The generalized conjugacy problem for virtually free groups

Manuel Ladra

Departamento de Álgebra, Universidad de Santiago, Facultad de Matemáticas,
Campus Sur, E-15782 Santiago, Spain
e-mail: ladra@usc.es

and Pedro V. Silva

Centro de Matemática, Faculdade de Ciências, Universidade do Porto,
R. Campo Alegre 687, 4169-007 Porto, Portugal
e-mail: pvsilva@fc.up.pt

November 22, 2007

2000 Mathematics Subject Classification: 20F10, 5E15, 68R15

ABSTRACT

The generalized conjugacy problem (has g a conjugate in K for K rational?) is solved for [f.g. free]-by-finite groups with constraints that go beyond the context-free level, a new result for the free group itself. Moldavanskii's theorem on simultaneous conjugacy of f.g. subgroups of a free group is also generalized for [f.g. free]-by-finite groups and this wider class of constraints. The solution set of the equation $x^{-1}g\varphi(x) \in K$ in the free group (φ a virtually inner automorphism, K rational) is shown to be rational and effectively constructible, and a similar result is proved for the equation $xgx^{-1} \in K$ in a [f.g. free]-by-finite group. The twisted conjugacy problem with context-free constraints is also proved to be decidable for the free group.

1 Introduction

Given a group G, the *conjugacy problem* for G is said to be decidable if there exists an algorithm that decides, for arbitrary $g, h \in G$, whether or not they are conjugate. The terminology *generalized word problem* arises in combinatorial group theory when we replace the identity element in the equation $g = 1$ by an arbitrary finitely generated subgroup H through $g \in H$. What could be the analogous generalization for an arbitrary element h?

The standard notion of a *finitely generated subset* of a monoid/group is that of a *rational subset*, finite sets and finitely generated submonoids/subgroups constituting particular cases. Rational sets/languages play a most important role in language theory, automata theory and combinatorics on words (see [2] and [22]). We denote by RatG the set of all rational subsets of G.

The *generalized conjugacy problem* for G is said to be decidable if there exists an algorithm that decides, for arbitrary $g \in G$ and $K \in \mathrm{RatG}$, whether or not

$$\exists x \in G : \; xgx^{-1} \in K.$$

Further generalization is obtained through the use of *constraints*. Let $\mathcal{C}$ denote a collection of subsets of G. The *generalized conjugacy problem for G with constraints in $\mathcal{C}$* is said to be decidable if there exists an algorithm that decides, for arbitrary $g \in G$, $K \in \mathrm{RatG}$ and $C \in \mathcal{C}$, whether or not

$$\exists x \in C : \; xgx^{-1} \in K.$$

A group G is said to be virtually free if it has a free normal subgroup F of finite index. We consider in this paper the fundamental subcase of [finitely generated free]-by-finite groups, when F is assumed to be finitely generated as well. Clearly, every [f.g. free]-by-finite group is f.g., but the converse does not hold, most surface groups constituting counterexamples [4].

The conjugacy problem for [f.g. free]-by-finite groups is known to be decidable. This follows for instance from the fact they are hyperbolic, and hyperbolic groups have decidable conjugacy problem [12, 17]. The conjugacy problem has also been solved for [f.g. free]-by-cyclic groups by Bogopolski, Martino, Maslakova and Ventura [4].

On the other hand, Diekert, Gutiérrez and Hagenah proved in [7] a very strong generalization of the celebrated result of Makanin on free group equations [18]. They prove that the existential theory of equations with rational constraints in a free group F_A is decidable (PSPACE-complete, actually). As a consequence, the generalized conjugacy problem with rational constraints is decidable for F_A. Also, the problem of determining, for arbitrary $H_1, \ldots, H_n, K_1, \ldots, K_n \leq_{f.g.} F_A$ and $L \in \mathrm{RatF_A}$, whether or not

$$\exists x \in L : \; \forall i \in \{1, \ldots, n\} \; xH_ix^{-1} \subseteq K_i$$

turns out to be decidable as well, generalizing the classical result of Moldavanskii [20] (see also [16, Prop. I.2.23]), where no rational constraints are considered.

We concentrate our efforts on the one-variable equation

$$xgx^{-1} \in K$$

for a [f.g. free]-by-finite group G, $g \in G$ and $K \in \mathrm{RatG}$. We prove that its solution set is rational and effectively constructible. It follows that the generalized conjugacy problem for G with context-free constraints and many other types of constraints beyond rational is decidable. This seems to be a new result for the free group itself. We also obtain a generalization of the results of Moldavanskii for [f.g. free]-by-finite groups with context-free constraints. Example 5.1 shows that these results cannot be generalized to arbitrary one-variable equations, even for free groups.

On doing so, we are led to investigate the solution set of the equation $x^{-1}g\varphi(x) \in K$ for $g \in F_A$, $K \in \mathrm{RatF_A}$ and a virtually inner automorphism φ of F_A. An automorphism is said to be virtually inner if some of its powers is an inner automorphism. These are the type of automorphisms of F_A induced by inner automorphisms of [f.g. free]-by-finite groups. Bogopolski, Martino, Maslakova and Ventura proved in [4] that the equation $x^{-1}g\varphi(x) = h$

is solvable for arbitrary $g, h \in F_A$ and $\varphi \in \mathrm{AutF_A}$ (twisted conjugacy problem). We prove that the solution set of $x^{-1}g\varphi(x) \in K$ is rational and effectively constructible if φ is virtually inner. We also show (considering arbitrary automorphisms) that the twisted conjugacy problem for F_A with context-free constraints (and others) is decidable.

Example 5.2 shows that these results cannot be generalized to arbitrary automorphisms. The problem of determining the existence of solutions for arbitrary φ and K remains open.

The techniques used in this paper are essentially automata-theoretic, and various combinatorial aspects of finite and infinite words are explored. Topological and dynamical arguments play also an important role, namely when we need to involve the border of a free group and extensions of automorphisms to its end completion. Our results depend strongly on the following important theorems regarding $\varphi \in \mathrm{AutF_A}$: (1) the fixed point subgroup $\mathrm{Fix}\varphi$ is f.g. (Cooper [6] and Gersten [11]); (2) $\mathrm{Fix}\varphi$ is effectively constructible (Maslakova [19]); (3) every fixed point of the end extension $\widehat{\varphi}$ is either singular, an attractor or a repeller (Gaboriau, Jaeger, Levitt and Lustig [10]).

We describe now the structure of the paper.

In Section 2, all preliminary concepts and results needed for the main proofs are presented. This section is organized in four subsections (Languages and automata, Free groups, Automorphisms, Virtually free groups) and is intended to be fairly self-contained to make the paper readable for both group-theorists and automata-theorists.

Section 3 is devoted to the discussion of the equation $x^{-1}g\varphi(x) \in K$ in a free group F_A, for $g \in F_A$, $\varphi \in \mathrm{AutF_A}$ virtually inner and $K \in \mathrm{RatF_A}$. The main proofs of the paper can be found here.

Section 4 applies the results of Section 3 to [f.g. free]-by-finite groups, providing solutions for the generalized conjugacy problem with constraints, simultaneous conjugacy of subgroups and other problems.

Finally, we present in Section 5 several counterexamples that show that the most obvious generalizations of our results fail. We suggest also open problems that arise naturally from this work.

2 Preliminaries

2.1 Languages and automata

Given a finite alphabet A, we denote by A^* the *free monoid on* A, with 1 denoting the empty word. A subset of A^* is said to be an *A-language*.

We say that $\mathcal{A} = (Q, q_0, T, E)$ is a (finite) A-automaton if:

- Q is a (finite) set;
- $q_0 \in Q$ and $T \subseteq Q$;
- $E \subseteq Q \times A \times Q$.

A *nontrivial path* in $\mathcal{A}$ is a sequence

$$p_0 \xrightarrow{a_1} p_1 \xrightarrow{a_2} \dots \xrightarrow{a_n} p_n$$

with $(p_{i-1}, a_i, p_i) \in E$ for $i = 1, \ldots, n$. Its *label* is the word $a_1 \ldots a_n \in A^*$. It is said to be a *successful* path if $p_0 = q_0$ and $p_n \in T$. We consider also the *trivial path* $p \xrightarrow{1} p$ for $p \in Q$. It is successful if $p = p_0 \in T$. The *language* $L(\mathcal{A})$ *recognized by* $\mathcal{A}$ is the set of all labels of successful paths in $\mathcal{A}$. A path of minimal length between two vertices is called a *geodesic*, and so does its label by extension.

The automaton $\mathcal{A} = (Q, q_0, T, E)$ is said to be *deterministic* if, for all $p \in Q$ and $a \in A$, there is at most one edge of the form (p, a, q). We write then $q = pa$. We say that $\mathcal{A}$ is *trim* if every $q \in Q$ lies in some successful path.

The *star* operator on A-languages is defined by

$$L^* = \bigcup_{n \geq 0} L^n,$$

where $L^0 = \{1\}$. An A-language L is said to be *rational* if L can be obtained from finite languages using finitely many times the operators union, product and star. Alternatively, L is rational if and only if it is recognized by a finite (deterministic) A-automaton $\mathcal{A} = (Q, q_0, T, E)$. The set of all rational A-languages is denoted by RatA.

Given a finitely generated monoid M, we say that $K \subseteq M$ is a rational subset of M if K can be obtained from finite subsets of M using finitely many times the operators union, product and star. Alternatively, if we fix a surjective homomorphism $\varphi : A^* \to M$, K is rational if and only if $K = \varphi(L)$ for some $L \in \mathrm{RatA}$. The set of all rational subsets of M is denoted by RatM.

In the statement of a result, we shall say that $K \in \mathrm{RatM}$ is *effectively constructible* if there exists an algorithm to produce from the data implicit in the statement a finite A-automaton $\mathcal{A}$ such that $K = \varphi(L(\mathcal{A}))$.

2.2 Free groups

Let A denote a finite alphabet and let A^{-1} denote a set of formal inverses of A. The *free group on* A is the quotient

$$F_A = (A \cup A^{-1})^*/\eta,$$

where η denotes the congruence on $(A \cup A^{-1})^*$ generated by the relation

$$\{(aa^{-1}, 1) \mid a \in A \cup A^{-1}\}.$$

We denote the canonical projection $(A \cup A^{-1})^* \to F_A$ by π.

Let

$$R_A = (A \cup A^{-1})^* \setminus (\bigcup_{a \in A \cup A^{-1}} (A \cup A^{-1})^* aa^{-1} (A \cup A^{-1})^*)$$

denote the set of all reduced words in $(A \cup A^{-1})^*$ and let $\iota : (A \cup A^{-1})^* \to R_A$ denote the reduction map. Since $\eta = \mathrm{Ker}\iota$, we abuse notation and denote also by ι the induced bijection $F_A \to R_A$. The *length* of $g \in F_A$ is defined by $|g| = |\iota(g)|$. To simplify notation, we shall usually write $\overline{u} = \iota(u)$. We consider also sometimes the natural actions of $(A \cup A^{-1})^*$ on F_A defined by

$$\begin{aligned} (A \cup A^{-1})^* \times F_A &\to F_A \\ (u, g) &\mapsto ug = \pi(u)g \end{aligned} \qquad\qquad \begin{aligned} F_A \times (A \cup A^{-1})^* &\to F_A \\ (g, u) &\mapsto gu = g\pi(u). \end{aligned}$$

Basically, when we have a product of words and free group elements, we assume that the result is a free group element.

Let $u, v \in R_A$. If $u = vx$ for some $x \in R_A$, we say that v is a *prefix* of u and write $u \leq v$. This partial order on R_A induces the prefix partial order on F_A.

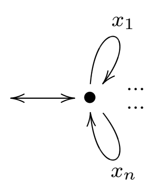
If $\mathcal{A} = (Q, q_0, T, E)$ is an $(A \cup A^{-1})$-automaton, the *dual* of an edge (p, a, q) is (q, a^{-1}, p). Then $\mathcal{A}$ is said to be *dual* if E contains the duals of all edges. It is said to be *inverse* if it is dual, deterministic, trim and $|T| = 1$.

Given a finitely generated subgroup H of F_A, we denote by $\mathcal{R}(H)$ the finite automaton associated to H by the construction often referred to by *Stallings foldings*. This construction, that can be traced back to the early part of the twentieth century [23, Chap. 11], was made explicit by Serre [24] and Stallings [26] (see also [14]).

We can describe it briefly as follows.

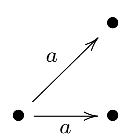
1. We take a finite generating set $X = \{x_1, \ldots, x_n\}$ for H in reduced form.

2. We build the *flower automaton*



where the petals are paths labelled by the generators and their dual edges.

3. We successively fold all edges of the form



$(a \in A \cup A^{-1})$ until no further folding applies.

The following proposition summarizes some of the relevant properties of $\mathcal{R}(H)$ (see [14]):

Proposition 2.1 *Let $H \leq_{f.g.} F_A$. Then:*

(i) *$\mathcal{R}(H)$ is a finite inverse automaton;*

(ii) *if $p \xrightarrow{u} q$ is a path in $\mathcal{R}(H)$, so is $p \xrightarrow{\overline{u}} q$;*

(iii) *$\mathcal{R}(H)$ does not depend on the finite reduced generating set chosen;*

(iv) *for every $u \in R_A$, $u \in L(\mathcal{R}(H))$ if and only if $\pi(u) \in H$;*

(v) *$L(\mathcal{R}(H)) \subseteq \pi^{-1}(H)$.*

We present now the important Benois Theorem, that establishes bridges between $\mathrm{RatF_A}$ and $\mathrm{Rat(A \cup A^{-1})}$:

Theorem 2.2 *[1]*

(i) If $L \in \mathrm{Rat}(\mathrm{A} \cup \mathrm{A}^{-1})$, *then* $\overline{L} \in \mathrm{Rat}(\mathrm{A} \cup \mathrm{A}^{-1})$ *and is effectively constructible.*

(ii) If $K \subseteq F_A$, *then* $K \in \mathrm{RatF_A}$ *if and only if* $\overline{K} \in \mathrm{Rat}(\mathrm{A} \cup \mathrm{A}^{-1})$.

It is convenient to summarize some of the properties of $\mathrm{Rat}(\mathrm{A} \cup \mathrm{A}^{-1})$ in the following result (see [2] e.g.):

Proposition 2.3 *Let* A *be a finite alphabet. Then:*

(i) $\mathrm{Rat}(\mathrm{A} \cup \mathrm{A}^{-1})$ *is closed for Boolean operations;*

(ii) if $L \in \mathrm{Rat}(\mathrm{A} \cup \mathrm{A}^{-1})$, *then* $L^{-1} \in \mathrm{Rat}(\mathrm{A} \cup \mathrm{A}^{-1})$.

Moreover, all the constructions are effective.

2.3 Automorphisms

Let $\mathrm{AutF_A}$ denote the group of all automorphisms of F_A. If $\varphi \in \mathrm{AutF_A}$ and no confusion arises, we shall denote also by φ the corresponding bijection of R_A.

The following result is immediate:

Proposition 2.4 *Let* $L \subseteq R_A$ *and* $\varphi \in \mathrm{AutF_A}$. *If* $L \in \mathrm{Rat}(\mathrm{A} \cup \mathrm{A}^{-1})$, *then* $\varphi(L) \in \mathrm{Rat}(\mathrm{A} \cup \mathrm{A}^{-1})$ *and the construction is effective.*

Indeed, it follows from the equality $\varphi(L) = \overline{\psi(L)}$, where $\psi : (A \cup A^{-1})^* \to (A \cup A^{-1})^*$ is the monoid homomorphism defined by $\psi(a) = \overline{\varphi(a)}$ $(a \in A \cup A^{-1})$.

Note that an endomorphism of F_A is an automorphism if and only if it is onto, due to F_A being hopfian [16, Prop. I.3.5]. The *inner* automorphisms of F_A are of the form

$$\begin{aligned} \lambda_g : F_A &\to F_A \qquad (g \in F_A). \\ x &\mapsto gxg^{-1} \end{aligned}$$

It is well known that the inner automorphisms of F_A constitute a normal subgroup of $\mathrm{AutF_A}$.

We say that $\varphi \in \mathrm{AutF_A}$ is *virtually inner* if φ^n is inner for some $n \geq 1$. We shall denote the subset of all virtually inner automorphisms of F_A by $\mathrm{ViaF_A}$.

Proposition 2.5 *Let* $\varphi \in \mathrm{ViaF_A}$ *and* $g \in F_A$. *Then* $\varphi^{-1}, \lambda_g\varphi, \varphi\lambda_g \in \mathrm{ViaF_A}$.

Proof. Assume that $\varphi^n = \lambda_z$. Then $(\varphi^{-1})^n = (\varphi^n)^{-1} = (\lambda_z)^{-1} = \lambda_{z^{-1}}$ and so $\varphi^{-1} \in \mathrm{ViaF_A}$.

It is immediate that

$$\varphi\lambda_h = \lambda_{\varphi(h)}\varphi \qquad (1)$$

holds for every $h \in F_A$, hence

$$(\lambda_g\varphi)^n = \lambda_g\lambda_{\varphi(g)} \ldots \lambda_{\varphi^{n-1}(g)}\varphi^n = \lambda_{g\varphi(g)\ldots\varphi^{n-1}(g)z}$$

and so $\lambda_g\varphi \in \mathrm{ViaF_A}$. Similarly,

$$(\varphi\lambda_g)^n = \lambda_{\varphi(g)\ldots\varphi^{n-1}(g)zg}$$

and $\varphi\lambda_g \in \mathrm{ViaF_A}$. □

A most important feature of automorphisms of F_A is the *bounded reduction* property:

Proposition 2.6 *[10] Let $\varphi \in \mathrm{AutF_A}$. Then there exists some $M \in \mathbb{N}$ such that, whenever $u, v \in R_A$ with uv reduced,*

$$|\overline{\varphi(u)\varphi(v)}| \geq |\varphi(u)| + |\varphi(v)| - 2M.$$

In other words, at most M letters of $\varphi(u)$ (or $\varphi(v)$) can be cancelled in the reduction of $\varphi(u)\varphi(v)$.

Given $\varphi \in \mathrm{AutF_A}$, we write

$$\mathrm{Fix}\varphi = \{\mathrm{x} \in \mathrm{F_A} \mid \varphi(\mathrm{x}) = \mathrm{x}\}.$$

Cooper [6] and Gersten [11] proved that $\mathrm{Fix}\varphi$ is a finitely generated subgroup of F_A, which implies that $\mathrm{Fix}\varphi \in \mathrm{RatF_A}$. Bestvina and Handel improved this result in their celebrated paper on *train tracks*:

Theorem 2.7 *[3] For every $\varphi \in \mathrm{AutF_A}$, $\mathrm{Fix}\varphi$ is a finitely generated subgroup of F_A of rank at most $|A|$.*

The following result from Maslakova implies that $\mathrm{Fix}\varphi$ is effectively constructible from φ.

Theorem 2.8 *[19] For every $\varphi \in \mathrm{AutF_A}$, it is possible to compute a finite generating set for $\mathrm{Fix}\varphi$.*

An infinite word $\alpha = a_1a_2\ldots$ ($a_i \in A \cup A^{-1}$) is said to be *irreducible* if a_ia_{i+1} is irreducible for every $i \in \mathbb{N}$. Let ∂F_A denote the set of all infinite irreducible words $a_1a_2\ldots$ ($a_i \in A \cup A^{-1}$). Write

$$\widehat{F_A} = F_A \cup \partial F_A.$$

Given $\alpha \in \widehat{F_A}$ (irreducible) and $n \in \mathbb{N}$, we denote by $\alpha^{(n)}$ the n-th letter of α (if $\alpha \in F_A$ and $n > |\alpha|$, we set $\alpha^{(n)} = 1$). We also write

$$\alpha^{[n]} = \alpha^{(1)}\alpha^{(2)}\ldots\alpha^{(n)}.$$

For all $\alpha, \beta \in \widehat{F_A}$, we define

$$r(\alpha,\beta) = \begin{cases} \min\{n \in \mathbb{N} \mid \alpha^{(n)} \neq \beta^{(n)}\} & \text{if } \alpha \neq \beta \\ \infty & \text{if } \alpha = \beta \end{cases}$$

and we write

$$d(\alpha,\beta) = 2^{-r(\alpha,\beta)},$$

using the convention $2^{-\infty} = 0$. It follows easily from the definition that d is an ultrametric on $\widehat{F_A}$, satisfying in particular the axiom

$$d(\alpha,\beta) \leq \max\{d(\alpha,\gamma), d(\gamma,\beta)\}.$$

It is well known that the metric space $\widehat{F_A}$ is compact (and therefore complete) (see [5] for a more general situation), in fact is the completion of its subspace F_A. We say that $\widehat{F_A}$

is the *end completion* of F_A and ∂F_A its *border*. Note that $\lim_{n\to\infty} \alpha_n = \alpha$ if and only if $\lim_{n\to\infty} r(\alpha_n, \alpha) = \infty$ if and only if

$$\forall k \in \mathbb{N}\, \exists m \in \mathbb{N}\, \forall n \in \mathbb{N}\, (n \geq m \Rightarrow \alpha_n^{[k]} = \alpha^{[k]}).$$

Furthermore, since $\widehat{F_A}$ is complete, a sequence $u_1, u_2, \ldots \in F_A$ converges if and only if it is a Cauchy sequence, i.e., if the condition

$$\forall k \in \mathbb{N}\, \exists m \in \mathbb{N}\, \forall n, n' \in \mathbb{N}\, (n, n' \geq m \Rightarrow u_n^{[k]} = u_{n'}^{[k]})$$

holds.

We also note that the product

$$\begin{aligned} F_A \times F_A &\to F_A \\ (u, v) &\mapsto uv \end{aligned}$$

and the mixed product

$$\begin{aligned} F_A \times \partial F_A &\to \partial F_A \\ (u, \alpha) &\mapsto u\alpha \end{aligned}$$

are continuous operations for the product topology.

If $u \in R_A$ is a nonempty cyclically reduced word, we denote by u^ω the infinite reduced word $uuu\ldots$ These words constitute important examples of elements in the border of F_A.

The following result is well known (see [5] for a more general discussion):

Proposition 2.9 *Let φ be an injective endomorphism of F_A. Then φ admits a unique continuous extension $\widehat{\varphi} : \widehat{F_A} \to \widehat{F_A}$. This extension is given by*

$$\widehat{\varphi}(\alpha) = \lim_{n\to\infty} \varphi(\alpha^{[n]}).$$

We shall refer to $\widehat{\varphi}$ as the *end extension* of φ.

Let $\varphi \in \mathrm{AutF_A}$ and $\alpha \in \mathrm{Fix}\widehat{\varphi}$. We say that α is *singular* if α is an adherence value of $\mathrm{Fix}\varphi$. Otherwise, we say that α is *regular*.

It is common knowledge that $\mathrm{Fix}\varphi = \mathrm{Fix}\varphi^{-1}$ yields $\mathrm{Fix}\widehat{\varphi} = \mathrm{Fix}\widehat{\varphi^{-1}}$: indeed, $\alpha = \widehat{\varphi}(\alpha) = \lim_{n\to\infty} \varphi(\alpha^{[n]})$ yields

$$\widehat{\varphi^{-1}}(\alpha) = \widehat{\varphi^{-1}}(\lim_{n\to\infty} \varphi(\alpha^{[n]})) = \lim_{n\to\infty} \varphi^{-1}\varphi(\alpha^{[n]})) = \lim_{n\to\infty} \alpha^{[n]} = \alpha$$

since continuous mappings commute with limits. Therefore we can define $\alpha \in \mathrm{Fix}\widehat{\varphi}$ regular to be

- an *attractor* if

$$\exists \varepsilon > 0\, \forall \beta \in \widehat{F_A}\, (d(\alpha, \beta) < \varepsilon \,\Rightarrow\, \lim_{n\to\infty} \widehat{\varphi}^n(\beta) = \alpha);$$

- a *repeller* if

$$\exists \varepsilon > 0\, \forall \beta \in \widehat{F_A}\, (d(\alpha, \beta) < \varepsilon \,\Rightarrow\, \lim_{n\to\infty} \widehat{\varphi^{-1}}^n(\beta) = \alpha).$$

Therefore α is a repeller for $\widehat{\varphi}$ if and only if it is an attractor for $\widehat{\varphi^{-1}}$.

The following result of Gaboriau, Jaeger, Levitt and Lustig is essential for the classification of the fixed points of the end extension:

Theorem 2.10 *[10] Let $\varphi \in \mathrm{AutF_A}$ and $\alpha \in \mathrm{Fix}\widehat{\varphi}$. Then α is either singular, an attractor or a repeller.*

2.4 Virtually free groups

We say that a group G is *virtually free* if G has a free (normal) subgroup F of finite index. Clearly, if F is finitely generated, so is G. However, the converse need not to be true. We shall be considering the case of F being f.g. Such groups are said to be *[f.g. free]-by-finite*.

Assume that $F = F_A$ is a f.g. free normal subgroup of finite index of the [f.g. free]-by-finite group G. We may decompose G as a disjoint union of cosets

$$G = Fb_0 \cup \ldots \cup Fb_m \tag{2}$$

with $b_0 = 1$. For $i = 1, \ldots, m$, and since $F \trianglelefteq G$, we can define $\varphi_i \in \mathrm{AutF}$ by $\varphi_i(u) = b_i u b_i^{-1}$. Since $|G/F| = m + 1$, we have $b_i^{m+1} \in F$ and so $\varphi_i \in \mathrm{ViaF}$. Taking in mind the normal form (2), it follows easily that for $i, j \in \{1, \ldots, m\}$ there exist $\varphi_i \in \mathrm{ViaF_A}$, $r_i, s_{ij} \in R_A$ and mappings $\alpha : \{1, \ldots, m\} \to \{1, \ldots, m\}$, $\beta : \{1, \ldots, m\}^2 \to \{0, \ldots, m\}$ such that G admits a (finite) presentation of the form

$$\langle A, b_1, \ldots, b_m \mid b_i a b_i^{-1} = \varphi_i(a),\ b_i^{-1} = r_i b_{\alpha(i)},\ b_i b_j = s_{ij} b_{\beta(i,j)}\ (i, j = 1, \ldots, m)\rangle, \tag{3}$$

which we shall fix as the *standard presentation* for G.

The following result is a particular case of [25, Proposition 4.1]:

Proposition 2.11 *Let $G = Fb_0 \cup \ldots \cup Fb_m$ be a [f.g. free]-by-finite group with $F_A = F \trianglelefteq G$ f.g. Then* RatG *consists of all subsets of the form*

$$\bigcup_{i=0}^{m} L_i b_i \qquad\qquad (L_i \in \mathrm{RatF_A}).$$

Moreover, it follows from the proof of [25, Proposition 4.1] that, given a standard presentation for G and $L \in \mathrm{RatG}$, the components L_i can be effectively computed from L. Thus it is fair to assume that a rational subset of G is supposedly given in this form. Therefore all questions regarding effectiveness of computations or constructions will be discussed at the component level.

3 The equation $x^{-1}g\varphi(x) \in K$ in the free group

We consider now the equation $x^{-1}g\varphi(x) \in K$ for $g \in F_A$, $\varphi \in \mathrm{AutF_A}$ and $K \in \mathrm{RatF_A}$. We shall use the notation

$$\mathrm{Sol}(g, \varphi, K) = \{x \in F_A \mid x^{-1}g\varphi(x) \in K\}.$$

Lemma 3.1 *Let $H \leq_{f.g.} F_A$ and $\mathcal{R}(H) = (Q, q_0, q_0, E)$. For every $q \in Q$, fix a geodesic $q_0 \xrightarrow{g_q} q$ in $\mathcal{R}(H)$. Write*

$$J = \{(q, a) \in Q \times (A \cup A^{-1}) \mid qa \textit{ is not defined}\}. \tag{4}$$

Then R_A decomposes as a union of rational $(A \cup A^{-1})$-languages through

$$R_A = (\bigcup_{q \in Q} \overline{Hg_q}) \bigcup (\bigcup_{(q,a) \in J} \overline{Hg_q} a R_A \cap R_A). \tag{5}$$

Proof. Let $x \in R_A$, and assume that $x \notin \bigcup_{q\in Q} \overline{Hg_q}$. Suppose that $q_0 \xrightarrow{x} q$ is a path in $\mathcal{R}(H)$. Then $xg_q^{-1} \in L(\mathcal{R}(H))$ and so $xg_q^{-1} \in L(\mathcal{R}(H))$. By Lemma 2.1(ii) and (iv), we obtain $\overline{xg_q^{-1}} \in L(\mathcal{R}(H))$ and $\pi(xg_q^{-1}) \in H$. Thus $\pi(x) \in Hg_q$ and so $x = \overline{x} \in \overline{Hg_q}$, hence a contradiction. Thus x labels no path $q_0 \xrightarrow{x} q$ in $\mathcal{R}(H)$ and so we may factor $x = x'ax''$ where $q_0 \xrightarrow{x'} q$ is a path in $\mathcal{R}(H)$ and $(q, a) \in J$. By the argument above, we have $x' \in \overline{Hg_q}$ and so $x \in \overline{Hg_q}aR_A \cap R_A$. Therefore (5) holds.

Since H is finitely generated, we have $H \in \mathrm{RatF_A}$. By Theorem 2.2(ii), $\overline{Hg_q} \in \mathrm{Rat}(\mathrm{A} \cup \mathrm{A}^{-1})$. Since $R_A = \overline{(A \cup A^{-1})^*} \in \mathrm{Rat}(\mathrm{A} \cup \mathrm{A}^{-1})$ by Theorem 2.2(i) and $\mathrm{Rat}(\mathrm{A} \cup \mathrm{A}^{-1})$ is closed for intersection by Proposition 2.3(i), we conclude that

$$\overline{Hg_q}aR_A \cap R_A \in \mathrm{Rat}(\mathrm{A} \cup \mathrm{A}^{-1})$$

as well. □

For the remaining part of this section, we fix $\varphi \in \mathrm{ViaF_A}$ such that $\varphi^n = \lambda_z$, $H = \mathrm{Fix}\varphi$ and $\mathcal{R}(H) = (Q, q_0, q_0, E)$. For every $q \in Q$, we fix a geodesic $q_0 \xrightarrow{g_q} q$ in $\mathcal{R}(H)$ and take J as in (4).

Recall that $u \in F_A$ is *primitive* if it is not a positive power of a different word.

Lemma 3.2 *For every $(q, a) \in J$, let*

$$Y = \{v \in R_A \mid g_q a \leq v \leq \varphi(v)\}$$

and write $z = rd^k r^{-1}$ with $l \geq 1$ and d primitive cyclically reduced. Then there exist finite subsets X_1, X_2, X_3 of R_A such that

$$Y = X_1 \cup rd^* X_2 \cup r(d^{-1})^* X_3. \tag{6}$$

Proof. We start with an auxiliary lemma that does most of the job:

Lemma 3.3 *Suppose that (v_i) is an infinite sequence of distinct elements of Y. Then:*

(i) $z \neq 1$;

(ii) $(v_i)_i$ *must have* rd^ω *or* $r(d^{-1})^\omega$ *as an adherence value;*

(iii) $\varphi(d) = td_2d_1t^{-1}$ *for some* $t \in R_A$ *and some factorization* $d = d_1d_2$;

(iv) *there exist* $i_0, j_0 \in \mathbb{N}$ *such that*

$$\varphi(rd^{i_0}) = rd^{j_0}d_1t^{-1}, \quad \varphi(rd^{-(j_0+1)}) = rd^{-i_0}d_2^{-1}t^{-1};$$

(v) *there exists* $M' \in \mathbb{N}$ *such that, for all* $f \in R_A$ *and* $k \in \mathbb{N}$,

$$rd^{M'+k}f \in Y \Leftrightarrow rd^{M'}f \in Y,$$

$$rd^{-M'-k}f \in Y \Leftrightarrow rd^{-M'}f \in Y.$$

Proof. Suppose that (v_i) is an infinite sequence of distinct elements of Y. Since $\widehat{F_A}$ is compact, (v_i) has an adherence value $\alpha \in \partial F_A$. Since d induces the discrete topology on F_A, we must have $\alpha \in \partial F_A$. Refining the sequence (v_i), we may assume that $\lim_{i\to\infty} v_i = \alpha$. Since $\widehat{\varphi}$ is continuous, we get

$$\widehat{\varphi}(\alpha) = \widehat{\varphi}(\lim_{i\to\infty} v_i) = \lim_{i\to\infty} \varphi(v_i).$$

Since $v_i \leq \varphi(v_i)$ for every i and $\lim_{i\to\infty} |v_i| = +\infty$ due to the v_i being distinct, it follows easily that $\lim_{i\to\infty} v_i = \lim_{i\to\infty} \varphi(v_i)$. Hence

$$\widehat{\varphi}(\alpha) = \lim_{i\to\infty} v_i = \alpha$$

and so $\alpha \in \mathrm{Fix}\widehat{\varphi}$.

By Theorem 2.10, α is either singular, an attractor or a repeller. Suppose that α is singular. Then there exists a sequence (h_i) in $H = \mathrm{Fix}\varphi$ such that $\alpha = \lim_{i\to\infty} h_i$. In particular, there exists some $h_j \in H$ such that $r(h_j, \alpha) \geq |g_q| + 2$. Since $\alpha = \lim_{i\to\infty} v_i$, it follows that $g_q a \leq \alpha$. Thus $g_q a \leq h_j$ and so $g_q a$ labels a path in $\mathcal{R}(H)$ out of the initial vertex, contradicting $(q, a) \in J$. Therefore α is either an attractor or a repeller.

Recall we are assuming $\varphi^n = \lambda_z$. Suppose that $z = 1$. Then the orbit

$$\{\varphi^i(u);\ i \in \mathbb{Z}\}$$

is finite for every $u \in F_A$. However, if α is an attractor (respectively, a repeller), there exists some $u \in F_A$ such that $\lim_{i\to\infty} \varphi^i(u) = \alpha$ (respectively, $\lim_{i\to\infty} \varphi^{-i}(u) = \alpha$), hence a contradiction since an infinite word cannot be the limit of finitely many finite words. Therefore $z \neq 1$ and (i) holds.

We have

$$\lim_{i\to\infty} z^i = rddd\ldots = rd^\omega$$

and $\lim_{i\to\infty} z^{-i} = r(d^{-1})^\omega$. We show next that

$$\alpha \in \{rd^\omega, r(d^{-1})^\omega\}. \tag{7}$$

Assume first that α is an attractor. Then there exists some $m \in \mathbb{N}$ such that

$$\forall \beta \in \widehat{F_A}\ (r(\beta, \alpha) > m\ \Rightarrow\ \lim_{i\to\infty} \widehat{\varphi}^i(\beta) = \alpha).$$

Since the sequence (v_i) is infinite and $\alpha = \lim_{i\to\infty} v_i$, there exists some $j \in \mathbb{N}$ such that $r(\alpha, v_j) > m$. Thus $\alpha = \lim_{i\to\infty} \varphi^i(v_j)$. In particular, since $\varphi^n = \lambda_z$,

$$\alpha = \lim_{i\to\infty} \varphi^{ni}(v_j) = \lim_{i\to\infty} z^i v_j z^{-i} = \lim_{i\to\infty} rs^i r^{-1} v_j r s^{-i} r^{-1}.$$

Hence $|s^k r^{-1} v_j r s^{-k}| > |\overline{r^{-1} v_j r}|$ for some k and so neither the first nor the last letter of $s^k r^{-1} v_j r s^{-k}$ are cancelled in its reduction. Hence, for every $i \geq k$,

$$\overline{z^i v_j z^{-i}} = rs^{i-k}\overline{s^k r^{-1} v_j r s^{-k}} s^{k-i} r^{-1}$$

and so $\alpha = rs^\omega = rd^\omega$ as claimed.

Assume now that α is a repeller. Then there exists some $m \in \mathbb{N}$ such that

$$\forall \beta \in \widehat{F_A}\ (r(\beta, \alpha) > m \ \Rightarrow\ \lim_{i\to\infty} \widehat{\varphi^{-1}}^i(\beta) = \alpha).$$

Similarly to the attractor case, we get

$$\alpha = \lim_{i\to\infty} \varphi^{-ni}(v_j) = \lim_{i\to\infty} z^{-i} v_j z^i$$

for some j, and finally $\alpha = r(d^{-1})^\omega$. Therefore (7) holds and so does (ii).

To prove (iii), we show that it follows from the equality $\widehat{\varphi}(rd^\omega) = rd^\omega$. So, even if $\alpha = r(d^{-1})^\omega$, we may derive that $\varphi(d^{-1}) = td_1^{-1}d_2^{-1}t^{-1}$ for some $t \in R_A$ and some factorization $d^{-1} = d_2^{-1}d_1^{-1}$, that yields (iii) as well after inversion.

Recall that $\beta \in \partial F_A$ has *period* p if $\beta^{(i+p)} = \beta^{(i)}$ for every $i \in \mathbb{N}$. Write $\varphi(d) = tct^{-1}$ with c cyclically reduced. Then $rd^\omega = \widehat{\varphi}(rd^\omega) = xc^\omega$ for some $x \in R_A$ and so d^ω has period $|c|$. Since d^ω has period $|d|$ trivially, it follows from the classical Fine and Wilf's Theorem [8] that $\gcd(|d|, |c|)$ is a period of d^ω as well. Since d is not a proper power, this implies that $|d|$ must divide $|c|$ and so $c = (d_2d_1)^k$ for some cyclic conjugate d_2d_1 of $d = d_1d_2$ and some $k \geq 1$. Now

$$\varphi(d) = tct^{-1} = t(d_2d_1)^k t^{-1} = (td_2d_1t^{-1})^k.$$

Since d is primitive, so must be $\varphi(d)$, hence $k = 1$ and so (iii) holds.

To prove (iv), assume first that $\alpha = rd^\omega$. Then

$$rd^\omega = \widehat{\varphi}(rd^\omega) = \overline{\varphi(r)t(d_2d_1)^\omega} = \overline{\varphi(r)td_2d^\omega},$$

hence $\overline{\varphi(r)td_2d^i} = rd^j$ for some $i, j \in \mathbb{N}$. Thus

$$\varphi(rd^{i+1}) = \overline{\varphi(r)t(d')^{i+1}t^{-1}} = \overline{\varphi(r)td_2d^id_1t^{-1}} = rd^jd_1t^{-1}.$$

Thus there exist $i_0, j_0 \in \mathbb{N}$ such that $\varphi(rd^{i_0}) = rd^{j_0}d_1t^{-1}$. Now in F_A we have

$$\begin{aligned}\varphi(rd^{-(j_0+1)}) &= \varphi(rd^{i_0})\varphi(d^{-(i_0+j_0+1)}) = rd^{j_0}d_1t^{-1}(td_2d_1t^{-1})^{-(i_0+j_0+1)} \\ &= rd^{j_0}d_1(d_1^{-1}d_2^{-1})^{i_0+j_0+1}t^{-1} = rd^{j_0}(d_2^{-1}d_1^{-1})^{i_0+j_0}d_2^{-1}t^{-1} \\ &= rd^{-i_0}d_2^{-1}t^{-1}.\end{aligned}$$

On the other hand, if $\alpha = r(d^{-1})^\omega$, we use a similar argument to show that there exist $i_0, j_0 \in \mathbb{N}$ such that $\varphi(rd^{-(j_0+1)}) = rd^{-i_0}d_2^{-1}t^{-1}$. Then we proceed to get $\varphi(rd^{i_0}) = rd^{j_0}d_1t^{-1}$ and so (iv) holds.

Let M be the constant from Proposition 2.6. Let $M' \geq i_0 + M, j_0 + 1 + M$ be such that $|rd^{M'}| > |g_q|$.

Since $|rd^{M'}| > |g_q|$, we have $rd^{M'+k}f \in g_qaR_A \cap R_A$ if and only if $rd^{M'}f \in g_qaR_A \cap R_A$. For every $i \geq i_0$, we have

$$\varphi(rd^i) = rd^{j_0}d_1t^{-1}(td_2d_1t^{-1})^{i-i_0} = rd^{j_0+i-i_0}d_1t^{-1}.$$

In particular,

$$\varphi(rd^{M'+k}) = rd^{j_0+M'+k-i_0}d_1t^{-1}, \quad \varphi(rd^{M'}) = rd^{j_0+M'-i_0}d_1t^{-1}. \tag{8}$$

By Proposition 2.6, the reduction between $\varphi(rd^{M'+k})$ and $\varphi(f)$ affects at most M letters in each word. Since $M' \geq i_0 + M$, it follows that the reduced factor between $\varphi(rd^{M'+k})$ and $\varphi(f)$ is the same as between $\varphi(rd^{M'})$ and $\varphi(f)$. Now $rd^{M'+k}f$ can be obtained from $rd^{M'}f$ by inserting d^k after r, and it follows from (8) and our comment on the type of reduction that also $\varphi(rd^{M'+k}f)$ can be obtained from $\varphi(rd^{M'}f)$ by inserting d^k after the prefix r. Thus

$$rd^{M'+k}f \leq \varphi(rd^{M'+k}f) \Leftrightarrow rd^{M'}f \leq \varphi(rd^{M'}f).$$

Since $|g_q a| \leq |rd^{M'}|$, it follows that $rd^{M'+k}f \in Y \Leftrightarrow rd^{M'}f \in Y$.

The proof for the equivalence with d^{-1} is absolutely similar and can therefore be omitted. Thus (v) holds. $\square$

Back to the proof of Lemma 3.2, we assume that Y is infinite. By Lemma 3.3(i), $z \neq 1$. We take M' from Lemma 3.3(v) and define

$$X_1 = \{v \in Y \mid (rd^{M'} \not\leq v) \ \wedge \ (rd^{-M'} \not\leq v)\},$$

$$X_2 = d^{M'}\{f \in R_A \setminus dR_A \mid rd^{M'}f \in Y\},$$

$$X_3 = d^{-M'}\{f \in R_A \setminus d^{-1}R_A \mid rd^{-M'}f \in Y\}.$$

Suppose that X_1 is infinite. By Lemma 3.3(ii), X_1 must have rd^ω or $r(d^{-1})^\omega$ as an adherence value, a contradiction since no word of X_1 has $rd^{M'}$ or $rd^{-M'}$ as a prefix. Thus X_1 is finite.

Suppose next that X_2 is infinite. By Lemma 3.3(ii), rX_2 must have rd^ω or $r(d^{-1})^\omega$ as an adherence value, a contradiction since $d \not\leq f$. Thus X_2 is finite. Similarly, we show that X_3 is finite.

We show now that (6) holds. We have $X_1 \subseteq Y$ by definition. Since $rX_2 \subseteq Y$, we get $rd^*X_2 \subseteq Y$ by Lemma 3.3(v). Similarly, $r(d^{-1})^*X_3 \subseteq Y$.

Conversely, let $v \in Y$. If $v \notin X_1$, then $rd^{M'} \leq v$ or $r(d^{-1})^{M'} \leq v$. Assume that $rd^{M'} \leq v$. Then we may write $v = rd^{M'+k}f$ with $d \not\leq f$. By Lemma 3.3(v), we get $rd^{M'}f \in Y$ and so $d^{M'}f \in X_2$. Thus $v = rd^k d^{M'}f \in rd^*X_2$. Similarly, if $r(d^{-1})^{M'} \leq v$, we get $v \in r(d^{-1})^*X_3$. Therefore (6) holds as required. $\square$

Theorem 3.4 *For every $\varphi \in \mathrm{ViaF_A}$,*

$$U_\varphi = \{u \in R_A \mid \varphi(x) = xu \textit{ for some } x \in R_A\}$$

is finite.

Proof. Consider $H = \mathrm{Fix}\varphi$, $\mathcal{R}(H) = (Q, q_0, q_0, E)$ and geodesics g_q as before. By Lemma 3.1 and Theorem 2.2, it is enough to show that, for all $q \in Q$ and $(q,a) \in J$,

$$U_q = \{u \in R_A \mid \varphi(x) = xu \text{ for some } x \in \overline{Hg_q}\}$$

and

$$U_{(q,a)} = \{u \in R_A \mid \varphi(x) = xu \text{ for some } x \in \overline{Hg_q}aR_A \cap R_A\}$$

are finite.

The claim is obvious for U_q since

$$(hg_q)^{-1}\varphi(hg_q) = g_q^{-1}h^{-1}\varphi(h)\varphi(g_q) = g_q^{-1}h^{-1}\varphi(h)\varphi(g_q)$$

holds for every $h \in H$.

Let $(q, a) \in J$. We show that

$$U' = \{u \in R_A \mid \varphi(x) = xu \text{ for some } x \in g_qaR_A \cap R_A\}$$

is finite. Indeed, by Lemma 3.2, and using its notation, we must have $x \in Y = X_1 \cup rd^*X_2 \cup r(d^{-1})^*X_3$ for some finite $X_1, X_2, X_3 \subseteq R_A$. Without loss of generality, we may assume that Y is infinite. By Lemma 3.3(iii), there exists some $m \in \mathbb{N}$ such that $|\varphi(d^k)| = m + |d^k|$ for every $k \in \mathbb{Z} \setminus \{0\}$. Hence $|\varphi(x)| - |x|$ is bounded for all $x \in Y$ and so U' is finite.

Now, every $x \in \overline{Hg_q}aR_A \cap R_A$ is equivalent in F_A to a product hy with $h \in H$ and $y \in g_qaR_A \cap R_A$: indeed, if $x = \overline{hg_q}av$, then $y = g_qav$ is reduced (and so is yu) since $(g_q, a) \in J$ and av is irreducible by assumption. Moreover,

$$\begin{aligned}\varphi(x) = xu &\Rightarrow \varphi(\overline{hg_q}av) = \overline{hg_q}avu \Rightarrow \varphi(h^{-1})\varphi(\overline{hg_q}av) = h^{-1}\overline{hg_q}avu \\ &\Rightarrow \varphi(g_qav) = g_qavu \Rightarrow \varphi(y) = yu.\end{aligned}$$

Thus $U_{(q,a)} = U'$ is finite as required. □

Corollary 3.5 *For every $\varphi \in \mathrm{ViaF_A}$,*

$$V_\varphi = \{v \in R_A \mid x = \varphi(x)v \text{ for some } x \in R_A\}$$

is finite.

Proof. By Proposition 2.6, we can take M to be a bounded reduction constant for φ^{-1}. By Theorem 3.4, we can define $N = \max\{|u|;\ u \in U_{\varphi^{-1}}\}$. Let also

$$M' = \max\{|\varphi^{-1}(u)|;\ |u| \le M\}.$$

Suppose that V_φ is infinite. Then there exist $x, v \in R_A$ such that $x = \varphi(x)v$ and $|\varphi^{-1}(v)| > N + M + M'$. It follows that $\varphi^{-1}(x) = \overline{x\varphi^{-1}(v)}$. By choice of M, and since $\varphi(x)v$ is irreducible, there exists a factorization $x = x_1x_2$ such that $\overline{x\varphi^{-1}(v)} = x_1\overline{x_2\varphi^{-1}(v)}$ and $|x_2| \le M$. Thus

$$\varphi^{-1}(x_1) = \overline{x_1\overline{x_2\varphi^{-1}(v)}\varphi^{-1}(x_2^{-1})} = x_1\overline{x_2\varphi^{-1}(v)\varphi^{-1}(x_2^{-1})}$$

since $|\varphi^{-1}(v)| > N+M+M'$ ensures that the reduction taking place between $\overline{x_2\varphi^{-1}(v)}$ and $\varphi^{-1}(x_2^{-1})$ does not cancel the first letter of $\overline{x_2\varphi^{-1}(v)}$. Thus $w = \overline{x_2\varphi^{-1}(v)\varphi^{-1}(x_2^{-1})} \in U_{\varphi^{-1}}$. Since $|x_2| \le M$, $|\varphi^{-1}(v)| > N + M + M'$ and $|\varphi^{-1}(x_2^{-1})| \le M'$, we get $|w| > N$, contradicting the definition of N. Therefore V_φ is finite. □

Given $u, v \in R_A$, we denote by $u \wedge v$ the longest common prefix of u and v. Given $u \in R_A$ and $k \in \mathbb{N}$, we define $S_k(u)$ to be the suffix of u of length k if $|u| > k$ and u otherwise. We write $u \leq_s v$ if u is a suffix of v. Given $u \in R_A$, we define

$$\sigma(u) = u \wedge \varphi(u).$$

We define also $\tau(u), \rho(u) \in R_A$ through

$$u = \sigma(u)\tau(u), \quad \varphi(u) = \sigma(u)\rho(u).$$

We fix now $M - 1$ to be a bounded reduction constant for φ. We define $\sigma' : R_A \to R_A$ inductively through $\sigma'(1) = 1$ and

$$\sigma'(ua) = S_M(\sigma'(u)\tau(u)a \;\wedge\; \overline{\sigma'(u)\rho(u)\varphi(a)})$$

for $a \in A \cup A^{-1}$ and ua irreducible.

Intuitively, the purpose of σ' is to encode the suffix of $\sigma(u)$ that is relevant to establish the profile of u as far as $u^{-1}\varphi(u)$ is concerned. In view of bounded reduction, we need at most M letters, but often less (if reduction in the φ part shortened the word).

Lemma 3.6 *(i) If $|\sigma(v)| < M$ for every $v < u$, then $\sigma'(u) = S_M(\sigma(u))$.*

(ii) $\sigma'(u) \leq_s \sigma(u)$.

(iii) If $\sigma'(u) = 1$, then $|\sigma'(v)| < M$ for every $v < u$.

(iv) If $\sigma'(u) = 1$, then $\sigma(u) = 1$.

(v) $\sigma'(u)\tau(u)a = (\sigma'(u)\tau(u)a \;\wedge\; \overline{\sigma'(u)\rho(u)\varphi(a)})\tau(ua)$ for $a \in A \cup A^{-1}$ and ua irreducible.

(vi) $\overline{\sigma'(u)\rho(u)\varphi(a)} = (\sigma'(u)\tau(u)a \;\wedge\; \overline{\sigma'(u)\rho(u)\varphi(a)})\rho(ua)$ for $a \in A \cup A^{-1}$ and ua irreducible.

Proof. (i) We use induction. The claim holds trivially for $u = 1$. Assume that $u = u'a$ ($a \in A \cup A^{-1}$), $|\sigma(v)| < M$ for every $v < u$ and the claim holds for u'. Then $\sigma'(u') = S_M(\sigma(u')) = \sigma(u')$. Hence

$$\begin{aligned}\sigma'(u) &= S_M(\sigma'(u')\tau(u')a \;\wedge\; \overline{\sigma'(u')\rho(u')\varphi(a)}) \\ &= S_M(\sigma(u')\tau(u')a \;\wedge\; \overline{\sigma(u')\rho(u')\varphi(a)}) \\ &= S_M(u'a \;\wedge\; \overline{\varphi(u')\varphi(a)}) = S_M(u \;\wedge\; \varphi(u)) = S_M(\sigma(u))\end{aligned}$$

as required.

(ii) We use induction again. The claim holds trivially for $u = 1$ and all he cases when $\sigma'(u) = 1$. Assume that $u = va$ ($a \in A \cup A^{-1}$), $\sigma'(u) \neq 1$ and the claim holds for v. Write $\sigma(v) = x\sigma'(v)$. Then

$$\sigma'(u) \leq_s \sigma'(v)\tau(v)a \;\wedge\; \overline{\sigma'(v)\rho(v)\varphi(a)} \leq_s x\sigma'(v)\tau(u')a \;\wedge\; \overline{x\sigma'(v)\rho(v)\varphi(a)}$$

since $\sigma'(u) \neq 1$ implies that $x\overline{\sigma'(v)\rho(v)\varphi(a)}$ is irreducible. Thus

$$\sigma'(u) \leq_s \sigma(v)\tau(v)a \;\wedge\; \overline{\sigma(v)\rho(v)\varphi(a)} = va \wedge \varphi(va) = \sigma(u)$$

as required.

(iii) Suppose that $\sigma'(u) < M$ but $|\sigma'(v)| = M$ for some $v \leq u$. Assume that v is the longest such prefix of u and $u = va_1 \ldots a_k$ ($a_i \in A \cup A^{-1}$). By (ii), we may write $\sigma(v) = x\sigma'(v)$ for some $x \in R_A$. Hence $\varphi(v) = x\sigma'(v)\rho(v)$. Write $\sigma'(v) = w_1w_2$ with $w_1 \in A \cup A^{-1}$. Since $M - 1$ is a bounded reduction constant for φ, we have

$$\varphi(va_1 \ldots a_i) = xw_1\overline{w_2\rho(v)\varphi(a_1 \ldots a_i)} \tag{9}$$

for every $i \in \{0, \ldots, k\}$. We show now that

$$\sigma(va_1 \ldots a_i) = x\sigma'(va_1 \ldots a_i), \quad w_1 \leq \sigma'(va_1 \ldots a_i) \tag{10}$$

holds for $i = 0, \ldots, k$ by induction. This is clear for $i = 0$, so assume that $i > 0$ and (10) holds for $i - 1$. Since $|\sigma(va_1 \ldots a_i)| < M$ by maximality of v, we have

$$\sigma'(va_1 \ldots a_i) = \sigma'(va_1 \ldots a_{i-1})\tau(va_1 \ldots a_{i-1})a_i \wedge \overline{\sigma'(va_1 \ldots a_{i-1})\rho(va_1 \ldots a_{i-1})\varphi(a_i)}. \tag{11}$$

By the induction hypothesis, w_1 is the first letter of $\sigma'(va_1 \ldots a_{i-1})$ and $\sigma(va_1 \ldots a_{i-1}) = x\sigma'(va_1 \ldots a_{i-1})$. Suppose that w_1 is cancelled in the reduction $\overline{\sigma'(va_1 \ldots a_{i-1})\rho(va_1 \ldots a_{i-1})\varphi(a_i)}$. Since

$$\begin{aligned}\varphi(va_1 \ldots a_i) &= \overline{\varphi(va_1 \ldots a_{i-1})\varphi(a_i)} = \overline{\sigma(va_1 \ldots a_{i-1})\rho(va_1 \ldots a_{i-1})\varphi(a_i)} \\ &= \overline{x\sigma'(va_1 \ldots a_{i-1})\rho(va_1 \ldots a_{i-1})\varphi(a_i)},\end{aligned}$$

this implies that w_1 is cancelled in the reduction $\overline{\varphi(v)\varphi(a_1 \ldots a_i)}$, contradicting (9). Thus $w_1 \leq \sigma'(va_1 \ldots a_i)$ by (11). Since xw_1 is irreducible, (11) yields

$$\begin{aligned}x\sigma'(va_1 \ldots a_i) &= x\sigma'(va_1 \ldots a_{i-1})\tau(va_1 \ldots a_{i-1})a_i \wedge x\overline{\sigma'(va_1 \ldots a_{i-1})\rho(va_1 \ldots a_{i-1})\varphi(a_i)} \\ &= \sigma(va_1 \ldots a_{i-1})\tau(va_1 \ldots a_{i-1})a_i \wedge \overline{x\sigma'(va_1 \ldots a_{i-1})\rho(va_1 \ldots a_{i-1})\varphi(a_i)} \\ &= va_1 \ldots a_i \wedge \overline{\sigma(va_1 \ldots a_{i-1})\rho(va_1 \ldots a_{i-1})\varphi(a_i)} = va_1 \ldots a_i \wedge \varphi(va_1 \ldots a_i) \\ &= \sigma(va_1 \ldots a_i)\end{aligned}$$

and so (10) holds. In particular, $w_1 \leq \sigma'(va_1 \ldots a_k) = \sigma'(u)$ and so $\sigma'(u) \neq 1$. Therefore (iii) holds.

(iv) Suppose that $\sigma'(u) = 1$. Then $|\sigma'(v)| < M$ for every $v < u$ by (iii) and so $1 = \sigma'(u) = S_M(\sigma(u))$ by (i). Therefore $\sigma(u) = 1$.

(v) Write $y = \sigma'(u)\tau(u)a \wedge \overline{\sigma'(u)\rho(u)\varphi(a)}$. We start by showing that

$$\sigma'(u)\tau(u)a \wedge \overline{\sigma'(u)\rho(u)\varphi(a)} = 1 \Rightarrow \sigma'(u) = \sigma(u). \tag{12}$$

Indeed, assume that $\sigma'(u) \neq \sigma(u)$. It follows from (i) that $|\sigma(z)| \geq M$ for some $z \leq u$. Let z have minimal length. Still by (i), we must have $\sigma'(z) = S_M(\sigma(z))$ and so $|\sigma'(z)| = M$. Let v be the longest prefix of u satisfying $|\sigma'(v)| = M$. Since $\sigma'(ua) \leq_s y$, we only have to worry about the possibility $\sigma'(ua) = 1$. However, by the proof of (10), this case cannot occur. Indeed, write $ua = va_1 \ldots a_k$. If $\sigma'(ua) < M$, then we have $|\sigma'(va_1 \ldots a_i)| < M$ for $i = 1, \ldots, k$ by maximality of v and so the conditions of (10) are satisfied. It follows that $\sigma'(ua) = \sigma'(va_1 \ldots a_k) \neq 1$ and so (12) holds.

Suppose first that $\sigma(u) = \sigma'(u)$. Then

$$\begin{aligned}\sigma'(u)\tau(u)a = y\tau(ua) &\Leftrightarrow \sigma(u)\tau(u)a = (\sigma(u)\tau(u)a \ \wedge \ \overline{\sigma(u)\rho(u)\varphi(a)})\tau(ua) \\ &\Leftrightarrow ua = (ua \ \wedge \ \varphi(ua))\tau(ua) \Leftrightarrow ua = \sigma(ua)\tau(ua).\end{aligned}$$

Assume now that $\sigma(u) \neq \sigma'(u)$. By (ii), $\sigma(u) = x\sigma'(u)$ for some $x \in R_A$. Thus $xy \in R_A$ and so

$$\begin{aligned}xy &= (x\sigma'(u)\tau(u)a \ \wedge \ x\overline{\sigma'(u)\rho(u)\varphi(a)}) \\ &= (\sigma(u)\tau(u)a \ \wedge \ \overline{\sigma(u)\rho(u)\varphi(a)}) = (ua \ \wedge \ \varphi(ua)) \\ &= \sigma(ua).\end{aligned}$$

Hence

$$\begin{aligned}\sigma'(u)\tau(u)a = y\tau(ua) &\Leftrightarrow x\sigma'(u)\tau(u)a = xy\tau(ua) \\ &\Leftrightarrow \sigma(u)\tau(u)a = \sigma(ua)\tau(ua).\end{aligned}$$

Therefore (v) holds.

(vi) Assume that $\sigma(u) \neq \sigma'(u)$. Let $\sigma(u) = x\sigma'(u)$. Thus $xy \in R_A$ and we saw in the proof of (v) that $xy = \sigma(ua)$. On the other hand, $y \neq 1$ implies that $x\overline{\sigma'(u)\rho(u)\varphi(a)} \in R_A$ and so

$$\begin{aligned}\overline{\sigma'(u)\rho(u)\varphi(a)} = y\rho(ua) &\Leftrightarrow x\overline{\sigma'(u)\rho(u)\varphi(a)} = xy\rho(ua) \\ &\Leftrightarrow \overline{x\sigma'(u)\rho(u)\varphi(a)} = \sigma(ua)\rho(ua) \\ &\Leftrightarrow \overline{\varphi(u)\varphi(a)} = \varphi(ua),\end{aligned}$$

proving the claim.

The proof for the case $\sigma(u) = \sigma'(u)$ is analogous to the corresponding case in (v) and can be omitted. □

Let $\theta : R_A \to R_A \times R_A \times R_A$ be the mapping defined by

$$\theta(u) = (\sigma(u), \tau(u), \rho(u)).$$

Let $K \in \mathrm{RatF_A}$. We define an $(A \cup A^{-1})$-automaton $\mathcal{C} = (P, p_0, T, D)$ by

- $P = \theta(R_A)$.
- $p_0 = (1, 1, 1)$;
- $T = \{\theta(u) \in P \mid \pi((\tau(u))^{-1}\rho(u)) \in K\}$;
- given $u \in R_A$ and $a \in A$,

  $$\theta(u) \xrightarrow{a} \theta(ua)$$

  is an edge of D if and only if $ua \in R_A$ and ($\tau(u) = 1$ or $|\rho(u)| \leq N$).

Let $\mathcal{C}' = (P', p_0, T', D')$ denote the subautomaton of $\mathcal{C}$ obtained by removing all vertices and edges that do NOT lie in some path starting at the initial vertex.

Lemma 3.7 *(i) Let $u, v \in R_A$ and $a \in A \cup A^{-1}$ be such that $ua \in R_A$ and $\theta(u) = \theta(v)$. Then $va \in R_A$ and $\theta(ua) = \theta(va)$.*

(ii) $\mathcal{C}$ is deterministic.

(iii) if $p_0 \xrightarrow{u} p$ is a path in $\mathcal{C}$, then $u \in R_A$ and $p = \theta(u)$.

(iv) $\mathcal{C}'$ is finite and effectively constructible.

Proof. (i) Suppose that $\sigma'(u) = \sigma'(v) = 1$. By Lemma 3.6(iv), we get $\sigma(u) = \sigma(v) = 1$ and so $u = \tau(u) = \tau(v) = v$. Hence we may assume that $\sigma'(u) = \sigma'(v) \neq 1$. Since $\theta(u) = \theta(v)$, Lemma 3.6(ii) yields

$$u = \sigma(u)\tau(u) \geq_s \sigma'(u)\tau(u) = \sigma'(v)\tau(v) \leq_s \sigma(v)\tau(v) = v$$

and so $ua \in R_A$ implies $va \in R_A$.

It follows from $\theta(u) = \theta(v)$ and the definition of σ' that $\sigma'(ua) = \sigma'(va)$. By Lemma 3.6(v) and (vi), we get $\tau(ua) = \tau(va)$ and $\rho(ua) = \rho(va)$ as well. Thus $\theta(ua) = \theta(va)$.

(ii) Immediate from (i).

(iii) We use induction. The case $u = 1$ being trivial, assume that $u = va$ with $a \in A \cup A^{-1}$ and the claim holds for v. Let

$$p_0 \xrightarrow{v} p' \xrightarrow{a} p$$

be a path in $\mathcal{C}$. By the induction hypothesis, we have $v \in R_A$ and $p' = \theta(v)$. Since $p' \xrightarrow{a} p$ is an edge, we have $p' = \theta(w)$ and $p = \theta(wa)$ for some $w \in R_A$ with $wa \in R_A$ and ($\tau(w) = 1$ or $|\rho(w)| \leq N$). By (i), it follows from $\theta(v) = \theta(w)$ and $wa \in R_A$ that $u = va \in R_A$ and $p = \theta(wa) = \theta(va) = \theta(u)$ as claimed.

(iv) For every $k \in \mathbb{N}$, let $\mathcal{C}_k$ denote the subautomaton of $\mathcal{C}$ induced by all paths $p_0 \xrightarrow{u} p$ with $|u| \leq k$. In view of (iii), each $\mathcal{C}_k$ is a finite effectively constructible $(A \cup A^{-1})$-automaton. To complete the proof, it suffices to show that $\mathcal{C}_k = \mathcal{C}_{k+1}$ for some $k \in \mathbb{N}$.

By Theorem 3.4 and Corollary 3.5, we may define

$$N = \max\{|u|;\ u \in U_\varphi \cup V_\varphi\}.$$

Let also

$$N_1 = \max\{|\varphi^{-1}(x)|;\ x \in R_A,\ |x| \leq M\}.$$

We show that if $p_0 \xrightarrow{u} p$ is a path in $\mathcal{C}$ and $u = va$ ($a \in A \cup A^{-1}$), then

$$|\tau(v)|, |\rho(v)| \leq \max\{N + N_1, M\}. \tag{13}$$

By (iii), our path decomposes as

$$p_0 \xrightarrow{v} \theta(v) \xrightarrow{a} \theta(u) = p.$$

Since $\theta(v) \xrightarrow{a} \theta(u)$ is an edge, we have either $\tau(v) = 1$ or $|\rho(v)| \leq M$.

Assume first that $\tau(v) = 1$. Then $v = \sigma(v) \leq \sigma(v)\rho(v) = \varphi(v)$ and so $\rho(v) \in U_\varphi$. Hence $|\rho(v)| \leq N$ and the claim holds.

Assume now that $|\rho(v)| \leq M$. Suppose that $|\tau(v)| > N + N_1$ and let $z = \varphi^{-1}((\rho(v))^{-1})$. Then $|z| \leq N_1$ and

$$\varphi(vz) = \sigma(v) \leq \sigma(v)\overline{\tau(v)z} = \overline{vz}$$

since z cannot erase the whole of $\tau(v)$ in the reduction process. Thus $\overline{\tau(v)z} \in V_\varphi$ and so $|\overline{\tau(v)z}| \leq N$. Since $|z| \leq N_1$, it follows that $|\tau(v)| \leq N + N_1$, a contradiction. Therefore $|\tau(v)| \leq N + N_1$ and so (13) holds in any case.

It follows from (13) that there exist only finitely many vertices of $\mathcal{C}'$ that can be prolonged by edges. Since $\mathcal{C}$ is deterministic, it follows that $\mathcal{C}'$ is finite and so we can indeed reach some $k \in \mathbb{N}$ such that $\mathcal{C}_k = \mathcal{C}_{k+1}$. □

Let $\mathcal{C}'' = (P', p_0, T'', D')$ denote the $(A \cup A^{-1})$-automaton obtained from $\mathcal{C}'$ by taking

$$T'' = \{\theta(u) \in P' \mid \tau(u) \neq 1 \text{ and } |\rho(u)| \ > M\}.$$

Given $p \in T''$, we denote by L_p the set of all labels of paths $p_0 \to p$ in $\mathcal{C}''$.

Lemma 3.8 *For every $p = (p_1, p_2, p_3) \in T''$, let*

$$W_p = \{w \in R_A \mid \pi(w^{-1}p_2^{-1}p_3\varphi(w)) \in K,\ p_2 w \in R_A\}.$$

Then

$$\overline{\mathrm{Sol}(1, \varphi, \mathrm{K})} = L(\mathcal{C}') \cup (\bigcup_{p \in T''} L_p W_p \ \cap \ R_A). \tag{14}$$

Proof. Let $u \in L(\mathcal{C}')$. By Lemma 3.7(iii), we have $u \in R_A$ and a path $p_0 \xrightarrow{u} \theta(u)$ in $\mathcal{C}'$. Moreover, $\theta(u) \in T' = T \cap P'$ and so $\pi((\tau(u))^{-1}\rho(u)) \in K$. Hence

$$\pi(u^{-1}\varphi(u)) = \pi((\tau(u))^{-1}(\sigma(u))^{-1}\sigma(u)\rho(u)) = \pi((\tau(u))^{-1}\rho(u)) \in K.$$

Thus $\pi(u) \in \mathrm{Sol}(1, \varphi, \mathrm{K})$ and so $u = \overline{\pi(u)} \in \overline{\mathrm{Sol}(1, \varphi, \mathrm{K})}$.

Assume now that $p = (p_1, p_2, p_3) \in T''$, $u \in L_p$ and $w \in W_p$ with $uw \in R_A$. Since $w \in W_p$, we have $\pi(w^{-1}p_2^{-1}p_3\varphi(w)) \in K$ and $p_2 w \in R_A$. Since $u \in L_p$ yields $p = \theta(u)$ by Lemma 3.7(iii) and so $(\tau(u))^{-1}\rho(u) = p_2^{-1}p_3$, we obtain

$$\pi(w^{-1}u^{-1}\varphi(uw)) = \pi(w^{-1}(\tau(u))^{-1}(\sigma(u))^{-1}\sigma(u)\rho(u)\varphi(w)) = \pi(w^{-1}p_2^{-1}p_3\varphi(w)) \in K.$$

Hence $\pi(uw) \in \mathrm{Sol}(1, \varphi, \mathrm{K})$ and so $uw = \overline{\pi(uw)} \in \overline{\mathrm{Sol}(1, \varphi, \mathrm{K})}$. Thus

$$L(\mathcal{C}') \cup (\bigcup_{p \in T''} L_p W_p \ \cap \ R_A) \subseteq \overline{\mathrm{Sol}(1, \varphi, \mathrm{K})}.$$

Conversely, let $u \in \overline{\mathrm{Sol}(1, \varphi, \mathrm{K})}$. Suppose that there exists some path $p_0 \xrightarrow{u} p$ in $\mathcal{C}'$. Then $p = \theta(u)$ by Lemma 3.7(iii) and

$$\pi((\tau(u))^{-1}\rho(u)) = \pi(u^{-1}\varphi(u)) \in K$$

since $\pi(u) \in \mathrm{Sol}(1, \varphi, \mathrm{K})$. Thus $p \in T'$ and so $u \in L(\mathcal{C}')$.

Hence we may assume that there exists no path $p_0 \xrightarrow{u} p$ in $\mathcal{C}'$. Write $u = vw$ where v is the longest prefix of u labelling a path in $\mathcal{C}'$ from the initial vertex. Let a denote the first letter of w. We have a path $\varphi_0 \xrightarrow{v} p = \theta(v)$ but no edge $\theta(v) \xrightarrow{a} \theta(va)$. Since $va \leq vw = u \in R_A$, this can only happen due to both $\tau(v) \neq 1$ and $|\rho(v)| \ > M$. Hence $p \in T''$ and $v \in L_p$. Since $vw = u \in R_A$, it remains to show that $w \in W_p$. Indeed,

$$\pi(w^{-1}(\tau(v))^{-1}\rho(v)\varphi(w)) = \pi(w^{-1}v^{-1}\varphi(v)\varphi(w)) = \pi(u^{-1}\varphi(u)) \in K$$

since $\pi(u) \in \mathrm{Sol}(1, \varphi, \mathrm{K})$ and $\tau(v)w \leq_s vw = u \in R_A$ yields $\tau(v)w \in R_A$. Thus $w \in W_p$ as required. $\square$

Theorem 3.9 *Let* $\varphi \in \mathrm{ViaF_A}$ *and* $K \in \mathrm{RatF_A}$*. Then* $\mathrm{Sol}(1, \varphi, \mathrm{K}) \in \mathrm{RatF_A}$ *and is effectively constructible.*

Proof. By Theorem 2.2, it suffices to show that $\overline{\mathrm{Sol}(1, \varphi, \mathrm{K})} \in \mathrm{Rat}(\mathrm{A} \cup \mathrm{A}^{-1})$ and is effectively constructible. By Lemma 3.7(iv), the languages $L(\mathcal{C}')$ and L_p ($p \in T''$) are rational and effectively constructible. So is R_A. By Lemma 3.8 and Proposition 2.3(i), we only need to show that W_p is rational and effectively constructible for every $p \in T''$.

Fix $p = (p_1, p_2, p_3) = \theta(u) \in T''$. In view of Theorem 2.2, we may assume to have a finite $(A \cup A^{-1})$-automaton $\mathcal{A}_0 = (Q_0, i_0, T_0, E_0)$ such that $L(\mathcal{A}_0) = \overline{K}$. Moreover, we may assume $\mathcal{A}_0$ to be deterministic and trim. For all $j, k \in Q_0$, we write

$$Y_j = L(Q_0, j, T_0, E_0), \quad Y_{jk} = L(Q_0, j, k, E_0).$$

Given $u \in R_A$, let

$$\xi(u) = \{(j, k) \in Q_0 \times Q_0 \mid u \in L_{jk}\}.$$

Note that $p_2^{-1}p_3 = (\tau(u))^{-1}\rho(u) \in R_A$ by maximality of $\sigma(u)$. We show that

$$W_p = \bigcup_{rs=p_3} \bigcup_{(j,k)\in\xi(p_2^{-1}r)} Y_{i_0j}^{-1} \cap \varphi^{-1}(\overline{s^{-1}Y_k}). \tag{15}$$

Note that, since $r \leq p_3$ and $p_2^{-1}p_3 \in R_A$, we have $p_2^{-1}r \in R_A$ as well.

Let $p_3 = rs$ and $(j, k) \in \xi(p_2^{-1}r)$. Take $w \in Y_{i_0j}^{-1} \cap \varphi^{-1}(\overline{s^{-1}Y_k})$. Then $\overline{s\varphi(w)} \in Y_k$ and so we have a path

$$i_0 \xrightarrow{w^{-1}} j \xrightarrow{p_2^{-1}r} k \xrightarrow{\overline{s\varphi(w)}} t \in T_0$$

in $\mathcal{A}_0$. Hence

$$\pi(w^{-1}p_2^{-1}p_3\varphi(w)) = \pi(w^{-1}p_2^{-1}r\overline{s\varphi(w)}) \in \pi(\overline{K}) = K.$$

On the other hand, $w^{-1}p_2^{-1}$ labels a path in $\mathcal{A}_0$. Since $\mathcal{A}_0$ is trim and $L(\mathcal{A}_0) \subseteq R_A$, it follows that $w^{-1}p_2^{-1} \in R_A$ and so $p_2 w \in R_A$ as well. Thus $w \in W_p$.

Conversely, let $w \in W_p$. Then $w^{-1}p_2^{-1} \in R_A$. We have already noted that $p_2^{-1}p_3 \in R_A$. Since $p \in T''$, we have $p_2 = \tau(u) \neq 1$ and so $w^{-1}p_2^{-1}p_3 \in R_A$ as well and also

$$uw = \sigma(u)\tau(u)w = \sigma(u)p_2 w \in R_A.$$

Now, since M is a bounded reduction constant for φ, no more than M letters of $\varphi(u)$ are reduced in $\overline{\varphi(u)\varphi(w)}$. Since $p_3 = \rho(u) \leq_s \varphi(u)$ and $|p_3| > M$, it follows that

$$\overline{w^{-1}p_2^{-1}p_3\varphi(w)} = w^{-1}p_2^{-1}\overline{p_3\varphi(w)}$$

and so $w^{-1}p_2^{-1}\overline{p_3\varphi(w)} \in \overline{K} = L(\mathcal{A}_0)$. Write $p_3 = rs$, $\varphi(w) = s^{-1}z$ so that $\overline{p_3\varphi(w)} = rz$. Thus we have a path in $\mathcal{A}_0$ of the form

$$i_0 \xrightarrow{w^{-1}} j \xrightarrow{p_2^{-1}r} k \xrightarrow{z} t \in T_0.$$

Hence $(j, k) \in \xi(p_2^{-1}r)$. Clearly, $w \in Y_{i_0j}^{-1}$. On the other hand, $\overline{s\varphi(w)} = z \in Y_k$ so that $w \in \varphi^{-1}(\overline{s^{-1}Y_k})$. Therefore (15) holds.

By Theorem 2.2 and Propositions 2.3 and 2.4, it follows that W_p is rational and effectively constructible, and so is $\mathrm{Sol}(1, \varphi, \mathrm{K})$. □

Corollary 3.10 *Let $g \in F_A$, $\varphi \in \mathrm{ViaF_A}$ and $K \in \mathrm{RatF_A}$. Then* $\mathrm{Sol(g, \varphi, K)} \in \mathrm{RatF_A}$ *and is effectively constructible.*

Proof. Given $x \in F_A$, we have

$$x^{-1}g\varphi(x) \in K \Leftrightarrow x^{-1}g\varphi(x)g^{-1} \in Kg^{-1} \Leftrightarrow x^{-1}(\lambda_g\varphi)(x) \in Kg^{-1},$$

hence $\mathrm{Sol(g, \varphi, K)} = \mathrm{Sol(1, \lambda_g\varphi, Kg^{-1})}$. By Proposition 2.5, we have $\lambda_g\varphi \in \mathrm{ViaF_A}$. Since $Kg^{-1} \in ratF_A$, we may apply Theorem 3.9. Hence $\mathrm{Sol(g, \varphi, K)} = \mathrm{Sol(1, \lambda_g\varphi, Kg^{-1})}$ is rational and effectively constructible. □

We end this section by showing that being virtually inner is a decidable property.

Theorem 3.11 *It is decidable, given $\varphi \in \mathrm{AutF_A}$, whether or not $\varphi \in \mathrm{ViaF_A}$.*

Proof. Assume that $A = \{a_1, \ldots, a_m\}$. Given $u \in (A \cup A^{-1})^*$, denote by $|u|_i$ the sum of all exponents (positive and negative) of occurrences of a_i in u. Given $\varphi \in \mathrm{AutF_A}$, it is known (see [16, Prop. I.4.4]) that φ induces $\widetilde{\varphi} \in \mathrm{Aut\mathbb{Z}^m}$ defined by

$$\widetilde{\varphi}(i_1, \ldots, i_m) = (|\varphi(a_1^{i_1} \ldots a_m^{i_m})|_1, \ldots, |\varphi(a_1^{i_1} \ldots a_m^{i_m})|_m).$$

Moreover,

$$\begin{aligned} \mathrm{AutF_A} &\to \mathrm{Aut\mathbb{Z}^n} \\ \varphi &\mapsto \widetilde{\varphi} \end{aligned}$$

is a group homomorphism. Clearly, $\mathrm{Aut\mathbb{Z}^m}$ is, up to isomorphism, the (multiplicative) group $GL_n(\mathbb{Z})$.

It is decidable, given $M \in GL_m(\mathbb{Z})$, whether or not $M^k = \mathrm{id}$ for some $k \geq 1$. Indeed,$M^k = \mathrm{id}$ for some $k \geq 1$ holds if and only if $M^k = M^{-1}$ for some $k \geq 0$, and this is a decidable condition by [13].

Let $\varphi \in \mathrm{AutF_A}$. If $\varphi \in \mathrm{ViaF_A}$, say with $\varphi^n = \lambda_z$ $(n \geq 1)$, then

$$\widetilde{\varphi}^n = \widetilde{\varphi^n} = \widetilde{\lambda_z} = \mathrm{id}.$$

By the preceding comment, we can decide whether or not $\widetilde{\varphi}^k = \mathrm{id}$ holds for some $k \geq 1$. Thus we may assume that the necessary condition $\widetilde{\varphi}^k = \mathrm{id}$ is satisfied for some k and k can therefore be effectively computed. We show that $\varphi \in \mathrm{ViaF_A}$ if and only if φ^k is inner.

Assume that $\varphi \in \mathrm{ViaF_A}$. Then φ^n is inner for some $n \geq 1$, and so is φ^{nk}. Since $\widetilde{\varphi^k} = \mathrm{id}$, it follows from [16, Prop. I.4.11] that φ^{nk} inner implies φ^k inner.

The converse implication being trivial, we conclude that $\varphi \in \mathrm{ViaF_A}$ if and only if φ^k is inner. Since it is clearly decidable whether or not a given automorphism is inner, decidability is proven. □

4 Conjugacy in [f.g. free]-by-finite groups

Let G be a [f.g. free]-by-finite group. Throughout the section, we assume that G is given by the standard presentation (3) and has consequently (2) as a set of normal forms. In particular, every $X \subseteq G$ admits a unique decomposition $X = \cup_{i=0}^m X_i b_i$. We shall refer to the X_i as the *components* of X.

We consider now the equation $xgx^{-1} \in K$ for $g \in F_A$ and $K \in \mathrm{RatG}$. We shall use the notation

$$\mathrm{Sol(g,K) = \{x \in F_A \mid xgx^{-1} \in K\}}.$$

Theorem 4.1 *Let G be a [f.g. free]-by-finite group, $g \in G$ and $K \in \mathrm{RatG}$. Then $\mathrm{Sol(g,K)} \in \mathrm{RatG}$ and is effectively constructible.*

Proof. Assume that G is given by the standard presentation (3). In view of Proposition 2.11, we assume that K has components $K_0, \ldots, K_m \in \mathrm{RatF_A}$.

Decompose $\mathrm{Sol(g,K) = \cup_{i=0}^m S_i b_i}$ in its components. Let $i \in \{0, \ldots, m\}$. Then $b_i g b_i^{-1} = ub_j$ for some $u \in F_A$ and $j \in \{0, \ldots, m\}$. Given $x \in F_A$, we have

$$\begin{aligned} x \in S_i &\Leftrightarrow xb_i \in \mathrm{Sol(g,K)} \Leftrightarrow \mathrm{xb_i g b_i^{-1} x^{-1} \in K} \\ &\Leftrightarrow xub_jx^{-1} \in K \Leftrightarrow xu\varphi_j(x^{-1})b_j \in K \\ &\Leftrightarrow xu\varphi_j(x^{-1})b_j \in K_jb_j \Leftrightarrow xu\varphi_j(x^{-1}) \in K_j \\ &\Leftrightarrow x^{-1} \in \mathrm{Sol(u,\varphi_j,K_j)} \Leftrightarrow \mathrm{x \in (Sol(u,\varphi_j,K_j))^{-1}}. \end{aligned}$$

Thus $S_i = \mathrm{(Sol(u,\varphi_j,K_j))^{-1}}$. Since $\varphi_j \in \mathrm{ViaF_A}$ and $K_j \in \mathrm{RatF_A}$ are given, it follows from Corollary 3.10 that $\mathrm{Sol(u,\varphi_j,K_j)} \in \mathrm{RatF_A}$ and is effectively constructible. By Theorem 2.2 and Proposition 2.3(ii), so is S_i. Therefore $\mathrm{Sol(g,K)} \in \mathrm{RatG}$ and is effectively constructible.
□

Given a finitely generated monoid M, and $X \subseteq M$, we say that X has the *DIRL property* (decidable if it intersects a rational language) if it is decidable whether or not $X \cap K = \emptyset$ for an arbitrary $K \in \mathrm{RatM}$.

Lemma 4.2 *(i) Let $K \subseteq F_A$. Then K has the DIRL property if and only if $\overline{K}$ has the DIRL property as an $(A \cup A^{-1})$-language.*

(ii) Let $G = \cup_{i=0}^m Fb_i$ be a [f.g. free]-by-finite group with $F \trianglelefteq G$. Let $K \subseteq G$. Then K has the DIRL property if and only if each of its components K_i has the DIRL property.

Proof. (i) Assume that K has the DIRL property. Let $L \in \mathrm{Rat(A \cup A^{-1})}$. By Proposition 2.3(i), $L \cap R_A \in \mathrm{Rat(A \cup A^{-1})}$ and is effectively constructible. It is immediate that

$$\overline{K} \cap L = \emptyset \Leftrightarrow \overline{K} \cap (L \cap R_A) = \emptyset \Leftrightarrow K \cap \pi(L \cap R_A) = \emptyset.$$

Since $\pi(L \cap R_A) \in \mathrm{RatF_A}$, it follows that $\overline{K}$ has the DIRL property.

Conversely, assume that $\overline{K}$ has the DIRL property. Let $X \in \mathrm{RatF_A}$. Then

$$K \cap X = \emptyset \Leftrightarrow \overline{K} \cap \overline{X} = \emptyset$$

and so K has the DIRL property.

(ii) Assume that K has the DIRL property. Let $i \in \{0, \ldots, m\}$ and let $X_i \in \mathrm{RatF_A}$. Then $X_i b_i \in \mathrm{RatG}$ and

$$K_i \cap X_i = \emptyset \Leftrightarrow K \cap X_i b_i = \emptyset$$

shows that K_i has the DIRL property.

Conversely, assume that all K_i have the DIRL property. Let $X = \cup_{i=0}^m X_i b_i \in \mathrm{RatG}$ with $X_i \subseteq F_A$. Then

$$K \cap X = \emptyset \Leftrightarrow \forall i \in \{0,\ldots,m\} K_i \cap X_i = \emptyset.$$

Since $X_i \in \mathrm{RatF_A}$ for every i by Proposition 2.11, it follows that $K \cap X = \emptyset$ is decidable and so K has the DIRL property. □

A very important class of languages with the DIRL property is the class of *context-free* languages (see [2] for details), a proper extension of the class of rational languages. We say that $K \subseteq F_A$ is *context-free* if $\overline{K}$ is a context-free $(A \cup A^{-1})$-language. This is NOT equivalent to say that $K = \pi(L)$ for some $L \subseteq (A \cup A^{-1})^*$ context-free. Indeed, Frougny, Sakarovitch and Schupp proved that the Benois Theorem cannot be generalized to the context-free level: $\overline{L}$ does not have to be recursive [9].

Let G be [f.g. free]-by-finite and $K \subseteq G$. We say that $K = \cup_{i=0}^m K_i b_i$ $(K_i \subseteq F_A)$ is *context-free* if each K_i is context-free.

Theorem 4.3 *Let G be a [f.g. free]-by-finite group, $g \in G$ and $K \in \mathrm{RatG}$. Let $X \subseteq G$ have the DIRL property. Then it is decidable whether or not $xgx^{-1} \in K$ for some $x \in X$.*

Proof. Indeed, $xgx^{-1} \in K$ for some $x \in X$ if and only if $X \cap \mathrm{Sol(g,K)} = \emptyset$. By Theorem 4.1, $\mathrm{Sol(g,K)} \in \mathrm{RatG}$ and is effectively constructible. Since X has the DIRL property, we can decide whether or not $X \cap \mathrm{Sol(g,K)} = \emptyset$. □

Corollary 4.4 *Let G be a [f.g. free]-by-finite group, $g \in G$ and $K \in \mathrm{RatG}$. Let $X \subseteq G$ be context-free. Then it is decidable whether or not $xgx^{-1} \in K$ for some $x \in X$.*

As far as we are aware, this result is new even for the free group itself. It follows from the results of [7] that the equation $xgx^{-1} \in K$ in the free group with rational constraints for x is decidable, but we know no results on context-free constraints.

Lemma 4.5 *Let G be a [f.g. free]-by-finite group. Then* RatG *is closed for Boolean operations and inversion, and the constructions are effective.*

Proof. We know that $\mathrm{RatF_A}$ is closed for Boolean operations and inversion by Theorem 2.2 and Proposition 2.3 with effective constructions. It follows immediately from Proposition 2.11 that RatG is closed for Boolean operations. Finally, if $L \in \mathrm{RatG}$, then

$$L^{-1} = (\cup_{i=0}^m L_i b_i)^{-1} = \cup_{i=0}^m b_i^{-1} L_i^{-1} \in \mathrm{RatG}$$

follows from $L_i^{-1} \in \mathrm{RatF_A}$. All constructions are effective. □

We consider now (simultaneous) conjugacy of finitely generated subgroups with DIRL constraints, obtaining new generalizations of the classical theorem of Moldavanskii [20] [16, Prop. I.2.23].

Corollary 4.6 *Let G be a [f.g. free]-by-finite group and $H_i, K_i \leq_{f.g.} G$ $(i = 1,\ldots,n)$. Then:*

(i) $X = \{x \in G \mid xH_ix^{-1} \subseteq K_i \ \forall i \in \{1,\ldots,n\}\}$ *is rational and effectively constructible;*

(ii) $Y = \{x \in G \mid xH_ix^{-1} = K_i \ \forall i \in \{1,\ldots,n\}\}$ *is rational and effectively constructible.*

Proof. Every f.g. subgroup is of course rational. In both (i) and (ii), the condition considered is equivalent to finitely many conditions of type $xgx^{-1} \in K$, $x^{-1}gx \in K$ and so both X and Y are finite intersections of sets of the form $\mathrm{Sol(g,K)}$ and $(\mathrm{Sol(g,K)})^{-1}$. Each set $\mathrm{Sol(g,K)}$ is rational and effectively constructible by Theorem 4.1. By Lemma 4.5, X and Y are rational and effectively constructible. □

Similarly to the proof of Theorem 4.3, we get:

Corollary 4.7 *Let G be a [f.g. free]-by-finite group and $H_i, K_i \leq_{f.g.} G$ $(i = 1, \ldots, n)$. Let $X \subseteq G$ have the DIRL property. Then it is decidable whether or not there exists some $x \in X$ such that:*

(i) $xH_ix^{-1} \subseteq K_i$ for $i = 1, \ldots, n$;

(ii) $xH_ix^{-1} = K_i$ for $i = 1, \ldots, n$.

Corollary 4.8 *Let G be a [f.g. free]-by-finite group and $H_i, K_i \leq_{f.g.} G$ $(i = 1, \ldots, n)$. Let $X \subseteq G$ be context-free. Then it is decidable whether or not there exists some $x \in X$ such that:*

(i) $xH_ix^{-1} \subseteq K_i$ for $i = 1, \ldots, n$;

(ii) $xH_ix^{-1} = K_i$ for $i = 1, \ldots, n$.

5 Counterexamples and open problems

Theorem 4.1 cannot be generalized to other one-variable equations, even in the free group case:

Example 5.1 *Let $A = \{a, b\}$ and*

$$X = \{x \in F_A \mid x^2 \in (a^{-1})^* b^2 a^*\}.$$

Then $X \notin \mathrm{RatF_A}$.

Proof. We show that

$$X = \{a^{-k}ba^k \mid k \in \mathbb{N}\}. \tag{16}$$

Clearly, $a^{-k}ba^k \in X$ for every $k \geq 0$. Conversely, let $x \in X$. Write $\overline{x} = uvu^{-1}$ with v cyclically reduced. Then $uvvu^{-1} = \overline{x^2} = a^{-m}bba^n$ for some $m, n \in \mathbb{N}$. It follows that b must occur in v and so $v = b$. Thus $u = a^{-m}$, $m = n$ and so $x = a^{-m}ba^m$. Thus (16) holds.

In view of Theorem 2.2(ii), it suffices to note that X cannot be rational as a subset of R_A, since it clearly fails the Pumping Lemma test (see [2] for details). □

Now we show that Theorem 3.9 cannot be generalized to arbitrary automorphisms:

Example 5.2 *Let $A = \{a, b\}$ and let $\varphi \in \mathrm{AutF_A}$ be defined by $\varphi(a) = ab, \varphi(b) = a$. Then* $\mathrm{Sol}(1, \varphi, \mathrm{A}^*) \notin \mathrm{RatF_A}$.

Proof. First of all, note that φ is onto. Since free groups of finite rank are hopfian, it follows that $\varphi \in \mathrm{AutF_A}$.

Suppose that $\mathrm{Sol}(1, \varphi, \mathrm{A}^*) \in \mathrm{RatF_A}$. Then Theorem 2.2(ii) and Proposition 2.3(i) yield

$$L = \overline{\mathrm{Sol}(1, \varphi, \mathrm{A}^*)} \cap A^* \in \mathrm{Rat}(\mathrm{A} \cup \mathrm{A}^{-1}). \tag{17}$$

We show that

$$L = \{u \in A^* \mid u \leq \varphi(u)\}. \tag{18}$$

Since $\varphi(A^*) \subseteq A^*$, it follows that, given $u \in A^*$,

$$u \leq \varphi(u) \Rightarrow \overline{u^{-1}\varphi(u)} = \rho(u) \in A^* \Rightarrow u \in L.$$

Conversely, let $u \in L$. Then $u \in R_A$ and $(\tau(u))^{-1}\rho(u) = \overline{u^{-1}\varphi(u)} \in A^*$, hence $\tau(u) = 1$. Thus $u \leq \varphi(u)$ and (18) holds.

Since $a < \varphi(a)$, it is immediate that $a < \varphi(a) < \varphi^2(a) < \ldots$ Let $\alpha = \lim_{i\to\infty} \varphi^i(a)$. Then α is the famous *Fibonacci infinite word* (see [15] for details). We show that

$$L = \{u \in A^* \mid u < \alpha\}. \tag{19}$$

Let $u < \alpha$. Since $1 \in L$, we may assume that $u \neq 1$. Since $a < \alpha$, it follows that $a < u$ and so $|u| < |\varphi(u)|$. Now $\alpha = \lim_{i\to\infty} \varphi^i(a)$ yields by continuity (recall Proposition 2.9)

$$\widehat{\varphi}(\alpha) = \widehat{\varphi}(\lim_{i\to\infty} \varphi^i(a)) = \lim_{i\to\infty} \varphi^{i+1}(a) = \alpha$$

and so $\alpha \in \mathrm{Fix}\widehat{\varphi}$. Hence $u, \varphi(u) < \alpha$ and so $u < \varphi(u)$. Thus $u \in L$.

Conversely, let $u \in L$ and write $v = u \wedge \alpha$. Suppose that $v = 1$. Since $b \leq u$ would imply $a \leq \varphi(u)$, contradicting $u \leq \varphi(u)$, it follows that $b \not\leq u$. On the other hand, $a \leq u$ would contradict the definition of v, hence $u = 1$ and so $u < \alpha$.

Assume now that $v \neq 1$. Since $v < \alpha$, we have already proved that $v \in L$. Since $a < \alpha$, it follows that $a < v$ and so $v < \varphi(v)$. Write $\varphi(v) = vcw$ with $c \in A$. Suppose that $v < u$. Since $u, \varphi(v) \leq \varphi(u)$ and $\varphi(v) = vcw$, it follows that $vc \leq u$. On the other hand, $v < \alpha$ yields $\varphi(v) < \alpha$ since $\alpha \in \mathrm{Fix}\widehat{\varphi}$, hence $vc < \alpha$ and the maximality of v is contradicted. Thus $v = u$ and so $u < \alpha$. Therefore (19) holds.

Now, by (17), it follows that $\{u \in A^* \mid u < \alpha\} = L \in \mathrm{RatA}$. Let $\mathcal{A}$ be a finite deterministic trim automaton recognizing L. Since L is the set of prefixes of an infinite word, there exists exactly one edge leaving each vertex, and α would be an ultimately periodic word of the form $\alpha = vw^\omega$. However, α is a classical example of a *Sturmian* word, notoriously non ultimately periodic [15]. Therefore $\mathrm{Sol}(1, \varphi, \mathrm{A}^*) \notin \mathrm{R_A}$. $\square$

Next we show that the proof of Theorem 4.1 cannot be generalized to [f.g free]-by-cyclic groups. We say that G is *[f.g free]-by-cyclic* if G has a f.g. free normal subgroup F such that G/F is cyclic.

Example 5.3 *Let G be the group defined by the presentation*

$$\langle a, b, c \mid cac^{-1} = ab, cbc^{-1} = a\rangle.$$

Write $A = \{a, b\}$. Then:

(i) G *is [f.g free]-by-cyclic and* $F_A \lhd G$*;*

(ii) $\mathrm{Sol(c, A^*c) \cap F_A \notin RatF_A}$.

Proof. Write $A = \{a, b\}$. First of all, we note that $\varphi : F_A \to F_A$ defined by $\varphi(a) = ab$, $\varphi(b) = a$ is the Fibonacci automorphism of Example 5.2. It is easy to see (see e.g. [4]) that G is indeed [f.g free]-by-cyclic with $F_A \lhd G$, having $R_A(c^* \cup (c^{-1})^*)$ as a set of normal forms and satisfying $cuc^{-1} = \varphi(u)$ for every $u \in F_A$.

Let

$$\mathrm{Sol}(1, \varphi, \mathrm{A}^*) = \{\mathrm{x} \in \mathrm{F_A} \mid \mathrm{x}^{-1}\varphi(\mathrm{x}) \in \mathrm{A}^*\}.$$

We show that

$$\mathrm{Sol(c, A^*c) \cap F_A} = (\mathrm{Sol}(1, \varphi, \mathrm{A}^*))^{-1}. \tag{20}$$

Let $x \in F_A$. We have

$$\begin{aligned} x \in \mathrm{Sol(c, A^*c)} &\Leftrightarrow xcx^{-1} \in A^*c \Leftrightarrow xcx^{-1}c^{-1} \in A^* \\ &\Leftrightarrow x\varphi(x^{-1}) \in A^* \Leftrightarrow x^{-1} \in \mathrm{Sol}(1, \varphi, \mathrm{A}^*) \\ &\Leftrightarrow x \in (\mathrm{Sol}(1, \varphi, \mathrm{A}^*))^{-1} \end{aligned}$$

and so (20) holds.

We saw in Example 5.2 that $\mathrm{Sol}(1, \varphi, \mathrm{A}^*) \notin \mathrm{RatF_A}$. By Theorem 2.2 and Proposition 2.3(ii), it follows that

$$\mathrm{Sol(c, A^*c) \cap F_A} = (\mathrm{Sol}(1, \varphi, \mathrm{A}^*))^{-1} \notin \mathrm{RatF_A}$$

either. □

We say that $\varphi \in \mathrm{AutF_A}$ is a *letter permutation* if φ is induced by some permutation of $A \cup A^{-1}$. Letter permutations and inner automorphisms constitute the simplest examples of virtually inner automorphisms. These two classes are clearly closed for composition. In view of (1) and Proposition 1, any composition of letter permutations and inner automorphisms is still virtually inner. These compositions are called *simple* automorphisms by Myasnikov and Shpilrain in [21]. We produce next a nice example of a virtually inner automorphism that is not simple.

Example 5.4 *Let* $A = \{a, b\}$ *and define* $\varphi \in \mathrm{AutF_A}$ *by* $\varphi(a) = b$*,* $\varphi(b) = a^{-1}b^{-1}$*. Then* $\varphi \in \mathrm{ViaF_A}$ *but* φ *is not simple.*

Proof. Since φ is clearly onto, it is an automorphism by the hopfian property. Since φ^3 is the identity, φ is virtually inner. To show that φ is not simple, it suffices to note that

$$\forall u \in R_A \ (|u| \text{ odd } \Rightarrow |\psi(u)| \text{ odd })$$

holds whenever ψ is a letter permutation or an inner automorphism of F_A. This is clear for letter permutations since they are length-preserving. On the other hand, if $|u|$ is odd, then vuv^{-1} has odd length as a word of $(A \cup A^{-1})^*$. Since reduction erases pairs of letters, $|\overline{vuv^{-1}}|$ must be odd as well.

Since $|\varphi(b)| = 2$, it follows that φ is not simple. □

We consider now some open problems that arise naturally from our results.

The first one concerns a weaker generalization of Corollary 3.10, replacing virtually inner automorphisms by arbitrary automorphisms:

Problem 5.5 *Is it decidable, given* $g \in F_A$, $\varphi \in \mathrm{AutF_A}$ *and* $K \in \mathrm{RatF_A}$, *whether or not* $\mathrm{Sol(g, \varphi, K)} \neq \emptyset$*?*

The problem is of course decidable for $\varphi \in \mathrm{ViaF_A}$ in view of Corollary 3.10, since we can always test emptiness for an effectively constructible rational language.

A partial answer can be given for finite K:

Lemma 5.6 *Let* $g \in F_A$, $\varphi \in \mathrm{AutF_A}$ *and* $K \in \mathrm{RatF_A}$. *Write* $B = A \cup \{b\}$ *and let* $\Phi \in \mathrm{AutF_B}$ *be the extension of* φ *defined by* $\Phi(b) = bg$. *Then*

$$\mathrm{Sol(g, \varphi, K) = b^{-1}Sol(1, \Phi, K) \cap F_A}.$$

Proof. First of all, we show that Φ is a well-defined automorphism. Indeed, $b = bgg^{-1} = \Phi(b\varphi^{-1}(g^{-1}))$ and so Φ is onto. Since free groups of finite rank are hopfian, it follows that $\Phi \in \mathrm{AutF_B}$. Let $x \in F_A$. Then

$$x \in b^{-1}\mathrm{Sol(1, \Phi, K) \Leftrightarrow x^{-1}b^{-1}\Phi(bx) \in K \Leftrightarrow x^{-1}g\varphi(x) \in K \Leftrightarrow x \in Sol(g, \varphi, K)}$$

as claimed. □

Proposition 5.7 *Let* $g \in F_A$, $\varphi \in \mathrm{AutF_A}$ *and* $K \subseteq F_A$ *finite. Then* $\mathrm{Sol(g, \varphi, K) \in RatF_A}$ *and is effectively constructible.*

Proof. Without loss of generality, we may assume that $K = \{h\}$. For every $x \in F_A$, we have

$$x^{-1}g\varphi(x) = h \Leftrightarrow x^{-1}gh^{-1}h\varphi(x)h^{-1} = 1 \Leftrightarrow x^{-1}gh^{-1}(\lambda_h\varphi)(x) = 1,$$

hence $\mathrm{Sol(g, \varphi, h) = Sol(gh^{-1}, \lambda_h\varphi, 1)}$. Let $B = A \cup \{b\}$. By Lemma 5.6, we can construct an extension $\Phi \in \mathrm{AutF_B}$ such that

$$\mathrm{Sol(gh^{-1}, \lambda_h\varphi, 1) = b^{-1}Sol(1, \Phi, 1) \cap F_A = b^{-1}Fix\Phi \cap F_A}.$$

By Theorem 2.8, $\mathrm{Fix}\Phi$ is an effectively constructible rational subset of F_A and so is $\mathrm{Sol(g, \varphi, h)}$ since, by Theorem 2.2 and Proposition 2.3(i), $\mathrm{RatF_A}$ is closed for intersection and the construction is effective. □

As a consequence, we obtain a generalization of the result of Bogopolski, Martino, Maslakova and Ventura:

Corollary 5.8 *The twisted conjugacy problem is decidable in the free group with context-free constraints.*

Proof. Given $g, h \in F_A$, $\varphi \in \mathrm{AutF_A}$ and $C \subseteq R_A$ context-free, we must decide if $\overline{\mathrm{Sol(g, \varphi, h)}} \cap C \neq \emptyset$. By Proposition 5.7 and Theorem 2.2(ii), $\overline{\mathrm{Sol(g, \varphi, h)}} \in \mathrm{Rat(A \cup A^{-1})}$ and is effectively constructible. Since context-free languages have the DIRL property, the result follows. □

The above result holds of course for constraints in any language with the DIRL property.

The second open problem concerns the wilder class of [f.g free]-by-cyclic groups:

Problem 5.9 *Is the generalized conjugacy problem for a [f.g free]-by-cyclic group decidable?*

Acknowledgement

The first author acknowledges support from M.E.C. (Spain), Grant MTM2006-15338-C02-01 (European FEDER support included). The second author acknowledges support from Project ASA (PTDC/MAT/65481/2006) and 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 Xunta de Galicia, Grant PGIDITI06PXIB371128PR.

References

[1] M. Benois, Parties rationnelles du groupe libre, *C. R. Acad. Sci. Paris* 269 (1969), 1188–1190.

[2] J. Berstel, *Transductions and Context-free Languages*, Teubner, 1979.

[3] M. Bestvina and M. Handel, Train tracks and automorphisms of free groups, *Ann. Math.* 135 (1992), 1–51.

[4] O. Bogopolski, A. Martino, O. Maslakova and E. Ventura, The conjugacy problem is solvable in free-by-cyclic groups, *Bull. London Math. Soc.* 38 (2006), 787–794.

[5] J. Cassaigne and P. V. Silva, Infinite words and confluent rewriting systems: endomorphism extensions, preprint, CMUP 2006-47.

[6] D. Cooper, Automorphisms of free groups have finitely generated fixed point sets, *J. Algebra* 111 (1987), 453–456.

[7] V. Diekert, C. Gutiérrez and C. Hagenah, The existential theory of equations with rational constraints in free groups is PSPACE-complete, preprint, 2005.

[8] N. J. Fine and H. S. Wilf, Uniqueness theorem for periodic functions, *Proc. Amer. Math. Soc.* 16 (1965), 109–114.

[9] C. Frougny, J. Sakarovitch and P. Schupp, Finiteness conditions on subgroups and formal language theory, *Proc. London Math. Soc.* (3) 58 (1989), 74–88.

[10] D. Gaboriau, A. Jaeger, G. Levitt and M. Lustig, An index for counting fixed points of automorphisms of free groups, *Duke Math. J.* 93 (1998), 425–452.

[11] S. Gersten, On fixed points of certain automorphisms of free groups, *Proc. London Math. Soc.* (3) 48 (1984), 72–90.

[12] M. Gromov, Hyperbolic groups. In: *Essays in Group Theory*, S. M. Gersten (ed.), MSRI Publ.8, Springer, 1987, 75–263.

[13] R. Kannan and R. Lipton, Polynomial-time algorithms for the orbit problem, *J. Assoc. Comput. Mach.* 33.4 (1986), 808–821.

[14] I. Kapovich and A. Myasnikov, Stallings foldings and subgroups of free groups, *J. Algebra* 248 (2002), 608–668.

[15] M. Lothaire, *Algebraic Combinatorics on Words*, Cambridge University Press, Cambridge, 2002.

[16] R. C. Lyndon and P. E. Schupp, *Combinatorial Group Theory*, Springer-Verlag 1977.

[17] I. Lysenök, Some algorithmic properties of hyperbolic groups (Russian), *Izv. Akad. Nauk. SSSR* Ser. Mat. 53 (1989), 814–832; English translation in *Math. USSR Izv.* 35 (1990), 145–163.

[18] G. S. Makanin, Equations in a free group (Russian), *Izv. Akad. Nauk. SSSR* Ser. Mat. 46 (1983), 1199–1273; English translation in *Math. USSR Izv.* 21 (1983).

[19] O. S. Maslakova, The fixed point group of a free group automorphism, *Algebra i Logika* 42.4 (2003), 422–472. English translation in: *Algebra and Logic* 42.4 (2003), 237–265.

[20] D. I. Moldavanskii, Conjugacy of subgroups of a free group, *Algebra i Logika* 8 (1969), 691–694.

[21] A. Myasnikov and V. Shpilrain, Some metric properties of automorphisms of groups, *J. Algebra* 304 (2006), 782–792.

[22] J.-E. Pin, *Varieties of Formal Languages*, North Oxford, London and Plenum, New York, 1986.

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

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

[25] P. V. Silva, Recognizable subsets of a group: finite extensions and the abelian case, *Bulletin of the E.A.T.C.S.* 77 (2002), 195–215.

[26] J. Stallings. Topology of finite graphs, *Invent. Math.* 71 (1983), 551–565.