THE CONJUGACY PROBLEM FOR FREE-BY-CYCLIC GROUPS.

A. MARTINO AND E. VENTURA

ABSTRACT. We show that the conjugacy problem is solvable in [finitely generated free]-by-cyclic groups, by using a result of O. Maslakova that one can algorithmically find generating sets for the fixed subgroups of free group automorphisms, and one of P. Brinkmann that one can determine whether two cyclic words in a free group are mapped to each other by some power of a given automorphism. The algorithm effectively computes a conjugating element, if it exists. We also solve the power conjugacy problem and give an algorithm to recognize if two given elements of a finitely generated free group are Reidemeister equivalent with respect to a given automorphism.

1. INTRODUCTION

A *free-by-cyclic* group is a group G having a free normal subgroup F with cyclic quotient $C = G/F$. If F can be chosen to be finitely generated then G is a *[f.g. free]-by-cyclic* group. (Note that the parenthesis are relevant here since surface groups are both free-by-cyclic and finitely generated, but are not [f.g. free]-by-cyclic.)

We shall be concerned with [f.g. free]-by-cyclic groups. Let $x_1, \ldots, x_n$ be a basis for F and let t be a pre-image in G of a generator of C. Right conjugation by t in G induces an automorphism of F, which we denote ϕ. The following is then a presentation of G

$$G = \langle x_1, \ldots, x_n, t \; : \; t^{-1} x_i t = x_i \phi, \; t^m = h \rangle,$$

where m is the cardinal of C and h is some element in F, understanding that the relation $t^m = h$ is not present when $m = \infty$. Our main result is the following

Theorem 1.1. *The conjugacy problem in [f.g. free]-by-cyclic groups is solvable.*

For some special cases, this result is already known. The automorphism ϕ is said to have no periodic conjugacy classes if one cannot find an integer k and elements $g, h \in F$ such that $g \phi^k = h^{-1} g h$. This is equivalent to saying

that G has no $\mathbb{Z}\oplus\mathbb{Z}$ subgroups and hence, by [5] and [2], that G is hyperbolic. Also, if C is finite, the group G is virtually free and hence hyperbolic. In all these cases, then, it is well known that G has solvable conjugacy problem. But, clearly, not all free-by-cyclic groups are hyperbolic. It has even been announced, [4], that they fail to be automatic, in general.

Some other partial results are already known in this direction. For example, in the preprint [1] the authors consider the case where some power of ϕ is inner, and give an algorithm to decide if two given elements in G of the form tu, tv for $u, v \in F$ are conjugate by some element in F.

Our proof of Theorem 1.1 will work, in general, for arbitrary [f.g. free]-by-cyclic groups, including the known particular cases. The algorithm provided also computes a conjugating element, when it exists. Our proof relies on the following recent theorems.

Theorem 1.2 (Maslakova, [11]). *There exists an algorithm to compute a generating set for the fixed point subgroup of an arbitrary automorphism of a free group of finite rank.*

Theorem 1.3 (Brinkmann, [6]). *Given a finitely generated free group F, two elements u, v of F and an automorphism ϕ of F it is decidable whether there exists an integer k such that $u\phi^k$ is conjugate to v. Moreover, if such a k exists, it can be computed.*

Our solution to the conjugacy problem for G proceeds by showing that, in the light of Theorem 1.3, it can be reduced to the *twisted conjugacy problem* for F. Then, we solve this classical problem providing an algorithm to recognize Reidemeister classes with respect to automorphisms of finitely generated free groups.

Let F be a free group and ϕ an automorphism of F. Two elements $u, v \in F$ are said to be ϕ-*twisted conjugate*, denoted $u \sim_\phi v$, if there exists $g \in F$ such that $(g\phi)^{-1}ug = v$. The equivalence relation $\sim_\phi$ was first introduced by Reidemeister, and has an important role in the research works dedicated to bound the rank of the fixed subgroup of an automorphism of F. See for example [8], where Problem 3 (i) in the Open Problem section asks for an algorithm recognizing ϕ-twisted conjugacy classes.

It is said that the ϕ-*twisted conjugacy problem* is solvable in F if, for any elements, $u, v \in F$, we can algorithmically decide if $u \sim_\phi v$ (for example, the id-twisted conjugacy problem is the standard conjugacy problem in F). And it is said that the *twisted conjugacy problem* is solvable in F if the ϕ-twisted conjugacy problem is solvable for any $\phi \in Aut(F)$.

We first prove the following

Proposition 1.4. *Let F be a finitely generated free group. If the twisted conjugacy problem is solvable in F then the standard conjugacy problem is solvable in G.*

Then, we give a solution for the twisted conjugacy problem in a finitely generated free group F, thus extending the result in [1], where it is done for virtually inner automorphisms, and answering question 3(i) of [8] in the affirmative.

Theorem 1.5. *Let F be a finitely generated free group. The twisted conjugacy problem is solvable in F.*

Now, Theorem 1.1 follows immediately from Proposition 1.4 and Theorem 1.5.

Finally, in the last section we develop few technical lemmas that will allow us to extend Theorem 1.1 (essentially with the same proof) to the following result.

Theorem 1.6. *The power conjugacy problem in [f.g. free]-by-cyclic groups is solvable.*

In an arbitrary group, two elements u and v are said to be *power conjugated* when there exist integers p, q such that u^p and v^q are non-trivial and conjugated to each other in the group. The *power conjugacy problem* in a group consists on deciding if two given elements in the group are power conjugated (and find such exponents and conjugating element if they exist).

It was pointed out to us by Ilya Kapovich that many one-relator groups are [f.g. free]-by-cyclic (one can prove this by imposing few assumptions on the relator). It seems that there is evidence to think that these assumptions are quite weak, meaning that most relators satisfy them and, hence, most of 1-relator groups fall in the family of groups considered in this paper. However, this has not been expressed yet in a precise form at this time.

2. The conjugacy problem

First note that, using the relations $wt = t(w\phi)$ and $wt^{-1} = t^{-1}(w\phi^{-1})$ for $w \in F$, every element in G can be algorithmically re-written as a word of the form $t^r u$, where r is an integer and $u \in F$. In the case where C is finite and we also have the relation $t^m = h$, we may further assume that $0 \le r \le m - 1$. In either case, we get a unique representation for elements of G, which is algorithmically computable from a given arbitrary word on the generators.

If we conjugate $t^r u$ by an arbitrary element $t^k g$, we obtain

$$(t^k g)^{-1}(t^r u)(t^k g) = t^r (g\phi^r)^{-1} t^{-k} u t^k g = t^r (g\phi^r)^{-1}(u\phi^k)g.$$

Hence, two elements in G, say $t^r u$ and $t^s v$ (with $0 \le r, s \le m - 1$ in the case where $|C| = m < \infty$), are conjugate in G if and only if $r = s$ and $v \sim_{\phi^r} (u\phi^k)$ for some integer k. This is the key fact in the following discussion.

Proof of Prop. 1.4. Suppose two elements in G are given, say $t^r u$ and $t^s v$. We have to decide if they are conjugate to each other in G.

We first deal with the case where $r = 0$. Note that u is only conjugate in G to other elements v of the base group F. Moreover, u is conjugate to v in G if and only if, some power of the automorphism ϕ, maps u to a conjugate of v. This is decidable by Theorem 1.3, so we can decide if $u, v \in F$ are conjugate in G.

For the case $r \ne 0$, note that $u\phi^k \sim_{\phi^r} u\phi^{k \pm r}$. Hence, $t^r u$ and $t^s v$ are one conjugate to the other in G if, and only if, $r = s$ and $v \sim_{\phi^r} (u\phi^k)$ for some integer $0 \le k \le |r| - 1$. Thus, a solution for the twisted conjugacy problem in F provides a solution for the standard conjugacy problem in G. $\square$

Proof of Th. 1.5. Let ϕ be an automorphism of F, and suppose $u, v \in F$ are given. We need to algorithmically decide whether $u \sim_{\phi} v$.

Choose a free basis for F and, adding a new letter z, we get a free basis for $F' = F * \langle z \rangle$. Let $\phi' \in Aut(F')$ be the extension of ϕ defined by $z\phi' = uzu^{-1}$. Let γ_g denote the inner automorphism of F' given by right conjugation by $g \in F'$, $x\gamma_g = g^{-1}xg$.

We claim that $u \sim_{\phi} v$ if, and only if, $Fix\,(\phi'\gamma_v)$ contains an element of the form $g^{-1}zg$ for some $g \in F$ (and, in this case, g itself is a valid twisted conjugating element).

In fact, suppose that $v = (g\phi)^{-1}ug$ for some $g \in F$. A simple calculation shows that $g^{-1}zg$ is then fixed by $\phi'\gamma_v$. Conversely, if $g^{-1}zg$ is fixed by $\phi'\gamma_v$ for some $g \in F$, then $gv^{-1}(g\phi)^{-1}u$ commutes with z. And this implies $gv^{-1}(g\phi)^{-1}u = 1$, since this word contains no occurrences of z. Hence, $v = (g\phi)^{-1}ug$ and $u \sim_{\phi} v$ (with g being a twisted conjugating element).

Since, by Theorem 1.2, we can algorithmically find a generating set for $Fix\,(\phi'\gamma_v)$, we can also decide if this subgroup contains an element of the form $g^{-1}zg$ for some $g \in F$. One can, for example, look at the corresponding (finite) core-graph for $Fix\,(\phi'\gamma_v)$ (algorithmically computable from a set of generators) and see if there is some loop labelled z at some vertex connected to the base-point by a path not using the letter z. And, if this is the case, the label of such a path provides the g, i.e. the required twisted conjugating element.

(It is not difficult to show that $Fix\,(\phi'\gamma_v)$ contains an element of the form $g^{-1}zg$ if, and only if, it contains some word involving the letter z; and, in this case, the longest initial F-segment in such a word provides the twisted

conjugating element. With this observation, one can slightly simplify the algorithm given, by just looking if some of the generators of $Fix\,(\phi'\gamma_v)$ does involve z.) □

3. THE POWER CONJUGACY PROBLEM

With the help of a few technical lemmas, the argument given to solve the conjugacy problem in G also works, in much the same way, to solve the power conjugacy problem.

Theorem 1.2 can be extended to consider periodic subgroups. Recall that, given an automorphism ϕ of F, the *periodic subgroup* of ϕ is the subgroup $Per\,\phi = \{w \in F : w\phi^k = w \text{ for some } k\}$.

Proposition 3.1. *There exists an algorithm to compute a generating set for the periodic subgroup of any given automorphism, ϕ, of a finitely generated free group F. More precisely, there exists a computable integer p_0 (independent of ϕ) such that $Per\,\phi = Fix\,\phi^{p_0}$.*

Proof. It is a folk result that, for a finitely generated free group F or rank $n \geq 0$, the group $Aut(F)$ has bounded torsion. Here is a possible proof. Clearly, if $n = 0$ or $n = 1$, the bound can be taken to be 1 and 2, respectively. For $n \geq 2$, we can invoke the result of [7], which says that every finite order element of $Out(F)$ can be realised as a graph automorphism of a finite graph with no degree 1 and degree 2 vertices. It is easy to see that such a graph has at most $3n - 3$ edges, which total to a maximum of $6n - 6$ oriented edges. Hence, every finite order element of $Out(F)$ has order dividing $(6n - 6)!$. The same is true for $Aut(F)$, since the natural map $Aut(F) \to Out(F)$ has torsion free kernel.

The result we have to prove is clear when F is cyclic. So, we can assume $n = r(F) \geq 2$.

By Corollary 2.8 of [10], there exists m such that $Per\,\phi = Fix\,\phi^m$. In particular, $Per\,\phi$ has rank $r \leq n$ (see [3]), and ϕ restricts to a finite order automorphism $\phi' \in Aut(Per\,\phi)$. So, the order of ϕ' either divides 2 (if $r = 0, 1$) or $(6r - 6)!$ (otherwise). In any case, it divides $p_0 = (6n - 6)!$. This means that every ϕ-periodic element in F has period dividing p_0. So, $Per\,\phi = Fix\,\phi^{p_0}$. Finally, using Theorem 1.2, we are done. □

Let ϕ be an automorphism of a finitely generated free group F.

For any $p \geq 1$, and any $w \in F$, we define $w_{\phi,\,p} = (w\phi^{p-1})(w\phi^{p-2})\cdots(w\phi)w$. This notation will be useful because, for every integer r and every $u \in F$, $(t^r u)^p = t^{rp}u_{\phi^r,\,p}$. Note that $w_{\mathrm{id},\,p} = w^p$. Note also that, for every other automorphism ψ commuting with ϕ, we have $w_{\phi,\,p}\psi = (w\psi)_{\phi,\,p}$.

Lemma 3.2. *Let $u, v \in F$. If $u \sim_\phi v$ then $u_{\phi,\,p} \sim_{\phi^p} v_{\phi,\,p}$ for every $p \geq 1$.*

Proof. Assume the existence of an element $g \in F$ satisfying $(g\phi)^{-1}ug = v$. Then, applying ϕ^i on both sides, we obtain $(g\phi^{i+1})^{-1}(u\phi^i)(g\phi^i) = v\phi^i$. Now, multiplying all these equations,

$$(g\phi^p)^{-1}u_{\phi, p}g = \Pi_{i=p-1}^0(g\phi^{i+1})^{-1}(u\phi^i)(g\phi^i) = \Pi_{i=p-1}^0 v\phi^i = v_{\phi, p}.$$

This proves that $u_{\phi, p} \sim_{\phi^p} v_{\phi, p}$ (with, in fact, the same twisted-conjugating element g). $\square$

Adapting the proof of Theorem 1.5, we can obtain the following technical result.

Lemma 3.3. *Given $u, v \in F$, one can algorithmically decide if $u_{\phi, p} \sim_{\phi^p} v_{\phi, p}$ for some $p \geq 1$.*

Proof. As before, add a new generator z to F and consider the extension $\phi' \in Aut(F * \langle z \rangle)$ of ϕ given by $z\phi' = uzu^{-1}$. Exactly the same arguments as above show now that, for $p \geq 1$ and $g \in F$, $v_{\phi, p} = (g\phi^p)^{-1}u_{\phi, p}g$ if and only if $g^{-1}zg \in Fix\, (\phi'\gamma_v)^p$ (to do this computation, note that $(\phi'\gamma_v)^p = \phi'^p\gamma_{v_{\phi, p}}$ and $z\phi'^p = u_{\phi, p}zu_{\phi, p}^{-1}$). So, we are done by invoking Proposition 3.1 (and the computability of p_0 there ensures that we can compute the value of p here). $\square$

Now, we can adapt the proof of Proposition 1.4 to solve the power conjugacy problem in G.

Proof of Th. 1.6.

Suppose we are given two elements, $t^r u$ and $t^s v$, from G, $r, s \in \mathbb{Z}$, $u, v \in F$. We need to decide whether they are power conjugated in G.

As before, we deal first with the case $r = s = 0$. Here, given $u, v \in F$ we have to decide whether for some integers p, q, u^p is mapped to a conjugate of v^q by some power of ϕ. In a free group we can algorithmically find *roots* of elements, which are unique. That is, there is a unique element u' of F such that u is a power of u', and u' is not itself a proper power. Similarly, there exists a root, v' for v. Since roots are unique, u^p is mapped to a conjugate of v^q by some power of ϕ if, and only if, u' is mapped to a conjugate of v' by some power of ϕ. Thus, we are done by invoking Theorem 1.3.

Now, if m is finite, then any element of G raised to the power m lies in F. Moreover, $t^r u$ has infinite order if and only if, $(t^r u)^m \neq 1$. Thus, if $t^r u$ and $t^s v$ are to be power conjugate, then either $(t^r u)^m = 1 = (t^s v)^m$ or $1 \neq (t^r u)^m, (t^s v)^m \in F$. In the former case we can solve the power conjugacy problem by finitely many checks of the standard conjugacy problem for G. In the latter case, we are done by the argument in the preceding paragraph, applied to the pair $(t^r u)^m, (t^s v)^m$.

So, we can restrict our attention to the case $m = \infty$. In this case G is torsion-free and so, two elements $t^r u$ and $t^s v$ are power conjugated in G

if and only if there exist non-zero exponents p and q such that $(t^r u)^p$ and $(t^s v)^q$ are conjugated to each other in G.

By applying the future algorithm twice (once for the pair of elements $t^r u$, $t^s v$, and again for $t^r u$, $(t^s v)^{-1}$) we may, without loss of generality, restrict our attention to positive exponents, p, q. Note that, if for some integers $p, q \geq 1$, $(t^r u)^p = t^{rp} u_{\phi^r, p}$ and $(t^s v)^q = t^{sq} v_{\phi^s, q}$ are conjugated to each other in G, then $rp = sq$. In particular, $r = 0$ if and only if $s = 0$. And if both r and s are not zero then $t^r u$ and $t^s v$ are power conjugated in G if and only if $(t^r u)^s$ and $(t^s v)^r$ also are. Thus, our problem reduces to the case $r = s$ (and hence, $p = q$).

So, given elements of the form $t^r u$ and $t^r v$, we have to decide if there exists an integer $p \geq 1$ such that $(t^r u)^p$ and $(t^r v)^p$ are conjugate to each other in G, i.e. such that $v_{\phi^r, p} \sim_{\phi^{rp}} (u_{\phi^r, p} \phi^k)$ for some integer k.

Since we have dealt with the case $r = s = 0$ above, it remains to consider the situation where $r \neq 0$. Here, we claim that $(u_{\phi^r, p} \phi^k) \sim_{\phi^{rp}} (u_{\phi^r, p} \phi^{k \pm r})$ for every $p \geq 1$. In fact, $u \sim_{\phi^r} (u \phi^{\pm r})$ so, by Lemma 3.2, $u_{\phi^r, p} \sim_{\phi^{rp}} (u \phi^{\pm r})_{\phi^r, p} = (u_{\phi^r, p} \phi^{\pm r})$. Then, $(u_{\phi^r, p} \phi^k) \sim_{\phi^{rp}} (u_{\phi^r, p} \phi^{k \pm r})$, for every $k, p \in \mathbb{Z}$, $p \geq 1$. Thus it only remains to decide whether there exists an integer $p \geq 1$ such that $v_{\phi^r, p} \sim_{\phi^{rp}} (u_{\phi^r, p} \phi^k)$ for some integer $0 \leq k \leq |r| - 1$. But $(u_{\phi^r, p} \phi^k) = (u \phi^k)_{\phi^r, p}$ so, using Lemma 3.3 at most r times, we are done. $\square$

References

[1] V. Bardakov, L. Bokut and A. Vesnin, *Twisted conjugacy in free groups and Makanin's question*, preprint, http://arxiv.org/abs/math.GR/0401349.

[2] M. Bestvina and M. Feighn, *A combination theorem for negatively curved groups*, J. Differential Geom. **35** (1992), no. 1, 85–101.

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

[4] M.R. Bridson and L. Reeves, *On the absence of automaticity of certain free-by-cyclic groups.*, In preparation.

[5] P. Brinkmann, *Hyperbolic automorphisms of free groups*, Geom. Funct. Anal. **10** (2000), no. 5, 1071–1089.

[6] P. Brinkmann, *Dynamics of free group automorphisms*, preprint.

[7] M. Culler, in *Contributions to group theory*, 197–207, Contemp. Math., 33, Amer. Math. Soc., Providence, RI, 1984.

[8] W. Dicks, E. Ventura, The group fixed by a family of injective endomorphism of a free group, *Contemp. Math.*, **195** (1996), 1-81.

[9] J.L. Dyer, G.P. Scott, Periodic automorphisms of free groups, *Comm. Alg.*, **3** (1975), 195-201.

[10] A. Martino, E. Ventura, On automorphism-fixed subgroups of a free group, *J. Alg.*, **230** (2000), 596-607.

[11] O. S. Maslakova, *The fixed point group of a free group automorphism*, Algebra Logika **42** (2003), no. 4, 422–472, 510–511.

A. Martino
Centre de Recerca Matemàtica
E-mail: AMartino@crm.es

E. Ventura
Dept. Mat. Apl. III, Univ. Pol. Catalunya, Barcelona (Spain) and
Dept. of Math., University of Nebraska-Lincoln
E-mail: enric.ventura@upc.es