The monomorphism problem in free groups

L. Ciobanu and A. Ould Houcine

Abstract

Let F be a free group of finite rank. We say that the monomorphism problem in F is decidable if there is an algorithm such that, for any two elements u and v in F, it determines whether there exists a monomorphism of F that sends u to v. In this paper we show that the monomorphism problem is decidable and we provide an effective algorithm that solves the problem.

2000 Mathematics Subject Classification: 20E05, 68Q25.
Key words: free groups, decision problems, complexity of algorithms.

1 Introduction

Let F be a free group of finite rank. Given two elements u and v in F, one can formulate the following natural decision problems. Is there an algorithm that determines whether there is a homomorphism $\phi : F \to F$ such that $\phi(u) = v$? If we require ϕ to be an automorphism, we call the decision problem the automorphism problem in free groups, and similarly define the endomorphism and the monomorphism problems. In the case of the automorphism problem, the question has been answered positively by Whitehead in 1936 [10] and his algorithm is one of the most important and useful tools when computing in free groups and beyond. Answering the endomorphism problem is equivalent to solving an equation in free groups in which the variables and constants appear on different sides of the equality. Thus the solvability of the endomorphism problem in free groups is a consequence of Makanin's algorithm [5].

Answering the monomorphism problem is equivalent to deciding if the following infinite system

$$u(X_1, \ldots, X_n) = v(x_1, \ldots, x_n) \tag{1}$$

$$\bigwedge_{w \in W} w(X_1, \ldots, X_n) \neq 1, \tag{2}$$

has a solution in F, where $x_1, \ldots, x_n$ form a basis of F and W is the set of nontrivial reduced words in F. The existence of a solution of the infinite system in (1)-(2) can be expressed as an existential sentence in the language $\mathcal{L}_{\omega_1\omega}$, where $\mathcal{L}$ denotes the usual language of groups and $\mathcal{L}_{\omega_1\omega}$ is built, roughly speaking, from $\mathcal{L}$ by allowing infinite conjunctions and disjunctions of formulas. Thus the solvability of the monomorphism problem in free groups can be seen as the problem of deciding the truth of a subset of the set of existential sentences of $\mathcal{L}_{\omega_1\omega}$ in F.

It is worth pointing out that when $n = 2$ the system (2) is equivalent to $[X_1, X_2] \neq 1$ and thus the monomorphism problem in this case is reduced to the decidability of the existential theory of F. However, for $n \geq 3$, the infinite system in (2) is not equivalent to a finite subsystem and thus the same method cannot be used to reduce the problem to the decidability of the existential theory of F.

Also note that while being in the same automorphic orbit is an equivalence relation between words, being an endomorphic or monomorphic image is not symmetric: for example, while there exists a monomorphism sending x_1 to x_1^2, there is no monomorphism sending x_1^2 to x_1. In this paper we give a positive answer to the monomorphism problem in free groups. We provide an algorithm that is polynomial in the lengths of u and v, except for parts that involve the Whitehead algorithm, which is conjectured to be polynomial, but this has not yet been proven.

2 Preliminaries

Let $F = F_n$ be a free group of rank $n \geq 2$ with free generating set $A = \{x_1, \ldots, x_n\}$, viewed as the fundamental group of the wedge of n circles. This naturally leads to working with graphs. All graphs considered here are going to be oriented and finite (unless otherwise stated).

Let H be a finitely generated subgroup of rank m of the free group F, and let X_H be the corresponding covering space of the wedge of n circles (infinite except when H has finite index in F). That is, vertices of X_H are cosets, $V(X_H) = \{Hx \mid x \in F\}$, and edges are of the form (Hx, a) going from Hx to Hxa, for all $x \in F$ and $a \in A$. Note that X_H is an A-labeled oriented graph, with a distinguished basepoint $* = H1$, and with every vertex being the initial vertex (and the terminal vertex as well) of exactly n edges, labeled by the n symbols in A (see [2] for more details).

The *core* of H, denoted C_H, is the smallest subgraph of X_H containing the basepoint $*$, and having fundamental group H. So all vertices in C_H have degree at least two except possibly $*$ and, since H is finitely generated, C_H is a finite graph. Like X_H, the graph C_H is an A-labeled oriented graph, with every vertex being the initial vertex (and the terminal vertex) of at most n edges, labeled by pairwise different letters in A.

We will later make use of some particular type of graphs, which we call topological graphs.

Definition 2.1. A *topological graph* of rank m is a finite graph with a distinguished vertex $*$ in which all vertices have degree at least 3 except possibly $*$, and whose fundamental group is the free group F_m of rank m. Let $Top(m)$ be the set of topological graphs of rank m.

It is worth pointing out that, if H is a finitely generated subgroup of F, then one can associate to H a topological graph obtained from C_H by deleting all vertices of C_H of degree 2 (except $*$). The next lemma provides some basic information about the set $Top(m)$.

Lemma 2.2. *The set $Top(m)$ is finite, the number of edges in a topological graph of rank m is at most $3m - 1$ and the number of vertices at most $2m$.*

Proof. Let Γ be a topological graph of rank m. The Euler characteristic formula gives $|E(\Gamma)| - |V(\Gamma)| + 1 = m$, where $|E(\Gamma)|$ and $|V(\Gamma)|$ are the number of edges and vertices of Γ, respectively. This can be rewritten as

$$\frac{\sum_{v \in V(\Gamma)} (\deg(v) - 2)}{2} + 1 = \frac{\sum_{v \in V(\Gamma)} \deg(v)}{2} - |V(\Gamma)| + 1 = m.$$

Set $V(\Gamma)^* = V(\Gamma) \setminus \{*\}$. Then

$$2(m-1) = \sum_{v \in V(\Gamma)^*} (\deg(v) - 2) + (\deg(*) - 2),$$

so Γ has at most $2m$ vertices since $\deg(v) - 2 \geq 1$ for all $v \in V(\Gamma)^*$ and $\deg(*) - 2 \geq -1$. A consequence of this is that $|E(\Gamma)| = m + |V(\Gamma)| - 1 \leq m + 2m - 1 = 3m - 1$.

Since $Top(m)$ is a set of graphs with a bounded number of vertices and edges, this set is finite. □

In our main result we will need the notion of a Nielsen-reduced set, which is defined as follows. Let $|u|$ denote the length of a word u in F with respect to the basis A. A subset $U \subseteq F \setminus \{1\}$ is called *Nielsen-reduced* if for any $v_1, v_2, v_3 \in U^{\pm 1}$ the following conditions hold:

1. $v_1 v_2 \neq 1$ implies $|v_1 v_2| \geq |v_1|, |v_2|$,
2. $v_1 v_2 \neq 1$ and $v_2 v_3 \neq 1$ implies $|v_1 v_2 v_3| > |v_1| - |v_2| + |v_3|$.

Such a set has some very desirable properties. Let H be a subgroup of F generated by a Nielsen-reduced set U. Then

1. H is free with U as a basis [4, Proposition 2.5, Ch I],
2. if $w \in H$ has the form $w = u_1 u_2 \dots u_t$ where each $u_i \in U^{\pm 1}$, $u_i u_{i+1} \neq 1$ and $t \geq 1$, then $|w| \geq t$ and $|w| \geq |u_i|$ for any $1 \leq i \leq t$ [4, Proposition 2.13, Ch I].

It is well-known that any subgroup of F has a Nielsen-reduced basis. We can conclude the previous two remarks with the following corollary.

Corollary 2.3. *Let F be a free group of rank $n \geq 2$. Then any finitely generated subgroup H of F has a basis $B = \{b_1, \dots, b_m\}$ such that for any reduced nontrivial word w on B one has $|w| \geq |b|$ for any $b \in B$ which appears in the reduced form of w with respect to the basis B.* □

The previous corollary states that, in some sense, H has a basis consisting of "minimal" elements, and an example of such a basis could be a Nielsen-reduced one. Under some natural conditions, there is also a generalisation of it to the context of valuated groups [7, Lemma 4.2].

We will also need the following lemma.

Lemma 2.4. *Let F be a free group of rank $n \geq 2$. If H is a subgroup of rank $m < n$, then there are elements $c_1, \dots, c_{n-m}$ such that the subgroup generated by H and $\{c_1, \dots, c_{n-m}\}$ is of rank n.*

Proof. One shows that H is contained in a subgroup of infinite rank. If it is not the case, by [4, Proposition 3.15, Ch I], H has finite index. But in that case, since $|F : H|(rk(F) - 1) = (rk(H) - 1)$, we have $rk(H) \geq n$. □

3 The main result

Theorem 3.1. *Let F be a free group of rank $n \geq 2$. Then there is an algorithm which decides, given $u, v \in F$, whether there exists a monomorphism $f : F \to F$ such that $f(u) = v$.*

Theorem 3.1 relies on the following key proposition.

Proposition 3.2. *Let F be a free group on $x_1, \ldots, x_n$. Let $u = u(x_1, \cdots, x_n)$ be a reduced word and let $v \in F$. The following properties are equivalent:*

(1) there is a monomorphism $f : F \to F$ such that $f(u) = v$;

(2) there exist m, $1 \leq m \leq n$, and elements $b_1, \ldots, b_m$ in F such that:

(i) the group $H = \langle b_1, \cdots, b_m \rangle$ is free of rank m, $|b_i| \leq |v|$, $v \in H$,

(ii) there exists an automorphism h of $H * \langle y_1, \ldots, y_{n-m} | \rangle$ such that

$$h(u(b_1, \ldots, b_m, y_1, \ldots, y_{n-m})) = v.$$

(3) there exist m, $1 \leq m \leq n$, and elements $b_1, \ldots, b_m$ in F such that:

(i') the group $H = \langle b_1, \cdots, b_m \rangle$ is free of rank m and $v \in H$,

(ii') there exists an automorphism h of $H * \langle y_1, \ldots, y_{n-m} | \rangle$ such that

$$h(u(b_1, \ldots, b_m, y_1, \ldots, y_{n-m})) = v.$$

Proof. (1) $\Rightarrow$ (2). Let $f : F \to F$ be a monomorphism such that $f(u) = v$. By Corollary 2.3, the subgroup $f(F)$ has a basis $B = \{b_1, \ldots, b_n\}$ such that for any reduced nontrivial word w on B one has $|w| \geq |b|$ for any $b \in B$ which appears in the reduced form of w.

Since $v \in f(F)$, v can be written on B, and thus there exists, relabeling the $b_i's$ if necessary, $1 \leq m \leq n$ such that $v \in H = \langle b_1, \ldots, b_m \rangle$ and $|b_i| \leq |v|$ for $1 \leq i \leq m$. We have

$$f(u(x_1, \cdots, x_n)) = u(f(x_1), \ldots, f(x_n)) = v.$$

Since $\{f(x_1), \ldots, f(x_n)\}$ is a basis of $f(F)$, by defining $h : f(F) \to f(F)$ as

$$h(b_i) = f(x_i),$$

h is an automorphism of $f(F)$ and

$$h(u(b_1, \cdots, b_n)) = u(h(b_1), \ldots, h(b_n)) = u(f(x_1), \ldots, f(x_n)) = v.$$

Thus there exists an automorphism h of $f(F)$ such that $h(u(b_1, \cdots, b_n)) = v$. Since $H * \langle y_1, \ldots, y_{n-m} | \rangle$ is isomorphic to $f(F)$ and $v \in H$, the same conclusion applies also for $H * \langle y_1, \ldots, y_{n-m} | \rangle$; that is, there exists an automorphism h of $H * \langle y_1, \ldots, y_{n-m} | \rangle$ such that $h(u(b_1, \ldots, b_m, y_1, \ldots, y_{n-m})) = v$.

(2) $\Rightarrow$ (3) is obvious.

(3) $\Rightarrow$ (1). Suppose first that $m = n$. By defining $f : F \to F$ as

$$f(x_i) = h(b_i),$$

we have

$$f(u(x_1,\dots,x_n)) = u(h(b_1),\dots,h(b_n)) = v,$$

and thus f is a monomorphism such that $f(u) = v$.

Suppose now that $m < n$. By Lemma 2.4, there exist $c_1,\dots,c_{n-m} \in F$ such that the subgroup $K = \langle b_1,\dots,b_m,c_1,\dots,c_{n-m}\rangle$ is free of rank n.

Therefore there exists an automorphism h of K such that

$$h(u(b_1,\dots,b_m,c_1,\dots,c_{n-m})) = v.$$

By defining $f : F \to F$ as

$$f(x_i) = h(b_i) \text{ for } 1 \le i \le m, \quad f(x_{m+j}) = h(c_j), \text{ for } 1 \le j \le n-m,$$

we have

$$\begin{aligned} f(u(x_1,\dots,x_n)) &= u(f(x_1),\dots,f(x_n)) \\ &= u(h(b_1),\dots,h(b_m),h(c_1),\dots,h(c_{n-m})) \\ &= h(u(b_1,\dots,b_m,c_1,\dots,c_{n-m})) = v, \end{aligned}$$

and thus f is a monomorphism such that $f(u) = v$. □

The following result is well-known, see for example [2].

Proposition 3.3. *Let F be a free group. Then there is an algorithm which, given a finite subset U of F and an element v of F, gives the rank of $\langle U\rangle$ and decides if $v \in \langle U\rangle$ and if so it gives a word w on U such that $v = w$.*

Proof of Theorem 3.1

The algorithm that solves the monomorphism problem is the following.
Input: $u(x_1,\dots,x_n)$ and v in F
Output: YES or NO (there exists a monomorphism sending u to v or not)

(1) List all sets $U_1,\dots,U_p$ such that $|U_i| \le n$ and for any $x \in U_i$, $|x| \le |v|$.

(2) For $i = 1$ to p do

  (3) Determine the rank of $H_i = \langle U_i\rangle$ by using Proposition 3.3.

  (4) If $rk(H_i) \ne |U_i|$ then go to $i+1$ else determine if $v \in H_i$.

  (5) If $v \notin H_i$ then go to $i+1$ else find the unique word w on U_i such that $v = w$.

  (6) Let $m = |U_i|$.

  (7) By using Whitehead's algorithm, determine if there exists an automorphism h of $H_i * \langle y_1,\dots,y_{n-m}|\rangle$ such that

$$h(u(b_1,\dots,b_m,y_1,\dots,y_{n-m})) = w.$$

  (8) If h exists then by Proposition 3.2 return YES, else go to $i+1$.

(9) If there is no positive output, then return NO.

□

4 A polynomial time algorithm

The algorithm in the proof of Theorem 3.1 consists of two main parts.

(I) First one finds all tuples $\{b_1, \ldots, b_m\}$ such that $v \in \langle b_1, \ldots, b_m \rangle$, $|b_i| \leq |v|$ and $\{b_1, \ldots, b_m\}$ freely generate $\langle b_1, \ldots, b_m \rangle$. Then one finds $w \in \langle b_1, \ldots, b_m \rangle$ such that $w(b_1, \ldots, b_m) = v$.

(II) The second part consists of applying Whitehead's algorithm to the words u and w, for w found in (I). That is, one needs to check whether there is an automorphism

$$\alpha : \langle b_1, b_2, \ldots, b_m, y_1, \ldots y_{n-m} \rangle \to \langle b_1, b_2, \ldots, b_m, y_1, \ldots y_{n-m} \rangle$$

such that $\alpha(u(b_1, b_2, \ldots, b_m, y_1, \ldots y_{n-m})) = w(b_1, \ldots, b_m)$.

As presented in the proof of Theorem 3.1, line (1) is exponential in the length of v. Part (II), Whitehead's algorithm, is known to be at most exponential, but conjectured to be polynomial in the lengths of the words [6, 8]. It has been shown in [3] that, under some technical conditions on the given words u and v, the automorphism problem can be solved in polynomial time in the lengths of u and v.

Here we provide an alternate algorithm for part (I) that can replace lines (1) - (5) and can be performed in time polynomial in $|v|$. Instead of producing all possible tuples of words of bounded length, which form an exponentially big set, we reduce the search to a polynomial size set. We directly generate candidates for the subgroups that satisfy the properties described by Proposition 3.2(3). The subgroups that we produce are called *test subgroups* and are defined in 4.3. Roughly speaking, we generate topological graphs of rank up to n whose edges we thereafter label with words in F such that the corresponding group H has rank $m \leq n$, contains v, and the core graph C_H has a minimal number of edges. We simultaneously get a basis $b_1, \ldots, b_m$ of H and the word w such that $w(b_1, \ldots, b_m) = v$.

For the remainder of the paper, we will use the term *arc* in a graph for maximal paths whose interior vertices have degree 2, which implicitly contain the case of single edges between vertices of degree greater than 3. Each core graph corresponds to a topological graph whose edges are labeled by words in the free group in such a way that no partial foldings can be performed after the labeling. The fact that v can be read as a loop in a the core graph is equivalent to writing v as the concatenation of the labels on a sequence of arcs in the graph. First we need to bound the lengths of arcs that don't occur in v when written as the concatenation of arc labels.

Definition 4.1. Let H be a subgroup of F_n, $v \in H$, and C_H the core graph of H. An arc c of C_H is said to be *visible* (relative to v) if it is traversed when we read v along arcs of C_H. The other arcs are called *invisible.*

Proposition 4.2. *If condition (2) of Proposition 3.2 is satisfied, then we can choose H such that any invisible arc, relative to v, is of length at most* 3.

Proof. Let $H = \langle b_1, \ldots, b_m \rangle$, satisfying (2) of Proposition 3.2, be such that C_H has a minimal number of edges. We claim that any invisible arc, relative to v, in C_H has length at most 3. Suppose by contradiction that there exists an invisible arc c of length greater than 3. To obtain the desired contradiction, we

will show that there is a subgroup H' that meets condition (2) of Proposition 3.2 and such that $C_{H'}$ has fewer edges than C_H.

Write $c = e_1 e_2 \cdots e_t$ with $t \geq 4$ (where e_i denotes an edge). Replace c by $e_1 \alpha e_t$, where α is a new edge. We claim that there is a labeling of α in a way such that the obtained graph is reduced. Let a (resp. b) to be the label of e_1 (resp. e_t). If $a \neq b^{-1}$ then we label α by a. If $a = b^{-1}$ then we pick $a' \in A$ with $a' \neq b, b^{-1}$ and we label α by a'. Hence we get a reduced graph Γ' as claimed.

Let H' be the subgroup of F whose core graph is Γ'. Using the Euler characteristic formula, a simple count shows that H' has the same rank as H. Let b'_i be the element of H' obtained by replacing each occurence of c in b_i by its new label in Γ'. Clearly $|b'_i| \leq |b_i| \leq v$ and $H' = \langle b'_1, \ldots, b'_m \rangle$. Since c is an invisible arc, $v \in H'$.

Now H' satisfies condition (2)-(i) of Proposition 3.2 and $C_{H'}$ has fewer edges than C_H. To get a contradiction and to finish the proof, it is enough to show that there exists a word $w(x_1, \cdots, x_m)$ such that $v = w(b_1, \cdots, b_m) = w(b'_1, \cdots, b'_m)$. Indeed, since H satisfies condition (2) of Proposition 3.2, there exists an automorphism h of $H * \langle y_1, \ldots, y_{n-m} | \rangle$ such that

$$h(u(b_1, \ldots, b_m, y_1, \ldots, y_{n-m})) = v,$$

and since $v = w(b_1, \cdots, b_m) = w(b'_1, \cdots, b'_m)$, the same conclusion applies to H'.

We now show that there exists a word $w(x_1, \cdots, x_m)$ such that

$$v = w(b_1, \cdots, b_m) = w(b'_1, \cdots, b'_m).$$

Let x be a new variable and let $L = F * \langle x | \rangle$. Let Γ be the $A \cup \{x\}$-labeled graph obtained by labeling c by x (i.e., deleting all interior vertices of c and labeling c by x). Clearly Γ is reduced and a simple count shows that the rank of Γ is equal to the rank of C_H. Let G be the group whose core graph is Γ. Let g_i be the element of G obtained by replacing each occurence of c in b_i by its new label in Γ. Proceeding as above, we conclude that $G = \langle g_1, \cdots, g_m \rangle$ and $v \in G$. Let $w(x_1, \cdots, x_m)$ such that $v = w(g_1, \cdots, g_m)$.

Let f (resp. f') be the homomorphism from L to F which fixes every element of F and which sends x to the label of c in C_H (resp. $C_{H'}$). We have $v = f(v) = w(f(g_1), \ldots, f(g_m))$ and $v = f'(v) = w(f'(g_1), \ldots, f'(g_m))$. But $f(g_i) = b_i$ and $f'(g_i) = b'_i$. Hence we obtain the desired conclusion. □

Definition 4.3. A subgroup H of F is called a *test subgroup* (relative to v) if it contains v and satisfies the conclusion of Proposition 4.2.

The following lemma is a mere consequence of Propositions 3.2 and 4.2.

Lemma 4.4. *Let F be a free group on $x_1, \ldots, x_n$. Let $u = u(x_1, \cdots, x_n)$ be a reduced word and let $v \in F$. Then the existence of a monomorphism which sends u to v is equivalent to the existence of a test subgroup H relative to v with basis $\{b_1, \ldots, b_m\}$, where $m \leq n$, and an automorphism of $H * \langle y_1, \ldots, y_{n-m} | \rangle$ which sends $u(b_1, \ldots, b_m, y_1, \ldots, y_{n-m})$ to v.* □

The above lemma reduces the search from among tuples of words of bounded length to test subgroups. The following lemma shows that a test subgroup satisfies the required properties (4.3) independent of the choice of basis. That

is, working with one basis will be sufficient. Notice that the length condition for invisible arcs in Proposition 4.2 depends on the core graph of a subgroup, and not its basis either.

Lemma 4.5. *Let F be a free group on $x_1, \ldots, x_n$. Let $u = u(x_1, \cdots, x_n)$ be a reduced word and let $v \in F$. Let H be a subgroup of F of rank $m \leq n$. Then the following properties are equivalent:*

(1) there is a basis $b_1, \ldots, b_m$ of H and an automorphism of $H * \langle y_1, \ldots, y_{n-m} | \rangle$ which sends $u(b_1, \ldots, b_m, y_1, \ldots, y_{n-m})$ to v.

(2) for any basis $d_1, \ldots, d_m$ of H there exists an automorphism of $H * \langle y_1, \ldots, y_{n-m} | \rangle$ which sends $u(d_1, \ldots, d_m, y_1, \ldots, y_{n-m})$ to v.

Proof. (2) $\Rightarrow$ (1) is obvious, so we show (1) $\Rightarrow$ (2). Let h be an automorphism of $H * \langle y_1, \ldots, y_{n-m} | \rangle$ which sends $u(b_1, \ldots, b_m, y_1, \ldots, y_{n-m})$ to v. Let $d_1, \ldots, d_m$ a basis of H. Then the map f defined by

$$f(d_i) = b_i, 1 \leq i \leq m,\ f(y_j) = y_j, 1 \leq j \leq n - m,$$

is an automorphism of $H * \langle y_1, \ldots, y_{n-m} | \rangle$. We have

$$f(u(d_1, \ldots, d_m, y_1, \ldots, y_{n-1})) = u(b_1, \ldots, b_m, y_1, \ldots, y_{n-m}),$$

and thus $h \circ f$ is an automorphism of $H * \langle y_1, \ldots, y_{n-m} | \rangle$ which sends $u(d_1, \ldots, d_m, y_1, \ldots, y_{n-m})$ to v. □

The next step is to count the number of labelings of the arcs of a topological graph, which will become the core graph of a test subgroup (relative to v).

Lemma 4.6. *Let v be a word in F_n with $|v| = l$ and $l, k \geq 1$. Then the number of morphisms $\phi : F_k \to F_n$ with the properties:*

(a) there exists a word $w \in F_k$ such that $\phi(w) = v$,

(b) for any i, $\phi(x_i) \neq 1$ and no cancellation occurs between the images $\{\phi(x_i)\}$ when forming v,

(c) if x_i does not appear in w then $\phi(x_i)$ has length at most 3,

is less than $p_k(l, n)$, where $p_k(l, n)$ is a polynomial in l and n of degree $2k$ with respect to l. Here $x_1, \ldots, x_k$ denote the generators of F_k.

Proof. Since there is no cancellation when forming v, each of the $\phi(x_i)$, where x_i is a letter in w, appears as a subword in v. As any word of length l has l^2 possible subwords, there are $(l^2)^k$ possible values for the tuples $(\phi(x_1), \ldots, \phi(x_k))$. Now the number of nontrivial reduced words in F_n of length at most 3 is

$$\alpha(n) = 2n + 2n(2n - 1) + 2n(2n - 1)^2,$$

and thus we can take $p_k(l, n) = \alpha(n) l^{2k}$. □

The work in this section shows that, given a topological graph Γ, it is sufficient to consider a number that is polynomial in $|v|$, of ways to label Γ, in order to generate all test subgroups H. A priory the number of labelings is exponential, since each arc could be labeled by a word of length smaller than $|v|$. Since the number of topological graphs that we use is given by $\sum_{i \leq n} |Top(i)|$, which is a function of n only, these results provide the polynomial time algorithm we are interested in.

4.1 Generating test subgroups

Part (I) of the algorithm now follows the outline:
Input: free group of rank n, word v of length l.
Output: the set of tuples $(\{b_1, \ldots, b_m\}, w(x_1, \ldots, x_m))$ satisfying the property that the subgroup $\langle b_1, \ldots, b_m \rangle$ is a test subgroup of rank m and $w(b_1, \ldots, b_m) = v$ where $1 \leq m \leq n$.

(1) For $i = 1$ to n generate $Top(i)$.

(2) For $\Gamma \in Top(i)$ do

(3) Let $k := |E(\Gamma)|$. Generate morphisms $F_k \to F_n$ as in Lemma 4.6. Let us denote by $H(F_k, F_n)$ that set of morphisms.

(4) For $\phi \in H(F_k, F_n)$ do

(5) Generate the set $\chi(\phi)$ of labelings of $E(\Gamma)$ with ϕ; i.e., the set of surjective maps $\chi : E(\Gamma) \to \{\phi(x_1), \ldots, \phi(x_k)\}$.

(6) For $\chi \in \chi(\phi)$ let $\Gamma(\chi)$ be the new graph obtained from the labeling χ and do

(7) Check if $\Gamma(\chi)$ is reduced.

(8) If yes, find a Nielsen-basis $\{b_1, \ldots, b_i\}$ of $\Gamma(\chi)$, else go to (11).

(9) Check if v can be read as a loop at $\star$ in $\Gamma(\chi)$.

(10) If yes, find the word w on $b_1, \ldots, b_i$ such that $v = w$ and return w and $\{b_1, \ldots, b_i\}$, else go to (11).

(11) Go to the next labeling χ.

(12) Go to next ϕ.

(13) Go to next Γ.

(14) Go to $i + 1$.

Proposition 4.7. *The number of operations performed in the above algorithm is bounded above by*

$$\left(\sum_{i=1}^{n} |Top(i)|(3i-1)! \right) Q(l, n), \qquad (\star)$$

where Q is a function which is polynomial in l.

Proof. Let $1 \leq i \leq n$ and $\Gamma \in Top(i)$ be fixed. Since Γ has rank i, Lemma 2.2 implies that the number of arcs of Γ is $|E(\Gamma)| \leq 3i - 1$. Let $k = |E(\Gamma)|$.

At step (4) we choose a morphism $\phi : F_k \to F_n$ with the properties given in Lemma 4.6. The number of possible choices of such morphisms is bounded above by $p_k(l, n)$ as in Lemma 4.6. Now the number of possible labelings of Γ by ϕ is the same as the number of surjective maps χ from $E(\Gamma)$ to $\{\phi(x_1), \ldots, \phi(x_k)\}$. Let (ϕ) to be the cardinal of $\{\phi(x_1), \ldots, \phi(x_k)\}$. Then the number of these surjections is $S(k, (\phi))$, the second Stirling number. This is bounded by $k!$ which is in turn bounded by $(3i - 1)!$.

This shows that, for a fixed Γ, we need to run through a set of $p_k(l, n)k!$ labelings (steps (4) and (5)). Then, for a fixed Γ and a fixed labeling χ, we need to perform steps (7)-(10).

Step (7) can be performed in time polynomial in the size of the graph $\Gamma(\chi)$. It is shown in [9, Theorem 1.6] that the time required to completely fold a graph Δ is $O(E+(V+E)\log^\star(V))$, where E and V are the number of vertices and edges in Δ, respectively. In our case the number of arcs in Γ is $k \leq 3i-1$ and each arc will generate at most $max(3,l)$ edges in $\Gamma(\chi)$, while the number of vertices in Γ is at most $2i$ (see Lemma 2.2), and will be at most $2i + (3i-1)max(2,(l-1))$ in $\Gamma(\chi)$. We thus obtain a complexity of $O(l\log^\star(l))$ for step (7).

Step (8) requires finding a spanning tree using the breadth first method, which takes time linear in the number of vertices in the graph, thus giving us $O(l)$ complexity for step (8). Step (9) can be performed in a time linear in the length of v, leading again to an $O(l)$ complexity (see [9, Corollary 1.5]). Step (10) can be performed in time polynomial in l due to the fact that v can be written as a word of length less than l in a Nielsen-basis [4, Proposition 2.13, Ch I], and the exact reading in the core graph of the each of the letters b_j appearing in v can be done in time less than $|v|$. Thus the total number of operations leads to an $O(l^2)$ complexity for this step.

The above analysis shows that steps (7)-(10) can be performed in a polynomial number of operations, polynomial in l that also depends on n and the size of the graph $\Gamma(\chi)$. Let $q_{\Gamma(\chi)}(n,l)$ be this polynomial and let $q_\Gamma(l)$ be the maximum of $q_{\Gamma(\chi)}(n,l)$ over all χ and fixed Γ. Then $q_\Gamma(l)$ is a quadratic polynomial in l.

Thus for a fixed $1 \leq i \leq n$, the number of operations is given by

$$\sum_{\Gamma \in Top(i)} p_k(l,n)k!q_\Gamma(l),$$

which is bounded above by

$$\sum_{\Gamma \in Top(i)} p_{3i-1}(l,n)(3i-1)!q_\Gamma(l). \qquad (\star\star)$$

Although as described above $q_\Gamma(l)$ depends on Γ and implicitly on i, since it is always a quadratic polynomial in l, we can consider the maximum of $q_\Gamma(l)$ over all i and all $\Gamma \in Top(i)$ and still obtain a quadratic polynomial.

Now summing the expressions of type $(\star\star)$ over all the $1 \leq i \leq n$ we obtain that the total number of operations performed by this algorithm has the form

$$\left(\sum_{i=1}^{n} |Top(i)|(3i-1)!\right) Q(l,n), \qquad (\star)$$

where $Q(l,n)$ a function which is polynomial in l □

5 Conclusions

The algorithm that we provided for the monomorphism problem, with the exception of the part involving Whitehead's algorithm, is polynomial in the lengths of the words u and v. However, the constants involved in the time complexity in $(\star)$ are exponential in the rank of the group F, and thus we cannot claim that our algorithm is a practical one. For free groups of small rank the constants are manageable due to the fact that the number of topological graphs is small, and

the degree of the polynomial $Q(n, l)$ is also small. In particular, if F has rank 2, it is known that the Whitehead algorithm has polynomial complexity, which leads us to the following corollary.

Corollary 5.1. *The monomorphism problem in the free group of rank* 2 *has a time complexity that is polynomial in the lengths of the words* u *and* v*.*

The rank 2 free group is possibly the only one in which the three related decision problems, the endomorphism [1], monomorphism and automorphism [6] problem, can be solved in a time polynomial in the lengths of the words involved.

A consequence of our method is also the following.

Corollary 5.2. *The multiple monomorphism problem in free groups is solvable. That is, for any* $r \geq 1$ *and any two tuples of words* $(u_1, \ldots, u_r)$ *and* $(v_1, \ldots, v_r)$ *in* F*, one can decide whether there is a monomorphism* $f : F \to F$ *such that* $f(u_i) = v_i$ *for all* $1 \leq i \leq r$*.*

Proof. The proof of Proposition 3.2 easily extends to the tuple case. The existence of a monomorphism f is equivalent to the existence of a subgroup $H = \langle b_1, \cdots, b_m \rangle$, free of rank $m \leq n$, such that

$$|b_i| \leq \max_{1 \leq j \leq r} |v_j| \text{ and } v_j \in H, \text{ for all } 1 \leq i \leq m, 1 \leq j \leq r$$

which is the analogous condition of Proposition 3.2(2)(i), and the existence of an automorphism h such that

$$h(u_j(b_1, \ldots, b_m, y_1, \ldots, y_{n-m})) = v_j$$

for all $1 \leq i \leq m$, $1 \leq j \leq r$ (condition Proposition 3.2(2)(ii)).

One then follows the outline of the algorithm given in Theorem 3.1. One finds subgroups $H = \langle b_1, \cdots, b_m \rangle$ as above by enumerating tuples (line (1) of the algorithm) and then checking whether they satisfy all the required properties (lines (3), (4) and (5)). Then one writes each v_i as a word w_i in the generators $b_1, \cdots, b_m$ (line (5)) and applies the Whitehead algorithm for tuples in the group $H * \langle y_1, \ldots, y_{n-m} | \rangle$ in order to determine whether there exists an automorphism h such that $h(u_j(b_1, \ldots, b_m, y_1, \ldots, y_{n-m})) = v_j$ for all $1 \leq j \leq r$. □

Acknowledgments

The first-named author was partially supported by the SNF (Switzerland) through project number 200020-121506 and by the Marie Curie Reintegration Grant 230889. We would like to thank Saša Radomirović for helpful discussions.

References

[1] L. Ciobanu. Polynomial-time complexity for instances of the endomorphism problem in free groups. *International Journal of Algebra and Computation*, 17(2):289-328, 2007.

[2] I. Kapovich, A. Myasnikov. Stallings Foldings and Subgroups of Free Groups. *Journal of Algebra*, 248:608–668, 2002.

[3] D. Lee. A tighter bound on the number of words of minimum length in an automorphic orbit. *Journal of Algebra*, 305:1093–1101, 2006.

[4] R. Lyndon and P. Schupp. Combinatorial group theory. *Springer-Verlag*, 1977.

[5] G. S. Makanin. Equations in free groups (Russian). *Izv. Akad. Nauk SSSR Ser. Mat. 46*, 1982.

[6] A. G. Myasnikov and V. Shpilrain. Automorphic orbits in free groups. *Journal of Algebra*, 269(1):18–27, 2003.

[7] A. Ould Houcine. Satisfaction of existential theories in finitely presented groups and some embedding theorems. *Annals of Pure and Applied Logic*, 142(1-3):351-365, 2006.

[8] A. Roig, E. Ventura, P. Weil. On the complexity of the Whitehead minimization problem. *International Journal of Algebra and Computation*, 17(8):1611–1634, 2007.

[9] N.W.M. Touikan. A fast algorithm for Stallings' folding process. *International Journal of Algebra and Computation*, 16(6):1031–1045, 2006.

[10] J. H. C. Whitehead. On equivalent set of elements in a free group. *Ann. of Math.*, 37: 782–800, 1936.

Laura CIOBANU, Département de mathèmatiques, Université de Fribourg, Chemin du Musée 23, CH-1700 Fribourg Pérolles, Switzerland.
E-mail: laura.ciobanu@unifr.ch

Abderezak OULD HOUCINE,
Université de Mons-Hainaut, Institut de Mathmatique, Bâtiment Le Pentagone, Avenue du Champ de Mars 6, B-7000 Mons, Belgique.

Université de Lyon; Université Lyon 1; INSA de Lyon, F-69621; Ecole Centrale de Lyon; CNRS, UMR5208, Institut Camille Jordan, 43 blvd du 11 novembre 1918, F-69622 Villeurbanne-Cedex, France. *E-mail*: ould@math.univ-lyon1.fr