

# AUTOMORPHIC ORBITS IN FREE GROUPS: RECENT PROGRESS

VLADIMIR SHPILRAIN

ABSTRACT. In this survey, we describe recent progress on asymptotic properties of various automorphic orbits in free groups. In particular, we address the problem of counting potentially positive elements of a given length. We also discuss complexity (worst-case, average-case, and generic-case) of Whitehead’s automorphism problem and relevant properties of automorphic orbits, including orbit-blocking words.

To Alexei Myasnikov on his special birthday

## 1. INTRODUCTION

In this survey article,  $F_r$  will denote a free group of rank  $r$ . Free groups and their properties are at the core of combinatorial group theory; they have been studied for over 100 years now. Automorphisms of free groups, in particular, proved to be attractive objects of research, bridging group theory, topology, geometry, and dynamics.

Given an element  $u \in F_r$ , by the *automorphic orbit* of  $u$  we mean the set of all automorphic images of  $u$ , i.e., the set  $\{\varphi(u)\}$  where  $\varphi$  runs over all automorphisms of  $F_r$ . Automorphic orbits in free groups were studied by J. H. C. Whitehead in his now classical papers [32] and [33].

Since then, there was a vast amount of research on various properties of automorphic orbits in  $F_r$ . We can single out the research avenue focused on fixed points of automorphisms that was popular in the late 20th century and culminated in a seminal paper by Bestvina and Handel [4].

The early 21st century saw a surge in interactions between group theory and theoretical computer science. Most of these interactions are well covered in the monograph [2], but one particular trend that stands out is emerging interest in complexity of group-theoretic algorithms. This includes not only the “traditional” worst-case complexity but also generic-case and average-case complexity introduced into group theory in [15] and [16], respectively.

In this article, we briefly survey research directions that stemmed from the paper [27]. The main theme is complexity of Whitehead’s problem (Section 3) that led to exciting progress on orbit-blocking words (Section 2). Then, there are automorphic orbits of potentially positive elements (Section 4); these, too, saw remarkable progress recently.

In Section 5, we consider pairs of elements of  $F_r$  that have “similar” automorphic orbits; elements like that are called (boundedly) translation equivalent following [14]. Somewhat surprisingly, there was no progress on characterizing or recognizing (boundedly) translation equivalent elements in the last 15 years or so, but we include this problem here in the hope that the right tools to attack it will eventually be found.

Another interesting direction (not covered in the present survey) is studying intersection of the automorphic orbit of a given element of  $F_r$  with a given subgroup or a rational subset of  $F_r$ , see [30]. This is also relevant to potential positivity, see our Section 4.

Finally, we note that sometimes the words “automorphic orbit” mean something different (smaller), see e.g. [5] or [31]. Namely, given an element  $u \in F_r$  and an automorphism  $\varphi$  of  $F_r$ , an automorphic orbit is defined as the set  $\{\varphi^n(u), n = 1, 2, \dots\}$ . This, too, leads to various interesting questions that are not in the scope of the present survey.

## 2. ORBIT-BLOCKING WORDS

Let  $F_r$  be a free group generated by  $x_1, \dots, x_r$ . For a given element  $w \in F_r$ , we say that a word  $v$  is  $w$ -orbit-blocking (or just orbit-blocking if  $w$  is clear from the context) if for any automorphism  $\varphi \in \text{Aut}(F_r)$ , the word  $v$  is not a subword of the cyclic reduction of  $\varphi(w)$ .

*Primitivity-blocking* words are the same as  $x_1$ -orbit-blocking. The existence of primitivity-blocking words easily follows from Whitehead’s observation that the Whitehead graph of any cyclically reduced primitive element is either disconnected or has a cut vertex.

The *Whitehead graph*  $\text{Wh}(w)$  of  $w \in F_r$  has  $2r$  vertices that correspond to the generators  $x_i$  and their inverses. For each occurrence of a subword  $x_i x_j$  in the word  $w \in F_r$ , there is an edge in  $\text{Wh}(w)$  that connects the vertex  $x_i$  to the vertex  $x_j^{-1}$ ; if  $w$  has a subword  $x_i x_j^{-1}$ , then there is an edge connecting  $x_i$  to  $x_j$ , etc. There is one more edge (the external edge): this is the edge that connects the vertex corresponding to the last letter of  $w$  to the vertex corresponding to the inverse of the first letter.

It was observed by Whitehead himself in his *cut vertex lemma* (see [33]) that the Whitehead graph of any cyclically reduced primitive element  $w$  is either disconnected or has a cut vertex, i.e., a vertex that, having been removed from the graph together with all incident edges, increases the number of connected components of the graph. A short and elementary proof of this result was recently given in [11], and a more general case of primitive elements in subgroups of  $F_r$  was recently treated in [1].

Thus, for example, if the Whitehead graph of  $w$  (without the external edge) is complete (i.e., any two vertices are connected by at least one edge), then  $w$  is primitivity-blocking because in this case, if  $w$  is a subword of  $u$ , then the Whitehead graph of  $u$ , too, is complete and therefore is connected and does not have a cut vertex. Here are some examples of primitivity-blocking words:  $x_1^n x_2^n \cdots x_r^n x_1$  (for any  $n \geq 2$ ),  $[x_1, x_2][x_3, x_4] \cdots [x_{n-1}, x_n] x_1^{-1}$  (for an even  $n$ ), etc. Here  $[x, y]$  denotes  $x^{-1} y^{-1} x y$ .

In [13], it was shown that for any  $w \in F_2$ , there are  $w$ -orbit-blocking words. This was based on an explicit description of bases (equivalently, of automorphisms) of  $F_2$  from [7]. Then, in [21], the following general result was established:

**Theorem 1.** *Let  $w \in F_r$  have cyclically reduced length  $\ell$ . Let  $\{v_i\}_{i=1}^{\ell+1}$  be a sequence of primitivity-blocking words such that there is no cancellation between adjacent terms of the sequence, nor between  $v_{\ell+1}$  and  $v_1$ . Then  $\prod_{i=1}^{\ell+1} v_i$  is  $w$ -orbit-blocking.*

Note that, interestingly,  $w$ -orbit-blocking words described in Theorem 1 depend on the length of  $w$  but not on the actual  $w$ .

As can be seen from the statement of Theorem 1, primitivity-blocking words play an important role, so we are going to discuss them separately.

**2.1. Primitivity-blocking words.** By definition, primitivity-blocking words are those that cannot be subwords of any *cyclically reduced* primitive elements. What is needed to prove Theorem 1 is words with somewhat stronger property: they cannot be subwords even of some primitive elements that are not cyclically reduced.

**Definition 2.1.** *Call a basis of  $F_r$  strongly reduced if there is no element  $g \in F_r$  such that conjugating each element of the basis by  $g$  decreases the sum of the lengths of the basis elements.*

Then there is the following technical result of independent interest.

**Lemma 2.2.** [21] *Let  $B$  be a strongly reduced basis of  $F_r$ . Then no primitivity-blocking word appears as a subword of any element in  $B$ .*

Even though Lemma 2.2 suffices to prove Theorem 1, it can be generalized further.

**Definition 2.3.** *Call a basis  $B$  weakly reduced if there is no letter  $p$  such that every element of  $B$  begins with  $p$  and ends with  $p^{-1}$ .*

Then we have:

**Lemma 2.4.** [21] *Let  $B$  be a weakly reduced basis of  $F_r$ , where  $r \geq 3$ , and let  $w \in B$ . Then  $w$  does not contain any primitivity-blocking subwords.*

Note that in  $F_2$ , a weakly reduced basis can contain a primitivity-blocking word. For instance, the basis  $\{x_1x_2x_1^{-1}, x_2x_1^{-1}\}$  is weakly reduced, but contains  $x_1x_2x_1^{-1}$ , which is primitivity-blocking in  $F_2$ .

Then, to show that blocking primitivity does not have to be due to connectivity properties of the Whitehead graph, we include the following examples.

**Proposition 2.5.** [21] **(a)** *In the group  $F_2$ , the words  $x_1^kx_2^k$  are primitivity-blocking for any  $k \geq 2$ .*

**(b)** *In the group  $F_r$ ,  $r \geq 3$ , the words  $x_1^k \dots x_r^k$  are not primitivity-blocking for any  $k \geq 1$ .*

Part (b) of Proposition 2.5 can be generalized as follows:

**Proposition 2.6.** [21] *Let  $F_r$  where  $r \geq 3$  be generated by the set  $X \sqcup Y$ . Let  $\langle X \rangle$  and  $\langle Y \rangle$  denote the subgroups of  $F_r$  generated by  $X$  and  $Y$ , respectively. Let  $w = w_Xw_Y$ , where  $w_X \in \langle X \rangle$ ,  $w_Y \in \langle Y \rangle$ . Then  $w$  is not a primitivity-blocking word.*

We note that the shortest primitivity-blocking word in  $F_2$  is  $x_1^{-1}x_2x_1$ . The Whitehead graph (with or without the external edge) of this word does have a cut vertex though.

It is natural then to look for the shortest primitivity-blocking words in  $F_r$  for  $r > 2$ .

**Theorem 2.** [21] *The word  $w = x_1x_2x_3 \dots x_{r-1}x_r^2x_{r-1} \dots x_3x_2x_1^{-1} \in F_r$  is the shortest primitivity-blocking word for  $r > 2$ .*

A similar word  $w = x_1x_2 \dots x_{r-1}x_r^2x_{r-1} \dots x_2x_1$  is not primitivity-blocking in any  $F_r$ ,  $r \geq 2$ . Indeed, for  $r = 2$ ,  $w$  is a subword of  $x_2x_1x_2^2x_1$ , which is a cyclically reduced primitive word.

For  $r > 2$ , let  $u = x_2x_3 \dots x_{r-1}x_r^2x_{r-1} \dots x_3x_2$ . Consider the word  $v = ux_1ux_1x_3$ . This  $v$  clearly contains  $w$  as a subword and is cyclically reduced. Apply the automorphism  $\varphi = x_1 \mapsto u^{-1}x_1, x_i \mapsto x_i, i \geq 2$ . Then  $\varphi(v) = x_1^2x_3$  is a primitive element, and therefore so is  $v$ .

Finally, we mention that primitivity-blocking words in  $F_2$  can be algorithmically recognized. For  $F_r, r > 2$ , the problem is open.

**Theorem 3.** [21] *There is an algorithm that decides, for a given word  $u \in F_2$  of length  $n$ , whether or not  $u$  is primitivity-blocking and has the worst-case time complexity  $O(n^2)$ .*

## 3. WHITEHEAD'S AUTOMORPHISM PROBLEM

Let  $F_r$  be a free group with a free generating set  $x_1, \dots, x_r$ . Whitehead's automorphism problem is: given  $u, v \in F_r$ , decide whether or not  $v$  is an automorphic image of  $u$ . The problem is solved by *Whitehead's algorithm* that dates back to 1936 [32]:

(1) First reduce  $u$  to a word of minimal possible length by applying "elementary" Whitehead automorphisms. The same for  $v$ . This part is "greedy" and has quadratic time complexity with respect to the length of the input.

(2) If the reduced words are not of the same length, then  $u$  and  $v$  are not in the same automorphic orbit. If they are of the same length, then things get interesting (in terms of complexity). Indeed, the procedure outlined in the original paper by Whitehead suggested this part of the algorithm to be of exponential time with respect to the length of the words since it involves going through all images of a given  $u$ , having the same length as  $u$  does, under elementary Whitehead automorphisms. This raises a natural question about the maximum possible number of elements of length  $m$  in the automorphic orbit of  $u$ .

Thus, a challenging open problem is:

**Problem 1.** *What is the worst-case time complexity of the second part of Whitehead's algorithm?*

In  $F_2$ , the worst-case time complexity was shown to be at most quadratic [27]. Actually, if the length of  $u \in F_2$  is  $m$  and it cannot be reduced by any Whitehead automorphism, then the maximum possible number of elements of length  $m$  in the automorphic orbit of  $u$  is precisely  $8m - 40$  for  $m \geq 10$ , see [18].

In  $F_3$ , the maximum number is  $48m^3 - 480m^2 + 1104m - 672$  for  $m \geq 11$  as suggested (but not proved) by C. Sims based on computer experiments. A particular Whitehead-reduced word of length  $m$  whose automorphic orbit (limited to elements of length  $m$ ) has the cardinality given by the latter polynomial is  $u = x_1^k x_2 x_1 x_2^{-1} x_1 x_2^2 x_3^2$ , where  $k = m - 8$ .

Let  $A(u)$  denote the set of elements  $\{v \in F_r; |v| = |u|, \varphi(v) = u \text{ for some } \varphi \in \text{Aut}(F_r)\}$ . D. Lee [22] came close to solving Problem 1 completely. Specifically, she proved that the cardinality of  $A(u)$  is bounded by a polynomial function of  $|u|$  under the following condition: If two letters  $x_i$  (or  $x_i^{-1}$ ) and  $x_j$  (or  $x_j^{-1}$ ) with  $i < j$  occur in  $u$ , then the total number of  $x_i^{\pm 1}$  occurring in  $u$  is strictly less than the total number of  $x_j^{\pm 1}$  occurring in  $u$ .

Then, D. Lee [23] proved that, under the same assumption on  $u$ , the cardinality of  $A(u)$  is bounded by a polynomial function of  $m = |u|$  of degree  $2r - 3$ , and that this bound is sharp.

We can therefore make Problem 1 somewhat more specific:

**Problem 2.** *Let  $u$  be a Whitehead-reduced word of length  $m$ , and let  $A(u)$  be the set of automorphic images of  $u$  that have length  $m$ . Is the cardinality of  $A(u)$  bounded by a polynomial function of  $m$ ?*

**3.1. Generic-case and average-case complexity of Whitehead's problem.** Informally, generic-case complexity of an algorithm is complexity on "most" inputs, or on "random" inputs. For a formal treatment, see [15].

Generic-case complexity of the classical Whitehead's algorithm (see above) is linear, as shown in [17]. The reason is that for a word  $u$  selected uniformly at random from the set of elements of length  $n$  in  $F_r$ , applying any Whitehead's automorphism (except permutations on the set of generators and their inverses) increases the length of  $u$  with probability  $1 - O(2^{-n})$ .

To get a meaningful (e.g. subexponential) estimate of the average-case complexity of Whitehead’s problem, one has to get a more precise (than just “exponential”) upper bound on the worst-case complexity. It may be then possible to get a subexponential bound on the average-case complexity of Whitehead’s problem without getting a subexponential bound on the worst-case complexity.

In [29], [13], [21], the following variant of Whitehead’s problem was considered: given a fixed  $u \in F_r$ , decide, on an input  $v \in F_r$  of length  $n$ , whether or not  $v$  is an automorphic image of  $u$ . Thus, in this variant the input consists of just one word.

It turns out that the average-case complexity of this version of the Whitehead problem is constant if the input  $v$  is a cyclically reduced word. For a formal definition of the average-case complexity of an algorithm in the context of group theory we refer the reader to [16].

The algorithm with constant average-case complexity from [21] is a combination of two different algorithms running in parallel: one is fast but may be inconclusive, whereas the other one is conclusive but relatively slow. This idea has been used for group-theoretic algorithms since at least [16].

Before running the two algorithms, a pre-computation would be performed on  $u$ . Specifically,  $u$  is reduced to an element of minimum length in its automorphic orbit. This takes worst-case quadratic time in  $|u|$ . However, since  $u$  is a fixed word, this amounts to constant time for the algorithm. Denote the obtained element of minimum length in the orbit of  $u$  by  $\bar{u}$ . Once the word’s length has been minimized, the two algorithms will be run in parallel on the result.

A fast algorithm  $\mathcal{T}$  would detect a  $\bar{u}$ -orbit-blocking subword  $B(\bar{u})$  of a (cyclically reduced) input word  $v$ , as follows. Let  $n$  be the length of  $v$ . The algorithm  $\mathcal{T}$  would read the initial segments of  $v$  of length  $k$ ,  $k = 1, 2, \dots$ , adding one letter at a time, and check if this initial segment has  $B(\bar{u})$  as a subword. This takes time bounded by  $C \cdot k$  for some constant  $C$ , see e.g. [19, p. 338].

The “usual” Whitehead algorithm, call it  $\mathcal{W}$ , would minimize  $|v|$  taking time quadratic in  $|v|$ . Denote the obtained element of minimum length in the orbit of  $v$  by  $\bar{v}$ . If  $|\bar{v}| \neq |\bar{u}|$ , then  $\mathcal{W}$  stops and reports that  $v$  is not in the automorphic orbit of  $u$ . If  $|\bar{v}| = |\bar{u}|$ , then the algorithm  $\mathcal{W}$  would apply all possible sequences of elementary Whitehead automorphisms that do not change the length of  $\bar{v}$  to see if any of the resulting elements are equal to  $\bar{u}$ . This part may take exponential time in  $|\bar{v}| = |\bar{u}|$ , but since we consider  $|u|$  constant with respect to  $|v|$  and  $|u|$  bounds  $|\bar{u}|$  above, exponential time in  $|\bar{u}|$  is still constant with respect to  $|v|$ . Thus, the total time that the algorithm  $\mathcal{W}$  takes is quadratic in  $|v|$ .

Finally, the algorithm  $\mathcal{A}$  will consist of the algorithms  $\mathcal{T}$  and  $\mathcal{W}$  running in parallel. Then we have:

**Theorem 1.** [21] *Suppose possible inputs of the above algorithm  $\mathcal{A}$  are cyclically reduced words that are selected uniformly at random from the set of cyclically reduced words of length  $n$ . Then the average-case time complexity (i.e., the expected runtime) of the algorithm  $\mathcal{A}$ , working on a classical Turing machine, is  $O(1)$ , a constant that does not depend on  $n$ . If one uses the “Deque” (double-ended queue) model of computing [9] instead of a classical Turing machine, then the “cyclically reduced” condition on the input can be dropped.*

## 4. POTENTIALLY POSITIVE ELEMENTS

An element  $u$  of  $F_r$  is called *positive* if no  $x_i$  occurs in  $u$  to a negative exponent. An element  $u$  is called *potentially positive* if  $\alpha(u)$  is positive for some automorphism  $\alpha$  of the group  $F_r$ .

An element  $u$  is called *stably potentially positive* if  $\alpha(u)$  is positive for some automorphism  $\alpha$  of the group  $F_n$  for some  $n \geq r$ . (Here we tacitly assume that  $F_r$  is canonically embedded in  $F_n$ .)

Motivation for considering potentially positive elements comes from the fact that various properties of one-relator groups are easier to establish if the relator is a positive word. For example, Baumslag [3] showed that one-relator groups with a positive relator are residually solvable, and Wise [34] showed that one-relator groups with a positive relator (satisfying a small cancellation condition) are residually finite. All these properties obviously hold upon replacing “positive” with “potentially positive” or even “stably potentially positive”.

Clark and Goldstein [6] proved that all stably potentially positive elements are potentially positive.

Goldstein [10] and D. Lee [26] offered (exponential time) algorithms for deciding potential positivity in  $F_2$ . Another algorithm was offered by Silva and Weil [30].

Recently, Koch-Hyde, O’Connor, and Olive [20] reported an algorithm with the worst-case time complexity  $O(n^2)$ . This algorithm has linear generic-case complexity. If inputs are cyclically reduced, then the average-case complexity of this algorithm is constant. This is because, as shown in [20], there are potential positivity-blocking words in  $F_2$ , i.e., words that cannot be subwords of any potentially positive word. An example would be  $xyx^{-1}y^{-1}x$ .

A very interesting and challenging question is: how many potentially positive elements of length  $n$  are there in  $F_r$ ?

The set of positive elements is exponentially negligible in the set of potentially positive elements because any element with only positive occurrences of all but one of the generators is potentially positive. (Note that the number of positive elements of length  $n$  in  $F_r$  is  $r^n$ , whereas the total number of elements of length  $n$  is  $2r \cdot (2r - 1)^n$ .)

The number of potentially positive elements of length  $n$  is bounded from below by the number of elements of length  $n$  with only positive occurrences of all but one of the generators. The latter number is  $> \left(\frac{r^2+2r-1}{r+1}\right)^n$ .

For  $r > 3$ , a larger lower bound is provided by the number of primitive elements of length  $n$ , which is  $O(n(2r - 3)^n)$  by [28].

Recently, [8] obtained a tight estimate for the growth rate in the case  $r = 2$  by proving that the number of potentially positive elements of length  $n$  in  $F_2$  is  $O((\lambda + \epsilon)^n)$  for any  $\epsilon > 0$ , where  $\lambda \approx 2.505$  is the largest root of the polynomial  $\lambda^4 - 3\lambda^3 + \lambda^2 + \lambda - 1$ .

Summing up, we ask:

**Problem 3.** *Let  $P(r, n)$  denote the number of potentially positive elements of length  $n$  in  $F_r$ . What is the growth of  $P(r, n)$  as a function of  $n$ , with  $r$  fixed ?*

## 5. TRANSLATION EQUIVALENCE

Two elements  $u, v$  of a free group  $F_r$  are called *translation equivalent* if for every free and discrete isometric action of  $F_r$  on an  $\mathbb{R}$ -tree, translation lengths of  $u$  and  $v$  are equal.

A purely combinatorial characterization of translation equivalence was given in [14]: elements  $u, v$  are translation equivalent if the cyclic length of  $\varphi(u)$  equals the cyclic length of  $\varphi(v)$  for every automorphism  $\varphi$  of the group  $F_r$ .

A ramification of this definition is: two elements  $u, v$  are called *boundedly translation equivalent* if the ratio of the cyclic lengths of  $\varphi(u)$  and  $\varphi(v)$  is bounded away from 0 and from  $\infty$  when  $\varphi$  runs through all automorphisms of  $F_r$ .

It is natural to ask:

**Problem 4.** *Is there an algorithm which, when given two elements of a finitely generated free group, decides whether or not they are (boundedly) translation equivalent?*

It is not quite trivial to even produce examples of (boundedly) translation equivalent elements. In [14], it was shown that in  $F_2$ , any  $u(x, y)$  is translation equivalent to  $u(x, y)$  read backwards.

Another source of translation equivalent elements comes from *character equivalence*. We say that  $u$  and  $v$  are *trace equivalent* or *character equivalent* if for every representation  $\alpha : F_r \rightarrow SL_2(\mathbb{C})$  one has  $\text{tr}(\alpha(u)) = \text{tr}(\alpha(v))$ . Character equivalent words come from the so-called “trace identities” in  $SL_2(\mathbb{C})$  and are quite plentiful (see, for example, [12]).

D. Lee showed [24] that whenever  $g$  is translation equivalent to  $h$  in  $F_r$  and  $w(x, y)$  is arbitrary, one has  $w(g, h)$  translation equivalent to  $w(h, g)$  in  $F_r$ . She also reported an algorithm that decides translation equivalence in  $F_2$ .

In [25], D. Lee offered an algorithm that decides bounded translation equivalence in  $F_2$ .

Surprisingly, there has not been any progress on (bounded) translation equivalence since then.

## REFERENCES

- [1] D. Ascari, *A fine property of Whitehead’s algorithm*, Groups Geom. Dyn. **18** (2024), 235–264.
- [2] F. Bassino, I. Kapovich, M. Lohrey, A. Myasnikov, C. Nicaud, A. Nikolaev, I. Rivin, V. Shpilrain, A. Ushakov, P. Weil, *Complexity and Randomness in Group Theory: GAGTA Book 1*. Walter de Gruyter, 2020.
- [3] G. Baumslag, *Positive one-relator groups*, Trans. Amer. Math. Soc. **156** (1971), 165–183.
- [4] M. Bestvina and M. Handel, *Train tracks and automorphisms of free groups*, Ann. of Math. **135** (1992), 1–53.
- [5] P. Brinkmann, *Detecting automorphic orbits in free groups*, J. Algebra **324** (2010), 1083–1097.
- [6] A. Clark and R. Goldstein, *Stability of numerical invariants in free groups*, Comm. Algebra **33** (2005), 4097–4104.
- [7] M. Cohen, W. Metzler, A. Zimmermann, *What does a basis of  $F(a, b)$  look like?*, Math. Ann. **257** (1981), 435–445.
- [8] E. Dinowitz, L. Koch-Hyde, S. O’Connor, E. Olive, *Growth of potentially positive elements in the free group on two generators*, preprint.
- [9] *Double-ended queue*, Wikipedia (2024), [https://en.wikipedia.org/w/index.php?title=Double-ended\\_queue&oldid=1225841227](https://en.wikipedia.org/w/index.php?title=Double-ended_queue&oldid=1225841227)
- [10] R. Goldstein, *An algorithm for potentially positive words in  $F_2$* , Contemp. Math. Amer. Math. Soc. **421** (2006), 157–168.
- [11] M. Heusener, R. Weidmann, *A remark on Whitehead’s cut-vertex lemma*, J. Group Theory **22** (2019), 15–21.
- [12] R. Horowitz, *Characters of free groups represented in the two-dimensional special linear group*, Comm. Pure Appl. Math. **25** (1972), 635–649.
- [13] L. Hyde, S. O’Connor, V. Shpilrain, *Orbit-blocking words and the average-case complexity of Whitehead’s problem in the free group of rank 2*, J. Group Theory **28** (2025), 423–430.

- [14] I. Kapovich, G. Levitt, P. Schupp, V. Shpilrain, *Translation equivalence in free groups*, Trans. Amer. Math. Soc. **359** (2007), 1527–1546.
- [15] I. Kapovich, A. G. Myasnikov, P. Schupp, V. Shpilrain, *Generic-case complexity, decision problems in group theory and random walks*, J. Algebra **264** (2003), 665–694.
- [16] I. Kapovich, A. G. Myasnikov, P. Schupp, V. Shpilrain, *Average-case complexity and decision problems in group theory*, Advances in Math. **190** (2005), 343–359.
- [17] I. Kapovich, P. Schupp, V. Shpilrain, *Generic properties of Whitehead’s algorithm and isomorphism rigidity of random one-relator groups*, Pacific J. Math. **223** (2006), 113–140.
- [18] B. Khan, *The structure of automorphic conjugacy in the free group of rank 2*, Contemp. Math. Amer. Math. Soc. **349** (2004), 115–196.
- [19] D. Knuth, J. H. Morris, V. Pratt, *Fast pattern matching in strings*, SIAM Journal on Computing **6** (2) (1977), 323–350.
- [20] L. Koch-Hyde, S. O’Connor, E. Olive, *A new algorithm for determining potential positivity in the free group of rank 2*, Int. J. Alg. Comput., to appear.
- [21] L. Koch-Hyde, S. O’Connor, E. Olive, V. Shpilrain, *Orbit-blocking words in free groups*, J. Group Theory **29** (2026), 335–350.
- [22] D. Lee, *Counting words of minimum length in an automorphic orbit*, J. Algebra **301** (2006), 35–58.
- [23] D. Lee, *A tighter bound for the number of words of minimum length in an automorphic orbit*, J. Algebra **305** (2006), 1093–1101.
- [24] D. Lee, *Translation equivalent elements in free groups*, J. Group Theory **9** (2006), 809–814.
- [25] D. Lee, *An algorithm that decides translation equivalence in a free group of rank two*, J. Group Theory **10** (2007), 561–569.
- [26] D. Lee, *On several problems about automorphisms of the free group of rank two*, J. Algebra **321** (2009), 167–193.
- [27] A. G. Myasnikov, V. Shpilrain, *Automorphic orbits in free groups*, J. Algebra **269** (2003), 18–27.
- [28] D. Puder, C. Wu, *Growth of primitive elements in free groups*, J. London Math. Soc. **90** (2014), 89–104.
- [29] V. Shpilrain, *Average-case complexity of the Whitehead problem for free groups*, Comm. Algebra **51** (2023), 799–806.
- [30] P. V. Silva, P. Weil, *Automorphic orbits in free groups: words versus subgroups*, Int. J. Algebra Comput. **20** (2010), 561–590.
- [31] E. Ventura, *Group-theoretic orbit decidability*, Groups Complex. Cryptol. **6** (2014), 133–148.
- [32] J. H. C. Whitehead, *On equivalent sets of elements in free groups*, Ann. of Math. **37** (1936), 782–800.
- [33] J. H. C. Whitehead, *On certain sets of elements in a free group*, Proc. London Math. Soc. **41** (1936), 48–56.
- [34] D. Wise, *The residual finiteness of positive one-relator groups*, Comment. Math. Helv. **76** (2001), 314–338.

DEPARTMENT OF MATHEMATICS, THE CITY COLLEGE OF NEW YORK, NEW YORK, NY 10031  
 Email address: shpilrain@yahoo.com