1)$, we are done. □

Lemma 5.8. Any computable function $f : \mathbb{N} \to \mathbb{N}$ with a non-recursive image can be transformed to one with the same properties that is injective. [6]

Proof. Let $\Phi(n) := 2^{\kappa(n)}3^{f(n)}$, where κ counts the amount of occurrences of $f(n)$ in $f(1), f(2), \ldots, f(n)$. This is injective and the required properties are preserved. □

Definition 5.9. The *finite order problem* for a group G asks for an algorithm which given a word in the generators determines whether it has finite order or not.

Obviously the decidability of the freeness problem implies the decidability of the finite order problem.

Theorem 5.10. Let Φ be the function $\mathbb{N} \to \mathbb{N}$ from the previous lemma that is injective, computable but has a non-recursive image. Then $G := \langle x_1, x_2, \ldots \mid x_{\Phi(n)}^{n!} \rangle$ has solvable word problem but unsolvable finite order problem (hence unsolvable freeness problem)

Proof. Solving the finite order problem for the generators of G clearly amounts to finding a decision algorithm for membership of the image of Φ. That the word problem is solvable is proven by McCool in [20]. □

Definition 5.11. The *order problem* for a group G asks for an algorithm which given a word in the generators determines whether it has finite order or not, and if so, what this order is.

We will think a bit about the interplay of the order, finite order and word problem. We have seen that the word problem does *not* imply the finite order problem. How about the other way around? As said above, a torsion-free group with undecidable word problem shows that the converse also does not hold. The following is clear:

Claim 5.12. A group with solvable finite order and word problem also has solvable order problem.

Proof. If the finite order problem outputs NO, we are done. If it is YES, apply the algorithm for the word problem on successive powers until we get YES. □

Claim 5.13. The order problem implies both the word and the finite order problem.

The word problem implies neither of the others, and the finite order problem doesn't imply the order problem since it would then imply the word problem. We have not been able to find anything regarding the following.

Open problem. Does there exist a group with solvable finite order problem but unsolvable word problem?

As a last remark note that the finite order problem is solvable for rational matrix groups, and hence by Claim 5.13 also the order problem. [18]

6 Further matrix group problems

We will now turn our focus to further problems regarding matrix groups. We will make extensive use of the embedding in Lemma 4.22.

Definition 6.1. The *generalised word problem* or the *membership problem* for a group G asks for an algorithm which given a finite set of words $\{g_1, \ldots, g_k\}$ in the generators and another word w determines whether $w \in \langle g_1, \ldots, g_k \rangle$ or not.

The name should be clear - we get the word problem by setting $k = 1, g_1 = 1$.

Definition 6.2. The *conjugacy problem* for a group G asks for an algorithm which given two words in the generators determines whether they are conjugate *within* G or not.

We will prove now that both are undecidable for $F_2 \times F_2$ and hence get the result for invertible 4x4 integer matrices.

Note

Obviously the conjugacy problem is decidable for the entire general linear group over a field – two matrices are similar if and only if they share Jordan normal forms (up to permutation). But we ask if this can be done for any subgroup, where we only allow conjugation by elements *within* that subgroup.

We can get both problems using the so-called *Mihailova construction*. [23] [22].

Definition 6.3. The *Mihailova subgroup* $M(G)$ of $F_n \times F_n$ based on a given group G is the subgroup $\{(x, y) \in F_n \times F_n |\ x = y \text{ in } G\}$.

What n is will become clear in the next claim, but by our known encoding in Lemma 4.22 we can assume this number is 2. We can check that this is a subgroup. In particular we have

Claim 6.4. If G is given by $\langle x_1, \ldots, x_n |\ r_1, \ldots, r_m \rangle$ then $M(G)$ is generated by

$$\{(x_1, x_1), \ldots, (x_n, x_n), (1, r_1), \ldots, (1, r_m)\}.$$

This is because we can build any word on the left using the first n generators, and then add any relations in any way we would like to create any equivalent word on the right side. Check [23] for a formal proof. But now the following theorem is immediate.

Theorem 6.5. The generalised word problem is undecidable for $\mathrm{GL}_4(\mathbb{Z})$.

Proof. Pick a group G with undecidable word problem. Then $M(G)$ is generated as above, and deciding whether $w_1 = 1$ in G is equivalent to deciding whether or not $(w_1, 1) \in M(G)$. Now embed $M(G)$ in $\mathrm{GL}_4(\mathbb{Z})$ via Lemma 4.22. □

Remark 6.6. Borisov gives an example of a group with 5 generators and 12 relations in [4] that has undecidable word problem. This means that the generalised word problem remains undecidable for 17-generated matrix groups.

We have not been able to find a group with undecidable word problem in the literature with a smaller sum of generators and relators. Solving the following problem seems absolutely hopeless.

Open problem. What is the smallest possible sum of the amount of generators and relators in a group with unsolvable word problem?

The Mihailova construction also gives the same result for the conjugacy problem thanks to the following lemma.

Lemma 6.7. Let $w \in F_{n+1}$. Rewrite G as $\langle x_1, \ldots, x_n, x_{n+1} |\ r_1, \ldots, r_m \rangle$. Then $w = 1$ in G if and only if (x_{n+1}, x_{n+1}) is conjugate to $(x_{n+1}, w^{-1} x_{n+1} w)$.

Proof. The only reason for rewriting the presentation of G is that we would like x_{n+1} to be the identity in G but not in the free group. Now obviously the one direction of the implication is clear since if $w = 1$, then $(1, w) \in M(G)$ and we can conjugate (x_{n+1}, x_{n+1}) to get $(x_{n+1}, w^{-1} x_{n+1} w)$.
Now assume

$$\begin{aligned}(X, Y)^{-1}(x_{n+1}, x_{n+1})(X, Y) &= (x_{n+1}, w^{-1} x_{n+1} w) \\ \Rightarrow X^{-1} x_{n+1} X = x_{n+1} &\wedge (wY)^{-1} x_{n+1} wY = x_{n+1}\end{aligned}$$

Claim. If two elements $a, b \in F_n$ commute, they must be powers of a common word $s \in F_n$.

Proof. In this case $\langle a, b \rangle \leq F_n$ is abelian, but by Nielsen-Schreier is also free. So $\langle a, b \rangle \cong \mathbb{Z} \Rightarrow \langle a, b \rangle = \langle s \rangle$. □

Using the claim we see that $X = x_{n+1}^k, wY = x_{n+1}^l$. But then $X = wY = 1$ in G. Notice that since $(X, Y) \in M(G)$ we have $X = Y$ in G, so $w = 1$ as expected. □

Corollary 6.8. The conjugacy problem is undecidable for 17-generated subgroups of $\mathrm{GL}_4(\mathbb{Z})$.

So we have used the Mihailova construction to fairly easily get these two important results. We will also present the *Rips construction*, an idea functioning similarly and also giving the undecidability of the membership problem for matrices via small cancellation groups. The classical reference for this is [31].

Theorem 6.9 (Rips construction)**.** Let G be a finitely presented group and $\lambda \in [0, 1]$. Then there exists a short exact sequence

$$1 \longrightarrow K \longrightarrow H \xrightarrow{\psi} G \longrightarrow 1$$

with H having small cancellation λ and K being finitely generated.

Proof. See [31]. □

The proof in the cited paper is short and simple enough that we feel we have little to add. Now since ψ is surjective we see how to prove Theorem 6.5 in albeit a somewhat weaker form – picking a G with unsolvable word problem gives that H has unsolvable generalised word problem since $w = 1$ in G is equivalent to $\psi^{-1}(w) \in \ker \psi$ in H. Now Theorem 5.6 gives that we can embed H in an (integer) matrix group.

Definition 6.10. The *orbit problem* for a linear group G of dimension n asks for an algorithm which given a finite set of invertible matrices $\{G_1, \ldots, G_k\} \subseteq G$ and two vectors $\vec{u}, \vec{v}$ determines whether $\exists M \in \langle g_1, \ldots, g_k \rangle$ with $M\vec{u} = \vec{v}$ or not. [10]

Theorem 6.11. The orbit problem is undecidable for $\mathrm{GL}_{16}(\mathbb{Z})$.

Proof. We reduce the conjugacy problem on $\mathrm{GL}_n(\mathbb{Z})$ to the orbit problem on $\mathrm{GL}_{n^2}(\mathbb{Z})$. We can identify elements of $\mathrm{GL}_n(\mathbb{Z})$ with vectors in $\mathbb{Z}^{n^2}$. Conjugation with an $n \times n$ matrix is then a linear map on the space of these vectors and can thus be identified with a $n^2 \times n^2$-matrix. So solving the conjugacy problem on n dimensions is actually a subproblem of the orbit problem on n^2. □

Definition 6.12. The *identity problem* for a linear group G asks for an algorithm which given a finite set of matrices $\{G_1, \ldots, G_k\} \subseteq G$ determines whether $I \in \{G_1, \ldots, G_k\}^+$.

We can solve this problem interestingly using a variation of the PCP, called the ICP.

Definition 6.13. The *Identity Correspondence Problem* (ICP) over a free semigroup asks, given two morphisms $h, g : \Sigma^+ \to \langle \Delta \rangle$, if there exists a word $w \in \Sigma^+$ so that $h(w) = g(w) = 1$.

Notice that we map to a group alphabet (which we can again assume to be binary).

Theorem 6.14. The ICP is undecidable on 36 letters. [1]

The proof is very complicated and shows that if we can solve ICP on $8(n-1)$ letters, we can solve PCP on n letters. Now we can use this to easily show the following.

Theorem 6.15. The identity problem is undecidable for $\mathrm{GL}_4(\mathbb{Z})$.

Proof. Given an instance (h, g), Take the mapping in Lemma 4.22 again and regard the semigroup generated by the images of $(h(a), g(a)) \forall a \in \Sigma$, then it will contain the identity if and only if there is a solution the ICP. □

We are also somewhat interested, following the main aim of this report, to think about the ICP on a free group instead of a semigroup.

Definition 6.16. The *Identity Correspondence Problem* (ICP) over a free group asks, given two morphisms $h, g : \langle \Sigma \rangle \to \langle \Delta \rangle$, if there exists a nontrivial word $w \in \langle \Sigma \rangle$ so that $h(w) = g(w) = 1$.

We have actually noticed that this is decidable, in contrast to the semigroup ICP.

Theorem 6.17. ICP over a free group is decidable.

Proof. This is the same as asking if $\{(h(a), g(a)), a \in \Sigma\} \subseteq F_2 \times F_2\}$ has a nontrivial relation – but this is exactly the freeness problem on $F_2 \times F_2$ which we know to be decidable by Corollary 4.24. □

This provokes the following, which we have been unable to solve.

Open problem. Does there exist an analogue of Theorem 6.14 for groups, i.e. using the decidability of ICP to show the decidability of the PCP?

7 Limitations of our methods

So far we have used the mappings in the beginning of Chapter 4.2 and the one in Lemma 4.22 many times. This gave us results about 3×3 and 4×4 matrices respectively. How do we know we can't do better? The first result we found of this form is in the paper also introducing the MMPCP for the first time.

Theorem 7.1. There is no injective semigroup morphism $\phi : \Sigma^+ \times \Sigma^+ \to \mathbb{C}^{2\times 2}$. [7]

Proof. Write $\Sigma = \{a, b\}$, w.l.o.g. assumed to be binary as always. If ϕ is a morphism, then conjugating it will preserve this property. So we can assume that the image of $(a, 1)$ is in Jordan form. $(a, 1)$ commutes with $(1, a)$ and $(1, b)$.

- Case 1: If its image is diagonal with two different eigenvalues, then the images of these two other elements must then also be diagonal in order to commute with $\phi(a, 1)$, but then they commute with each other, a contradiction.
- Case 2: $\phi(a, 1)$ cannot be a multiple of the identity since then it would commute with everything, so also with the image of $\phi(b, 1)$.
- Case 3: $\phi(a, 1) = \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$. But here again the matrices commuting with it have the form $\begin{pmatrix} x & y \\ 0 & x \end{pmatrix}$, which commute together, which is a contradiction as in Case 1.

□

The interpretation for this is that if we want to prove similar results for 2×2-matrices, we will have to develop new strategies as our ideas so far cannot work here.
Inspired by this theorem we wondered if it is possible to find a similar result for the group case, i.e. the embedding in Lemma 4.22, and we were successful. Many thanks to Emmanuel Breuillard whose valuable comments made the completion of the following theorem (7.8) possible.
Before this we prove a few important lemmas, which are also very interesting statements in their own right. A standard reference for solvable groups is [13].

Definition 7.2. A group G is called *solvable* if its derived series, i.e. repeated taking of commutator subgroups terminates in the trivial group in finitely many steps.

Lemma 7.3. Every subgroup of a solvable group is solvable.

Proof. Clear. □

Lemma 7.4. If G has a normal subgroup K so that K is solvable and $\frac{G}{K}$ is solvable, then G is solvable.

Proof. Check Corollary 9.2.1 of [13]. □

Lemma 7.5. The group of upper triangular matrices U is solvable.

Proof. This is fairly easy to see. First we show that the subgroup of upper triangular matrices with only ones on the diagonal is solvable – this can easily be computationally checked. Then we notice that this is a normal subgroup of U, and the quotient is the group of diagonal matrices, which is abelian and thus solvable – so we are done by Lemma 7.4. □

Lemma 7.6. Every nontrivial finitely generated normal subgroup of the free group F_2 has finite index.

Proof. A non-topological, combinatorial argument can be found in [17]. □

Note

An intuitive argument for the above is the following: Given a subgroup of F_2, we can construct the corresponding covering graph. If the subgroup is normal then the graph is regular, and if it is finitely generated it has finitely many loops deviating it from a tree – but then it has to be finite since in an infinite regular graph we could map one of the finitely many loops to a vertex so far away that there aren't any loops there.

Lemma 7.7. The free group F_2 does not contain a nontrivial abelian normal subgroup.

Proof. The Nielsen-Schreier theorem gives that any abelian subgroup is cyclic and so finitely generated. If we can show that no cyclic subgroup has finite index, then we are done by the previous lemma. Proceed by contradiction. Assume that $\langle a \rangle \leq F_2$ has finite index, i.e. there exists a finite set S so that every element in F_2 can be written as sa^k with $s \in S$. If m is the length of the longest element in S, Pick $K \in \mathbb{N}$ so that $|a^K| > m$. If a is freely reduced, then $|a^n|$ is increasing and has a constant last letter. Picking a word w with length longer than $|s| + k \cdot |a|$ and ending with a different letter than a, we see that w cannot be written in the form sa^k, a contradiction. □

Theorem 7.8. There exists no embedding of $F_2 \times F_2$ into $\mathrm{GL}_3(\mathbb{C})$.

Proof. Write $F_2 \times F_2 \cong \langle a, b \rangle \times \langle c, d \rangle$. Let $\phi : F_2 \times F_2 \to \mathrm{GL}_3(\mathbb{C})$ be an injective homomorphism and proceed by contradiction. Note that the elements in the second free group commute with the ones in the first.
If ϕ exists, we can conjugate it by a matrix in $\mathrm{GL}_3(\mathbb{C})$ to be able to w.l.o.g. assume that $A := \phi(a)$ is in Jordan normal form.

- Case 1: A diagonal, but does not have exactly two eigenvalue that are the same. If the three eigenvalues are the same, then A is a multiple of the identity, i.e. in the center of $\mathrm{GL}_3(\mathbb{C})$, and thus commutes with $B := \phi(b)$, a contradiction. If they are all distinct, then $C := \phi(c)$ and $D = \phi(d)$ must be diagonal since they commute with A, but then C and D commute with each other, a contradiction.

- Case 2:

$$A = \begin{pmatrix} \lambda & 1 & 0 \\ 0 & \lambda & 1 \\ 0 & 0 & \lambda \end{pmatrix}$$

  We calculate the centraliser of A.

$$\begin{pmatrix} \lambda & 1 & 0 \\ 0 & \lambda & 1 \\ 0 & 0 & \lambda \end{pmatrix} \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} \begin{pmatrix} \lambda & 1 & 0 \\ 0 & \lambda & 1 \\ 0 & 0 & \lambda \end{pmatrix}$$
$$\Leftrightarrow \begin{pmatrix} d+\lambda a & e+\lambda b & f+\lambda c \\ g+\lambda d & h+\lambda e & i+\lambda f \\ \lambda g & \lambda h & \lambda i \end{pmatrix} = \begin{pmatrix} \lambda a & a+\lambda b & b+\lambda c \\ \lambda d & d+\lambda e & e+\lambda f \\ \lambda g & g+\lambda h & h+\lambda i \end{pmatrix}$$

  Which is equivalent to saying $a = e = i, d = h = g = 0, b = f$ or

$$C_{\mathrm{GL}_3(\mathbb{C})}(A) = \{ \begin{pmatrix} \mu & x & y \\ 0 & \mu & x \\ 0 & 0 & \mu \end{pmatrix} \mid \mu, x, y \in \mathbb{C} \}.$$

  This is impossible though since $F_2 = \langle C, D \rangle \leq C_{\mathrm{GL}_3(\mathbb{C})}(A)$, and the latter as a subgroup of upper-triangular matrices is solvable, hence cannot contain a free group as it is not solvable.

- Case 3:

$$A = \begin{pmatrix} \lambda & 1 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & \mu \end{pmatrix}$$

  We proceed as in Case 2, but we will see that we will have to differentiate between two further cases.

$$\begin{pmatrix} \lambda & 1 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & \mu \end{pmatrix} \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} \begin{pmatrix} \lambda & 1 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & \mu \end{pmatrix}$$
$$\Leftrightarrow \begin{pmatrix} \lambda a & a+\lambda b & \mu c \\ \lambda d & d+\lambda e & \mu f \\ \lambda g & g+\lambda h & \mu i \end{pmatrix} = \begin{pmatrix} d+\lambda a & e+\lambda b & f+\lambda c \\ \lambda d & \lambda e & \lambda f \\ \mu g & \mu h & \mu i \end{pmatrix}$$

– Case 3a: $\lambda \neq \mu$:
This gives $c = d = f = g = h = 0, a = e$, or written more succintly

$$C_{\mathrm{GL}_3(\mathbb{C})}(A) = \{\begin{pmatrix} \alpha & x & 0 \\ 0 & \alpha & 0 \\ 0 & 0 & \beta \end{pmatrix} \mid \mu, x, y, z \in \mathbb{C}\}.$$

Now a contradiction can either be reached as in Case 2 by invoking solvability of upper triangular subgroups, or simply by checking that the given subgroup is even abelian.

– Case 3b: $\lambda = \mu$ (or A diagonal with an eigenvalue of multiplicity 2)
We also take care of the remaining possibility in Case 1 here: All these cases have as a common point that A has an eigenspace that is a plane. In fact, we may assume that A, B, C, D all have a planar eigenspace since else we can interchange the roles of the matrices and use one of the other cases to lead to a contradiction.

Claim. A and B have the same planar eigenspace.

Proof. Since C and D commute with A and B, they must preserve their eigenspaces. So if the eigenspaces are distinct, the entirety of $F_2 \cong \langle C, D\rangle$ preserves two different planes, i.e. their intersection, i.e. a plane and a line it contains, so under a suitable basis change the group would only consist of upper triangular matrices, a contradiction as above. □

Now change basis so that A is in Jordan normal form. This forces

$$A = \begin{pmatrix} \lambda & 1 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & \lambda \end{pmatrix} \qquad B = \begin{pmatrix} a & 0 & c \\ 0 & a & f \\ 0 & 0 & i \end{pmatrix},$$

or

$$A = \begin{pmatrix} \lambda & 0 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & \mu \end{pmatrix}$$

with $\mu \neq \lambda$. In particular we can now calculate the centralisers of the two possibilites for A. In the same fashion as above we get that

$$C_{\mathrm{GL}_3(\mathbb{C})}(A) \subseteq \{\begin{pmatrix} \alpha & w & x \\ 0 & \beta & y \\ 0 & z & \gamma \end{pmatrix} \mid \alpha, \beta, \gamma, x, y, z \in \mathbb{C}\}.$$

In particular notice that now $F_2 \times F_2 \subseteq C_{\mathrm{GL}_3(\mathbb{C})}(A)$. Consider the mapping

$$\begin{aligned} \psi : F_2 \times F_2 \cong \langle A, B\rangle \times \langle C, D\rangle &\to \mathrm{GL}_2(\mathbb{C}) \\ \begin{pmatrix} \alpha & w & x \\ 0 & \beta & y \\ 0 & z & \gamma \end{pmatrix} &\mapsto \begin{pmatrix} \beta & y \\ z & \gamma \end{pmatrix} \end{aligned}$$

By Theorem 7.1 we must have that ψ is not injective, i.e. the kernel is nonempty. But

$$\ker \psi = \begin{pmatrix} \alpha & x & y \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

is abelian and normal, and a subgroup of $F_2 \times F_2$. There must exist an element with a nontrivial element on either the left or the right, and the canonical mapping to this F_2 gives a nontrivial abelian normal subgroup of it, a contradiction to the lemma.

□

So also in the group case of the conjugacy and generalised membership problem – if we want analogous results for say, 3×3 - matrices, we will need a new approach.

8 The hyperplane problem

Firstly we are interested in the mortality problem for semigroups of matrices – the main reference for this is [12].

Definition 8.1. The *mortality problem* for a linear group G asks for an algorithm which given a finite set of matrices $\{G_1, \dots, G_k\} \subseteq G$ determines whether $0 \in \{G_1, \dots, G_k\}^+$.

Definition 8.2. The *upper-left-corner problem* for a linear group G asks for an algorithm which given a finite set of matrices $\{G_1, \dots, G_k\} \subseteq G$ determines whether $\exists M \in \{G_1, \dots, G_k\}^+$ with $M_{11} = 0$.

Lemma 8.3. The solvability of the mortality problem for $\mathrm{GL}_3(\mathbb{Z})$ implies the solvability of the upper left corner problem for $\mathrm{GL}_3(\mathbb{Z})$.

Proof. Consider the matrix $B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$. Note that $B^2 = B$. Given a set of matrices S we want to decide the upper left corner problem on, we can apply the mortality algorithm on the same set with B added. Now if there is a matrix $M \in S^+$ with $M_{11} = 0$, then $BMB = 0$ and the mortality algorithm will output YES. If there is none, then the mortality algorithm will output NO since if it outputs YES, there must be $M_i \in S^+$ with

$$\begin{aligned} BM_1BM_2 \cdots BM_nB &= 0 \\ (BM_1B)(BM_2B) \cdots (BM_nB) &= 0 \\ M_{1_{11}} M_{2_{11}} \cdots M_{n_{11}} &= 0, \end{aligned}$$

which is a contradiction. □

Theorem 8.4. The upper-left-corner problem is undecidable for sets of 5 3×3 - matrices.

Proof. See Theorem 3 in [12], where they prove this for 7, since this was the amount of letters PCP was known to be undecidable on at that time. □

Corollary 8.5. The mortality problem is undecidable for sets of 6 3×3 - matrices.

Similarly as before we want to think about generalising this to groups instead of semigroups. Obviously the mortality problem makes no sense for groups since we cannot get the zero matrix from invertible matrices with nonzero determinant. But the upper-left-corner problem is a new question that we can ask for groups. We attempted to reduce this problem to both the orbit problem as well as to the membership problem. We will first sketch a failed attempt for the former, and then a successful proof resulting from the latter. We also will switch to $\mathbb{Q}$ since this makes everything easier.
The core idea for reducing the upper-left-corner problem to the orbit problem for $\mathrm{GL}_n(\mathbb{Q})$ is noticing that the former is equivalent to asking the hyperplane problem:

Definition 8.6. The *hyperplane problem* asks to find an algorithm deciding for a finitely generated subgroup $\langle S \rangle \subseteq \mathrm{GL}_n(\mathbb{Q})$, a hyperplane $H \subseteq Q^n$ and a vector $\vec{u}$, if $\exists M \in \langle S \rangle$ with $M\vec{u} \in H$.

The upper-left-corner problem is equivalent (after basis changes) to asking, given a hyperplane H through the origin, a vector $\vec{u}$ and a finite set of invertible matrices S, if there exists a matrix M generated by those in S so that $M\vec{v} \in H$. (We have called this the hyperplane problem.) We show that if we can decide this problem in a slight variation in d dimensions, we can decide the orbit problem in d dimensions.
Consider the following variation (we call it V) of the problem: Pick an algebraic number α of degree $d-1$. Given a vector $\vec{u} \in \mathbb{Z}^d$, an $d-1$ dimensional subspace, i.e. hyperplane through the origin we call $H \subseteq \mathbb{Q}[\alpha]^d$ and a finite subset $S \subseteq GL_d(\mathbb{Z})$, we pose the same hyperplane problem. We claim that variation V is undecidable, because we can use it to solve the orbit problem as follows.

Lemma 8.7. We can find an appropriate 17-generated subgroup $\langle S \rangle \subseteq GL_{16}(\mathbb{Q})$ as above so that if there exists an $M \in \langle S \rangle$ with $M\vec{u} = \vec{v}$, then for no $M' \in \langle S \rangle$ do we have $M'\vec{u} = n\vec{v}$ or $M'\vec{u} = \frac{1}{n}\vec{v}$ for any $n \in \mathbb{Z} \backslash \{0, 1\}$.

Proof. The original undecidable problem we get the orbit problem from is the conjugacy problem (on 4x4 matrices). We claim that the given embedding already has this property.
Given M and M' violating the claim in the lemma, this is equivalent to finding 4x4 matrices M, M', P, Q in the embedding of $F_2 \times F_2$ so that $M^{-1}PM = Q$ and $M'^{-1}PM' = nQ$. But then

$$M^{-1}PM = Q = \frac{1}{n}M'^{-1}PM' \Leftrightarrow (MM'^{-1})^{-1}PMM'^{-1} = \frac{1}{n}P,$$

and since P is invertible taking determinants on both sides implies $n = 1$. □

Theorem 8.8. Variation V is undecidable.

Proof. Let S have the properties of Lemma 8.7. Now we are given vectors $\vec{u}, \vec{v}$.

Claim. There exists an enumeration of hyperplanes in $\mathbb{Q}[\alpha]^d$ that intersect the integer lattice in $\vec{v}$.

Proof. Let $z_i \in \mathbb{Q}[\alpha]$, and $\{x_i\}$ be the canonical basis of $\mathbb{Z}^d$. Each hyperplane in $\mathbb{Q}[\alpha]^d$ through the origin is of the form $x_1 + z_2x_2 + \ldots + z_dx_d = 0$. Since we can enumerate the elements of $\mathbb{Q}[\alpha]$ (there are countably many), we can enumerate $d-$tuples of them. We can then check if $\vec{v}$ lies on the hyperplane and add the hyperplane to our target enumeration if it does. □

An extension of this idea involves the dual space of $\mathbb{Q}[\alpha]^d$. By duality we can regard the hyperplanes containing $\vec{v}$ as forming a hyperplane themselves in the dual space, which we call H_v. This hyperspace has a basis of integer vectors. (This is a well known fact which can be looked up in i.e. paragraph 108 of [38].)

Claim. There exists a hyperplane in $\mathbb{Q}[\alpha]^d$ that only intersects the integer lattice in $\vec{v}$ and its integer multiples, and integer vectors of which it is a multiple.

Clearly this is the best we can do, any hyperplane containing $\vec{v}$ will necessarily contain these points as well.

Proof. Can obviously assume that $\vec{v}$ is primitive. If a hyperplane contains $\vec{v}$ and another primitive vector $\vec{w}$, then the vector corresponding to this hyperplane in the dual is in both H_v and H_w, i.e. in a proper subspace of H_v. Conversely, if the vector corresponding to this hyperplane is in no proper subspace, then the hyperplane only intersects the integer lattice in $\vec{v}$ and its multiples, as required. So the problem reduces to this:
Given the vector space $\mathbb{Q}[\alpha]^{d-1}$, show that it contains a vector that cannot be written as a linear combination over $\mathbb{Q}[\alpha]$ of less than $d-1$ integer vectors. We claim that this vector is $\vec{x} = \vec{e_1} + \alpha\vec{e_2} + \ldots + \alpha^{d-2}\vec{e_{d-1}}$, where the $\vec{e_1}$ are the standard basis vectors. To see this, assume we can write it as $\vec{x} = z_1\vec{v_1} + \ldots + z_n\vec{v_n}$, $\vec{v_i} \in \mathbb{Z}^{d-1}$, where $n < d-1$. But this is equivalent to

$$\vec{x} = \begin{pmatrix} 1 \\ \alpha \\ \vdots \\ \alpha^{d-2} \end{pmatrix} = \begin{pmatrix} \vec{v_1} & \vec{v_2} & \cdots & \vec{v_n} \end{pmatrix} \vec{z} = \begin{pmatrix} \vec{v_1} & \vec{v_2} & \cdots & \vec{v_n} \end{pmatrix} Z \begin{pmatrix} 1 \\ \alpha \\ \vdots \\ \alpha^{d-2} \end{pmatrix},$$

where Z is the matrix with Z_{ij} being the coefficient of α^{i-1} in z_j and $\vec{z}$ contains the z_i.
Now since α is of degree $d-1$, the only way this can hold is if the matrix multiplying the vector on the right is the identity, since no other linear relations hold between the $d-1$ entries. But the matrix $\begin{pmatrix} \vec{v_1} & \vec{v_2} & \cdots & \vec{v_n} \end{pmatrix}$ has more rows than columns since $n < d-1$ and hence has no right inverse.

□

Call this enumeration H_i.
Assume there exists an algorithm solving variation V. Now let x_i be an enumeration of the countable set $(\mathbb{Z}\backslash\{0\}) \cup \{\frac{1}{n} |\ n \in \mathbb{Z}\backslash\{0\}\}$. The following algorithm solves the orbit problem for $S, \vec{u}, \vec{v}$:
Run the two following procedures in parallel, while keeping in mind Lemma 8.7:

- Check if any one letter words in S map u to $x_1\vec{v}$. Then check if any two letter words in S map u to $x_1\vec{v}$. Then check if any one letter words in S map $\vec{u}$ to $x_2\vec{v}$. Then check if any three letter words in S map $\vec{u}$ to $x_1\vec{v}$. Then check if any two letter words in S map $\vec{u}$ to $x_2\vec{v}$. Then check if any one letter words in S map $\vec{u}$ to $x_3\vec{v}$. Proceeding in this triangular fashion, this procedure will halt if there exists a $M \in \langle S \rangle$ so that $M\vec{u} = n\vec{v}$ or $\frac{1}{n}\vec{v}$. Not only this, but we will know the value of n. By Lemma 8.7, in this case we can give a correct answer.

- Take the enumeration H_i and run the algorithm solving variation V on each one in order. Halt if the algorithm gives the answer NO for any hyperplane. This procedure halts if if there *does not* exist a $M \in \langle S \rangle$ so that $M\vec{u} = n\vec{v}$ or $\frac{1}{n}\vec{v}$, which is exactly the complementary case of the first procedure. But in this case the correct answer is NO, since $n = 1$ is also impossible.

So this completes the proof that variation V is undecidable. □

We hoped that we could reduce the hyperplane problem in higher dimensions to variation V, for example by mappings such as

$$\phi : \mathbb{Q}[\alpha]^d \to \mathbb{Q}^{d^2-d} \qquad \psi : \mathrm{GL}_d(\mathbb{Q}) \to \mathrm{GL}_{d^2-d}(\mathbb{Q})$$

$$\vec{a_0} + \alpha \cdot \vec{a_1} + \ldots + \alpha^{d-2} \cdot \vec{a_{d-2}} \mapsto \begin{pmatrix} \vec{a_0} \\ \vec{a_1} \\ \vdots \\ \vec{a_{d-2}} \end{pmatrix} \qquad A \mapsto \begin{pmatrix} A & & & \\ & A & & \\ & & \ddots & \\ & & & A \end{pmatrix}$$

It is true that

$$\psi(A)\phi(\vec{u}) = \phi(\vec{v}) \Leftrightarrow A\vec{u} = \vec{v},$$

but $\psi(H)$ is no longer a hyperplane in the vector space of dimension $d^2 - d$.

Open problem. Can we reduce the hyperplane problem to Variation V of the hyperplane problem?

But it turns out that we can still prove the undecidability of the hyperplane problem, even in 6×6 - matrices. The following argument is due to Emmanuel Breuillard.

Lemma 8.9. There exists a free subgroup F_2 of $\mathrm{SL}_2(\mathbb{Z})$ on two generators, that does not contain any nontrivial unipotent elements.

Proof. □

Lemma 8.10. There exists a free subgroup F of $\mathrm{SL}_3(\mathbb{Z})$ on two generators, a rational linear form $f : \mathbb{Q}^3 \to \mathbb{Q}$ and a vector $\vec{u}$ with the property that $\forall g \in F$:

- $f(g\vec{u}) \geq 0$
- $f(g\vec{u}) = 0 \Rightarrow g = 1$

Proof. Consider the double cone in three dimensions given by $x^2 + yz = 0$. We firstly want a free subgroup on two generators of matrices in $\mathrm{SL}_3(\mathbb{Z})$ so that it preserves each of the two cones seperately – this can be constructed by interpreting a vector on the cone as a matrix in $\begin{pmatrix} x & y \\ z & -x \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ with zero determinant and zero trace. Then the conjugation action of $\mathrm{SL}_2(\mathbb{R})$ preserves these two properties, so keeps the vector on the double cone.

Claim. This action even keeps a vector on the same cone.

Proof. The defining feature of one cone is $y > 0, z < 0$ and the other has $y < 0, z > 0$. Now we have

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x & y \\ z & -x \end{pmatrix} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} x' & y' \\ z' & -x' \end{pmatrix}$$
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} dx - cy & ay - bx \\ dz + cx & -bz - ax \end{pmatrix} = \begin{pmatrix} x' & y' \\ z' & -x' \end{pmatrix}$$

Now if $y > 0, z < 0$ and $x^2 = -yz$, we have that

$$y' = a^2y - abx - b^2z - abx = a^2y - 2abx + b^2 \cdot \frac{x^2}{y} = \frac{1}{y}(ay - bx)^2 > 0$$

$$z' = cdx - c^2y + d^2z + cdx = -(c^2y - 2cdx + d^2\frac{x^2}{y}) = -\frac{1}{y}(cy - dx)^2 < 0$$

And the other cone works analogously. □

Similarly as in Theorem 6.11 we can identify this conjugation action (now with one more constraint, since they are in $\mathrm{SL}_2(\mathbb{Z})$) with matrix multiplication in $\mathrm{GL}_3(\mathbb{Z})$. In particular this correspondence can be checked to preserve unipotence, i.e. that all eigenvalues are 1. Now pick any integer vector on the cone, say

$$\vec{u} = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}.$$

We have $Q(\vec{u}) = 0$ for the defining quadratic form of the cone, that is, $Q(\vec{x}) = -(x^2 + yz)$. The associated symmetric bilinear form B is $B(\vec{x}, \vec{y}) = \frac{1}{2}(Q(\vec{x}) + Q(\vec{y}) - Q(\vec{x} - \vec{y}))$.

Note

In fields of characteristic $\neq 2$, so also $\mathbb{Q}$, there is a one-one correspondence of quadratic and symmetric bilinear forms. This is via $Q(\vec{x}) = B(\vec{x}, \vec{x})$ and

$$\begin{aligned} B(\vec{u}, \vec{v}) &= B(\vec{u}, \vec{u}) + B(\vec{u}, \vec{v} - \vec{u}) = Q(\vec{u}) + B(\vec{v} - \vec{u}, \vec{u}) \\ &= Q(\vec{u}) + B(\vec{v} - \vec{u}, \vec{u} - \vec{v}) + B(\vec{v} - \vec{u}, \vec{v}) = \\ &= Q(\vec{u}) - Q(\vec{v} - \vec{u}) + B(\vec{v}, \vec{v}) - B(\vec{u}, \vec{v}) \\ &\Rightarrow B(\vec{u}, \vec{v}) = \frac{1}{2}(Q(\vec{u}) + Q(\vec{v}) - Q(\vec{v} - \vec{u})) \end{aligned}$$

We now claim that the linear form given by $f(\vec{x}) = B(\vec{u}, \vec{x})$ and the hyperplane $H = \{\vec{x} |\ B(\vec{u}, \vec{x}) = 0\}$ are the ones with the required properties. The hyperplane is simply given by

$$\begin{aligned} B(\vec{u}, \vec{x}) &= 0 \\ \frac{1}{2}(Q(\vec{u}) + Q(\vec{x}) - Q(\vec{x} - \vec{u})) &= 0 \\ Q(\vec{x}) &= Q(\vec{x} - \vec{u})) \\ x^2 + yz &= x^2 + (y-1)z \\ z &= 0 \end{aligned}$$

This is precisely the hyperplane tangent to the double cone that contains $\vec{u}$. Let F in the statement of this lemma be the free subgroup of $\mathrm{GL}_3(\mathbb{Q})$ that is associated with the conjugation by the subgroup given by Lemma 8.9. Now we want to check the condition of the lemma. Pick a $g \in F$. Now $f(g\vec{u}) \geq 0$, by the previous calculation, holds iff

$$\begin{aligned} &B(\vec{u}, g\vec{u}) \geq 0 \\ &\Leftrightarrow (g\vec{u})_z \geq 0, \end{aligned}$$

which simply means that it is on the same side of the hyperplane as the cone that $\vec{u}$ is in – but by our above claim we have that always happens for any g, so the first condition is shown.
Now we want to show that if this equals zero, we must have had $g = 1$. If this is zero it means that $g\vec{u}$ is in the hyperplane and on the cone, so it must be a rational multiple of $\vec{u}$. Since the correspondence between g as a 3×3 - matrix and g as a conjugation via $\mathrm{SL}_2(\mathbb{Z})$ preserves eigenvalues, we are looking for an $M \in \mathrm{SL}_2(\mathbb{Z})$ with a rational eigenvalue. But then the other eigenvalue has to be rational as well, and their product is 1, so we can write them as $\frac{p}{q}$ and $\frac{q}{p}$ with coprime $p, q \in \mathbb{Z}$. Now their trace is an integer, so

$$pq | p^2 + q^2 \Rightarrow p | q^2, q | p^2 \Rightarrow p = q = \pm 1.$$

They cannot differ in sign since then the determinant would not be 1. Also they cannot both be -1 since then $\vec{u}$ would be mapped to $-\vec{u}$ which is on the other cone. So we see that g has to be unipotent to map $\vec{u}$ to a rational multiple to itself, but Lemma 8.9 then implies that g is the identity. □

Theorem 8.11. The hyperplane problem for groups is undecidable on $\mathrm{GL}_6(\mathbb{Q})$.

Proof. We reduce it to the membership problem for $F_2 \times F_2$. We are given $g \in F_2 \times F_2$ and $\langle g_1, \ldots, g_m \rangle \leq F_2 \times F_2$. Pick two copies of everything in the previous lemma, say $F_1, F_2, \vec{u_1}, \vec{u_2}$ and f_1, f_2. Write

$$\vec{u} = \begin{pmatrix} \vec{u_1} \\ \vec{u_2} \end{pmatrix}.$$

Let H be the hyperplane defined by the kernel of the linear form $f_1(\vec{u_1}) + f_2(\vec{u_2})$. Now obviously we can embed $F_2 \times F_2$ in $\mathrm{GL}_6(\mathbb{Q})$ via a direct sum of the matrices in F_1, F_2 we had from the previous lemma.
Now we apply the hypothetical algorithm for the hyperplane problem by asking if $\langle g_1, \ldots, g_m \rangle$ maps $g\vec{u}$ to H. By the properties of f, this happens if and only if $g\vec{u}$ can be mapped to $\vec{u}$, or equivalently if

$$g^{-1} \in \langle g_1, \ldots, g_m \rangle \Leftrightarrow g \in \langle g_1, \ldots, g_m \rangle.$$

□

Remark 8.12. In the same way as before the hyperplane (upper-left-corner) problem remains undecidable for 17-generated groups of matrices in $\mathrm{GL}_6(\mathbb{Q})$.

Remark 8.13. By conjugation via permutation matrices we see that the upper-left-corner problem is equivalent to the $(i, i) = 0$ problem, i.e. where we ask if any element on the diagonal vanishes. [19] shows the undecidability of the upper-right-corner problem for matrix semigroups, which we can change by conjugation to any entry of the matrix save the ones of the diagonal.

So this completes the hyperplane problem.

Remark 8.14. Note that our proof above of the undecidability of the hyperplane problem is easily extendable to subspaces of dimension lower than 5, since we just need to make H smaller while still containing $\vec{u}$,, which preserves all of the properties we need.

Definition 8.15. The *subspace problem* asks to find an algorithm deciding for a finitely generated subgroup $\langle S \rangle \subseteq \mathrm{GL}_n(\mathbb{Q})$, a subspace $H \subseteq Q^n$ and a vector $\vec{u}$, if $\exists M \in \langle S \rangle$ with $M\vec{u} \in H$.

This is obviously more difficult than the hyperplane problem, i.e. the latter is a subproblem of it.

Corollary 8.16. The subspace problem is undecidable for 17-generated subgroups of $\mathrm{GL}_6(\mathbb{Q})$.

The orbit problem was originally presented in [10] for groups of matrices. We can ask the same problem for semigroups - since every group is a semigroup, this is a harder problem which is then also undecidable. We restate this for convenience.

Definition 8.17. The *semigroup orbit problem* for a linear semigroup S of dimension n asks for an algorithm which given a finite set of matrices $\{S_1, \ldots, S_k\} \subseteq S$ and two vectors $\vec{u}, \vec{v}$ determines whether $\exists M \in \{S_1, \ldots, S_k\}^+$ with $M\vec{u} = \vec{v}$ or not.

We have discovered a peculiar relationship between the semigroup orbit problem and the subspace problem.

Definition 8.18. We say that a problem A has higher *Turing complexity* than a problem B if a hypothetical algorithm for A can be used to decide B. Conversely, we say that B has lower Turing complexity or that B can be Turing reduced to A.

Note

We do not require A to be decidable! This definition just makes precise the intuition for an undecidable problem to be harder than another undecidable problem.

Theorem 8.19. The semigroup orbit problem for a recursive (thus potentially infinite) set S on $\mathrm{GL}_n(\mathbb{Q})$ has higher Turing complexity than the subspace problem for groups on $\mathrm{GL}_n(\mathbb{Q})$.

Proof. We are given an instance of the subspace problem, i.e. a vector $\vec{u}$, a subspace X and a finite set $S \subseteq \mathrm{GL}_n(\mathbb{Q})$.
Now let K be the recursive semigroup of matrices which projects everything that is not in X to X, and acts as $\mathrm{GL}_{\dim X}(X)$ on X (we just need that its action on X is transitive). Pick a nontrivial vector $\vec{x} \in X$. If none exists, we are done.
Now apply the hypothetical semigroup orbit algorithm on $S' = S \cup S^{-1} \cup K, \vec{x}$ and $\vec{u}$, i.e. we will find out if there exists a matrix in S'^{+} that maps $\vec{x}$ to $\vec{u}$.
If this algorithm says NO, then the answer to the subspace problem must also be NO since otherwise we can map $\vec{u}$ to some $\vec{x'} \in X$, and then via K to $\vec{x}$.

If this algorithm says YES, then there exists a matrix of the form $S_1K_1\cdots S_nK_n$ mapping $\vec{x}$ to $\vec{u}$. But for $\vec{x}\in X$ any vector of the form $S_iK_i(\vec{x})$ is equal to $K_j(\vec{x})$ for some $K_j\in K$ since K acts transitively on X. So we can write $S_mK_m(\vec{x})=\vec{u}$, but since K_m fixes X we see that S_m^{-1} will map $\vec{u}$ into X, so the answer to the subspace problem is YES. □

Open problem. Can we somehow tweak the proof in the previous theorem so we only require the semigroup orbit problem for a finite set S?

9 Free subgroups of SO_3

We were motivated to study this because of the proof of the *Banach-Tarski paradox*. This result shows that it is possible to use the axiom of choice to partition the unit sphere into 5 parts so that we can rotate these parts to get two unit spheres. The classic reference for this is [39]. A key step in the proof is finding a subgroup of SO_3, the group of rotations of the sphere, that is free.

$$r_x^{\pm\alpha}=\begin{pmatrix}1&0&0\\0&\cos\alpha&\mp\sin\alpha\\0&\pm\sin\alpha&\cos\alpha\end{pmatrix}\qquad r_z^{\pm\alpha}=\begin{pmatrix}\cos\alpha&\mp\sin\alpha&0\\\pm\sin\alpha&\cos\alpha&0\\0&0&1\end{pmatrix}$$

are the rotations by an angle α around the x and z axis respectively. We ask for what α we have that $\langle r_x^\alpha, r_z^\alpha\rangle$ is a free group of rank 2.
For the proof of Banach-Tarski we just require the fact that any such value of α exists. [39] proves in Theorem 2.1. that if $\cos\alpha=\frac{1}{3}$, we do get a free group. We are able to extend the idea of their proof, showing a stronger result.

Theorem 9.1. If $\cos\alpha=\frac{2q}{q^2+1}$ for $q\in\mathbb{Q}, q\neq 0,1$ then $\langle r_x^\alpha, r_z^\alpha\rangle$ is a free group of rank 2.

Proof. Let x,y,z be coprime integers with $x^2+y^2=z^2$.. We claim that if $\cos\alpha=\frac{x}{z}$, we get a free group. Then we have

$$r_x^\alpha=\begin{pmatrix}1&0&0\\0&\frac{x}{z}&-\frac{y}{z}\\0&\frac{y}{z}&\frac{x}{z}\end{pmatrix}\qquad r_z^\alpha=\begin{pmatrix}\frac{x}{z}&-\frac{y}{z}&0\\\frac{y}{z}&\frac{x}{z}&0\\0&0&1\end{pmatrix}.$$

Now we want to prove that the vector $\vec{v}=\begin{pmatrix}0\\1\\0\end{pmatrix}$ cannot be mapped to itself by a nontrivial word in r_x^α, r_z^α, so we cannot get the identity, i.e. there is no relation.

Claim. $\vec{v}$ is only mapped to vectors of the form $\frac{1}{z^k}\begin{pmatrix}a\\b\\c\end{pmatrix}$, where $b\not\equiv 0 \pmod z$.

This can be shown by induction, where it turns out that k is the length of the word. If we always pull out a factor of $\frac{1}{z}$ with every additional letter, we can check that we have the mappings

$$\begin{aligned}r_x^\alpha: a&\mapsto a'=za\\ b&\mapsto b'=bx-cy\\ c&\mapsto c'=by+cx\end{aligned}\qquad\begin{aligned}r_x^{-\alpha}: a&\mapsto a'=za\\ b&\mapsto b'=bx+cy\\ c&\mapsto c'=cx-by\end{aligned}$$

$$\begin{aligned}r_z^\alpha: a&\mapsto a'=ax-by\\ b&\mapsto b'=ay+bx\\ c&\mapsto c'=zc\end{aligned}\qquad\begin{aligned}r_z^{-\alpha}: a&\mapsto a'=ax+by\\ b&\mapsto b'=bx-ay\\ c&\mapsto c'=zc\end{aligned}$$

First we can calculate by hand that this is true for words of length 2 or less. The only possibilities we get for b'' are x^2 or x^2-y^2. We know that the former is not divisible by z by assumption. For the latter we see that

$$(x^2-y^2,z)\le(x^2-y^2,z^2)=(x^2-y^2,x^2+y^2)=(x^2+y^2,2x^2)=(x^2+y^2,x^2)=(x^2,y^2)=1$$

where we have used that z is odd (this is because the only quadratic residues mod 4 are 0,1, and if $z^2 \equiv 0(4)$, we could not add to it using two odd squares).
Now we will use induction, fixing a vector $\frac{1}{z^k}\begin{pmatrix} a \\ b \\ c \end{pmatrix}$ with $b \not\equiv 0 \pmod z$ and its successor with $b' \not\equiv 0 \pmod z$ to show that the vector after this has $b'' \not\equiv 0 \pmod z$. This is why we needed to check the *two* length words and not just the one length ones.
Now assume w is a word with length larger than 2. We know that $z|c'$.

- Case 1: $w = r_x^{\pm\alpha} \circ r_z^{\pm\alpha} \circ v$

$$b'' = b'x \pm c'y \equiv b'x \not\equiv 0 \pmod z$$

- Case 2: $w = r_z^{\pm\alpha} \circ r_x^{\pm\alpha} \circ v$, same as above.
- Case 3: $w = r_x^{\pm\alpha} \circ r_x^{\pm\alpha} \circ v$

$$\begin{aligned} b'' &\equiv b'x \mp c'y \equiv xb' \mp (cx \pm by)y = xb' \mp cxy - by^2 = \\ &= xb' + x^2b \mp cxy - b(y^2 + x^2) = xb' + x(xb - cy) - bz^2 \equiv \\ &\equiv xb' + xb' \not\equiv 2xb' \equiv 0 \pmod z \end{aligned}$$

- Case 4: $w = r_z^{\pm\alpha} \circ r_x^{\pm\alpha} \circ v$, same as above.

Now this shows that $\vec{v}$ cannot be mapped to a vector with an integer as the second entry, and in particular not to itself. Now it is well known that we can get a primitive Pythagorean triple (this is even in Euclid's elements) by plugging in coprime m, n with not both of them odd into

$$\begin{aligned} x &= 2mn \\ y &= m^2 - n^2 \\ z &= m^2 + n^2 \end{aligned} \tag{†}$$

Actually we can allow both of them to be odd since we only care about the ratio $\frac{x}{z}$, and dividing both by 2 again yields a primitive triple. So we have seen that for

$$\cos\alpha = \frac{2mn}{m^2+n^2} = \frac{2}{\frac{m}{n} + \frac{n}{m}} = \frac{2q}{q^2+1}$$

for $q = \frac{m}{n}$, we get a free group. We obviously don't allow $m = 0$, nor do we allow $m = n = 1$ since then $y = 0$, and then y, z are not coprime. □

Corollary 9.2. The numbers $\cos\alpha$ for which we get a free group lie dense in $[0, 1]$.

Proof. $\mathbb{Q}$ lies dense in $\mathbb{R}$, and the continuous mapping $q \mapsto \frac{2q}{q^2+1}$ preserves this property. □

We can say more for rational $\cos\alpha$. The following result was sketched to the author by Emmanuel Breuillard.

Lemma 9.3. If $A, B \in \mathrm{SL}_2(\mathbb{C})$, then

$$\operatorname{tr} A = \operatorname{tr} A^{-1} \tag{9.1}$$

$$\operatorname{tr} AB = \operatorname{tr} A \operatorname{tr} B - \operatorname{tr} AB^{-1} \tag{9.2}$$

Interpret F_2 to be the free group on the letters A and B.

Theorem 9.4 (2-generator version of Fricke-Klein)**.** For matrices $A, B \in \mathrm{SL}_2(\mathbb{C})$ and a word $w \in F_2$, we have that $\operatorname{tr} w$ is a polynomial in $\operatorname{tr} A, \operatorname{tr} B$ and $\operatorname{tr} AB$. [14]

Proof. We use induction over the length l of the freely and cyclically reduced w. This is allowed since the trace is unchanged by cyclic permutations. Clearly $l = 1, 2$ is obvious using the relations above. Write $w = A^{m_1}B^{m_2}\cdots A^{m_k}, m_i \in \mathbb{Z}\backslash\{0\}$

- Case 1: $k > 2$.
  Here, by (9.2) we can write

$$\operatorname{tr}(A^{m_1}B^{m_2}\cdots A^{m_k}) = \operatorname{tr} A^{m_1} \operatorname{tr}(B^{m_2}\cdots A^{m_k}) - \operatorname{tr}(A^{m_1-m_k}B^{-m_2}\cdots B^{-m_{k-1}}),$$

  for which k is smaller, so we can assume $k \leq 2$. A similar argument takes care of the case when w ends with a power of B.

- Case 2: $w = A^{m_1}B^{m_2}$, where w.l.o.g. $m_2 \geq 2$.

$$\operatorname{tr}(A^{m_1}B^{m_2}) = \operatorname{tr}(A^{m_1}B^{m_2-1}) \operatorname{tr} B - \operatorname{tr}(A^{m_1}B^{m_2-2}),$$

  and all words on the right hand side have a smaller length than $|m_1| + |m_2|$, so we are done.

- Case 3: $w = A^m$
  Then we can check that $\operatorname{tr} w = T_m(\operatorname{tr} A)$, where $T_0 = 2, T_1 = x, T_m = x \cdot T_{m-1} - T_{m-2}$ are a modified version of the Chebyshev polynomials.

□

We can actually use elements of SO_3 in the theorem above instead of $\mathrm{SL}_2(\mathbb{C})$ because of the following theorem.

Theorem 9.5. SU_2 is a double cover of SO_3. [32]

Proof. This is well known, SU_2 is isomorphic to the group of unit quaterniona, which (modulo sign) correspond to rotations of three dimensional space. □

Lemma 9.6. Assuming $\operatorname{tr} A = \operatorname{tr} B = 2x + 1, \operatorname{tr} AB = 2x + x^2$, the resulting polynomial $\operatorname{tr} w$ in x has

(a) degree l

(b) a leading coefficient that is a power of two.

Proof. For both use induction. For (a), the claim is again obvious for $l = 1, 2$. In case 1 of Theorem 9.4, we see that $|m_1 - m_k| < |m_1| + |m_k|$ given that $-m_1 \neq m_k$, i.e. w is cyclically reduced, so the second term on the right side is actually shorter than $\sum m_i$. The first term will have degree l by induction though, so we are done. Similarly we get Case 2 and 3. For (b), the induction is again started since $l = 1, 2$ is obvious. Since in every case the second term has a smaller degree than the first, the property of having a leading coefficient that is a power of two is preserved. □

Corollary 9.7. If $\cos\alpha$ is rational but not dyadic, then the rotation matrices by α around the x and z axes generate a free group.

Proof. Set

$$A := \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\alpha & -\sin\alpha \\ 0 & \sin\alpha & \cos\alpha \end{pmatrix} \qquad B := \begin{pmatrix} \cos\alpha & -\sin\alpha & 0 \\ \sin\alpha & \cos\alpha & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

we see that we have the conditions of the previous lemma with $x = \cos\alpha$, so if $\cos\alpha$ is a rational root of the resulting polynomial, by the rational roots theorem its denominator must divide the leading coefficient, i.e. be a power of 2. □

Corollary 9.8. If $\cos\alpha$ is transcendental then again the rotation matrices by α around the x and z axes generate a free group.

Proof. Again by the same argument as in the previous lemma, x is a root of an integer polynomial if there is a relation. □

Actually we can show that Corollary 9.7 is strictly better than Theorem 9.1.

Proposition 9.9. No rational number of the form $\frac{2q}{q^2+1}$ is dyadic unless $q = 0, 1$.

Proof. Writing

$$\frac{2q}{q^2+1} = \frac{a}{2^k}$$

is equivalent to saying

$$m^2 + n^2 | 2^k \cdot mn, \tag{9.1}$$

where $k > 2$ and m, n coprime. Now if an odd prime p divides m, then it cannot divide n. But then it doesn't divide $m^2 + n^2$. So in fact no odd prime can divide $m^2 + n^2$, since then by 9.1. it would divide either m or n, a contradiction to the above argument. This means that $m^2 + n^2 = 2^l$, and since m and n are coprime they aren't both even, and then none of them are even, and then $m^2 + n^2 \equiv 2 \pmod 4$. This means that $l = 1$ and $m = n = 1$, but we had removed the possibility of $q = 1$. □

Interestingly, both of these methods can be trumped by the following result from a paper by Swierczkowski [40].

Theorem 9.10. If $\cos\alpha \in \mathbb{Q}\backslash\{0, \pm\frac{1}{2}, \pm 1\}$, then again the rotation matrices by α around the x and z axes generate a free group.

References

[1] Paul C Bell and Igor Potapov. The identity correspondence problem and its applications. In *International Symposium on Algorithms and Computation*, pages 657–667. Springer, 2009.

[2] Nicolas Bergeron. Toute variété de dimension 3 compacte et asphérique est virtuellement de haken. *Séminaire BOURBAKI*, page 66ème, 2014.

[3] Jean Berstel. *Theory of codes Jean Berstel, Dominique Perrin.* Pure and applied mathematics (Academic Press) ; 117. Academic Press, Orlando, 1985.

[4] V. V. Borisov. Simple examples of groups with unsolvable word problem. *Mat. Zametki*, 6:521–532, 1969.

[5] Emmanuel Breuillard. Random groups and related topics [lecture]. University of Cambridge, 2021.

[6] J. L. Britton. Solution of the word problem for certain types of groups i. *Glasgow Mathematical Journal*, 3:68–90, 1956.

[7] Julien Cassaigne, Tero Harju, and Juhani Karhumäki. On the undecidability of freeness of matrix semigroups. *International Journal of Algebra and Computation*, 9(03n04):295–305, 1999.

[8] Julien Cassaigne and François Nicolas. On the decidability of semigroup freeness. *RAIRO-Theoretical Informatics and Applications*, 46(3):355–399, 2012.

[9] Matt Clay. *Office hours with a geometric group theorist / edited by Matt Clay and Dan Margalit.* 2017.

[10] John D Dixon. The orbit-stabilizer problem for linear groups. *Canadian Journal of Mathematics*, 37(2):238–259, 1985.

[11] A. Ehrenfeucht, J. Karhumäki, and G. Rozenberg. The (generalized) post correspondence problem with lists consisting of two words is decidable. *Theoretical Computer Science*, 21(2):119–144, 1982.

[12] Vesa Halava and Tero Harju. Mortality in matrix semigroups. *The American Mathematical Monthly*, 108(7):649, 2001.

[13] Marshall Hall. *The theory of groups.* [s.n.], s.l.], 1959.

[14] Robert D Horowitz. Characters of free groups represented in the two-dimensional special linear group. *Communications on Pure and Applied Mathematics*, 25(6):635–649, 1972.

[15] Ilya Kapovich and Alexei Myasnikov. Stallings foldings and subgroups of free groups. *Journal of algebra*, 248(2):608–668, 2002.

[16] RC Lyndon and JL Ullman. Groups generated by two parabolic linear fractional transformations. *Canadian Journal of Mathematics*, 21:1388–1403, 1969.

[17] Roger C Lyndon. *Combinatorial Group Theory by Roger C. Lyndon, Paul E. Schupp.* Classics in Mathematics. 1st ed. 2001. edition, 2001.

[18] Arnaldo Mandel and Imre Simon. On finite semigroups of matrices. *Theoretical Computer Science*, 5(2):101–111, 1977.

[19] Z Manna. Mathematical theory of computation, 1974.

[20] James McCool. The order problem and the power problem for free product sixth-groups. *Glasgow Mathematical Journal*, 10(1):1–9, 1969.

[21] John Charles Chenoweth McKinsey. The decision problem for some classes of sentences without quantifiers. *The Journal of Symbolic Logic*, 8(3):61–76, 1943.

[22] K A Mihailova. THE OCCURRENCE PROBLEM FOR FREE PRODUCTS OF GROUPS. *Mathematics of the USSR-Sbornik*, 4(2):181–190, feb 1968.

[23] Charles F Miller. *On Group-Theoretic Decision Problems and Their Classification. (AM-68) / Charles F. Miller.* Annals of Mathematics Studies ; 68. 2016.

[24] mmwolf. Lecture on undecidability 8: Post correspondence problem [blog post].

[25] Th Motzkin. From among n conjugate algebraic integers, $n-1$ can be approximately given. *Bulletin of the American Mathematical Society*, 53(2):156–162, 1947.

[26] Alexei Myasnikov, Andrey Nikolaev, and Alexander Ushakov. The post correspondence problem in groups. *Journal of group theory*, 17(6):991–1008, 2014.

[27] Turlough Neary. Undecidability in Binary Tag Systems and the Post Correspondence Problem for Five Pairs of Words. In Ernst W. Mayr and Nicolas Ollinger, editors, *32nd International Symposium on Theoretical Aspects of Computer Science (STACS 2015)*, volume 30 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 649–661, Dagstuhl, Germany, 2015. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik.

[28] Bogdan Nica. Linear groups-malcev's theorem and selberg's lemma. *arXiv preprint arXiv:1306.2385*, 2013.

[29] A Yu Ol'shanskiI. *Geometry of defining relations in groups*, volume 70. Springer Science & Business Media, 2012.

[30] Emil L Post. A variant of a recursively unsolvable problem. *Bulletin of the American Mathematical Society*, 52(4):264–268, 1946.

[31] Eliyahu Rips. Subgroups of small cancellation groups. *Bulletin of the London Mathematical Society*, 14(1):45–47, 1982.

[32] Wulf Rossmann. *Lie groups : an introduction through linear groups / Wulf Rossmann.* Oxford graduate texts in mathematics ; 5. Oxford University Press, Oxford, 2002.

[33] Joseph J. Rotman. *An introduction to the theory of groups / Joseph J. Rotman.* Allyn and Bacon, Boston, Mass. ; London, 3rd ed. edition, 1984.

[34] Arto Salomaa. *Formal languages.* ACM monograph series. Academic Press, New York, 1973.

[35] Arto Salomaa. *Jewels of formal language theory / Arto Salomaa.* Pitman, London, 1981.

[36] A. M Turing. On computable numbers, with an application to the entscheidungsproblem. a correction. *Proceedings of the London Mathematical Society*, s2-43(1):544–546, 1938.

[37] A. M. Turing. The word problem in semi-groups with cancellation. *Annals of Mathematics*, 52(2):491–505, 1950.

[38] B. L. van der Waerden. *Modern algebra / by B.L. van der Waerden ; in part a development from lectures by E. Artin and E. Noether. Vol. 2 / translated from the German edition by Theodore J. Benac.* Frederick Ungar, New York, 1950.

[39] Stan Wagon. *The Banach-Tarski paradox*, volume 24 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, 2012.

[40] S. Świerczkowski. A class of free rotation groups. *Indagationes Mathematicae*, 5(2):221–226, 1994.