

Geodesic languages for rational subsets and conjugates in virtually free groups

André Carvalho* and Pedro V. Silva†

Centre of Mathematics, Department of Mathematics
Faculty of Sciences of the University of Porto
R. Campo Alegre, 4169-007 Porto,
Portugal

June 26, 2026

Abstract

We prove that a subset of a virtually free group is rational if and only if the language of geodesic words representing its elements (in any generating set) is rational and that the language of geodesics representing conjugates of elements in a rational subset of a virtually free group is context-free. As a corollary, the doubly generalized conjugacy problem is decidable for rational subsets of finitely generated virtually free groups: there is an algorithm taking as input two rational subsets K_1 and K_2 of a virtually free group that decides whether there is one element of K_1 conjugate to an element of K_2 . For free groups, we prove that the same problem is decidable with rational constraints on the set of conjugators.

1 Introduction

Given a group G , two elements $x, y \in G$ are said to be *conjugate* if there is some $z \in G$ such that $x = z^{-1}yz$, in which case we write $x \sim y$. The *conjugacy problem* $\text{CP}(G)$ consists of, given $x, y \in G$, deciding whether $x \sim y$ or not. This was one of the three algorithmic problems introduced by Dehn [7], together with the *word problem* and the *isomorphism problem*.

The word problem, $\text{WP}(G)$, is possibly the most well-studied algorithmic problem in group theory and consists of, given a word on the generators of a group, deciding whether the element represented by that word is the identity or not, or, equivalently, given two words on the generators, deciding whether they represent the same group element. The *membership problem*, $\text{MP}(G)$, also known as the *generalized word problem* consists of, given a finitely generated subgroup $H \leq G$ and an element $x \in G$, deciding whether $x \in H$ or not. This can be considered more generally for subsets belonging to a reasonably well-behaved class instead of subgroups (e.g. rational or context-free subsets). This can also be rewritten as the question of deciding whether there is some $y \in H$ such that $x = y$ (see [16] for a survey on this problem). In the same spirit, a generalization of the conjugacy problem was considered in [14] and proven to be decidable with respect to rational subsets of finitely generated virtually free groups. The *generalized conjugacy problem with respect to $\mathcal{C}$* , $\text{GCP}_{\mathcal{C}}(G)$, where $\mathcal{C}$ is a class of subsets of G consists then of, given $x \in G$ and $K \in \mathcal{C}$, deciding whether there is some $y \in K$ such that $x \sim y$. Clearly, if $\mathcal{C}$ contains all singletons

*andreacruzcarvalho@gmail.com

†pvsilva@fc.up.pt

(which occurs if $\mathcal{C}$ is the class of rational subsets or the class of cosets of finitely generated subgroups), this is indeed a generalization of the conjugacy problem.

The *intersection problem* $\text{IP}_{\mathcal{C}}(G)$ consists of, given two subsets $K_1, K_2 \in \mathcal{C}$, deciding whether $K_1 \cap K_2 = \emptyset$. Naturally, if $\mathcal{C}$ is a class of subsets containing all singletons, if we can decide the intersection problem with respect to $\mathcal{C}$, we can decide the membership problem with respect to $\mathcal{C}$. Thus, in some sense, the intersection problem can be seen as the doubly generalized word problem and, as done above, it can also be rewritten as the question of deciding whether there are some $x \in K_2$ and $y \in K_2$ such that $x = y$. However, if the class of subsets is closed under product of subsets and inversion, this is equivalent to the membership problem, as it consists of deciding whether $1 \in K_1 K_2^{-1}$. This is the case when considering rational or algebraic subsets, but does not hold in general. In this paper, we consider the *doubly generalized conjugacy problem with respect to $\mathcal{C}$* , $\text{DGCP}_{\mathcal{C}}(G)$, which is the natural generalization of the conjugacy problem corresponding to the intersection problem, that is, the problem of, given $K_1, K_2 \in \mathcal{C}$, deciding whether there are some $x \in K_2$ and $y \in K_2$ such that $x \sim y$.

In case $\mathcal{C}$ is the class of the rational subsets of G , the following is easy to see (where $\leq$ means that the problem on the left-hand side is reducible to the one on the right-hand side and $\equiv$ means that the problems are equivalent):

$$\begin{array}{ccccc} \text{WP}(G) & \leq & \text{MP}_{\text{Rat}}(G) & \equiv & \text{IP}_{\text{Rat}}(G) \\ \mid \wedge & & \mid \wedge & & \mid \wedge \\ \text{CP}(G) & \leq & \text{GCP}_{\text{Rat}}(G) & \leq & \text{DGCP}_{\text{Rat}}(G) \end{array}$$

Notice that $\text{IP}_{\text{Rat}}(G) \leq \text{DGCP}_{\text{Rat}}(G)$, since $K_1 \cap K_2 = \emptyset$ if and only if there is an element in $K_1 K_2^{-1}$ conjugate to an element in $\{1\}$.

We will additionally consider versions of the conjugacy problems with certain *constraints* on the conjugators. In [14], it is proved that the *generalized conjugacy problem with rational constraints* with respect to rational subsets of finitely generated virtually free groups is decidable, meaning that, given a virtually free group G , there is an algorithm taking as input two rational subsets $L, K \in \text{Rat}(G)$ and an element $x \in G$ and decides if there is some $z \in L$ such that $z^{-1}xz \in K$.

Given $K, L \subseteq G$, let

$$\alpha(K, L) = \bigcup_{u \in L} u^{-1} K u.$$

When $L = G$, we simply write $\alpha(K)$ to denote $\alpha(K, G)$

In this paper, we will present a language-theoretical proof of the decidability of the doubly generalized conjugacy problem with rational constraints with respect to rational subsets of finitely generated free groups. To do so, we prove that, in a finitely generated free group, the set $\alpha(K, L)$ of all elements conjugate to an element of K by an element of L is a context-free subset of the ambient free group. It is proved in [15] that a group is virtually free if and only if its conjugacy classes are context-free subsets. Equivalently, a group is virtually free if and only if $\alpha(S)$ is context-free for all singletons S . We prove something much stronger in the case of free groups, namely that $\alpha(K, L)$ is context-free if both K and L are rational.

Theorem 3.5. Let $K, L \in \text{Rat } F_A$. Then $\alpha(K, L)$ is a context-free subset of F_A .

Since context-free languages are closed under intersection with regular languages and emptiness of context-free languages is decidable, we have the following corollary:

Corollary 3.7. The doubly generalized conjugacy problem with rational constraints is decidable with respect to rational subsets of a finitely generated free group.

Regarding virtually free groups, we prove a generalization of the well-known Benois's theorem, showing that a subset is rational if and only if the language of geodesics representing its elements is rational.

Corollary 3.13. Let G be a finitely generated virtually free group and $K \subseteq G$. The following are equivalent:

1. $K \in \text{Rat}(G)$.
2. $\text{Geo}_X(K)$ is a rational language for some finite generating set X .
3. $\text{Geo}_X(K)$ is a rational language for every finite generating set X .

Moreover, the constructions are effective.

We then prove that the language of geodesics representing conjugates of a given rational subset is context-free, which yields a language-theoretic proof of the decidability of the doubly generalized conjugacy problem for rational subsets of finitely generated virtually free groups. Again, it follows from [15] that, for a virtually free group and a singleton $S \subseteq G$, $\text{Geo}(\alpha(S)) = S\pi^{-1} \cap \text{Geo}(G)$ is a context-free language. We prove that this holds for every rational subset of G .

Theorem 3.21. Let G be a virtually free group and $K \in \text{Rat}(G)$. Then $\text{Geo}(\alpha(K))$ is context-free.

Corollary 3.22. Let G be a virtually free group. Then the doubly generalized conjugacy problem in G is decidable.

We remark that Corollaries 3.7 and 3.22 were already known, as it follows directly from the fact that the existential theory of equations with rational constraints in free groups is PSPACE-complete, which was proved by Diekert, Gutiérrez and Hagenah in [8], since, for $L, K_1, K_2 \in \text{Rat}(G)$, the statement that there is an element of K_1 conjugate to an element of K_2 by an element of L can be expressed as:

$$\exists z \in L \exists x \in K_1 \exists y \in K_2 : z^{-1}xz = y.$$

Similarly, for virtually free groups, we can use the analogous result for virtually free groups proved in [6]. However, to the best of our knowledge, these are the first language-theoretic proofs of Corollaries 3.7 and 3.22. We currently do not know of a language-theoretic proof for the doubly generalized conjugacy problem with rational constraints on virtually free groups.

2 Preliminaries

In this section, we will present basic definitions and results on rational, algebraic and context-free subsets of groups (for more details, the reader is referred to [2] and [1]) and on virtually free groups.

2.1 Subsets of groups

The set $\{1, \dots, n\}$ will be denoted by $[n]$. Let $G = \langle A \rangle$ be a finitely generated group, A be a finite generating set, $\tilde{A} = A \cup A^{-1}$ and $\pi : \tilde{A}^* \rightarrow G$ be the canonical (surjective) homomorphism. This notation will be kept throughout the paper.

A subset $K \subseteq G$ is said to be *rational* if there is some rational language $L \subseteq \tilde{A}^*$ such that $L\pi = K$ and *recognizable* if $K\pi^{-1}$ is rational.

We will denote by $\text{Rat}(G)$ and $\text{Rec}(G)$ the class of rational and recognizable subsets of G , respectively. Rational subsets generalize the notion of finitely generated subgroups.

Theorem 2.1 ([2], Theorem III.2.7). Let H be a subgroup of a group G . Then $H \in \text{Rat}(G)$ if and only if H is finitely generated.

Similarly, recognizable subsets generalize the notion of finite index subgroups.

Proposition 2.2. Let H be a subgroup of a group G . Then $H \in \text{Rec}(G)$ if and only if H has finite index in G .

In fact, if G is a group and K is a subset of G then K is recognizable if and only if K is a (finite) union of cosets of a subgroup of finite index.

In case the group G is a free group with basis A with surjective homomorphism $\pi : \tilde{A}^* \rightarrow G$, given $L \subseteq A^*$, we define the set of reduced words representing elements in $L\pi$ by

$$\bar{L} = \{w \in \tilde{A}^* \mid w \text{ is reduced and there exists } u \in L \text{ such that } u\pi = w\pi\}.$$

Benois' Theorem provides us with a useful characterization of rational subsets in terms of reduced words representing the elements in the subset.

Theorem 2.3 (Benois). Let F be a finitely generated free group with basis A and let $L \subseteq \tilde{A}^*$. Then $\bar{L}$ is a rational language of $\tilde{A}^*$ if and only if $L\pi$ is a rational subset of F .

A natural generalization of these concepts concerns the class of context-free languages. A subset $K \subseteq G$ is said to be *algebraic* if there is some context-free language $L \subseteq \tilde{A}^*$ such that $L\pi = K$ and *context-free* if $K\pi^{-1}$ is context-free. We will denote by $\text{Alg}(G)$ and $\text{CF}(G)$ the class of algebraic and context-free subsets of G , respectively. It follows from [10, Lemma 2.1] that these definitions, as well as the definitions of rational and recognizable subsets, do not depend on the finite alphabet A or the surjective homomorphism π .

It is obvious from the definitions that $\text{Rec}(G)$, $\text{Rat}(G)$, $\text{CF}(G)$ and $\text{Alg}(G)$ are closed under union, since both rational and context-free languages are closed under union. The intersection case is distinct: from the fact that rational languages are closed under intersection, it follows that $\text{Rec}(G)$ must be closed under intersection too. However $\text{Rat}(G)$, $\text{Alg}(G)$ and $\text{CF}(G)$ might not be. For instance, if a group G does not have the Howson property, that is, the property that the intersection of two finitely generated subgroups is finitely generated, then $\text{Rat}(G)$ (and so $\text{Alg}(G)$) is not closed under intersection. Regarding $\text{CF}(G)$, it is proved in [5, Proposition 3.10], that if G is virtually free or virtually abelian, then $\text{CF}(G)$ is closed under intersection if and only if G is virtually cyclic, and the author conjectures that, in general, $\text{CF}(G)$ is closed under intersection if and only if G is virtually cyclic. Another important closure property is given by the following lemma from [10].

Lemma 2.4. [10, Lemma 4.1] Let G be a finitely generated group, $R \in \text{Rat}(G)$ and $C \in \{\text{Rec}, \text{CF}\}$. If $K \in C(G)$, then $KR, RK \in C(G)$.

The following is an immediate consequence of the previous lemma.

Corollary 2.5. Let $K \subseteq F_A$ and $u \in F_A$. Then $u^{-1}Ku$ is context-free if and only if K is context-free.

For a finitely generated group G , it is immediate from the definitions that

$$\text{Rec}(G) \subseteq \text{CF}(G) \subseteq \text{Alg}(G)$$

and that

$$\text{Rec}(G) \subseteq \text{Rat}(G) \subseteq \text{Alg}(G).$$

Lemma 2.6. [10, Lemma 4.3] Let X, Y be finite alphabets and let $\psi : Y^* \rightarrow M$, $\varphi : X^* \rightarrow M'$ be homomorphisms onto monoids M, M' . Then every homomorphism $\tau : M' \rightarrow M$ can be lifted to a homomorphism $h : X^* \rightarrow Y^*$ such that the diagram

$$\begin{array}{ccc} X^* & \xrightarrow{\quad h \quad} & Y^* \\ \varphi \downarrow & & \downarrow \psi \\ M' & \xrightarrow{\quad \tau \quad} & M \end{array}$$

commutes. As a consequence, $T\tau^{-1}\varphi^{-1} = T\psi^{-1}h^{-1}$ for every $T \subseteq M$.

However, there is no general inclusion between $\text{Rat}(G)$ and $\text{CF}(G)$. For example, if G is virtually abelian, then $\text{CF}(G) \subseteq \text{Alg}(G) = \text{Rat}(G)$ (and the inclusion is strict if the group is not virtually cyclic) and if the group is virtually free, then $\text{Rat}(G) \subseteq \text{CF}(G)$ (see [10, Lemma 4.2]).

In the case of the free group F_n of rank $n \geq 1$, Herbst proves in [10] an analogue of Benois's Theorem for context-free subsets:

Lemma 2.7. [10, Lemma 4.6] Let F be a finitely generated free group with basis A and let $L \subseteq \tilde{A}^*$. Then $\bar{L}$ is a context-free language of $\tilde{A}^*$ if and only if $L\pi$ is a context-free subset of F .

A slight improvement of the previous lemma can be easily obtained:

Lemma 2.8. Let F be a finitely generated free group and $K \subseteq F$. Then $K \in \text{CF}(F)$ if and only if there is a context-free language L such that $\bar{K} \subseteq L \subseteq K\pi^{-1}$.

We will also make use of the following lemma, which is a simple exercise:

Lemma 2.9. Let $L \in \text{Rat } A^*$ and let $u, v \in A^*$. Then the languages

$$\bigcup_{n \geq 0} u^n L v^n, \quad \bigcup_{0 \leq m \leq n} u^m L v^n \quad \text{and} \quad \bigcup_{0 \leq m \leq n} u^n L v^m$$

are all context-free.

2.2 Virtually free groups

A group G is said to be *virtually free* if it has a free subgroup F of finite index. Since subgroups of free groups are free and every finite index subgroup contains a finite index normal subgroup, we can assume that $F \trianglelefteq_{f.i.} G$. We will usually write

$$G = Fb_1 \cup \dots \cup Fb_n,$$

where all cosets Fb_i are disjoint.

Algebraic and context-free subsets of virtually free groups are studied in [5]. In particular, it is proved in [5, Theorem 4.3] that, if G is a finitely generated virtually free group and $H \leq_{f.g.} G$, then

$$\text{CF}(H) = \{K \subseteq H \mid K \in \text{CF}(G)\}. \quad (1)$$

Also, combining [17, Proposition 4.1] and Propositions 3.6 and 3.7 of [5] we have that $\text{Rec}(G)$ (resp. $\text{Rat}(G)$, $\text{Alg}(G)$, $\text{CF}(G)$) consists of sets of the form $L_i b_i$, where $L_i \in \text{Rec}(F)$ (resp. $\text{Rat}(F)$, $\text{Alg}(F)$, $\text{CF}(F)$).

A word $u = u_1 \dots u_k$ is said to be *cyclically reduced* if $u_1 \neq u_k^{-1}$. Every reduced word u can be decomposed as $u = w^{-1} \tilde{u} w$, where $\tilde{u}$ is cyclically reduced. We refer to $\tilde{u}$ as the *cyclically reduced core* of u .

3 Conjugates of elements in a rational subset

In this section, we will prove that, in a free group, the set of conjugates of elements in a rational subset K with a conjugator in a rational subset L , $\alpha(K, L)$, is context free and that a context-free grammar representing it can be effectively computed. As a corollary, we have a language-theoretical proof that the doubly generalized conjugacy problem with respect to rational subsets with rational constraints is decidable on a free group F . This result also follows from the very strong theorem by Diekert, Gutiérrez and Hagenah [8] stating that the existential theory of equations with rational constraints in free groups is PSPACE-complete.

We will then consider the case of virtually free groups. We start by proving a generalization of Benois's theorem: a subset of a virtually free group is rational if and only if the language of geodesic words representing its elements is rational. Then, we show that the language of geodesic words representing a conjugate of an element in a rational subset K is context-free (and computable), obtaining a language-theoretical proof for the doubly generalized conjugacy problem. This problem was already known to be decidable, as its decidability follows from the solution of equations with rational constraints for virtually free groups [6].

3.1 Free groups

Given $K, L \subseteq F_A$, we say that the product KL is reduced if $\overline{KL} \subseteq \widetilde{A}^*$. The purpose of this subsection is to prove that, given $K, L \in \text{Rat } F_A$, then $\alpha(K, L)$ is a context-free subset of F_A . We start by solving the particular cases where L and K satisfy some reducibility conditions.

Lemma 3.1. Let $K, L \in \text{Rat } \widetilde{A}^*$. Then $\bigcup_{u \in L} u^{-1}Ku \subseteq \widetilde{A}^*$ is a context-free language.

Proof. Let $\mathcal{G} = (V, P, S)$ be the context-free grammar on the alphabet $\widetilde{A} \cup \{\$, \}$ defined by $V = \widetilde{A} \cup \{\$, S\}$ and $P = \{(S, aSa^{-1}) \mid a \in \widetilde{A}\} \cup \{(S, \$)\}$. It is immediate that $L(\mathcal{G}) = \{u^{-1}\$u \mid u \in \widetilde{A}^*\}$. Since context-free languages are closed under intersection with regular languages, it follows that

$$\{u^{-1}\$u \mid u \in L\} = \{u^{-1}\$u \mid u \in \widetilde{A}^*\} \cap L^{-1}\$L$$

is context-free. Since context-free languages are closed under substitution, we can replace the letter $\$$ by the rational (hence context-free) language K and remain context-free. Therefore $\bigcup_{u \in L} u^{-1}Ku$ is a context-free language. $\square$

Lemma 3.2. Let $K, L \in \text{Rat } F_A$ with both $L^{-1}K$ and KL reduced. Then $\alpha(K, L)$ is a context-free subset of F_A .

Proof. By Lemma 2.7, it suffices to show that $\overline{\alpha(K, L)}$ is a context-free language. This same argument will be used in the next proofs without further reference.

Now $\overline{\alpha(K, L)} = \{u^{-1}\overline{K}u \mid u \in \overline{L}\}$ and it follows from Benois' Theorem that $\overline{K}$ and $\overline{L}$ are both rational languages. By Lemma 3.1, $\overline{\alpha(K, L)}$ is a context-free language. $\square$

Lemma 3.3. Let $K, L \in \text{Rat } F_A$ with KL reduced. Then $\alpha(K, L)$ is a context-free subset of F_A .

Proof. We may assume that K and L are both nonempty. Let C denote the set of all cyclically reduced elements of F_A , which is clearly a rational subset. Then $K \cap C$ and $K \setminus C$ are both rational subsets of F_A . Since $L^{-1}(K \setminus C)$ and $(K \setminus C)L$ are both reduced, it follows from Lemma 3.2 that $\alpha(K \setminus C, L)$ is a context-free subset of F_A . Thus it suffices to show that $\alpha(K \cap C, L)$ is a context-free subset of F_A . Therefore we may assume that $K \subseteq C$, and we may also assume that $1 \notin K$.

Let $\mathcal{A} = (Q, q_0, T, E)$ and $\mathcal{A}' = (Q', q'_0, T', E')$ denote respectively the minimal automata of $\overline{L}$ and $\overline{K}$. For all $I, J \subseteq Q$, let $L_{IJ} = L(Q, I, J, E)$. For all $I', J' \subseteq Q'$, let $L'_{I'J'} = L(Q', I', J', E')$. Let

$$X = \bigcup_{m=0}^{|Q|-1} Q^{2m+1} \times Q'.$$

We show that

$$\begin{aligned} \overline{\alpha(K, L)} &= \{w^{-1}v_2v_1w \mid \exists (p_1, q_1, \dots, p_m, q_m, p_{m+1}, q') \in X, v_1 \in L'_{q'_0q'} \cap (\bigcap_{i=0}^m L_{q_i p_{i+1}}), \\ &\quad v_2 \in L'_{q'T'} \cap (\bigcap_{i=1}^m L_{p_i q_i}), w \in L_{p_{m+1}T}\} \cap \widetilde{A^*}. \end{aligned} \quad (2)$$

Indeed, let $w^{-1}v_2v_1w$ belong to the right hand side of (2) for some $(p_1, q_1, \dots, p_m, q_m, p_{m+1}, q') \in X$. Then we have a path $q'_0 \xrightarrow{v_1} q' \xrightarrow{v_2} t' \in T'$ in $\mathcal{A}'$ and a path

$$q_0 \xrightarrow{v_1} p_1 \xrightarrow{v_2} q_1 \xrightarrow{v_1} \dots \xrightarrow{v_2} q_{m-1} \xrightarrow{v_1} p_m \xrightarrow{v_2} q_m \xrightarrow{v_1} p_{m+1} \xrightarrow{w} t \in T$$

in $\mathcal{A}$. Hence $v_1v_2 \in L(\mathcal{A}') = \overline{K}$ and $(v_1v_2)^m v_1w \in L(\mathcal{A}) = \overline{L}$. It follows that

$$w^{-1}v_2v_1w = w^{-1}v_1^{-1}(v_2^{-1}v_1^{-1})^m v_1v_2(v_1v_2)^m v_1w \in \alpha(K, L).$$

Since $w^{-1}v_2v_1w$ is a reduced word by hypothesis, we get $w^{-1}v_2v_1w \in \overline{\alpha(K, L)}$.

Conversely, assume that $u \in \overline{L}$ and $v \in \overline{K}$. We consider the longest prefix of u which is a prefix of some power of v . More precisely, write $u = v^m v_1w$ such that $m \geq 0$ and $v = v_1v_2$ with $v_2 \neq 1$. Then

$$\overline{u^{-1}vu} = \overline{w^{-1}v_1^{-1}v^{-m}vv^mv_1w} = \overline{w^{-1}v_2v_1w}.$$

Note that every path of the form $p \xrightarrow{v^m} q$ in $\mathcal{A}$ with $m \geq |Q|$ must contain some loop labelled by v^s with $1 \leq s \leq |Q|$, hence we may replace $u = v^m v_1w$ by $u' = v^{m-s} v_1w$ without changing the final outcome $\overline{w^{-1}v_2v_1w}$. Thus we assume that $m < |Q|$. We must have a path

$$q_0 \xrightarrow{v_1} p_1 \xrightarrow{v_2} q_1 \xrightarrow{v_1} \dots \xrightarrow{v_2} q_{m-1} \xrightarrow{v_1} p_m \xrightarrow{v_2} q_m \xrightarrow{v_1} p_{m+1} \xrightarrow{w} t \in T$$

in $\mathcal{A}$ and a path $q'_0 \xrightarrow{v_1} q' \xrightarrow{v_2} t' \in T'$ in $\mathcal{A}'$. It follows that $(p_1, q_1, \dots, p_m, q_m, p_{m+1}, q') \in X$, $v_1 \in L'_{q'_0q'} \cap (\bigcap_{i=0}^m L_{q_i p_{i+1}})$, $v_2 \in L'_{q'T'} \cap (\bigcap_{i=1}^m L_{p_i q_i})$ and $w \in L_{p_{m+1}T}$. It remains to show that $w^{-1}v_2v_1w$ is reduced.

Indeed, v_2v_1w labels a path in a trim automaton recognizing a reduced language, hence must be a reduced word itself. Suppose that $w^{-1}v_2$ is not reduced. Then v_2 and w_2 share the same first letter, say a . Then $v^m v_1a$ is a prefix of u which is a prefix of v^{m+1} , contradicting the maximality of $v^m v_1$. Hence $w^{-1}v_2$ is reduced. Since v_2v_1w is reduced and $v_2 \neq 1$, then $w^{-1}v_2v_1w$ is itself reduced and so (2) holds. Now, applying Lemma 3.1 $|X|$ times to the rational languages featuring the right hand side of (2), and taking into account that context-free languages are closed under intersection with rational languages and union, we conclude that $\overline{\alpha(K, L)}$ is a context-free language as intended. $\square$

Lemma 3.4. Let $K, L \in \text{Rat } F_A$ with $L^{-1}K$ reduced. Then $\alpha(K, L)$ is a context-free subset of F_A .

Proof. We may assume that K and L are both nonempty. Since K rational implies K^{-1} rational and $L^{-1}K$ reduced implies $K^{-1}L$ reduced, it follows from the proof of Lemma 3.3 that $\overline{\alpha(K^{-1}, L)}$ is a context-free language. Now

$$\overline{\alpha(K, L)} = \bigcup_{u \in L} \overline{u^{-1}Ku} = \left(\bigcup_{u \in L} \overline{u^{-1}K^{-1}u} \right)^{-1} = \left(\overline{\alpha(K^{-1}, L)} \right)^{-1}.$$

Since context-free languages are closed under reversal and homomorphism, it follows easily that $\left(\overline{\alpha(K^{-1}, L)} \right)^{-1}$ is a context-free language. Thus $\overline{\alpha(K, L)}$ is a context-free language and we are done. $\square$

Now, we can prove the main result of this subsection.

Theorem 3.5. Let $K, L \in \text{Rat } F_A$. Then $\alpha(K, L)$ is a context-free subset of F_A .

Proof. We may assume that K and L are both nonempty. Since $\alpha(1, L) = 1$, we may assume that $1 \notin K$.

Let $\mathcal{A} = (Q, q_0, T, E)$ and $\mathcal{A}' = (Q', q'_0, T', E')$ denote respectively the minimal automata of $\bar{L}$ and $\bar{K}$. We keep the notation introduced in the proof of Lemma 3.3. We define

$$X = \{(q, p', q') \in Q \times Q' \times Q' \mid L_{q_0q} \cap L'_{q'_0p'} \cap (L'_{q'T'})^{-1}, L'_{p'q'} \setminus \{1\} \neq \emptyset\}.$$

For every $a \in \tilde{A}$, we define the possibly empty subsets of F_A

$$Y_a = \{w^{-1}v_2w \mid \exists (q, p', q') \in X, v_2 \in L'_{p'q'} \cap \tilde{A}^*a, w \in L_{qT} \setminus a^{-1}\tilde{A}^*\},$$

$$Z_a = \{w^{-1}v_2w \mid \exists (q, p', q') \in X, v_2 \in L'_{p'q'} \cap a\tilde{A}^*, w \in L_{qT} \setminus a\tilde{A}^*\}.$$

We show that

$$\alpha(K, L) = \bigcup_{a \in \tilde{A}} (Y_a \cup Z_a). \quad (3)$$

Let $y \in Y_a$. Then there exist $(q, p', q') \in X$, $v_2 \in L'_{p'q'} \cap \tilde{A}^*a$ and $w \in L_{qT} \setminus a^{-1}\tilde{A}^*$ such that $y = w^{-1}v_2w$. Since $(q, p', q') \in X$, there exists some $v_1 \in L_{q_0q} \cap L'_{q'_0p'} \cap (L'_{q'T'})^{-1}$. Then we have a path $q_0 \xrightarrow{v_1} q \xrightarrow{w} t \in T$ in $\mathcal{A}$ and a path

$$q'_0 \xrightarrow{v_1} p' \xrightarrow{v_2} q' \xrightarrow{v_1^{-1}} t' \in T'$$

in $\mathcal{A}'$. Hence $v_1v_2v_1^{-1} \in L(\mathcal{A}') = \bar{K}$ and $v_1w \in L(\mathcal{A}) = \bar{L}$. It follows that

$$y = w^{-1}v_2w = w^{-1}v_1^{-1}(v_1v_2v_1^{-1})v_1w \in \alpha(K, L).$$

Thus $Y_a \subseteq \alpha(K, L)$. The inclusion $Z_a \subseteq \alpha(K, L)$ is proved similarly.

Conversely, assume that $u \in \bar{L}$ and $v \in \bar{K}$. We may write $v = bcb^{-1}$ with c cyclically reduced. Since $1 \notin K$, we have $c \neq 1$. Let v_1 denote the longest common prefix of u and b (which may be the empty word). Write $u = v_1w$ and $v = v_1v_2v_1^{-1}$. We must have a path

$$q'_0 \xrightarrow{v_1} p' \xrightarrow{v_2} q' \xrightarrow{v_1^{-1}} t' \in T'$$

in $\mathcal{A}'$ and a path $q_0 \xrightarrow{v_1} q \xrightarrow{w} t \in T$ in $\mathcal{A}$. It follows that $v_1 \in L_{q_0q} \cap L'_{q'_0p'} \cap (L'_{q'T'})^{-1}$, $v_2 \in L'_{p'q'} \setminus \{1\}$ and $w \in L_{qT}$, hence $(q, p', q') \in X$. Moreover, $u^{-1}vu = w^{-1}v_1^{-1}(v_1v_2v_1^{-1})v_1w = w^{-1}v_2w$.

Now it follows from the maximality of v_1 that at least one of the products $w^{-1}v_2, v_2w$ must be reduced (if $v_1 = b$, this follows from $v_2 = c$ being cyclically reduced). If $w^{-1}v_2$ is reduced, then $u^{-1}vu \in Z_a$ when a denotes the first letter of v_2 . If v_2w is reduced, then $u^{-1}vu \in Y_a$ when a denotes the last letter of v_2 . Therefore (3) holds.

Since

$$Y_a = \bigcup_{(q, p', q') \in X} \alpha(L'_{p'q'} \cap \tilde{A}^*a, L_{qT} \setminus a^{-1}\tilde{A}^*)$$

and $(L'_{p'q'} \cap \tilde{A}^*a)(L_{qT} \setminus a^{-1}\tilde{A}^*)$ is reduced, it follows from Lemma 3.3 that Y_a is a context-free subset of F_A .

Since

$$Z_a = \bigcup_{(q, p', q') \in X} \alpha(L'_{p'q'} \cap a\tilde{A}^*, L_{qT} \setminus a\tilde{A}^*)$$

and $(L_{qT} \setminus a\tilde{A}^*)^{-1}(L'_{p'q'} \cap a\tilde{A}^*)$ is reduced, it follows from Lemma 3.4 that Z_a is a context-free subset of F_A .

Now it follows from (3) that $\alpha(K, L)$ is itself a context-free subset of F_A . $\square$

The following corollary follows as an immediate application of the previous theorem and will be useful in the next subsection to deal with the case of virtually free groups.

Corollary 3.6. Let $K \in \text{Rat } F_A$ and $u \in F_A$. Then $\bigcup_{n \in \mathbb{N}} u^{-n} K u^n$ is a context-free subset of F_A .

Proof. Since $u^* \in \text{Rat } F_A$, the claim follows immediately from Theorem 3.5. $\square$

Since context-free languages are closed under intersection with regular languages and emptiness of a context-free language can be decided, we can decide the doubly generalized conjugacy problem with rational constraints with respect to rational subsets of a finitely generated free groups. As mentioned in the introduction, this result follows from the fact that the existential theory of equations with rational constraints in free groups is PSPACE-complete, which was proved by Diekert, Gutiérrez and Hagenah in [8]. However, we provide an alternative language-theoretic proof.

Corollary 3.7. The doubly generalized conjugacy problem with rational constraints is decidable with respect to rational subsets of a finitely generated free groups.

Proof. Let $\pi : \tilde{A}^* \rightarrow F_A$ be the canonical surjective homomorphism and $K_0, K_1, K_2 \in \text{Rat}(F_A)$ be our input (by this we mean that we get three finite state automata recognizing languages $L_0, L_1, L_2 \subseteq \tilde{A}^*$ such that $L_i \pi = K_i$, for $i = 0, 1, 2$). We want to decide if there are some $u \in K_0, x_1 \in K_1, x_2 \in K_2$ such that $x_1 = u^{-1} x_2 u$, i.e., if $K_1 \cap \alpha(K_2, K_0) = \emptyset$. In view of Theorem 3.5, we can compute a context-free grammar $\mathcal{G}$ such that $L(\mathcal{G}) = (\alpha(K_2, K_0))\pi^{-1}$. Then $L_1 \cap L(\mathcal{G})$ is an effectively constructible context-free language and $K_1 \cap \alpha(K_2, K_0) = \emptyset$ if and only if $L_1 \cap L(\mathcal{G}) = \emptyset$, which can be decided. $\square$

3.2 Virtually free groups

Now we turn our attention to the case of virtually free groups. Our goal is to prove that, if K is a rational subset of a finitely generated virtually free group, then $\text{Geo}(\alpha(K))$ is a context-free language, which yields as a corollary that the doubly generalized conjugacy problem is decidable with respect to rational subsets. We will write G to denote a finitely generated virtually free group and put

$$G = Fb_1 \cup \dots \cup Fb_m,$$

where $F = F_A$ is a free normal subgroup of G of finite index m . We will also put $B = A \cup \{b_1, \dots, b_m\}$. Unless stated otherwise, B will be our standard generating set for G .

For a subset $K \subseteq G$ and a generating set X of G , let $\text{Geo}_X(K) \subseteq \tilde{X}^*$ denote the set of all geodesics with respect to X representing elements in K . In a hyperbolic group, the language of all geodesics, $\text{Geo}_X(G)$, is rational for every generating set X (see [3]). We say that a word $u \in \tilde{B}^*$ is in *normal form* if it is of the form vb_i , for some freely reduced word $v \in \tilde{A}^*$ and $i \in [m]$. Clearly, for every $u \in \tilde{B}^*$, there is a unique $\bar{u} \in \tilde{B}^*$ in normal form such that $\bar{u}\pi = u\pi$. Notice that, when the word u belongs to $\tilde{A}^*$ this corresponds to free reduction.

Given two words $u, v \in \tilde{X}^*$ we write $u \equiv v$ to emphasize that u and v are equal as words, while $u\pi = v\pi$ will be written to mean that they represent the same group element. We write $u \doteq u_1 \dots u_n$ if $u \equiv u_1 \dots u_n$ with $u_1, \dots, u_n \in \tilde{X}$. For all $1 \leq i \leq j \leq n$, we write then $u^{[i,j]} = u_i u_{i+1} \dots u_j$ and $u^{[j]} = u^{[1,j]}$. Given a language L , we denote by $\text{Cyc}(L)$ the language of all cyclic permutations of words in L . If L is rational (resp. context-free), then $\text{Cyc}(L)$ is also rational (resp. context-free [13, Exercise 6.4 c])).

In [11, Proposition 3.1], it is proved that if u and v are words in a δ -hyperbolic group with $u\pi = v\pi$, u is geodesic and v is (λ, ε) -quasigeodesic, then u and v *boundedly asynchronously K -fellow travel for some constant K and some asynchronicity bound M* , where K and M depend only on λ, ε and δ . With our notation, it follows from their proof that, given λ, ε , there exists a K such that for all geodesic words u and all (λ, ε) -quasigeodesic v such

that $u\pi = v\pi$, there is a (not necessarily strictly) increasing function $h : \{0, \dots, |v|\} \rightarrow \{0, \dots, |u|\}$ such that $h(0) = 0$, $h(|v|) = |u|$ and

$$d(v^{[i]}\pi, u^{[h(i)]}\pi) \leq K \quad \text{and} \quad |h(i) - h(i-1)| \leq 2K + 1 \quad (4)$$

for $i \in [|v|]$. We will denote the boundedly asynchronously fellow travel constant by $K(\lambda, \varepsilon, \delta)$ throughout the paper. In particular, (λ, ε) -quasigeodesics and geodesics representing the same elements are at Hausdorff distance at most $K(\lambda, \varepsilon, \delta)$.

For a finite alphabet A , we say that $\mathfrak{T} = (Q, q_0, F, \delta, \lambda)$ is a *finite state A-transducer* if Q is a finite set of states, $q_0 \in Q$ is the initial state, $F \subseteq Q$ is a set of final states, $\delta : Q \times A \rightarrow Q$ and $\lambda : Q \times A \rightarrow A^*$ are mappings. We will write $x \xrightarrow{c|d} y$ to mean that $(x, c)\delta = y$ and $(x, c)\lambda = d$. Given $L \subseteq A^*$, we write

$$\mathfrak{T}(L) = \{w_1 \dots w_n \mid \exists \text{ a path } q_0 \xrightarrow{a_1|w_1} q_1 \xrightarrow{a_2|w_2} \dots \xrightarrow{a_n|w_n} q_n \in T \text{ with } a_1 \dots a_n \in L\}.$$

Theorem 3.8. Let G be a finitely generated hyperbolic group, X be a generating set and L be a rational language of (λ, ε) -quasigeodesic words over $\tilde{X}$, for some (fixed) values λ and ε . Then $\text{Geo}_X(L\pi)$ is an (effectively computable) rational language.

Proof. Let K be the constant from (4) and Q be the set of all geodesic words over $\tilde{X}$ of length at most K . Consider the finite transducer $\mathfrak{T}$ with set of vertices Q , edges $w \xrightarrow{c|u} v$ for $c \in \tilde{X}$, $u \in \tilde{X}^*$ a geodesic word of length at most $2K + 1$, and v a geodesic word representing $(u^{-1}wc)\pi$, and with the empty word being the initial and (unique) final state. We claim that $(\mathfrak{T}(L))\pi \subseteq L\pi$ and that $\text{Geo}_X(L\pi) \subseteq \mathfrak{T}(L)$, and so $\text{Geo}_X(L\pi) = \text{Geo}_X(G) \cap \mathfrak{T}(L)$ is a rational language.

Let $u \in \mathfrak{T}(L)$. There must be some $v \doteq v_1 \dots v_n \in L$ and a path of the form

$$\varepsilon = p_0 \xrightarrow{v_1|u_1} p_1 \xrightarrow{v_2|u_2} p_2 \dots \xrightarrow{v_{n-1}|u_{n-1}} p_{n-1} \xrightarrow{v_n|u_n} p_n = \varepsilon$$

in $\mathfrak{T}$ with $u \equiv u_1 \dots u_n$. But then $(u_i^{-1}p_{i-1}v_i) = p_i$ for $i \in [n]$ and it follows easily by induction that $1 = p_n\pi = (u_n^{-1} \dots u_1^{-1}v_1 \dots v_n)\pi$, i.e., $u\pi = v\pi \in L\pi$. Therefore $(\mathfrak{T}(L))\pi \subseteq L\pi$. So, we have proved that a word in $\mathfrak{T}(L)$ must represent an element of $L\pi$. We will now show that $\mathfrak{T}(L)$ contains all geodesic words representing elements of $L\pi$. It might also contain non-geodesic words representing elements of $L\pi$, but that is not a problem, as we then will have that $\text{Geo}_X(L\pi) = \text{Geo}_X(G) \cap \mathfrak{T}(L)$ is a rational language.

Now, let $u \doteq u_1 \dots u_k \in \text{Geo}_X(L\pi)$. Then $u\pi = v\pi$ for some quasigeodesic $v \doteq v_1 \dots v_n \in L$. Let $h : [n] \rightarrow [k]$ be the function from (4). For $i = 0, \dots, n$, let $w_i \in \text{Geo}_X(((u^{[h(i)]})^{-1}v^{[i]})\pi)$. We claim that there is a path in $\mathfrak{T}$ of the form

$$\varepsilon = w_0 \xrightarrow{v_1|u^{[h(1)]}} w_1 \xrightarrow{v_2|u^{[h(1)+1, h(2)]}} \dots \xrightarrow{v_n|u^{[h(n-1)+1, h(n)]}} w_n = \varepsilon.$$

Indeed, it follows from (4) that $w_i \in Q$ and $|u^{[h(i-1)+1, h(i)]}| \leq 2K + 1$ for $i \in [n]$. The edges are well defined since

$$\begin{aligned} ((u^{[h(i-1)+1, h(i)]})^{-1}w_{i-1}v_i)\pi &= ((u^{[h(i-1)+1, h(i)]})^{-1}(u^{[h(i-1)]})^{-1}v^{[i-1]}v_i)\pi \\ &= ((u^{[h(i)]})^{-1}v^{[i]})\pi = w_i\pi \end{aligned}$$

holds for $i \in [n]$.

Hence

$$u = u_1 \dots u_k = u_1 \dots u_{h(n)} \in \mathfrak{T}(v_1 \dots v_n) = \mathfrak{T}(v) \subseteq \mathfrak{T}(L)$$

and so $\text{Geo}_X(L\pi) \subseteq \mathfrak{T}(L)$. Therefore $\text{Geo}_X(L\pi) = \text{Geo}_X(G) \cap \mathfrak{T}(L)$ is a rational language. $\square$

Remark 3.9. The theorem above is stated in terms of rational languages but works in the exact same way for any class of languages preserved by rational transduction, such as the class of context-free languages.

We will now prove that, in a finitely generated virtually free group, the language of normal forms of words consists of quasigeodesics. For $i \in [m]$ we will denote by φ_i the automorphism of F defined by $u\varphi_i = b_i u b_i^{-1}$.

Lemma 3.10. Let $w \in \tilde{B}^*$, $M = \max\{|a\varphi_i|_A \mid a \in A, i \in [m]\}$, $N = \max\{|u|_A : \exists i, j, k \in [m] : b_i b_j = u b_k\}$ and $C = \max\{M, N\}$. Then, $|\bar{w}| \leq C|w|$.

Proof. Let $w \in \tilde{B}^*$. We proceed by induction on $|w|$. If $|w| = 0$, then $\bar{w} = w$ and so $|\bar{w}| = |w|$. Now assume that the result holds for all words of length up to some n and let $w \in \tilde{B}^*$ be such that $|w| = n + 1$. Then $w = ux$ for some $x \in \tilde{B}$ and we may write $\bar{u} = vb_j$. From the induction hypothesis, it follows that $|vb_j| \leq C|u|$. If $x \in \tilde{A}$, we have that $w\pi = (\bar{u}x)\pi = (vb_jx)\pi = (v\pi)(x\pi\varphi_j)b_j$, hence $\bar{w} = \overline{v(x\varphi_j)b_j}$ and

$$|\bar{w}| \leq |v| + |\overline{x\varphi_j}| + 1 = |vb_j| + M \leq C|u| + C = C(|u| + 1) = C|w|.$$

If $x \in \widetilde{\{b_1, \dots, b_m\}}$, say $x = b_r$, then $\overline{b_jx} = yb_s$ for some $s \in [m]$ and $y \in F$ such that $|y| \leq N$. Hence $w\pi = (\bar{u}x)\pi = (vb_jx)\pi = (vyb_s)\pi$, yielding $\bar{w} = \overline{vyb_s}$ and

$$|\bar{w}| \leq |v| + |y| + 1 \leq |vb_j| + N \leq C|u| + C = C(|u| + 1) = C|w|.$$

□

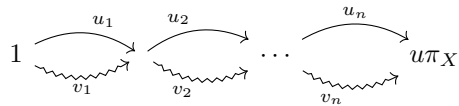
Corollary 3.11. Every word in normal form is a $(C, 0)$ -quasigeodesic for C defined as in the preceding lemma.

Proof. Let $w \in \tilde{B}^*$ be a word in normal form. We have to show that any subword of w of length k has geodesic length at least $\frac{k}{C}$. Since any subword of w is a word in normal form, we only need to prove that a word u in normal form has geodesic length of at least $\frac{|u|}{C}$. This follows from Lemma 3.10, since, for a word u in normal form, letting v be a geodesic word such that $v\pi = u\pi$, we have that $\bar{v} = u$, and so $|u| \leq C|v|$, i.e. $|v| \geq \frac{|u|}{C}$. □

Lemma 3.12. Let G be a hyperbolic group, X, Y be two generating sets and $\pi_X : \tilde{X} \rightarrow G$ and $\pi_Y : \tilde{Y} \rightarrow G$ be the natural surjective homomorphisms and put $N_{X,Y} = \max\{d_Y(1, x) \mid x \in X\}$. If $u \doteq x_1 \cdots x_n$ is a geodesic word in $\Gamma_X(G)$, then a word of the form $v = v_1 \cdots v_n$, where v_i is a geodesic word in $\Gamma_Y(G)$ representing $x_i\pi$, is a $(N_{X,Y}^2, 2N_{X,Y}^3)$ -quasigeodesic in $\Gamma_Y(G)$.

Proof. We have to prove that, for all $1 \leq i \leq j \leq |v|$,

$$j - i \leq N_{X,Y}^2 d_Y(v^{[i]}\pi_Y, v^{[j]}\pi_Y) + 2N_{X,Y}^3.$$



Let $1 \leq i \leq j \leq |v|$. Define k_i to be the largest integer such that $v_1 \cdots v_{k_i}$ is a prefix of $v^{[i]}$ and k_j to be the smallest integer such that $v^{[j]}$ is a prefix of $v_1 \cdots v_{k_j}$. Notice that, for all

$i, |v_i| \leq N_{X,Y}$. Then, we have that:

$$\begin{aligned}
j - i &\leq |v_{k_i+1} \cdots v_{k_j}| \\
&\leq |k_i - k_j| N_{X,Y} \\
&= N_{X,Y} d_X((v_1 \cdots v_{k_i})\pi_Y, (v_1 \cdots v_{k_j})\pi_Y) \\
&\leq N_{X,Y}^2 d_Y((v_1 \cdots v_{k_i})\pi_Y, (v_1 \cdots v_{k_j})\pi_Y) \\
&\leq N_{X,Y}^2 \left(d_Y((v_1 \cdots v_{k_i})\pi_Y, v^{[i]}\pi_Y) + d_Y(v^{[i]}\pi_Y, v^{[j]}\pi_Y) + d_Y(v^{[j]}\pi_Y, (v_1 \cdots v_{k_j})\pi_Y) \right) \\
&\leq N_{X,Y}^2 \left(N_{X,Y} + d_Y(v^{[i]}\pi_Y, v^{[j]}\pi_Y) + N_{X,Y} \right) \\
&= N_{X,Y}^2 d_Y(v^{[i]}\pi_Y, v^{[j]}\pi_Y) + 2N_{X,Y}^3.
\end{aligned}$$

□

We can now combine the previous results to prove a generalization of Benois's Theorem for virtually free groups.

Corollary 3.13. Let G be a finitely generated virtually free group and $K \subseteq G$. The following are equivalent:

1. $K \in \text{Rat}(G)$.
2. $\text{Geo}_X(K)$ is a rational language for some finite generating set X .
3. $\text{Geo}_X(K)$ is a rational language for every finite generating set X .

Moreover, the constructions are effective.

Proof. It is clear from the definitions that $3 \implies 2 \implies 1$. We will prove that $1 \implies 2$ and that $2 \implies 3$.

Compute the (rational) language L of normal forms of K : this can be done by computing rational subsets L_i of F such that $K = \bigcup_{i \in [m]} L_i b_i$ (see [17, Proposition 4.1]) and then using Benois's theorem to compute the language of reduced words $\overline{L_i}$ representing elements in L_i . We then obtain that

$$L = \bigcup_{i \in [m]} \overline{L_i} b_i.$$

In view of Corollary 3.11, the language L of normal forms representing elements in K is a language of $(C, 0)$ -quasigeodesics over $\tilde{B}$ such that $L\pi = K$. By Theorem 3.8, $\text{Geo}_B(K)$ is rational, so we have that $1 \implies 2$.

Now, using Lemma 3.12, we have that, given two finite generating sets X, Y and replacing every edge of an automaton representing $\text{Geo}_X(K)$ by a path labeling a geodesic word over $\tilde{Y}$ representing the letter from X labelling the edge, the language recognized by the new automaton will be a language L of $(N_{X,Y}^2, 2N_{X,Y}^3)$ -quasigeodesic words over $\tilde{Y}$ such that $L\pi_Y = K$. Hence, $\text{Geo}_Y(K)$ is rational by Theorem 3.8. □

Remark 3.14. Similarly to what happens in Remark 3.9, the equivalence between 2 and 3 holds for any class of languages closed under rational transductions. Since rationality (resp. context-freeness) of the language of geodesics representing a given subset is independent of the generating set we will usually say that, for a subset K , $\text{Geo}(K)$ is rational (resp. context-free) to mean that $\text{Geo}_X(K)$ is rational (resp. context-free) for some (and so, for every) finite generating set X .

We define w to be a *fully* (λ, ε) -quasireduced word if w and all of its cyclic conjugates are (λ, ε) -quasigeodesic words.

We now present three results from [12] and [4]:

Lemma 3.15. [12, Lemma 16] If u and v are fully (λ, ε) -quasireduced words representing conjugate elements of a δ -hyperbolic group, then either $\max(|u|, |v|) \leq \lambda(8\delta + 2K + \varepsilon + 1)$ or there exist cyclic conjugates u' and v' of u and v and a word α with $(\alpha u' \alpha^{-1})\pi = v'\pi$ and $|\alpha| \leq 2(\delta + K)$, where K is the boundedly asynchronous fellow travel constant satisfied by (λ, ε) -quasigeodesics with respect to geodesics (see (4)).

Proposition 3.16. [12, Proposition 18] Let u be a geodesic word in a δ -hyperbolic group G with $\delta \geq 1$. Then we have that $u \equiv u_1 u_2 u_3$, where $(u_3 u_1)\pi = \alpha\pi$ for some word α with $|\alpha| \leq \delta$, and $u_2\alpha$ is fully $(1, 3\delta + 1)$ -quasireduced.

In other words, the word $u' \equiv u_1 u_2 \alpha \alpha^{-1} u_3$ obtained by insertion of $\alpha \alpha^{-1}$ into u can be split as $u'_1 u'_2 u'_3$ such that $(u'_3 u'_1)\pi = 1$ and $u'_2 = u_2 \alpha$ is fully $(1, 3\delta + 1)$ -quasireduced.

Let G be a hyperbolic group with generating set A . Given $g, h, p \in G$, we define the Gromov product of g and h taking p as basepoint by

$$(g|h)_p^A = \frac{1}{2}(d_A(p, g) + d_A(p, h) - d_A(g, h)).$$

We will often write $(g|h)_p$ to denote $(g|h)_p^A$, when the generating set is clear from context.

Lemma 3.17. [4, Lemma 4.1] Let H be a hyperbolic group, $u, v \in H$ and $p \in \mathbb{N}$. Then the following are equivalent:

- (i) $(u|v)_1 \leq p$
- (ii) for any geodesics α and β from 1 to u^{-1} and v , respectively, we have that the concatenation

$$1 \xrightarrow{\alpha} u^{-1} \xrightarrow{\beta} u^{-1}v$$

is a $(1, 2p)$ -quasi-geodesic

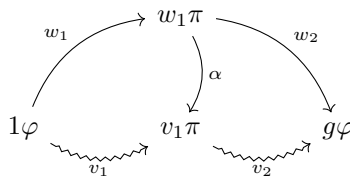
- (iii) there are geodesics α and β from 1 to u^{-1} and v , respectively, such that the concatenation

$$1 \xrightarrow{\alpha} u^{-1} \xrightarrow{\beta} u^{-1}v$$

is a $(1, 2p)$ -quasi-geodesic

Lemma 3.18. Let G be a δ -hyperbolic group and $g \in G$ be an element having a fully $(1, \varepsilon)$ -quasireduced representative word v . Then, all geodesic words w such that $w\pi = g$ are fully $(1, \varepsilon + 2K(1, \varepsilon, \delta) + 2)$ -quasireduced words.

Proof. Put $K = K(1, \varepsilon, \delta)$. Any geodesic w is clearly a $(1, \varepsilon + 2K + 2)$ -quasigeodesic. Now let $w = w_1 w_2$ and consider the cyclic permutation $w' = w_2 w_1$ of w . We have to prove that w' is a $(1, \varepsilon + 2K + 2)$ -quasigeodesic. Consider the bigon with sides $w = w_1 w_2$ (top side) and v (bottom side). Since v and w are at Hausdorff distance at most K , then there is a vertex on the bottom side at a distance at most $K + 1$ from the vertex reached after reading w_1 on the top side (the $+1$ comes from the possibility that the closest point of the bottom side to the vertex on the top side might not be a vertex itself) and so there is a geodesic word α of length at most $K + 1$ and words v_1, v_2 such that $v \equiv v_1 v_2$, $v_1 \pi = (w_1 \alpha)\pi$ and $v_2 \pi = (\alpha^{-1} w_2)\pi$.



We have that $(w_2w_1)\pi = (\alpha v_2v_1\alpha^{-1})\pi$ and so

$$\begin{aligned} d(1, (v_2v_1)\pi) &= d(1, (\alpha^{-1}w_2w_1\alpha)\pi) \\ &\leq 2|\alpha| + d(1, (w_2w_1)\pi) \\ &\leq d(w_2^{-1}\pi, w_1\pi) + 2(K+1). \end{aligned} \tag{5}$$

Hence, using (5) and the facts that $w \equiv w_1w_2$ is geodesic, $v \equiv v_1v_2$ is a $(1, \varepsilon)$ -quasigeodesic (and so $|v| \leq d(1, (v_1v_2)\pi) + \varepsilon$), and that v_2v_1 is a $(1, \varepsilon)$ -quasigeodesic (and so $|v_2v_1| \leq d(1, (v_2v_1)\pi) + \varepsilon$), we have that

$$\begin{aligned} (w_2^{-1}\pi|w_1\pi)_1 &= \frac{1}{2}(d(1, w_2^{-1}\pi) + d(1, w_1\pi) - d(w_2^{-1}\pi, w_1\pi)) \\ &= \frac{1}{2}(|w_2| + |w_1| - d(w_2^{-1}\pi, w_1\pi)) \\ &\leq \frac{1}{2}(|w| - d(1, (v_2v_1)\pi) + 2(K+1)) \\ &\leq \frac{1}{2}(|v| - d(1, (v_2v_1)\pi) + 2(K+1)) \\ &= \frac{1}{2}(|v_2v_1| - d(1, (v_2v_1)\pi) + 2(K+1)) \\ &\leq \frac{\varepsilon}{2} + (K+1) \end{aligned}$$

From Lemma 3.17, it follows that w_2w_1 is a $(1, \varepsilon + 2K(1, \varepsilon, \delta) + 2)$ -quasigeodesic. $\square$

For convenience, we will denote $K(1, 3\delta + 1, \delta)$ by R : this should cause no confusion, as the group, and so δ , will be fixed. Recall that, for a subset $K \subseteq G$, we denote the set of all conjugates of elements of K by $\alpha(K)$.

Proposition 3.19. Let G be a virtually free group and $K \in \text{Rat}(G)$. There is an effectively constructible rational language L_K such that $L_K\pi \subseteq \alpha(K)$ and, for every element $g \in K$, there is at least one fully $(1, 3\delta + 2R + 3)$ -quasireduced word in L_K representing a conjugate of g .

Proof. Since K is necessarily contained in some finitely generated subgroup of G , we may assume that G is finitely generated. By Corollary 3.13, we can construct a finite state automaton recognizing $\text{Geo}_B(K)$, where B is our standard generating set for G . Let δ be a hyperbolicity constant for G , $L_K = \text{Geo}_B(\text{Cyc}(\text{Geo}_B(K))\pi)$ and $S = \{\alpha_1, \dots, \alpha_n\}$ be the set of all words in $\tilde{B}^*$ of length at most δ . We claim that L_K has the desired properties.

The language $\text{Geo}_B(K)$ is rational in view of Corollary 3.13, and so $\text{Cyc}(\text{Geo}_B(K))$ is rational. Hence, $\text{Cyc}(\text{Geo}_B(K))\pi$ is a rational subset and $\text{Geo}_B(\text{Cyc}(\text{Geo}_B(K))\pi)$ is rational by Corollary 3.13, which also implies that the construction is effective. Also, $L_K\pi \subseteq \alpha(K)$, since, for every word $v \in L_K$, there is a word $u \in \text{Cyc}(\text{Geo}_B(K))$ such that $v\pi = u\pi$ and every word in $\text{Cyc}(\text{Geo}_B(K))$ represents a conjugate of an element in K .

Now, let $g \in K$ and $u \in \text{Geo}_B(K)$ be a geodesic such that $u\pi = g$. Then, by Proposition 3.16, there is some $i \in [n]$ such that $u \equiv u_1u_2u_3$, where $(u_3u_1)\pi = \alpha_i\pi$, and $u_2\alpha_i$ is fully $(1, 3\delta + 1)$ -quasireduced. But, $(u_2\alpha_i)\pi = (u_2u_3u_1)\pi$ and $u_2u_3u_1 \in \text{Cyc}(\text{Geo}_B(K))$. Now, any geodesic word representing $(u_2\alpha_i)\pi = (u_2u_3u_1)\pi$ belongs to $\text{Geo}_B(\text{Cyc}(\text{Geo}_B(K))\pi)$ and, by Lemma 3.18, it is a fully $(1, 3\delta + 2R + 3)$ -quasireduced word. $\square$

Theorem 3.20. Let G be a finitely generated virtually free group and $K \in \text{Rat}(G)$. There exists a context-free language L' such that $L'\pi \subseteq \alpha(K)$ and L' contains all the fully $(1, 3\delta + 2R + 3)$ -quasireduced words representing elements in $\alpha(K)$.

Proof. Let L_K be the language from Proposition 3.19,

$$S = \{g \in G \mid d_B(1, g) \leq 2\delta + 2K(1, 3\delta + 2R + 3, \delta)\}$$

(notice that S is finite), and $L = \text{Cyc}(L_K)$. Since $L_K\pi \subseteq \alpha(K)$, then $L\pi \subseteq \alpha(K)$.

By brute force, we build the set Q of all fully $(1, 3\delta + 2R + 3)$ -quasireduced words of length at most $11\delta + 2K(1, 3\delta + 2R + 3, \delta) + 2R + 4$ representing an element of $\alpha(K)$: it can be checked whether a word is a quasigeodesic, and so it can be checked whether a word is fully quasireduced or not and, in case it is, we check if it belongs to $\alpha(K)$ using the main result from [14].

Fix some $\beta \in S$. Since $L\pi \in \text{Rat}(G)$, then $L\pi \in \text{CF}(G)$ (see [10, Lemma 4.2]) and

$$S_\beta := \beta(L\pi)\beta^{-1} = L\pi\lambda_\beta \in \text{CF}(G),$$

which follows from Lemma 2.6 by taking $M = M' = G$, $\tau = \lambda_\beta^{-1}$ and $T = L\pi$ and the fact that context-free languages are closed under inverse morphism.

Put $L_\beta = S_\beta\pi^{-1}$. All words from L_β represent a conjugate (by β) of an element in $L\pi$, and so all words in L_β represent an element conjugate to an element in K , i.e., $L_\beta\pi \subseteq \alpha(K)$.

We claim that the language

$$L' = \bigcup_{\beta \in S} \text{Cyc}(L_\beta) \cup Q$$

has the desired properties. Clearly, it is context-free and $L'\pi \subseteq \alpha(K)$. We claim that it contains all the fully $(1, 3\delta + 2R + 3)$ -quasireduced words representing an element in $\alpha(K)$.

Let v be a fully $(1, 3\delta + 2R + 3)$ -quasireduced word representing an element in $\alpha(K)$. We know that there is at least one fully $(1, 3\delta + 2R + 3)$ -quasireduced word $u \in L_K$ such that $u\pi \sim v\pi$ by Proposition 3.19.

From Lemma 3.15, it follows that either $\max(|u|, |v|) \leq 11\delta + 2K(1, 3\delta + 2R + 3, \delta) + 2R + 4$ or there exist cyclic conjugates u' and v' of u and v and a word β with $(\beta u' \beta^{-1})\pi = v'\pi$ and $|\beta| \leq 2\delta + 2K(1, 3\delta + 2R + 3, \delta)$. In the first case, we have that $v \in Q$, and so, $v \in L'$. So, assume that $|v| > 11\delta + 2K(1, 3\delta + 2R + 3, \delta) + 2R + 4$ and that there exist some $\beta \in S$ and cyclic permutations u' and v' of u and v with $\beta(u'\pi)\beta^{-1} = v'\pi$. In this case $u' \in L$ and $\beta(u'\pi)\beta \in S_\beta$, thus $v' \in L_\beta$ and $v \in \text{Cyc}(L_\beta)$.

□

Theorem 3.21. Let G be a finitely generated virtually free group and $K \in \text{Rat}(G)$. Then $\text{Geo}(\alpha(K))$ is context-free.

Proof. We will show that $\text{Geo}_B(\alpha(K))$ is context-free. Let δ be the maximum between 1 and the hyperbolicity constant of G (so G is δ -hyperbolic and $\delta \geq 1$). It suffices to prove that there exists a context-free language L such that $L\pi \subseteq \alpha(K)$ and $\text{Geo}_B(\alpha(K)) \subseteq L$, since, in that case $\text{Geo}_B(\alpha(K)) = L \cap \text{Geo}_B(G)$ and context-free languages are closed under intersection with rational languages.

Let L' be the language given by Theorem 3.20. For every $\beta \in \tilde{A}^*$, the language $L' \cap \tilde{B}^*\beta$ is context-free and then, so is the language L''_β obtained by removing β from the end of every word in $L' \cap \tilde{B}^*\beta$. By the Muller-Schupp Theorem, $\{1\} \in \text{CF}(G)$, and so $\{\beta\pi\} \in \text{CF}(G)$, by Lemma 2.4. Hence, the language $\beta\pi\pi^{-1} \subseteq \tilde{B}^*$ is context-free and so is the language $\beta\pi\pi^{-1}\# \subseteq (\tilde{B} \cup \#)^*$. Moreover,

$$L_2 = \{u_1\#u_3 \mid u_3u_1 \in \beta\pi\pi^{-1}\} = \text{Cyc}(\beta\pi\pi^{-1}\#) \subseteq (\tilde{B} \cup \#)^*$$

is context-free. Since context-free languages are closed under substitution, the language

$$L_\beta = \{u_1u_2u_3 \mid u_2 \in L''_\beta, (u_3u_1)\pi = \beta\pi\}$$

obtained by replacing the symbol $\#$ by L''_β in L_2 is context-free. We claim that the language

$$L = \bigcup_{|\beta| \leq \delta} L_\beta$$

is context-free and that $L\pi \subseteq \alpha(K)$ and $\text{Geo}_B(\alpha(K)) \subseteq L$. It is obvious that L is context-free. Let $u_2 \in L''_\beta$ and u_1, u_3 be such that $(u_3u_1)\pi = \beta\pi$ for some β with $|\beta| \leq \delta$. Then $(u_1\pi)^{-1}(u_1u_2u_3)\pi(u_1\pi) = (u_2\beta)\pi$, and so $(u_1u_2u_3)\pi \sim (u_2\beta)\pi$. Since $u_2 \in L''_\beta$, then $u_2\beta \in L'$ and $L'\pi \subseteq \alpha(K)$. Thus, $(u_1u_2u_3)\pi \in \alpha(K)$. Since $u_1u_2u_3$ is an arbitrary element of L , we have that $L\pi \subseteq \alpha(K)$. It remains to show that $\text{Geo}_B(\alpha(K)) \subseteq L$. Let $w \in \text{Geo}_B(\alpha(K))$. Then, by Proposition 3.16, we have that $w \equiv u_1u_2u_3$, where $(u_3u_1)\pi = \beta\pi$ for some word β such that $|\beta| \leq \delta$ and $u_2\beta$ is fully $(1, 3\delta + 1)$ -quasireduced. It suffices to check that $u_2 \in L''_\beta$, i.e., that $u_2\beta \in L'$. This follows from Theorem 3.20, as every fully $(1, 3\delta + 1)$ -quasireduced word is also fully $(1, 3\delta + 2R + 3)$ -quasireduced and $(u_2\alpha)\pi = (u_2u_3u_1)\pi \sim w\pi \in \alpha(K)$. $\square$

As mentioned in the introduction, Dahmani and Guirardel prove in [6] that equations with rational constraints are solvable in virtually free groups, and so, the doubly generalized conjugacy problem with rational constraints is decidable for virtually free groups. Using the previous theorem, we provide a language-theoretic proof of the problem without constraints.

Corollary 3.22. Let G be a virtually free group. Then the doubly generalized conjugacy problem in G is decidable.

Proof. It amounts to deciding, on input $S, T \in \text{Rat}(G)$, whether $\text{Geo}_B(\alpha(S)) \cap \text{Geo}_B(T) = \emptyset$, which can be done since $\text{Geo}_B(\alpha(S))$ is context-free by Theorem 3.21 and $\text{Geo}_B(T)$ is rational by Corollary 3.13. $\square$

Currently, we are not aware of the existence of a language-theoretic proof for the constrained version of the problem.

Question 3.23. Is there a language-theoretic proof of the doubly generalized conjugacy problem with rational constraints for finitely generated virtually free groups?

Remark 3.24. We remark that, in general, hyperbolic groups have undecidable (subgroup) membership problem, and so undecidable GCP and DGCP. Most of the tools in our proof work for hyperbolic groups. In fact, the only obstruction is Corollary 3.13, which can be easily seen not to hold in hyperbolic groups without the Howson property.

This last result raises two natural questions involving a finite index subgroup H of a group G :

- if H has decidable DGCP, does G has decidable DGCP?
- if G has decidable DGCP, does H has decidable DGCP?

Since both implications fail for the CP, we conjecture that the same happens for the DGCP. However, we are so far unable to produce counterexamples (the counterexamples we know for the CP are not useful for this purpose).

But we can get something in particular cases. Recall that a *retract* of G is a subgroup H such that there exists a homomorphism $\varphi : G \rightarrow H$ fixing the elements of H . The second question has an affirmative answer if H is a retract of G (of finite or infinite index):

Proposition 3.25. Let H be a retract of a group G . If G has decidable DGCP, then H also has decidable DGCP.

Proof. Let $\varphi : G \rightarrow H$ be a homomorphism fixing the elements of H and let $K, L \in \text{Rat } H \subseteq \text{Rat } G$. It suffices to show that

$$\exists x \in K \exists y \in L \exists h \in H : y = hxh^{-1} \Leftrightarrow \exists x \in K \exists y \in L \exists g \in G : y = gxg^{-1}.$$

The direct implication holds trivially and the converse follows from

$$y = gxg^{-1} \Rightarrow y\varphi = (gxg^{-1})\varphi \Rightarrow y = (g\varphi)x(g\varphi)^{-1}.$$

□

We consider now a strengthening of the DGCP, which we call the *doubly generalized twisted conjugacy problem* (DGTCP) for a group G : given $K, L \in \text{Rat } G$ and $\varphi \in \text{Aut } G$, we must decide whether there are some $x \in K$, $y \in L$ and $g \in G$ such that $y = g^{-1}x(g\varphi)$.

Proposition 3.26. Let H be a finite index normal subgroup of a group G . If H has decidable DGTCP, then G has decidable DGCP.

Proof. Since $[G : H] < \infty$, there exist $b_0, \dots, b_m \in G$ such that $G = Hb_0 \dot{\cup} \dots \dot{\cup} Hb_m$ and $b_0 = 1$. Since $H \trianglelefteq G$, then $\varphi_i : H \rightarrow H$ defined by $h\varphi_i = b_ihb_i^{-1}$ is an automorphism of H for $i = 0, \dots, m$.

Let $K, L \in \text{Rat } G$. By [17, Proposition 4.1], there exist $K_0, \dots, K_m, L_0, \dots, L_m \in \text{Rat } H$ such that $K = K_0b_0 \dot{\cup} \dots \dot{\cup} K_mb_m$ and $L = L_0b_0 \dot{\cup} \dots \dot{\cup} L_mb_m$. Since $G = Hb_0 \dot{\cup} \dots \dot{\cup} Hb_m$, it suffices to show that, for all $i, j, k \in \{0, \dots, m\}$, we can decide whether there exists some $(x, y, z) \in L_i \times K_j \times H$ such that $(zb_k)^{-1}(xb_i)(zb_k) = yb_j$. Now

$$\begin{aligned} (zb_k)^{-1}(xb_i)(zb_k) = yb_j &\Leftrightarrow b_k^{-1}z^{-1}xb_izb_k = yb_j &\Leftrightarrow z^{-1}xb_iz = b_kyb_jb_k^{-1} \\ & &\Leftrightarrow z^{-1}x(z\varphi_i) = (y\varphi_k)b_kb_jb_k^{-1}b_i^{-1}, \end{aligned}$$

hence $b_kb_jb_k^{-1}b_i^{-1} \in H$ is an obvious necessary condition. Assuming that this holds, then since rational subsets are closed under homomorphism, we get that $K'_j = \{(y\varphi_k)b_kb_jb_k^{-1}b_i^{-1} : y \in K_j\} \in \text{Rat } H$. Since H has decidable DGTCP, then we can decide whether or not there are some $x \in L_i$, $y \in K'_j$ and $z \in H$ such that $y = z^{-1}x(z\varphi)$. Therefore G has decidable DGCP. □

A group is *virtually abelian* if it has an abelian subgroup of finite index. We can now prove the following result:

Theorem 3.27. Every finitely generated virtually abelian group has decidable DGCP.

Proof. A finite index subgroup of a finitely generated group is itself finitely generated. Hence, by Proposition 3.26, it is enough to show that every finitely generated abelian group has decidable DGTCP.

Let G be an abelian group generated by the finite set A , let $K, L \in \text{Rat } G$ and $\varphi \in \text{Aut } G$. Let $M = \{u^{-1}(u\varphi) : u \in G\}$. Since G is abelian, we have

$$(uv)^{-1}(uv)\varphi = v^{-1}u^{-1}(u\varphi)(v\varphi) = (v^{-1}(v\varphi))(u^{-1}(u\varphi))$$

for all $u, v \in G$, hence $M = \langle a^{-1}(a\varphi) : a \in A \rangle \in \text{Rat } G$. Since $y = g^{-1}x(g\varphi)$ for some $g \in G$ if and only if $y = xg^{-1}(g\varphi)$ for some $g \in G$ if and only if $x^{-1}y \in M$, then deciding whether or not there exist some $x \in K$, $y \in L$ and $g \in G$ such that $y = g^{-1}x(g\varphi)$ is equivalent to deciding whether or not $K^{-1}L \cap M \neq \emptyset$, which is equivalent to $1 \in K^{-1}LM^{-1}$. Since $K, L, M \in \text{Rat } G$, also K^{-1} , M^{-1} and $K^{-1}LM^{-1}$ are rational, so the result follows from finitely generated abelian groups having decidable membership problem for rational subsets [9]. □

Acknowledgements

The authors are grateful to the anonymous referee for several comments and corrections that improved the readability and the overall quality of the paper. Both authors were partially supported by CMUP, member of LASI, which is financed by national funds through FCT – Fundação para a Ciência e a Tecnologia, I.P., under the projects with reference UID/00144/2025 and associated DOI given by <https://doi.org/10.54499/UID/00144/2025>.

References

- [1] L. Bartholdi and P. V. Silva. Rational subsets of groups. In J.-E. Pin, editor, *Handbook of Automata Theory*, chapter 23. EMS Press, Berlin, 2021.
- [2] J. Berstel. *Transductions and Context-free Languages*. Teubner, Stuttgart, 1979.
- [3] J. W. Cannon. The combinatorial structure of cocompact discrete hyperbolic groups. *Geom. Dedicata*, 16(2):123–148, 1984.
- [4] A. Carvalho. On uniformly continuous endomorphisms of hyperbolic groups. *J. Algebra*, 602:197–223, 2022.
- [5] A. Carvalho. Algebraic and context-free subsets of subgroups. *Theor. Comput. Sci.*, 980:114229, 2023.
- [6] F. Dahmani and V. Guirardel. Foliations for solving equations in groups: free, virtually free, and hyperbolic groups. *J. Topol.*, 3(2):343–404, 2010.
- [7] M. Dehn. Über unendliche diskontinuierliche gruppen. *Math. Ann.*, 71(1):116–144, 1911.
- [8] V. Diekert, C. Gutiérrez, and C. Hagenah. The existential theory of equations with rational constraints in free groups is PSPACE-complete. *Inform. and Comput.*, 202:105–140, 2005.
- [9] Z. Grunschlag. *Algorithms in geometric group theory*. PhD thesis, University of California at Berkeley, 1999.
- [10] T. Herbst. On a subclass of context-free groups. *RAIRO Inform. Théor. Appl.*, 25:255–272, 1991.
- [11] D. Holt and S. Rees. Regularity of quasigeodesics in a hyperbolic group. *Internat. J. Algebra Comput.*, 12:747–754, 2002.
- [12] D. Holt, S. Rees, and C. Röver. Groups with context-free conjugacy problems. *Internat. J. Algebra Comput.*, 21(1-2):193–216, 2011.
- [13] J. E. Hopcroft and J. D. Ullman. *Introduction to automata theory, languages, and computation*. Addison-Wesley Series in Computer Science. Addison-Wesley Publishing Co., Reading, MA, 1979.
- [14] M. Ladra and P. V. Silva. The generalized conjugacy problem for virtually free groups. *Forum Math.*, 23:447–482, 2011.
- [15] A. Levine. Subsets of groups with context-free preimages. *arXiv: 2312.0419v2, preprint*, 2023.
- [16] M. Lohrey. The rational subset membership problem for groups: A survey. In C. M. Campbell, M. R. Quick, E. F. Robertson, and C. M. Roney-Dougal, editors, *Groups St Andrews 2013*, London Mathematical Society Lecture Note Series, pages 368–389. Cambridge University Press, Cambridge, 2015.
- [17] P. V. Silva. Recognizable subsets of a group: finite extensions and the abelian case. *Bull. Eur. Assoc. Theor. Comput. Sci. EATCS*, 77:195–215, 2002.