On an algorithm to decide whether a free group is a free factor of another[1]

Pedro V. Silva[2], Pascal Weil[3]

Abstract

We revisit the problem of deciding whether a finitely generated subgroup H is a free factor of a given free group F. Known algorithms solve this problem in time polynomial in the sum of the lengths of the generators of H and exponential in the rank of F. We show that the latter dependency can be made exponential in the rank difference $\mathsf{rank}(F) - \mathsf{rank}(H)$, which often makes a significant difference.

For the classical facts about free groups recorded below without a reference, we refer the reader to the book by Lyndon and Schupp [6].

It is well-known that the minimal sets of generators, or bases, of a free group F all have the same cardinality, called the rank of F. Moreover, if F has finite rank r, every r-element generating set of F is a basis, see [6, Prop. I.3.5]. In this paper, we will consider only finite rank free groups.

Let H be a subgroup of a free group F, written $H \leq F$. Then H itself is a free group whose rank may be greater than the rank of F. We say that H is a free factor of F, written $H \leq_{\mathsf{ff}} F$, if there exist bases B of H and A of F such that $B \subseteq A$ (free factors can be defined in all groups, by a universal property, but the operational definition given here is sufficient for the purpose of this study). It is well known that one can decide whether a given finite rank subgroup $H \leq F$ is a free factor of F, but the known algorithms have a rather high time complexity. More precisely, the best of these algorithms require time that is polynomial in the size of H and exponential in the rank of F. This point is discussed in more detail in Section 1.3 below.

Once a basis A of the ambient free group F is fixed, there is a natural and elegant representation of the finitely generated subgroups of F by A-labeled graphs (or inverse automata), which has been used to great profit by many authors since the late 1970s. This construction — a graphical representation of ideas that go back to the early part of the twentieth century [11, Chap. 11] — was made explicit by Serre [12] and Stallings [13], and is discussed and used in

[1]The first author acknowledges support from C.M.U.P., financed by F.C.T. (Portugal) through the programmes POCTI and POSI, with national and European Community structural funds. Both authors acknowledge support from the European Science Foundation program AutoMathA.

[2]Centro de Matemática, Faculdade de Ciências – Universidade do Porto – R. Campo Alegre 687 – 4169-007 Porto, Portugal. pvsilva@fc.up.pt

[3]LaBRI, CNRS – 351 cours de la Libération – 33405 Talence Cedex – France. pascal.weil@labri.fr

[7, 8, 2] and many others. Given a finite set of generators of H (as reduced words over the alphabet $A \cup A^{-1}$), this representation can be effectively constructed (see [13], [8], etc). Moreover the number of vertices and edges of this graph is bounded above by ℓ, the sum of the lengths of a set of generators of H, and the whole representation can be computed in time at most $O(\ell^2)$ (in fact, in time $O(\ell \log^* \ell)$ according to a recent announcement [15]). We discuss this representation in more detail in Section 1.2 below.

We propose a new algorithm to decide whether a given finitely generated subgroup of a free group F is a free factor of F, based on a careful analysis of the construction of the graph representation of H. This new algorithm is polynomial in the size of H and exponential in the rank difference between F and H. In many instances, this represents a substantial advantage over exponential dependency in the rank of F.

1 Background

If A is a basis of a free group F, we often write $F = F(A)$ and we represent the elements of F as reduced words over the alphabet A. More precisely, we consider the set of all words on the symmetrized alphabet $A \cup A^{-1}$, where $A^{-1} = \{a^{-1} \mid a \in A\}$ is a set that is disjoint from A, equipped with an explicit bijection with A, namely $a \mapsto a^{-1}$. Such a word is reduced if it contains no factor of the form aa^{-1} or $a^{-1}a$ with $a \in A$, and it is well known that F can be identified with the set of reduced words over A. We denote by ρ the map that assigns to each word u the corresponding reduced word $u\rho \in F(A)$, obtained by iteratively deleting all factors of the form aa^{-1} or $a^{-1}a$ ($a \in A$).

1.1 On inverse automata

We describe the main tool for the representation of subgroups of free groups in terms of automata (see [10]). Readers less familiar with this terminology may think of automata as edge-labeled graphs.

An automaton on alphabet A is a triple of the form $\mathcal{A} = (Q, q_0, E)$ where Q is a finite set called the state set, $q_0 \in Q$ is the initial state, and $E \subseteq Q \times A \times Q$ is the set of edges, or transitions. A transition (p, a, q) is said to be from state p, to state q, with label a. The label of a path in $\mathcal{A}$ (a finite sequence of consecutive transitions) is the sequence of the labels of its transitions, a word on alphabet A, that is, an element of the free monoid A^*. We write $p \xrightarrow{u} q$ if there is a path from state p to state q with label u. The language accepted by $\mathcal{A}$ is the set $L(\mathcal{A})$ of all words in A^* which label a path in $\mathcal{A}$ from q_0 to q_0.

This definition of automata leads naturally to the definition of a homomorphism φ from an automaton $\mathcal{A} = (Q, q_0, E)$ to an automaton $\mathcal{A}' = (Q', q_0', E')$ (over the same alphabet A): φ is a mapping from Q to Q' such that $\varphi(q_0) = q_0'$, and such that whenever $(p, a, q) \in E$, we also have $(\varphi(p), a, \varphi(q)) \in E'$.

The automaton $\mathcal{A}$ is called deterministic if no two distinct edges with the same initial state bear the same label, that is,

$$(p,a,q),(p,a,q') \in E \Longrightarrow q = q'.$$

The automaton is called trim if every state $q \in Q$ lies in some path from q_0 to q_0.

In the sequel, we consider automata where the alphabet is symmetrized, that is, the alphabet is of the form $A \cup A^{-1}$. We say that $\mathcal{A}$ is dual if for each $a \in A$, there is an a-labeled edge from state p to state q if and only if there is an a^{-1}-labeled edge from q to p,

$$(p,a,q) \in E \Longleftrightarrow (q,a^{-1},p) \in E.$$

Let us immediately record the following fact.

Fact 1.1 Let $\mathcal{A}$ be a dual automaton. If a word u labels a path in $\mathcal{A}$ from state p to state q, then so does the corresponding reduced word $u\rho$. Moreover $L(\mathcal{A})$ is a submonoid of $(A \cup A^{-1})^*$ and $L(\mathcal{A})\rho$ is a subgroup of $F(A)$. □

Now let $\mathcal{A} = (Q, q_0, E)$ be a trim dual automaton and let $p, q \in Q$ be states of $\mathcal{A}$. If $w = a_1 \cdots a_n \in (A \cup A^{-1})^*$ is a non-empty word, the expansion of $\mathcal{A}$ by (p, w, q) is the automaton obtained from $\mathcal{A}$ by adding $n-1$ vertices $q_1, \ldots, q_{n-1}$ and $2n$ edges

$$p \xrightarrow{a_1} q_1 \xrightarrow{a_2} \cdots \xrightarrow{a_{n-1}} q_{n-1} \xrightarrow{a_n} q$$

and

$$q \xrightarrow{a_n^{-1}} q_{n-1} \xrightarrow{a_{n-1}^{-1}} \cdots \xrightarrow{a_2^{-1}} q_1 \xrightarrow{a_1^{-1}} p.$$

Note that this automaton is still trim and dual. Moreover, if $p = q = q_0$, then we observe the following.

Proposition 1.2 *Let $\mathcal{A} = (Q, q_0, E)$ be a trim dual automaton, let $H = L(\mathcal{A})\rho$ and let w be a non-empty word. If $\mathcal{B}$ is the expansion of $\mathcal{A}$ by (q_0, w, q_0), then $L(\mathcal{B})\rho$ is the subgroup generated by H and $w\rho$, that is, $L(\mathcal{B})\rho = \langle H, w\rangle$.*

Proof. Let $\mathcal{C}$ be the dual automaton consisting of the state q_0 and the states and edges added to $\mathcal{A}$ in the expansion. It is immediate that $L(\mathcal{C})\rho$ is the subgroup of $F(A)$ generated by $w\rho$.

If $w \in L(\mathcal{B})$, we can factor a path $q_0 \xrightarrow{w} q_0$ according to the successive visits of state q_0. The resulting factorization of w makes it clear that w is a product of elements of $L(\mathcal{A})$ and $L(\mathcal{C})$. Thus, $L(\mathcal{B})$ is the submonoid generated by $L(\mathcal{A}) \cup L(\mathcal{C})$, and $L(\mathcal{B})\rho$ is the subgroup generated by $L(\mathcal{A})\rho$ and $w\rho$. This concludes the proof. □

1.2 Reduced inverse automata

The automaton $\mathcal{A}$ is called inverse if it is deterministic, trim and dual. It is reduced if every state $q \in Q$ lies in some path from q_0 to q_0, labeled by a (possibly empty) reduced word. We note the following result, a cousin of [14, Thm 1.16].

Proposition 1.3 *If $\mathcal{A}$ and $\mathcal{B}$ are reduced inverse automata and $L(\mathcal{A})\rho = L(\mathcal{B})\rho$, then $\mathcal{A}$ and $\mathcal{B}$ are isomorphic.*

Proof. Let $\mathcal{A} = (Q, q_0, E)$ and $\mathcal{B} = (P, p_0, D)$ be reduced inverse automata such that $L(\mathcal{A})\rho = L(\mathcal{B})\rho$. We construct an isomorphism φ between $\mathcal{A}$ and $\mathcal{B}$ as follows. We first let $\varphi(q_0) = p_0$.

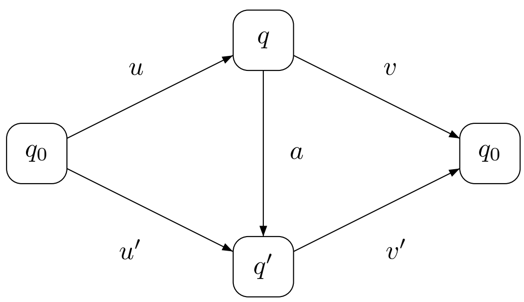
Let $q \in Q$. Since $\mathcal{A}$ is reduced, there exist reduced words u and v such that the word uv is reduced, $q_0 \xrightarrow{u} q$ and $q \xrightarrow{v} q_0$. Then $uv \in L(\mathcal{A})\rho$, so $uv \in L(\mathcal{B})\rho$, and since uv is reduced, we have $uv \in L(\mathcal{B})$. Thus uv labels a path in $\mathcal{B}$ from p_0 to p_0, and we let $\varphi(q)$ be the unique state in P such that $p_0 \xrightarrow{u} \varphi(q) \xrightarrow{v} p_0$.

We first verify that φ is well defined. Suppose that uv and $u'v'$ are reduced words such that $q_0 \xrightarrow{u} q \xrightarrow{v} q_0$ and $q_0 \xrightarrow{u'} q \xrightarrow{v'} q_0$. We want to show that if $p_0 \xrightarrow{u} p \xrightarrow{v} p_0$ and $p_0 \xrightarrow{u'} p' \xrightarrow{v'} p_0$ in $\mathcal{B}$, then $p = p'$. If $u'v$ is a reduced word, then as above, $u'v$ labels a path in $\mathcal{B}$ from p_0 to p_0, say, $p_0 \xrightarrow{u'} p'' \xrightarrow{v} p_0$ and the deterministic property of $\mathcal{B}$ implies that $p' = p'' = p$.

If $u'v$ is not reduced, and a is the first letter of v, then the last letter of u' is a^{-1} while the last letter of u is not a^{-1}. Therefore $u'u^{-1}$ is reduced, $u'u^{-1} \in L(\mathcal{A})$ and again, there is a path in $\mathcal{B}$ of the form $p_0 \xrightarrow{u'} p'' \xrightarrow{u^{-1}} p_0$. By determinism, it follows that $p' = p'' = p$.

This shows that φ is well defined. A dual construction yields a well-defined mapping ψ from P to Q such that, whenever uv is a reduced word and $p_0 \xrightarrow{u} p \xrightarrow{v} p_0$ in $\mathcal{B}$, then $q_0 \xrightarrow{u} \psi(p) \xrightarrow{v} q_0$ in $\mathcal{A}$. Using the determinism of $\mathcal{A}$ and $\mathcal{B}$, it is now immediate that $\psi \circ \varphi$ is the identity on Q and $\varphi \circ \psi$ is the identity on P.

There remains to verify that φ is a homomorphism. More precisely, let (q, a, q') be a transition in $\mathcal{A}$, and let uv and $u'v'$ be reduced words such that $q_0 \xrightarrow{u} q \xrightarrow{v} q_0$ and $q_0 \xrightarrow{u'} q' \xrightarrow{v'} q_0$. In particular, we have $p_0 \xrightarrow{u} \varphi(q) \xrightarrow{v} p_0$ and $p_0 \xrightarrow{u'} \varphi(q') \xrightarrow{v'} p_0$ in $\mathcal{B}$.



If uav' is reduced, then in $\mathcal{B}$, there is a path from p_0 to p_0 labeled uav', and by determinism, there is a transition $(\varphi(q), a, \varphi(q'))$. If uav' is not reduced, then either ua is not reduced or av' is not reduced. If ua is not reduced, then $u = u_1a^{-1}$ and by determinism, $q_0 \xrightarrow{u_1} q'$. As in the first part of the proof, it follows that at least one of u_1v' and $u_1u'^{-1}$ is reduced, so $p_0 \xrightarrow{u_1} \varphi(q')$ in $\mathcal{B}$ and hence there is a transition $(\varphi(q), a, \varphi(q'))$. The case where av' is not reduced is handled symmetrically, and this concludes the proof. $\square$

Let H be a subgroup of $F(A)$. Say that an automaton $\mathcal{A}$ on alphabet A represents H if $\mathcal{A}$ is reduced and inverse and if $L(\mathcal{A})\rho = H$. Proposition 1.3 shows that there exists at most one such automaton, and we denote it by $\Gamma_A(H)$ if it exists. We now discuss the existence and the construction of $\Gamma_A(H)$ when H is finitely generated. (As it turns out, $\Gamma_A(H)$ always exists, but our interest in this paper is restricted to algorithmic questions, and hence to the finite rank case.)

Let $\mathcal{A}$ be an automaton and let p, q be distinct states of $\mathcal{A}$. The automaton obtained from $\mathcal{A}$ by identifying states p and q is constructed as follows: its state set is $Q \setminus \{p, q\} \cup \{n\}$, where n is a new state; its initial state is q_0 (or n if p or q is equal to q_0); and its set of transitions is obtained from E by replacing everywhere p and q by n. If $\mathcal{A}$ is trim or dual, then so is the automaton obtained from $\mathcal{A}$ by identifying a pair of states.

Now let $\mathcal{A}$ be a dual automaton. If $\mathcal{A}$ is not deterministic, there exist transitions (r, a, p) and (r, a, q) with $p \neq q$ and $a \in A \cup A^{-1}$. Identifying p and q yields a new dual automaton $\mathcal{B}$, and we say that $\mathcal{B}$ is obtained from $\mathcal{A}$ by an elementary reduction of type 1.

Fact 1.4 Let $\mathcal{A}$ be a dual automaton and let $\mathcal{B}$ be obtained from $\mathcal{A}$ by an elementary reduction of type 1. Then $L(\mathcal{A})\rho = L(\mathcal{B})\rho$. $\square$

Proof. It is easily seen that $L(\mathcal{A}) \subseteq L(\mathcal{B})$. For the converse, we use the notation given above: in $\mathcal{B}$, the states p and q of $\mathcal{A}$ are replaced with a new state n. Let $u \in L(\mathcal{B})$. Then there exists a path labeled u from the initial state of $\mathcal{B}$ (say, q_0) to itself. If that path does not visit state n, then u also labels a path from q_0 to itself in $\mathcal{A}$ and hence $u \in L(\mathcal{A})$.

If that path does visit state n, we consider the factorization of u given by the passage of that path through n: we have $u = u_0u_1 \cdots u_r$, $r \geq 1$ and

$$q_0 \xrightarrow{u_0} n \xrightarrow{u_1} n \cdots n \xrightarrow{u_r} q_0.$$

It follows that in $\mathcal{A}$, u_i-labelled paths exist, with end states p or q. Then one of u_0 and $u_0a^{-1}a$ labels a path in $\mathcal{A}$ from q_0 to q. Similarly, one of u_r and $a^{-1}au_r$ labels a path from q to q_0. And for each $1 \leq i \leq r$, one of u_i, $a^{-1}au_i$, $u_ia^{-1}a$ and $a^{-1}au_ia^{-1}a$ labels a path in $\mathcal{A}$ from q to q. Therefore, there exists a path in $\mathcal{A}$ of the form $q_0 \xrightarrow{v} q_0$ such that $u\rho = v\rho$, which concludes the proof. $\square$

Again, let $\mathcal{A}$ be a deterministic dual automaton. If $\mathcal{A}$ is not reduced, let q be a state such that, for every pair of paths $q_0 \xrightarrow{x} q$ and $q \xrightarrow{y} q_0$ labeled by reduced words x and y, the product word xy fails to be reduced. Note that q cannot be equal to q_0. If $\mathcal{B}$ is obtained from $\mathcal{A}$ by omitting state q and the transitions involving it, we observe that $\mathcal{B}$ is again deterministic and dual, and we say that $\mathcal{B}$ is obtained from $\mathcal{A}$ by an elementary reduction of type 2.

Fact 1.5 Let $\mathcal{A}$ be a deterministic dual automaton and let $\mathcal{B}$ be obtained from $\mathcal{A}$ by an elementary reduction of type 2. Then $L(\mathcal{A})\rho = L(\mathcal{B})\rho$. $\square$

Proof. It is easily seen that $L(\mathcal{B}) \subseteq L(\mathcal{A})$. Conversely, let $u \in L(\mathcal{A})$ and suppose that $\mathcal{B}$ was obtained from $\mathcal{A}$ by omitting state q. In particular, there exists a uniquely determined state p and a uniquely determined letter $a \in A \cup A^{-1}$ such that the only transitions of $\mathcal{A}$ involving q are (p, a, q) and (q, a^{-1}, p). If the path $q_0 \xrightarrow{u} q_0$ in $\mathcal{A}$ does not visit state q, then it is also a path in $\mathcal{B}$ and $u \in L(\mathcal{B})$.

If that path does visit state q, we consider the factorization of u given by the passage of that path through q: we have $u = u_0 u_1 \cdots u_r$, $r \geq 1$ and

$$q_0 \xrightarrow{u_0} q \xrightarrow{u_1} q \cdots q \xrightarrow{u_r} q_0.$$

It follows that every u_i $(i < r)$ ends with a and every u_j $(0 < j)$ starts with a^{-1}. Cancelling the factors aa^{-1} that occur between the u_i yields a path from q_0 to q_0 in $\mathcal{B}$. Moreover, if v is the label of that path, then $v\rho = u\rho$, which concludes the proof. $\square$

Let $\mathcal{A}$ be a trim, dual automaton, and let $\mathcal{B}$ be an automaton obtained by iteratively performing elementary reductions, first of type 1 and then of type 2, until none is possible. Then $\mathcal{B}$ is a reduced inverse automaton, we write $\mathcal{B} = \mathcal{A}\rho$ and we say that $\mathcal{B}$ is obtained from $\mathcal{A}$ by reduction. Moreover, Facts 1.4 and 1.5 show that $L(\mathcal{A})\rho = L(\mathcal{B})\rho$.

This leads directly to the well-known algorithm to construct a reduced inverse automaton representing a given finitely generated subgroup H. Let $h_1, \ldots, h_n$ be generators of H, and let us consider the automaton obtained from the trivial automaton (one vertex q_0, no transitions) by performing successively expansions by (q_0, h_i, q_0) $(1 \leq i \leq n)$ and then reducing the automaton. It follows from Proposition 1.2 that the resulting automaton is $\Gamma_A(H)$. Note that it does not matter which set of generators of H was used, nor in which order the generators were used.

Remark 1.6 This construction of $\Gamma_A(H)$ is well known, and can be described in many different ways, notably in terms of immersions over the bouquet of circles (Stallings [13]) or of closed inverse submonoids of a free inverse monoid (Margolis and Meakin [7]). $\square$

There is a well-known converse to the above construction: if $\mathcal{A}$ is a reduced inverse automaton and $H = L(\mathcal{A})\rho$, then H has finite rank and a basis for H can be computed as follows (see Stallings [13]). Given a spanning tree T of the (graph underlying the) automaton $\mathcal{A}$, for each state p, let u_p be the reduced word labeling a path from q_0 to p inside the tree T. For each transition $e = (p, a, q)$, let $b_e = u_p a u_q^{-1}$: then a basis of H consists of the elements b_e, where e runs over the transitions $e = (p, a, q)$ not in T and such that $a \in A$.

We note that, given a finite set $h_1, \ldots, h_n$ of elements of $F(A)$ with total length $\ell = \sum_i |h_i|$, one can construct $\Gamma_A(H)$ in time at most $O(\ell^2)$ and $\Gamma_A(H)$ has $v \leq \ell - r + 1$ states. Moreover, finding a basis of H can be done in time at most $O(v^2)$ (this bound can be improved, see Touikan [15]).

1.3 On the complexity of Whitehead and other algorithms

It is well known that one can decide, given H a subgroup of a finite rank free group F, whether H is a free factor of F. We briefly describe here the main known algorithms and discuss their complexity.

Let H be a finitely generated subgroup of a free group F of rank r, with basis A. Let $h_1, \ldots, h_n$ be a generating set of H. By the results summarized in Section 1.2, up to a quadratic time computation, we may assume that $h_1, \ldots, h_n$ is a basis of H. Let $\ell = |h_1| + \cdots + |h_n|$ be the total length of the tuple $(h_i)_i$, and let $d = r - n$ be the rank difference between F and H – which we assume to be positive, since H can be a proper free factor of F only if $n < r$.

Federer and Jónsson (see [6, Prop. I.2.26]) gave the following observation and decision procedure: H is a free factor of F if and only if there exist d words $h_{n+1}, \ldots, h_r$, each of length at most $\max\{|h_i| \mid 1 \leq i \leq n\}$, such that $h_1, \ldots, h_n$ generate the whole of F. The resulting algorithm requires testing every suitable d-tuple of reduced words on alphabet A. Each of these tests (does a certain r-tuple of words generate F?) takes time polynomial in the total length of the r-tuple, and hence in $d\ell$. However, the number of tests is $O(r^{d\ell})$, which is exponential in ℓ and d.

This approach leads to the following.

Fact 1.7 Deciding whether $H \leq_{\mathsf{ff}} K$ is in NP, with respect to $d\ell$. $\square$

Proof. To verify that $H \leq_{\mathsf{ff}} K$, we need to guess d words of length at most ℓ, and verify that together with H, they generate F, which can be done in $O((d\ell)^2)$. $\square$

Another approach is based on the use of Whitehead automorphisms. We refer the readers to [6, Sec. I.4] for the definition of these automorphisms, it suffices to note here that the set W of non length preserving Whitehead automorphisms of F has exponential cardinality (in terms of r). A result of Whitehead [6, Prop. I.4.24] shows the following: if there exists an automorphism φ such that the total length of $(\varphi(h_i))_i$ is strictly less than ℓ, then there exists such an automorphism in W. In particular, an algorithm to compute the minimum total length of an automorphic image of the tuple $(h_i)_i$ consists in repeatedly applying the following step: try every automorphism $\psi \in W$ until the total length of $(\psi(h_i))_i$ is strictly less than the total length of $(h_i)_i$; if such a ψ exists, replace $(h_i)_i$ by $(\psi(h_i))_i$; otherwise, stop and output the total length of $(h_i)_i$.

This applies to the decision of the free factor relation since $H \leq_{\mathsf{ff}} F$ if and only if there exists an automorphism φ mapping $h_1, \ldots, h_n$ to a subset of A, that is, such that the total length of $(\varphi(h_i))_i$ is exactly n. This algorithm may require $O((\ell - n)\mathsf{card}(W))$ steps, each of which consists in computing the image of a tuple of length at most ℓ under an automorphism, and hence has complexity $O(\ell)$. Thus the time complexity of this algorithm is $O(\ell\ \mathsf{card}(W))$, which is linear in ℓ and exponential in r.

A variant of this algorithm was established by Gersten [1], who showed that a similar method applies to find the minimum size (number of vertices) of $\Gamma_A(\varphi(H))$, when φ runs over the automorphisms of $F(A)$. It is clear that H is a free factor of $F(A)$ if and only if there exists an automorphism φ such that $\Gamma_A(\varphi(H))$ has a single vertex. The time complexity is computed as above, where the number of vertices of $\Gamma_A(H)$ is substituted for the total length of a basis for H. As noted earlier, this number of vertices is usually substantially smaller than the total length of a basis, but the two values are linearly dependent, so the order of magnitude of the time complexity is not modified, notably the exponential dependence in r.

Remark 1.8 The discussion of Whitehead's algorithm above concerns only the so-called *easy part* of the algorithm (see for instance Kapovich, Myasnikov and Shpilrain [3]). Recent results by Myasnikov and Shpilrain [9], Khan [4] and Donghi Lee [5] on the possible polynomial complexity of the *hard part* of the algorithm also consider the rank of the ambient free group as a constant, and do not discuss the actual exponential dependence in that parameter. □

2 A careful look at the expansions and reductions of inverse automata

Let $\mathcal{A}$ be a reduced inverse automaton.

Let $\mathcal{B}$ be obtained from $\mathcal{A}$ by performing an expansion, say by (p, w, q), and then reducing the resulting automaton. In this situation, we write $\mathcal{A} \longrightarrow_{\mathsf{exp}}^{(p,w,q)} \mathcal{B}$, or simply $\mathcal{A} \longrightarrow_{\mathsf{exp}} \mathcal{B}$. We distinguish two special cases.

• If the reduction following the expansion does not involve identifying or omitting states of $\mathcal{A}$, or equivalently if $\mathcal{A}$ embeds in $\mathcal{B}$, we say that $\mathcal{B}$ is obtained from $\mathcal{A}$ by a *reduced expansion* and we write $\mathcal{A} \longrightarrow_{\mathsf{re}}^{(p,w,q)} \mathcal{B}$ or $\mathcal{A} \longrightarrow_{\mathsf{re}} \mathcal{B}$.

• If the states p and q are equal to the distinguished state q_0 of $\mathcal{A}$, we say that $\mathcal{B}$ is obtained from $\mathcal{A}$ by an *e-step* and we write $\mathcal{A} \longrightarrow_{\mathsf{e}}^{w} \mathcal{B}$, or simply $\mathcal{A} \longrightarrow_{\mathsf{e}} \mathcal{B}$.

Finally, let $\mathcal{B}$ be obtained from $\mathcal{A}$ by identifying two distinct vertices p and q, and then reducing the resulting automaton. Then we say that $\mathcal{B}$ is obtained from $\mathcal{A}$ by an *i-step* and we write $\mathcal{A} \longrightarrow_{\mathsf{i}}^{p=q} \mathcal{B}$, or simply $\mathcal{A} \longrightarrow_{\mathsf{i}} \mathcal{B}$.

Note that if $\mathcal{A} \longrightarrow_{\mathsf{exp}} \mathcal{B}$, $\mathcal{A} \longrightarrow_{\mathsf{re}} \mathcal{B}$, $\mathcal{A} \longrightarrow_{\mathsf{e}} \mathcal{B}$ or $\mathcal{A} \longrightarrow_{\mathsf{i}} \mathcal{B}$, then $\mathcal{B}$ is a reduced inverse automaton.

We first record a few facts.

Fact 2.1 Let u be a reduced word labeling a path in $\mathcal{A}$ from a state p to a state p', and from a state q to a state q',

$$p \xrightarrow{u} p', \quad q \xrightarrow{u} q'.$$

By definition of the reduction of dual automata, the identification of p and q implies that of p' and q', and the converse holds as well. Thus $\mathcal{A} \longrightarrow_{\mathsf{i}}^{p=q} \mathcal{B}$ if and only if $\mathcal{A} \longrightarrow_{\mathsf{i}}^{p'=q'} \mathcal{B}$. □

Let us now examine in detail the effect of an operation of the form $\longrightarrow_{\mathsf{exp}}$.

Fact 2.2 Let p, q be states of $\mathcal{A}$ and let w be a non-empty reduced word. Let u be the longest prefix of w that can be read in $\mathcal{A}$ from state p, and let v be the longest suffix of w that can be read in $\mathcal{A}$ to state q (that is, v^{-1} is the longest prefix of w^{-1} that can be read in $\mathcal{A}$ from state q). We distinguish two cases:

(1) If $|u| + |v| < |w|$, then $w = uw'v$ for some non-empty reduced word w'. If we let p' (resp. q') be the end (resp. start) state of the path labeled u (resp. v) and starting in p (resp. ending in q),

$$p \xrightarrow{u} p' \xrightarrow{w} q' \xrightarrow{v} q,$$

then the reduction process on the result of the expansion of $\mathcal{A}$ by (p, w, q) identifies the $|u|$ first edges and the $|v|$ last edges of the added path with existing edges of $\mathcal{A}$, so that $\mathcal{A} \longrightarrow_{\mathsf{exp}}^{(p,w,q)} \mathcal{B}$ if and only if $\mathcal{A} \longrightarrow_{\mathsf{exp}}^{(p',w',q')} \mathcal{B}$ and the latter is a reduced expansion.

(2) If $|u| + |v| \geq |w|$, then there exist words x, y, z, with y possibly empty, such that $u = xy$, $v = yz$ and $w = xyz$. Let p', p'', q', q'' be the states of $\mathcal{A}$ defined by the following paths

$$p \xrightarrow{x} p' \xrightarrow{y} p'', \quad q' \xrightarrow{y} q'' \xrightarrow{z} q.$$

Then $\mathcal{A} \longrightarrow_{\mathsf{exp}}^{(p,w,q)} \mathcal{B}$ if and only if $\mathcal{A} \longrightarrow_{\mathsf{i}}^{p'=q'} \mathcal{B}$, if and only if $\mathcal{A} \longrightarrow_{\mathsf{i}}^{p''=q''} \mathcal{B}$.

□

We derive from Fact 2.2 the following statement.

Proposition 2.3 *Let $\mathcal{A}$ and $\mathcal{B}$ be inverse automata. If $\mathcal{A} \longrightarrow_{\mathsf{e}}^{w} \mathcal{B}$, then $\mathcal{A} \longrightarrow_{\mathsf{i}} \mathcal{B}$ or $\mathcal{A} \longrightarrow_{\mathsf{re}}^{(p,u,q)} \mathcal{B}$ for some states p and q and a reduced word u such that $|u| \leq |w|$.*

The following converse statements are derived from Facts 2.1 and 2.2.

Proposition 2.4 *Let $\mathcal{A}$ be a reduced inverse automaton, let $H = L(\mathcal{A})\rho$, let u and v be reduced words labeling paths $q_0 \xrightarrow{u} p$ and $q_0 \xrightarrow{v} q$ in $\mathcal{A}$, and suppose that $\mathcal{A} \longrightarrow_{\mathsf{i}}^{p=q} \mathcal{B}$. Then $\mathcal{A} \longrightarrow_{\mathsf{e}}^{uv^{-1}} \mathcal{B}$ and $L(\mathcal{B})\rho = \langle H, uv^{-1}\rangle$.*

Proof. Let $\mathcal{A}'$ be the expansion of $\mathcal{A}$ by (q_0, uv^{-1}, q_0). The analysis in Fact 2.2 (2) shows that a step in the reduction of $\mathcal{A}'$ is provided by the automaton obtained in identifying p and q. The uniqueness statement in Proposition 1.3 then shows that $\mathcal{A} \longrightarrow_{\mathsf{e}}^{uv^{-1}} \mathcal{B}$ and we conclude by Proposition 1.2. □

Proposition 2.5 *Let $\mathcal{A}$ and $\mathcal{B}$ be reduced inverse automata, let w be a reduced word such that $\mathcal{A} \longrightarrow_{\mathsf{re}}^{(p,w,q)} \mathcal{B}$, let $H = L(\mathcal{A})\rho$, and let let u and v be reduced words labeling paths $q_0 \xrightarrow{u} p$ and $q_0 \xrightarrow{v} q$ in $\mathcal{A}$. Then $\mathcal{A} \longrightarrow_{\mathsf{e}}^{uwv^{-1}} \mathcal{B}$ and $L(\mathcal{B})\rho = \langle H, uwv^{-1}\rangle$.*

Proof. Since the expansion of $\mathcal{A}$ by (p, w, q) is a reduced expansion, the word uwv^{-1} is reduced and the expansion by (q_0, uwv^{-1}, q_0) falls in the situation described in Fact 2.2 (1). In view of Proposition 1.2, it follows that $\mathcal{A} \longrightarrow_{\mathsf{e}}^{uwv^{-1}} \mathcal{B}$, which concludes the proof.

□

We now introduce a measure of the *length* of a reduced expansion or an i-step σ, written $\lambda(\sigma)$: if σ is an i-step, then $\lambda(\sigma) = 0$; if σ is a reduced expansion, $\sigma = \longrightarrow_{\mathsf{re}}^{(p,w,q)}$, its length is the length of w, $\lambda(\sigma) = |w|$. We extend this notion of length to finite sequences of i-steps and reduced expansions: if $\bar{\sigma} = (\sigma_1, \ldots, \sigma_n)$ is such a sequence, we let

$$\lambda(\bar{\sigma}) = (\lambda(\sigma_1), \ldots, \lambda(\sigma_n)).$$

Finally, we introduce an order relation on the set of finite sequences of non-negative integers. Let $\bar{k} = (k_1, \ldots, k_n)$ and $\bar{\ell} = (\ell_1, \ldots, \ell_m)$ be such sequences. We say that $\bar{k} \preceq \bar{\ell}$ if

either $n < m$,

or $n = m$ and $\sum_{i=1}^{n} k_i^2 < \sum_{i=1}^{m} \ell_i^2$,

or $n = m$, $\sum_{i=1}^{n} k_i^2 = \sum_{i=1}^{m} \ell_i^2$ and $\bar{k}$ precedes $\bar{\ell}$ in the lexicographic order.

It is routine to check that $\preceq$ is a well-order on the set of finite sequences on non-negative integers, which is stable under the concatenation of sequences. We write $\bar{k} \prec \bar{\ell}$ if $\bar{k} \preceq \bar{\ell}$ and $\bar{k} \neq \bar{\ell}$.

Proposition 2.6 *Let $\mathcal{A}$, $\mathcal{A}'$ and $\mathcal{B}$ be inverse automata such that $\mathcal{A}'$ is obtained from $\mathcal{A}$ by a reduced expansion σ_1 and $\mathcal{B}$ is obtained from $\mathcal{A}'$ by an i-step σ_2,*

$$\mathcal{A} \longrightarrow_{\mathsf{re}} \mathcal{A}' \longrightarrow_{\mathsf{i}} \mathcal{B}.$$

Then there exist a sequence of reduced expansions or i-steps $\bar{\sigma}'$ of length 1 or 2 such that $\mathcal{B}$ is obtained from $\mathcal{A}$ by applying the steps in $\bar{\sigma}'$ and $\lambda(\bar{\sigma}') \prec \lambda(\sigma_1, \sigma_2)$.

Proof. Suppose that $\mathcal{A} \longrightarrow_{\mathsf{re}}^{(p,w,q)} \mathcal{A}' \longrightarrow_{\mathsf{i}}^{r=s} \mathcal{B}$. The length of this sequence of transformations is $(|w|, 0)$.

Let Q be the state set of $\mathcal{A}$ and let u and v be reduced paths from q_0 to p and q,

$$q_0 \xrightarrow{u} p, \quad q_0 \xrightarrow{v} q.$$

Then uwv^{-1} is a reduced word and $L(\mathcal{A}')\rho = \langle L(\mathcal{A})\rho, uwv^{-1}\rangle$ by Proposition 1.2. We distinguish three cases, depending whether or not r and s lie in Q.

Case 1: $r, s \in Q$. Let x and y be reduced words labeling paths in $\mathcal{A}$ from q_0 to r and s respectively. Then the same words label similar paths in $\mathcal{A}'$ and it follows from Proposition 2.4 that

$$L(\mathcal{B})\rho = \langle L(\mathcal{A}')\rho, xy^{-1}\rangle = \langle L(\mathcal{A})\rho, uwv^{-1}, xy^{-1}\rangle.$$

Let also $\mathcal{A}''$ and $\mathcal{B}'$ be determined by $\mathcal{A} \longrightarrow_{\mathsf{i}}^{r=s} \mathcal{A}'' \longrightarrow_{\mathsf{e}}^{uwv^{-1}} \mathcal{B}'$. Then $L(\mathcal{B}')\rho$ is also equal to $\langle L(\mathcal{A})\rho, xy^{-1}, uwv^{-1}\rangle$, so that $\mathcal{B} = \mathcal{B}'$ by Proposition 1.3.

Note that the words u and v label paths from state q_0 in $\mathcal{A}''$ as well. It follows from Proposition 2.3 that, if $uwv^{-1} \notin L(\mathcal{A}'')$, then $\mathcal{B}$ can be obtained from $\mathcal{A}''$ by an i-step or by a reduced expansion of the form $\longrightarrow_{\mathsf{re}}^{(t,z,t')}$ with $|z| \leq |w|$.

Thus $\mathcal{B}$ is obtained from $\mathcal{A}$ either by a sequence of 1 or 2 transformations, of length 0 or $(0, k)$ with $0 \leq k \leq |w|$. This is $\prec$-less than $(|w|, 0)$, as expected.

Case 2: $r \in Q$ and $s \notin Q$. Let z be a reduced word labeling a path from q_0 to r in $\mathcal{A}$, and hence also in $\mathcal{A}'$. Let g be the unique reduced word labeling a path from p to s in $\mathcal{A}'$, using only edges that were not in $\mathcal{A}$. By assumption, g is a proper, non-empty prefix of w. Moreover, by Propositions 1.2 and 2.4,

$$L(\mathcal{B})\rho = \langle L(\mathcal{A}')\rho, ugz^{-1}\rangle = \langle L(\mathcal{A})\rho, uwv^{-1}, ugz^{-1}\rangle.$$

Let h be the longest common suffix of g and z, so that $g = g'h$, $z = z'h$, $g'z'^{-1}$ is reduced and we have the following paths in $\mathcal{A}'$,

$$q_0 \xrightarrow{z'} r' \xrightarrow{h} r, \quad p \xrightarrow{g'} s' \xrightarrow{h} s.$$

Fact 2.1 shows that $\mathcal{A}' \longrightarrow_{\mathsf{i}}^{r'=s'} \mathcal{B}$, so we may assume that $h = 1$, $g = g'$ and $z = z'$. There is a possibility that the word g is now empty (if h was in fact equal to g), but in that case, we are returned to the situation of Case 1, with $s' = p$. Thus we may still assume that $g \neq 1$. In particular, the word ugz^{-1} is reduced.

Then let $\mathcal{A}''$ and $\mathcal{B}'$ be defined by $\mathcal{A} \longrightarrow_{\mathsf{e}}^{ugz^{-1}} \mathcal{A}'' \longrightarrow_{\mathsf{e}}^{uwv^{-1}} \mathcal{B}'$. Again $L(\mathcal{B}')\rho = \langle L(\mathcal{A})\rho, uwv^{-1}, ugz^{-1}\rangle$, so $\mathcal{B} = \mathcal{B}'$ by Proposition 1.3.

Proposition 2.3 states that each e-step can be replaced by an i-step or by a reduced expansion of length bounded above by the length of the e-step. Going back to Fact 2.2, we see that the e-step $\mathcal{A} \longrightarrow_{\mathsf{e}}^{ugz^{-1}} \mathcal{A}''$ can be replaced by a transformation of length $k \leq |g|$ since both u and z can be read from state q_0 in $\mathcal{A}$. As for the e-step $\mathcal{A}'' \longrightarrow_{\mathsf{e}}^{uwv^{-1}} \mathcal{B}$, it can be replaced by a transformation of length $\ell \leq |w| - |g|$ since ug (a prefix of uw) and v can be read from state q_0 in $\mathcal{A}''$.

Now, it suffices to verify that $(k, \ell) \prec (|w|, 0)$, which is easily done if we observe that $k + \ell \leq |w|$ (so $k^2 + \ell^2 \leq |w|^2$) and $k < |w|$.

Case 3: $r, s \notin Q$. In that case, the word w factors as $w = w_1 w_2 w_3$ and the path in $\mathcal{A}'$ made of edges added to $\mathcal{A}$ factors as

$$p \xrightarrow{w_1} r \xrightarrow{w_2} s \xrightarrow{w_3} q.$$

Since $r \neq s$ and these vertices are not in Q, each of the three factors w_1, w_2, w_3 is non-empty. Moreover,

$$L(\mathcal{B})\rho = \langle L(\mathcal{A}')\rho, uw_1w_3v^{-1}\rangle = \langle L(\mathcal{A})\rho, uwv^{-1}, uw_1w_3v^{-1}\rangle.$$

Let h be the longest common suffix of w_1 and w_3^{-1}, so that $w_1 = w_1'h$, $w_3 = h^{-1}w_3'$, $w_1'w_3'$ is reduced and we have the following paths in $\mathcal{A}'$,

$$p \xrightarrow{w_1'} r' \xrightarrow{h} r \xrightarrow{w_2} s \xleftarrow{h} s' \xrightarrow{w_3'} q.$$

Proposition 2.1 shows that $\mathcal{A}' \longrightarrow_{\mathsf{i}}^{r'=s'} \mathcal{B}$, so we may assume that $h = 1$, $w_1 = w_1'$ and $w_3 = w_3'$. There is a possibility that the words w_1 or w_3 be now empty (if h was in fact equal to w_1 or w_3), but in that case, we are returned to the situation of Cases 1 or 2, with $r' = p$ or $s' = q$. Thus we may still assume that $w_1 \neq 1$ and $w_3 \neq 1$. In particular, the word $uw_1w_3v^{-1}$ is reduced.

Then let $\mathcal{A}''$ and $\mathcal{B}'$ be defined by $\mathcal{A} \longrightarrow_{\mathsf{e}}^{uw_1w_3v^{-1}} \mathcal{A}'' \longrightarrow_{\mathsf{e}}^{uwv^{-1}} \mathcal{B}'$. Then $L(\mathcal{B}')\rho = \langle L(\mathcal{A})\rho, uwv^{-1}, uw_1w_3v^{-1}\rangle$, so $\mathcal{B} = \mathcal{B}'$ by Proposition 1.3.

As in Case 2, we use Fact 2.2 to verify that the e-step $\mathcal{A} \longrightarrow_{\mathsf{e}}^{uw_1w_3v^{-1}} \mathcal{A}''$ can be replaced by a reduced expansion of length $k = |w_1w_3|$ since u and v are the maximal prefixes of $uw_1w_3v^{-1}$ and its inverse that can be read from state q_0 in $\mathcal{A}$. As for the e-step $\mathcal{A}'' \longrightarrow_{\mathsf{e}}^{uwv^{-1}} \mathcal{B}$, it can be replaced by a reduced expansion of length $\ell = |w_2|$ since uw_1 and vw_3^{-1} are the maximal prefixes of uwv^{-1} and its inverse that can be read from state q_0 in $\mathcal{A}''$.

Now, it suffices to verify that $(k, \ell) \prec (|w|, 0)$, which is easily done if we observe that $k + \ell = |w|$ (so $k^2 + \ell^2 \leq |w|^2$) and $k < |w|$. $\square$

3 Deciding whether $H \leq_{\mathsf{ff}} F$

3.1 A geometric characterization of free factors

We put together the technical results from Section 2 to prove the following characterization of free factors.

Theorem 3.1 *Let H, K be finitely generated subgroups of $F = F(A)$ and assume that $d = \mathsf{rank}(K) - \mathsf{rank}(H) > 0$. Then H is a free factor of K if and only if the inverse automaton $\Gamma_A(H)$ can be transformed in $\Gamma_A(K)$ by a sequence of $d' \leq d$ i-steps followed by $d - d'$ reduced expansions.*

Proof. We first observe that H is a free factor of K if and only if there exist d elements $k_1, \ldots, k_d$ of $F(A)$ such that $\langle H \cup \{k_1, \ldots, k_d\}\rangle = K$. This follows from the fact that an r-element generating set in a rank r free group, is a basis [6, Prop. I.3.5].

By definition of e-steps, this means that $H \leq_{\mathsf{ff}} K$ if and only if $\Gamma_A(H)$ yields $\Gamma_A(K)$ by a sequence of d e-steps.

Now Propositions 2.3, 2.4 and 2.5 show that this is equivalent to the fact that $\Gamma_A(H)$ yields $\Gamma_A(F(A))$ by a sequence of d i-steps or reduced expansions.

Since $\preceq$ is a well-order on the set of finite sequences of non-negative integers, we may consider a sequence $\bar{\sigma}$ of d i-steps and reduced expansions leading from $\Gamma_A(H)$ to $\Gamma_A(K)$, which is $\preceq$-minimal. Proposition 2.6 then shows that the i-steps in $\bar{\sigma}$ come before the reduced expansions. Thus, $H \leq_{\mathsf{ff}} K$ if and only if $\Gamma_A(H)$ yields $\Gamma_A(K)$ by a sequence of d' i-steps followed by $d - d'$ reduced expansions. $\square$

Corollary 3.2 *Let H be a finitely generated subgroup of $F = F(A)$, let A_0 be the set of letters in A that occur in $\Gamma_A(H)$ and let $d = |A_0| - \mathsf{rank}(H) = \mathsf{rank}(F(A_0)) - \mathsf{rank}(H)$. Then H is a free factor of F if and only if $\Gamma_A(H)$ can be transformed into a one-vertex automaton by a sequence of d i-steps.*

Proof. We first observe that $H \leq F(A_0)$ and $F(A_0) \leq_{\mathsf{ff}} F(A)$. It follows from standard results that H is a free factor of $F(A)$ if and only if it is a free factor of $F(A_0)$.

Now Theorem 3.1 shows that $H \leq_{\mathsf{ff}} F(A_0)$ if and only if $\Gamma_A(H)$ yields some inverse automaton $\mathcal{B}$ by a sequence of d' i-steps, and $\mathcal{B}$ yields $\Gamma_A(F(A_0))$ by a sequence of $d - d'$ reduced expansions.

Note that every letter of A_0 occurs in $\mathcal{B}$. Moreover, since $\Gamma_A(F(A_0))$ has only one state, $\mathcal{B}$ must be a one-state automaton as well by definition of reduced expansions. Thus $\mathcal{B} = \Gamma_A(F(A_0))$ and $d' = d$. $\square$

3.2 The algorithm

With the notation of Corollary 3.2, the algorithm to decide whether $H \leq_{\mathsf{ff}} K$ consists of the following. For each pair (p, q) of distinct states of $\Gamma_A(H)$, compute $\mathcal{B}$ such that $\Gamma_A(H) \longrightarrow_{\mathsf{i}}^{p=q} \mathcal{B}$. Repeat the same process for each $\mathcal{B}$ and continue until you have computed the result of all sequences of d i-steps from $\Gamma_A(H)$. Then $H \leq_{\mathsf{ff}} F$ if and only if one of these automata has a single state.

Let v be the number of states of $\Gamma_A(H)$ (which is certainly less than the total length of a basis of H). Then there are $O(v^2)$ (more precisely $\frac{1}{2}(v^2 - v)$) possible i-steps, each of which takes $O(v^2)$ time, and the resulting automata have at most $v - 1$ states. The sequences of i-steps that need to be explored can be viewed as a tree, whose nodes have $O(v^2)$ children and whose depth is d. There are, therefore, at most $O(v^{2d})$ nodes to explore.

For each of them, we need to compute the reduction of an automaton, in time at most $O(v^2)$, so the time complexity is $O(v^{2d+2})$.

Theorem 3.3 *Given a tuple $h_1, \ldots, h_n$ of elements of $F(A)$ of total length ℓ, one can decide whether the subgroup H generated by the h_i is a free factor of $F(A)$ in time $O(\ell^{2d+2})$, where $d = |A_0| - \mathsf{rank}(H)$ and A_0 is the set of letters in A that occur in the h_i.*

Remark 3.4 The tree exploration described above can be somewhat speeded up by the following observation: for every i-step $\mathcal{A} \longrightarrow_{\mathsf{i}} \mathcal{B}$, we have $\mathsf{rank}(L(\mathcal{B})\rho) \leq \mathsf{rank}(L(\mathcal{B})\rho)$ or $\mathsf{rank}(L(\mathcal{B})\rho) = \mathsf{rank}(L(\mathcal{B})\rho) + 1$. In the first case, the i-step cannot be part of a sequence of d i-steps leading to an increase of the rank by d, and the subtree below $\mathcal{B}$ can be ignored.

There are naturally further implementation tricks and ideas that can reduce the decision process, however without changing the worst-case complexity. $\square$

The algorithm to decide whether $H \leq_{\mathsf{ff}} K$, for given subgroups $H, K \leq F$ as in Theorem 3.1, can be described in the same fashion, with identical time complexity.

References

[1] S. Gersten. On Whitehead's algorithm, *Bull. Am. Math. Soc.* **10** (1984) 281-284.

[2] I. Kapovich and A.G. Myasnikov. Stallings Foldings and Subgroups of Free Groups, *J. Algebra*, **248**, 2 (2002), 608-668.

[3] 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.

[4] B. Khan. The structure of automorphic conjugacy in the free group of rank two. In: *Proc. Special Session on Interactions between Logic, Group Theory and Computer Science*, Contemp. Mathematics **349** (2004).

[5] D. Lee. Counting words of minimum length in an automorphic orbit, eprint `arXiv:math.GR/0311410`.

[6] R. Lyndon and P. Schupp. *Combinatorial group theory*, Springer, (1977, reprinted 2001).

[7] S. Margolis and J. Meakin. Free inverse monoids and graph immersions, *Int. J. Algebra and Comput.* **3** (1993) 79–100.

[8] S. Margolis, M. Sapir, P. Weil. Closed subgroups in pro-**V** topologies and the extension problem for inverse automata, *Intern. J. Algebra and Computation* **11** (2001) 405–445.

[9] A.G. Myasnikov, V. Shpilrain. Automorphic orbits in free groups, *J. Algebra* **269** (2003) 18-27.

[10] D. Perrin. Automata, in (J. Leeuwen ed.) *Handbook of Theoretical Computer Science*, vol. B, Elsevier, 1990.

[11] J. Rotman. *An introduction to the theory of groups*, 4th edition, Springer, 1995.

[12] J.-P. Serre. *Arbres, amalgames, SL_2*, Astérisque **46**, Soc. Math. France, 1977. English translation: *Trees*, Springer Monographs in Mathematics, Springer, 2003.

[13] J. Stallings. The topology of graphs, *Inventiones Mathematicæ* **71** (1983) 551–565.

[14] J. Stephen. *Applications of automata theory to presentations of monoids and inverse monoids*, Ph.D. Dissertation, University of Nebraska, 1987.

[15] N. Touikan. `http://www.sci.ccny.cuny.edu/~shpil/algcryp2005.html`.

[16] E. Ventura. On fixed subgroups of maximal rank, *Comm. Algebra*, **25** (1997), 3361-3375.