

Review Article

Enric Ventura

Group-theoretic orbit decidability

Abstract: A recent collection of papers in the last years have given a renovated interest to the notion of *orbit decidability*. This is a new quite general algorithmic notion, connecting with several classical results, and closely related to the study of the conjugacy problem for extensions of groups. In the present survey we explain several of the classical results closely related to this concept, and we explain the main ideas behind the recent connection with the conjugacy problem made by Bogopolski–Martino–Ventura in [2]. All the consequences up to date, published in several other papers by other authors, are also commented and reviewed.

Keywords: Orbit decidability, conjugacy problem

MSC 2010: 20F10, 20F28

Enric Ventura: Departament de Matemàtica Aplicada III, Escola Politècnica Superior d'Enginyeria de Manresa, Universitat Politècnica de Catalunya, Av. Bases de Manresa 61-73 08242-Manresa, Barcelona (Catalonia), Spain, e-mail: enric.ventura@upc.edu

1 Introduction

In many areas of mathematics and in innumerable topics and situations, the notion of *transformation* plays an important role. If X is the set of objects we are interested in, a transformation of X is usually understood to be just a map $\alpha: X \rightarrow X$. (We will use the right notation for maps, $x \mapsto x\alpha$; so, $\alpha\beta$ means the composition of first α and then β , $x \mapsto x\alpha \mapsto x\alpha\beta$.)

The classical dynamical point of view consists on fixing such a map and then looking at their iterates $\alpha^n: X \rightarrow X$; here we have the notion of α -*orbit* of an element $x \in X$ as the collection of all its images under iterates of α , i.e., $\{x\alpha^n \mid n \in \mathbb{Z}\}$ (or just taking non-negative iterates, $n \in \mathbb{N}$, if α is not invertible). The study of orbits of interesting dynamical systems (i.e., interesting sets X and interesting maps α coming from many different parts of mathematics like geometry, topology, analysis, differential equations, statistics, discrete mathematics, etc.) constitutes today a whole branch of mathematics, with innumerable research papers published in this direction.

For a general set X , the collection $\text{Map}(X, X)$ of all self-maps is a wild object. However, there are many situations where, instead of looking at a particular map α , one is interested in considering a certain subset of “well-behaved” maps, $A \subseteq \text{Map}(X, X)$. For example, geometers and topologists use to take as X a geometric object, e.g., a topological space, an abstract metric space, a surface, a manifold, etc. and then look at the collection A of continuous self-maps, or homeomorphisms, or (quasi-)isometries, or geometrically meaningful homeomorphisms (pseudo-Anosov maps in the case of surfaces, or many other specific definitions for higher-dimensional manifolds). Combinatorialists use to take interesting discrete sets X and study their set of permutations $A = \text{Sym}(X)$. Algebraists tend to take X to be an algebraic structure (a monoid, group, a ring, a module, an algebra, etc.) and then look at the set of all endomorphisms $A = \text{End}(X)$, or automorphisms $A = \text{Aut}(X)$ of X , or many different subsets of these sets which could be meaningful in more specific situations.

Whenever a set X and a subset $A \subseteq \text{Map}(X, X)$ are fixed, we can define the A -*orbit* of an element $x \in X$ in the natural way: the collection of images of x under all maps in A ,

$$xA = \{x\alpha \mid \alpha \in A\} \subseteq X.$$

In this sense, the α -orbit defined above is just the A -orbit for $A = \{\alpha^n \mid n \in \mathbb{Z}\}$ (or $A = \{\alpha^n \mid n \in \mathbb{N}\}$ if α is not invertible).

About orbits one may ask many questions adapted to the special situation of interest (geometry, topology, combinatorics, algebra, etc.). But focussing on algorithmic issues, there is a natural decision problem which can be stated in full generality: “given X and $A \subseteq \text{Map}(X, X)$, decide algorithmically whether two elements $x, y \in X$ can be mapped to each other by some α in A ”. That is, on input $x, y \in X$ (with all the necessary precisions made on how elements from X are given to us), decide whether there exists a map $\alpha \in A$ such that $x\alpha = y$. The corresponding search problem would be to find such an $\alpha \in A$, assuming it exists.

Of course, with this big generality, the above problem is unsolvable; namely, there are sets X and A for which there exists no algorithm doing the above task (see the next section for specific examples). This allows us to distinguish between the (algorithmically) positive and negative situations, and give rise to the following natural concept:

Definition 1.1. Let X be a set, and let $A \subseteq \text{Map}(X, X)$ be a set of transformations (with all the necessary precisions made on how elements of X are given). We say that A is *orbit decidable* (OD for short) if there is an algorithm which, given $x, y \in X$, decides whether $x\alpha = y$ for some $\alpha \in A$. The *search* version of the problem asks the algorithm to provide such an α , in case it exists.

Although sometimes it is not stated in these terms, this notion of orbit decidability is present in many situations, and is usually central when studying algorithmic aspects of many of the interesting problems one can formulate about the objects in X and how do they relate to each other under the transformations in A .

Note that the concept of orbit decidability is stated in full generality and so, the reader can particularize and study it in any area of mathematics he/she is interested in.

We point out that there are classical situations, and very classical algorithms in a big variety of contexts, which apparently are not related to orbit decidability, but can be translated or expressed in a way that become direct particular cases. For example, consider the problem of deciding whether a given element $m \in M$ of a free (left or right) R -module M over a ring R is primitive (i.e., part of an R -basis) or not. This is apparently unrelated with orbit decidability but, fixing an R -basis $\{m_1, m_2, \dots\}$ of M , it is clear that m is primitive if and only if m_1 can be mapped to m by some R -automorphism of M . Hence, deciding primitiveness in M is a particular case of orbit decidability for $A = \text{Aut}_R(M)$. The classical problem of extending m to an R -basis of M , if possible, is just the search part of the above orbit decidability problem (once such an α is found, then $\{m = m_1\alpha, m_2\alpha, \dots\}$ is the desired R -basis for M).

In the present survey, we will focus on the algebraic setting and, more specifically, on groups. This is the meaning and the reason for the title of the paper, *Group-theoretic orbit decidability*.

2 Classical results for groups

Let us concentrate ourselves in Group Theory. In this area of mathematics one can find lots of examples of classical algorithmic problems which can be expressed as particular cases of orbit decidability.

For example, out of the three very classical Dehn problems, the first two are clearly of this kind. Let

$$G = \langle a_1, \dots, a_n \mid r_1, \dots, r_m \rangle$$

be a finitely presented group, and let us consider elements of G given to us (i.e., represented) as reduced words on the generators a_i . We represent equality in G by $=$ and conjugacy by \sim ($a \sim b$ if and only if there exists an element $g \in G$ such that $a^g := g^{-1}ag = b$). Clearly, the conjugacy problem for G is just the orbit decidability for the set of inner automorphisms,

$$A = \text{Inn}(G) = \{\gamma_g : G \rightarrow G, x \mapsto x^g \mid g \in G\} \leq \text{Aut}(G).$$

Hence, G has solvable conjugacy problem if and only if $\text{Inn}(G)$ is orbit decidable. Since the word problem is a particular case of the conjugacy problem (x equals 1 if and only if x is conjugated to 1), it is also a particular case of an orbit decidability problem. In particular, the existence of groups with unsolvable word and/or conjugacy problems gives us the first instances of orbit undecidability.

Whitehead [31, 32], in two of his classical and most influential papers, found an algorithm to decide, given two elements in the free group F_r , whether one can be mapped to the other by an automorphism of F_r , and, in the affirmative case, find such an automorphism. In other words:

Theorem 2.1 (Whitehead [31, 32]). *The full automorphism group $\text{Aut}(F_r)$ of a free group F_r is orbit decidable (including the search version).*

Several classical variations on this problem can also be expressed in orbit decidability terms. For example, Whitehead's argument also proves the following multiple version for cyclic words (see [20]):

Theorem 2.2 (Whitehead [31, 32]). *Let $X = (F_r/\sim)^n$ and*

$$A = \{\bar{\alpha}: X \rightarrow X, (\bar{x}_1, \dots, \bar{x}_n) \mapsto (\bar{x}_1\bar{\alpha}, \dots, \bar{x}_n\bar{\alpha}) \mid \alpha \in \text{Aut}(F_r)\} \subseteq \text{Map}(X, X).$$

Then, A is orbit decidable (including the corresponding search version).

McCool made a refinement of this argument in [23], and gave an algorithm which, given two n -tuples of real elements in F_r , say (x_1, \dots, x_n) and (y_1, \dots, y_n) , decides whether there exists an $\alpha \in \text{Aut}(F_r)$ such that $x_i\alpha = y_i$ for all $i = 1, \dots, n$; in other words:

Theorem 2.3 (McCool [23]). *Let $X = (F_r)^n$ and*

$$A = \{\bar{\alpha}: X \rightarrow X, (x_1, \dots, x_n) \mapsto (x_1\alpha, \dots, x_n\alpha) \mid \alpha \in \text{Aut}(F_r)\} \subseteq \text{Map}(X, X).$$

Then, A is orbit decidable (including the corresponding search version).

Even a later version for subgroups due to Gersten in 1984, see [13], also fits into this setting:

Theorem 2.4 (Gersten [13]). *Let F_r be a finitely generated free group, and let X be the set of conjugacy classes of finitely generated subgroups of F_r . Let*

$$A = \{\bar{\alpha}: X^n \rightarrow X^n, (\overline{H_1}, \dots, \overline{H_n}) \mapsto (\overline{H_1\alpha}, \dots, \overline{H_n\alpha}) \mid \alpha \in \text{Aut}(F_r)\} \subseteq \text{Map}(X^n, X^n).$$

Then, A is orbit decidable (including the corresponding search version).

We can also move our attention from automorphisms to other collections of maps, and we will find more results in the literature expressible in this orbit decidability fashion. For example, orbit decidability of the whole set of endomorphisms of a free group, $\text{End}(F_r)$ consists on deciding whether, given two words $u, v \in F_r$, there is an endomorphism $\alpha \in \text{End}(F_r)$ such that $u\alpha = v$. But, letting $\{a_1, \dots, a_r\}$ be a free basis of F_r and writing u and v as words on them, $u = u(a_1, \dots, a_r)$ and $v = v(a_1, \dots, a_r)$, this is the same as asking for the existence of some elements $X_1, \dots, X_r \in F_r$ (images of a_1, \dots, a_r under a potential endomorphism α) such that $u(X_1, \dots, X_r) = v$. This is precisely asking whether the given such equation has a solution in F_r . Similarly, the version of the same problem with tuples boils down to asking for solutions of a system of free equations. Makanin's result solving general systems of equations in the free group answers positively to this question:

Theorem 2.5 (Makanin [21]). *Let F_r be a finitely generated free group, and let $X = (F_r)^n$. Then, $\text{End}(F_r)$ is orbit decidable (including the corresponding search version).*

L. Ciobanu and A. Ould Houcine in [10] solved the interesting intermediate situation concerning monomorphisms: deciding whether there is a monomorphism $\alpha \in \text{Mon}(F_r)$ mapping a certain element to another is a third problem, sensibly different from both the automorphism case (Whitehead techniques) and the endomorphism case (equations); in some sense it consists on deciding the compatibility of a certain kind of infinite system of equations, see [10]. They solve the multiple version as well:

Theorem 2.6 (Ciobanu–Ould Houcine [10]). *Let F_r be a finitely generated free group, and let $X = (F_r)^n$. Then, $\text{Mon}(F_r)$ is orbit decidable (including the corresponding search version).*

Moving attention to other families of groups beyond free, we also find other interesting orbit decidability results in the literature. For example, the following are some examples of Whitehead-like results.

Theorem 2.7. *The following statements hold.*

- (i) (Levitt–Vogtman [19]) *Let $X = G$ be a surface group. Then, $A = \text{Aut}(G)$ is orbit decidable.*
- (ii) (Dahmani–Girardel [12]) *Let $X = G$ be a hyperbolic group. Then, $A = \text{Aut}(G)$ is orbit decidable.*
- (iii) (Kharlampovich–Ventura [18]) *Let G be a torsion-free relatively hyperbolic groups with abelian parabolic subgroups, and let $X = G^n$. Then, $A = \text{Aut}(G)$ is orbit decidable.*

In the three cases, the corresponding search version can effectively be resolved.

An extension of Whitehead problem, the so-called *mixed Whitehead problem*, was solved by Bogopolski–Ventura in [4] for torsion-free hyperbolic groups (this is a multiple version with the equalities being up to conjugacy, but forcing common conjugators in pre-established blocks, see [4] for details). A particular consequence of that result is the following:

Theorem 2.8 (Bogopolski–Ventura [4]). *Let G be a torsion-free hyperbolic group, and let $X = G/\sim$ be the set of conjugacy classes in G . Then, for every m -tuple $(g_1, \dots, g_m) \in G^n$, the subgroup*

$$\text{Stab}(g_1, \dots, g_m) = \text{Stab}(g_1) \cap \dots \cap \text{Stab}(g_m) \leq \text{Aut}(G)$$

acting on X^n in the natural way is orbit decidable (including the corresponding search version).

Concentrating now into free abelian groups, we also find here interesting orbit decidability results. The Whitehead type result for \mathbb{Z}^n is a very elementary observation in linear algebra:

Observation 2.9 (folklore). *Let $X = \mathbb{Z}^r$. Then, $A = \text{Aut}(\mathbb{Z}^r) = \text{GL}_r(\mathbb{Z})$ is orbit decidable.*

This is just based on the elementary fact that given two integral vectors $u, v \in \mathbb{Z}^r$, there exists an invertible matrix A such that $uA = v$ if and only if the highest common divisor of the entries of both u and v do coincide.

However, not every orbit decidability question is easy in \mathbb{Z}^r . In fact, $\text{GL}_r(\mathbb{Z})$ contains orbit undecidable subgroups, as will be seen below. To start with, cyclic subgroups of $\text{GL}_r(\mathbb{Z})$ are known to be orbit decidable, but this problem is more tricky than its superficial looking: given an invertible integral matrix $A \in \text{GL}_r(\mathbb{Z})$ and two vectors $u, v \in \mathbb{Z}^r$, we have to decide whether $uA^n = v$ for some $n \in \mathbb{Z}$ (i.e., whether u gets mapped to v by some element in the cyclic subgroup $\langle A \rangle \leq \text{GL}_r(\mathbb{Z})$). Of course, for any fixed value of n this is elementary checkable, but note that n is precisely the unknown of the problem. In 1986, Kannan–Lipton gave a polynomial time algorithm to solve this problem, see [17]; in fact, they did more, they covered all rational vectors and matrices (not necessarily invertible). An alternative way to solve this problem is using a more recent connection of the notion of orbit decidability with the conjugacy problem in groups (due to Bogopolski–Martino–Ventura and explained below): using this, orbit decidability of cyclic subgroups of $\text{GL}_r(\mathbb{Z})$ happens to be equivalent to the conjugacy problem for \mathbb{Z}^n -by- \mathbb{Z} groups. As particular cases of polycyclic groups, the conjugacy problem for those groups was already known to be solvable since 1969 (see [27]).

3 A mistake, the beginning of a new story

A recent result by Bogopolski–Martino–Ventura [2] has given a renovated protagonism to the notion of orbit decidability (see Theorem 4.1 below). It tightly connects this notion with the conjugacy problem for extensions of groups. Any short exact sequence of groups,

$$1 \rightarrow F \xrightarrow{\alpha} G \xrightarrow{\beta} H \rightarrow 1,$$

naturally determines a subgroup of $\text{Aut}(F)$: since $F\alpha$ is a normal subgroup of G , for every $g \in G$, the conjugation γ_g of G induces an automorphism of F , $\varphi_g: F \rightarrow F$, $x \mapsto g^{-1}xg$ (which does not necessarily belong to $\text{Inn}(F)$). The set of all such automorphisms, $A_G = \{\varphi_g \mid g \in G\}$, form a subgroup of $\text{Aut}(F)$ called the *action subgroup* of the given sequence.

Under certain conditions for the short exact sequence, Theorem 4.1 states that G has solvable conjugacy problem if and only if A_G is orbit decidable. This is an interesting result because, next to any orbit decidability

situation which one is able to solve, one can immediately deduce the solvability of the conjugacy problem for a certain family of groups. Conversely, from any unsolvable orbit decidability situation one can immediately deduce that certain groups have unsolvable conjugacy problem. This idea is proving to be quite fruitful, and a sequence of papers have been appearing in the last years exploiting it, and will probably continue to do so, both in the positive and in the negative direction (i.e., finding new families of groups with solvable conjugacy problem, or proving the existence of group of certain type with unsolvable conjugacy problem); we do an extensive review on this line in the next sections.

But, in order to give a deeper exposition of the ideas behind Theorem 4.1 (the main result from [2]), let us concentrate first on what it is, in my opinion, the key point that allowed its authors to get that result. And (not being a rare situation in mathematics, in general), this key point was essentially motivated by a previous mistake, momentarily done by the authors while working in their previous paper [1]. This is the reason for the title of the present section.

In the paper [1], Bogopolski–Martino–Maslakova–Ventura solved the conjugacy problem for free-by-cyclic groups. Their strategy was to reduce it to the twisted conjugacy problem for free groups (a more complicated problem in an easier group) and then solving this.

Definition 3.1. Let $G = \langle X \mid R \rangle$ be a finitely presented group. For an endomorphism $\phi \in \text{Aut}(G)$, we say that two elements $u, v \in G$ are ϕ -twisted conjugated, denoted $u \sim_\phi v$, if there exists an $x \in G$ such that $(x\phi)^{-1}ux = v$. The twisted conjugacy problem (for endomorphisms) for G , denoted $\text{TCP}(G)$ (resp. $\text{TCP}_e(G)$), consists on algorithmically deciding, given $\phi \in \text{Aut}(G)$ (resp. $\phi \in \text{End}(G)$) and given two elements $u, v \in G$, whether $u \sim_\phi v$. (To be more precise, u and v are given as words on X , and ϕ is given by words describing the images $x\phi$, for each $x \in X$.)

Note that, if α is the identity, this is precisely the standard conjugacy problem for G , denoted $\text{CP}(G)$. However, in general, it looks like a much more complicated algorithmic problem; intuitively, $\text{TCP}(G)$ encodes the difficulty of $\text{CP}(G)$ plus the difficulty of $\text{Aut}(G)$ (the more tricky endomorphisms or automorphisms G admits, the more complicated $\text{TCP}_e(G)$ or $\text{TCP}(G)$ will be compared to $\text{CP}(G)$). In fact, the twisted conjugacy problem is strictly stronger than the conjugacy problem, as shown in [2, Corollary 4.9], where the first known examples of groups G with solvable $\text{CP}(G)$ but unsolvable $\text{TCP}(G)$ were given.

Let us go back to free-by-cyclic groups. Let $F_n = \langle x_1, \dots, x_n \mid \rangle$ be the free group of rank n and $\phi \in \text{Aut}(F_n)$. We will refer to the corresponding free-by- \mathbb{Z} group with the notation

$$F_n \rtimes_\phi \mathbb{Z} = \langle x_1, \dots, x_n, t \mid t^{-1}x_i t = x_i \phi \rangle.$$

Normal forms are well known in such groups: every element from $F_n \rtimes_\phi \mathbb{Z}$ can be written in a unique way as $t^r u$ for some $r \in \mathbb{Z}$, and some reduced word u on the x_i (and, of course, this normal form is algorithmically computable from any word on the generators representing the element).

Using normal forms, the above mentioned reduction of the problem $\text{CP}(F_n \rtimes_\phi \mathbb{Z})$ to $\text{TCP}(F_n)$ follows easily from a straightforward calculation: if we conjugate an arbitrary element $t^r u \in F_n \rtimes_\phi \mathbb{Z}$ by an arbitrary other element $t^k g \in F_n \rtimes_\phi \mathbb{Z}$, we obtain

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

Hence, two elements in $F_n \rtimes_\phi \mathbb{Z}$, say $t^r u$ and $t^s v$, are conjugate in $F_n \rtimes_\phi \mathbb{Z}$ if and only if $r = s$ and v is ϕ^r -twisted conjugated to some iterated image of u under ϕ , namely $v \sim_{\phi^r} (u\phi^k)$ for some integer k . This reduces $\text{CP}(F_n \rtimes_\phi \mathbb{Z})$ to infinitely many instances of $\text{TCP}(F_n)$, but the following easy observation reduces it down to finitely many. Observe that, for any endomorphism $\psi \in \text{End}(F_n)$, the trivial equation $(g\psi)^{-1}(g\psi)g = g$ says that $g\psi \sim_\psi g$, for every $g \in F_n$. Hence, $u\phi^k \sim_{\phi^r} (u\phi^{k+\lambda r})$, making the parameter k work modulo r . Then, we have

$$t^r u \sim t^s v \iff r = s, \text{ and } v \sim_{\phi^r} u\phi^k \text{ for some } k = 0, \dots, r - 1. \tag{3.1}$$

This reduces $\text{CP}(F_n \rtimes_\phi \mathbb{Z})$ to finitely many instances of $\text{TCP}(F_n)$, i.e., to $\text{TCP}(F_n)$, a more complicated problem but in an easier group.

When working in [1], and after realizing about this reduction, we concentrated on $\text{TCP}(F_n)$ and solved it:

Theorem 3.2 (Bogopolski–Martino–Maslakova–Ventura [1, Theorem 1.5]). *Let F_n be a finitely generated free group. Then, $\text{TCP}(F_n)$ is solvable.*

But in the meantime, we realized a mistake made in the argument for the above reduction, that the reader probably already realized too: for (3.1) to make sense, one needs to assume $r \neq 0$. That is, in the case $r = s = 0$, the reduction to the finite situation does not work, and the problem to be solved still contains a parameter k running over infinitely many values: given $u, v \in F_n$ one should decide whether $v \sim u\phi^k$ for some integer k ; these are infinitely many instances of standard conjugacy in F_n . So, Theorem 3.2 only solves $\text{CP}(F_n \rtimes_{\phi} \mathbb{Z})$ in the special case $r = s \neq 0$, while the case $r = s = 0$ was still pending to be solved. An important observation here is that the problematic case $r = s = 0$ corresponds, precisely, to when the two inputs $t^r u$ and $t^s v$ belong to the free subgroup $F_n \triangleleft F_n \rtimes_{\phi} \mathbb{Z}$, while the case solved through Theorem 3.2 corresponds to the inputs being outside it. This observation will be crucial later on.

Fortunately, in the working process for the paper [1], a completely independent preprint appeared by P. Brinkmann solving precisely this missing case:

Theorem 3.3 (Brinkmann [8]). *Given a finitely generated free group F_n , two elements $u, v \in F_n$ and an automorphism $\phi \in \text{Aut}(F_n)$, it is decidable whether there exists an integer k such that $u\phi^k$ is conjugate to v .*

This is not just a fortunate coincidence. It is worth mentioning that, in that time, P. Brinkmann was also thinking about the conjugacy problem for $F_n \rtimes_{\phi} \mathbb{Z}$. He did not succeed but, as a side product, he got the above special case which happens to be precisely complementary to the other one solved by Bogopolski–Martino–Maslakova–Ventura in [1] (this is, indeed, a fortunate coincidence!). Even though the resolution of $\text{CP}(F_n \rtimes_{\phi} \mathbb{Z})$ is formally published in [1], it is honest to refer to it as Brinkmann–Bogopolski–Martino–Maslakova–Ventura theorem.

Theorem 3.4 (Brinkmann–Bogopolski–Martino–Maslakova–Ventura [1, 8]). *For every $\phi \in \text{Aut}(F_n)$, the problem $\text{CP}(F_n \rtimes_{\phi} \mathbb{Z})$ is solvable.*

This was the happy end of the paper [1], which got published in 2006. Later, three of the four authors of [1] kept thinking about possible extensions of Theorem 3.4, an effort that ended in 2010 with the publication of [2]. It is in this context when the distinction between the two cases highlighted by the mistake done took a renovated role. In fact, this was the crucial point connecting all this story with the notion of orbit decidability; we explain this further development in the next section. The reader probably already observed that Brinkmann’s result is easily expressible in orbit decidability terms: “for every $\phi \in \text{Aut}(F_n)$, the subgroup $\langle \phi \rangle \cdot \text{Inn}(F_n) \leq \text{Aut}(F_n)$ is orbit decidable”. Or, in a more informal language, “cyclic subgroups of $\text{Aut}(F_n)$ are orbit decidable up to conjugacy”.

Before going into this direction, let us mention a side event that happened later affecting the above results. The proofs of Theorems 3.2 and 3.3 both make essential use of the following previous result about computation of fixed points of automorphisms of free groups:

Theorem 3.5 (Maslakova [22]). *There exists an algorithm to compute a finite generating set for the fixed point subgroup of an arbitrary automorphism of a free group of finite rank.*

Some years after the publication of [1], the proof of Maslakova’s theorem was found to be wrong and incomplete. Several attempts to fix it have been uploaded to the arXiv by Bogopolski–Maslakova (see the sixth version, from January 2014, in [3]); no version has been firmly published yet.

However, the validity of Theorems 3.2 and 3.3 is not affected because there is another alternative and independent proof for them. Clearly, they are both consequences of Theorem 3.4 (corresponding to the two particular cases mentioned above), and Theorem 3.4 follows directly as a corollary of the following two deep results, from 2006 and 2010 respectively, and none of them using [22]:

Theorem 3.6 (Ol’shanskii–Sapir [26]). *(...) If $d(n)$ is the Dehn function of a multiple HNN extension of a free group and $\lim_{n \rightarrow \infty}^c d(n)/n^2 \log n = 0$, then the group has decidable conjugacy problem.*

Theorem 3.7 (Bridson–Groves [6]). *If F_n is a finitely generated free group and ϕ is an automorphism of F_n , then $F_n \rtimes_{\phi} \mathbb{Z}$ satisfies a quadratic isoperimetric inequality.*

In the Ol’shanskii–Sapir Theorem, \lim^c is a standard limit with an extra technical assumption of algorithmic nature (see [26] for details), which is verified by the limit hidden behind the Bridson–Groves Theorem.

4 Orbit decidability and extensions of groups

When one tries to generalize Theorem 3.4, as Bogopolski–Martino–Ventura did in 2005 after finishing [1], the natural place to look is at the family of free-by-free groups, namely groups of the form

$$F_n \rtimes_{\langle \phi_1, \dots, \phi_m \rangle} F_m = \langle x_1, \dots, x_n, t_1, \dots, t_m \mid t_j^{-1} x_i t_j = x_i \phi_j \ (i = 1, \dots, n, j = 1, \dots, m) \rangle,$$

where $\phi_1, \dots, \phi_m \in \text{Aut}(F_n)$, i.e., the same framework as for free-by- \mathbb{Z} groups but with several independent stable letters and several defining automorphisms. Exactly like in the free-by- \mathbb{Z} case, we have here normal forms of the type $w(t_1, \dots, t_m)u(x_1, \dots, x_n)$, where w and u are reduced words on t_1, \dots, t_m and x_1, \dots, x_n , respectively.

At a first look, it seemed quite reasonable to think that the techniques used to prove Theorem 3.4 could successfully extend to this much bigger family of groups. However, there is a classical result by C. F. Miller constructing explicit examples of free-by-free groups with unsolvable conjugacy problem; see [25]. Hence, the plan to generalize the arguments from [1] to the family of free-by-free groups must necessarily collide with some unavoidable obstacles.

Despite this certainty, we proceeded with the plan to adapt the argumentations from Theorem 3.4 to free-by-free groups. Of course we did not succeed, but we got the nice surprise of getting a very clear picture of the situation: the arguments for the case where the two inputs are outside F_n extended perfectly well to our new general situation and so, the conjugacy problem is solvable in this case (via its reduction to the twisted conjugacy problem for free groups). The case where the two inputs belong to F_n led directly to the following problem, intuitively much harder than Brinkmann’s one:

$$\text{Given } u, v \in F_n, \text{ decide whether } v \text{ is conjugate to } u\phi \text{ for some } \phi \in \langle \phi_1, \dots, \phi_m \rangle. \tag{4.1}$$

Note that, for $m = 1$, i.e., in the free-by- \mathbb{Z} case, this is exactly the contents of Brinkmann’s Theorem 3.3.

As said, some obstacle must have appeared because of the previously known existence of free-by-free groups with unsolvable conjugacy problem. The good new was that the above one is the very unique obstacle in that generalization process. Hence, we could conclude that a given free-by-free group has solvable conjugacy problem if and only if its corresponding problem (4.1) is solvable. In other words,

$$\text{CP}(F_n \rtimes_{\langle \phi_1, \dots, \phi_m \rangle} F_m) \text{ is solvable} \iff \langle \phi_1, \dots, \phi_m \rangle \leq \text{Aut}(F_n) \text{ is orbit decidable up to conjugacy} \tag{4.2}$$

(i.e., if and only if $\langle \phi_1, \dots, \phi_m \rangle \cdot \text{Inn}(F_n) \leq \text{Aut}(F_n)$ is orbit decidable). In particular, note that this equivalence immediately implies the existence of orbit undecidable subgroups of $\text{Aut}(F_n)$, corresponding to Miller’s examples of free-by-free groups with unsolvable conjugacy problem. This idea was exploited, as explained below.

Finally, a further generalization was done, based on the fact that the freeness of F_n and F_m is not essentially used along the argument. In [2], Bogopolski–Martino–Ventura were able to formulate and prove an analog of (4.2) for arbitrary short exact sequences of groups

$$1 \rightarrow F \rightarrow G \rightarrow H \rightarrow 1,$$

not just about the canonical sequence determined by a free-by-free group $1 \rightarrow F_n \rightarrow F_n \rtimes_{\langle \phi_1, \dots, \phi_m \rangle} F_m \rightarrow F_m \rightarrow 1$. As a toll, one has to assume a technical condition about centralizers at the quotient group (trivially satisfied in the free case).

The main result in [2] is the following, and we reproduce here the proof given there, so that the reader can appreciate the analogy with the motivating free case.

Theorem 4.1 (Bogopolski–Martino–Ventura [2]). *Let $1 \rightarrow F \xrightarrow{\alpha} G \xrightarrow{\beta} H \rightarrow 1$ be a short exact sequence of finitely presented groups (given by finite presentations and images of generators) such that*

- (i) *F has solvable TCP,*
 - (ii) *H has solvable CP,*
 - (iii) *for every $1 \neq h \in H$, the subgroup $\langle h \rangle$ has finite index in its centralizer $C_H(h)$, and there is an algorithm which computes a finite set of coset representatives, $z_{h,1}, \dots, z_{h,t_h} \in H$ (i.e., $C_H(h) = \langle h \rangle z_{h,1} \sqcup \dots \sqcup \langle h \rangle z_{h,t_h}$).*
- Then,*

$$G \text{ has solvable CP} \iff A_G = \{\varphi_g \mid g \in G\} \leq \text{Aut}(F) \text{ is orbit decidable.}$$

Proof. As a preliminary observation we note that in the given short exact sequence (since we have explicit presentations of the involved groups and images of the corresponding generators by α and β) one can algorithmically compute images and pre-images of elements by both morphisms. This will be implicitly used several times along the proof.

As usual, we shall identify F with $F\alpha \leq G$. By definition, $x\varphi_g = g^{-1}xg$ for every $g \in G$ and $x \in F$. So, given two elements $x, x' \in F$, finding $g \in G$ such that $x' = g^{-1}xg$ is the same as finding $\varphi \in A_G$ such that $x' = x\varphi$. Hence, the conjugacy problem in G with two inputs from F is exactly the orbit decidability problem for A_G . This shows the implication to the right.

Assume now that A_G is orbit decidable. Let $g, g' \in G$ be two given elements in G and let us decide whether they are conjugate to each other in G . Map them to H . Using (ii), we can decide whether $g\beta$ and $g'\beta$ are conjugate to each other in H . If they are not, then g and g' cannot either be conjugate to each other in G and we are done. Otherwise, (ii) gives us an element from H conjugating $g\beta$ into $g'\beta$. Compute a pre-image $u \in G$ of this element. It satisfies $(g^u)\beta = (g\beta)^{u\beta} = g'\beta$. Now, changing g to g^u , we may assume that $g\beta = g'\beta$. If this equals the trivial element in H (a fact that can effectively be checked using (ii)), then g and g' lie in F and, using our hypothesis, we are done. Hence, we are restricted to the case $g\beta = g'\beta \neq_H 1$.

Now, compute $f \in F$ such that $g' = gf$ (this is the α -pre-image of $g^{-1}g'$). Since $g\beta \neq_H 1$, we can use (iii) to compute elements $z_1, \dots, z_t \in H$ such that $C_H(g\beta) = \langle g\beta \rangle z_1 \sqcup \dots \sqcup \langle g\beta \rangle z_t$, and then compute a pre-image $y_i \in G$ for each z_i , $i = 1, \dots, t$. Note that, by construction, the β -images of g and y_i (respectively $g\beta$ and z_i) commute in H so, $y_i^{-1}gy_i = gp_i$ for some computable $p_i \in F$.

Since $g\beta = g'\beta$, every possible conjugator of g into g' must map under β to $C_H(g\beta)$ so, it must be of the form $g^r y_i x$ for some integer r , some $i \in \{1, \dots, t\}$, and some $x \in F$. Hence,

$$gf = g' = (x^{-1} y_i^{-1} g^{-r})g(g^r y_i x) = x^{-1}(y_i^{-1} g y_i)x = x^{-1} g p_i x.$$

Thus, deciding whether the elements g and g' are conjugate to each other in G amounts to decide whether there exists an $i \in \{1, \dots, t\}$ and $x \in F$ satisfying $gf = x^{-1} g p_i x$, which is equivalent to $f = (g^{-1} x^{-1} g) p_i x$ and so to $f = (x\varphi_g)^{-1} p_i x$. Since i takes finitely many values and the previous equation means precisely $f \sim_{\varphi_g} p_i$, we can algorithmically solve this problem using the hypothesis (i). This completes the proof. \square

Note that in the proof of Theorem 4.1 we did not use the full power of hypothesis (i). In fact, we used a solution to $\text{TCP}_\phi(F)$ only for the automorphisms in the action subgroup, $\phi \in A_G$. For specific examples, this may be a weaker assumption than a full solution to $\text{TCP}(F)$.

Hypothesis (iii) is somehow restrictive, but at the same time satisfied by many groups: for example, free groups (where the centralizer of an element $1 \neq h$ is cyclic and generated by its maximal root) and it is not difficult to see that torsion-free hyperbolic groups also satisfy it, see [2, Section 4.2].

The correct way to think about this theorem is the following: it reduces the CP for a group G to the TCP plus a certain OD problem in a certain normal subgroup $F \triangleleft G$. It is true that the TCP is harder than the standard CP, and the resulting OD problem is sometimes more technical than the original problem; but both of them take place entirely in the subgroup F rather than in G . In all situations when F is a group significantly easier than G , Theorem 4.1 promises to be useful: it reduces the CP for G to two independent problems, maybe more technical, but in an easier group, namely F . Or, from bottom to top: for any group F where one knows how to solve the TCP, Theorem 4.1 gives a great tool to investigate the solvability/unsolvability of the CP in a vast family of extensions of F , by means of finding orbit decidable/orbit undecidable subgroups of $\text{Aut}(F)$. This point of view has been quite fruitful in the last years, as explained in the following sections.

5 Negative results

After Theorem 4.1, the next natural thing to do is to analyze Miller’s construction of free-by-free groups with unsolvable conjugacy problem (see [25]), looking for explicit examples of orbit undecidable subgroups in $\text{Aut}(F_n)$. This was done in [2] and, in fact, a closer look to these negative examples revealed a more general way to construct orbit undecidable subgroups inside $\text{Aut}(F)$ for many other groups F , other than free. On its turn, this source of orbit undecidability determines then lots of new group extensions (of those groups F) with unsolvable conjugacy problem. Let us remind now these arguments, starting from Miller’s construction and highlighting then the generalization to other groups F .

Miller’s construction begins with an arbitrary finite presentation, say $H = \langle s_1, \dots, s_n \mid R_1, \dots, R_m \rangle$ (where the R_j are words on the s_i). Let $F_{n+1} = \langle q, s_1, \dots, s_n \mid \rangle$ and $F_{m+n} = \langle t_1, \dots, t_m, d_1, \dots, d_n \mid \rangle$ be the free groups of rank $n + 1$ and $m + n$, respectively, on the listed generators. Consider the $m + n$ automorphisms of F_{n+1} given by

$$\begin{aligned} \alpha_i &: F_{n+1} \rightarrow F_{n+1}, & q &\mapsto qR_i, & s_k &\mapsto s_k, \\ \beta_j &: F_{n+1} \rightarrow F_{n+1}, & q &\mapsto s_j^{-1}q s_j, & s_k &\mapsto s_k, \end{aligned}$$

for $i = 1, \dots, m$ and $j, k = 1, \dots, n$, and denote by $A(H) \leq \text{Aut}(F_{n+1})$ the group of automorphisms they generate. Next, consider the F_{n+1} -by- F_{m+n} group defined by these automorphisms,

$$G(H) = F_{n+1} \rtimes_{\alpha_1, \dots, \alpha_m, \beta_1, \dots, \beta_n} F_{m+n}.$$

The following theorem is [25, Chapter III, Corollary 5]. Below, we shall provide an alternative proof.

Theorem 5.1 (Miller [25]). *If H has unsolvable word problem, then $G(H)$ has unsolvable conjugacy problem.*

So, applying Miller’s construction to a presentation H with n generators, m relations, and with unsolvable word problem, one obtains an $(m + n)$ -generated subgroup of $\text{Aut}(F_{n+1})$, namely $A(H)$, which is orbit undecidable.

In [5], V. Borisov constructed a group presented with for generators, twelve relations, and having unsolvable word problem. By embedding it into a bigger group with two generators and the same number of relations via the Higman–Neumann–Neumann Embedding Theorem (see [16]), we get a group H with $n = 2$ generators, $m = 12$ relations, and having unsolvable word problem. Applying Miller’s construction to H , we conclude the existence of an F_3 -by- F_{14} group with unsolvable conjugacy problem. In other words,

Corollary 5.2. *There exists a 14-generated subgroup $A \leq \text{Aut}(F_3)$ which is orbit undecidable.*

Recall that this orbit undecidable subgroup is $A = \langle \alpha_1, \dots, \alpha_{12}, \beta_1, \beta_2 \rangle \leq \text{Aut}(F_3)$, where the α_i and the β_j are the above isomorphisms corresponding to a group $H = \langle s_1, s_2 \mid R_1, \dots, R_{12} \rangle$ with unsolvable word problem.

Looking at the details of the proof of Theorem 5.1, one can see the parallelism with the following more general construction.

Let F be an arbitrary group. Recall that the *stabilizer* of a given subgroup $K \leq F$, denoted $\text{Stab}(K)$, is

$$\text{Stab}(K) = \{ \varphi \in \text{Aut}(F) \mid k\varphi = k \text{ for all } k \in K \} \leq \text{Aut}(F).$$

For simplicity, we shall write $\text{Stab}(k)$ to denote $\text{Stab}(\langle k \rangle)$, $k \in F$. Furthermore, we define the *conjugacy stabilizer* of K , denoted $\text{Stab}^*(K)$, to be the set of automorphisms acting as conjugation on K , formally $\text{Stab}^*(K) = \text{Stab}(K) \cdot \text{Inn}(F) \leq \text{Aut}(F)$.

Proposition 5.3. *Let F be a group. Suppose we are given two subgroups $A \leq B \leq \text{Aut}(F)$ and an element $z \in F$ such that $B \cap \text{Stab}^*(z) = \{\text{Id}\}$. If $A \leq \text{Aut}(F)$ is orbit decidable up to conjugacy, then the membership problem $\text{MP}(A, B)$ is solvable (i.e., there is an algorithm which, given $\psi \in B$, decides whether ψ belongs to A or not).*

Proof. Suppose $\psi \in B \leq \text{Aut}(F)$ is given. Take $z' = z\psi$ and observe that

$$\{ \phi \in B \mid z\phi \sim z' \} = B \cap (\text{Stab}^*(z) \cdot \psi) = (B \cap \text{Stab}^*(z)) \cdot \psi = \{ \psi \}.$$

So, there exists some $\phi \in A$ such that $z\phi$ is conjugate to z' in F , if and only if $\psi \in A$. Hence, orbit decidability for $A \cdot \text{Inn}(F) \leq \text{Aut}(F)$ solves $\text{MP}(A, B)$. □

One can interpret Proposition 5.3 by saying that if, for a certain group F , $\text{Aut}(F)$ contains a pair of subgroups $A \leq B \leq \text{Aut}(F)$ with unsolvable $MP(A, B)$ (plus the existence of that special element z), then $A \cdot \text{Inn}(F) \leq \text{Aut}(F)$ is orbit undecidable.

The most classical example of unsolvability of the membership problem goes back to more than fifty years ago. In [24] (see also [25, Chapter III.C]) Mihailova gave a nice example of unsolvability of the membership problem. The construction goes as follows. Like before, start with any finite presentation,

$$H = \langle s_1, \dots, s_n \mid R_1, \dots, R_m \rangle,$$

and consider the subgroup $A = \{(x, y) \in F_n \times F_n \mid x =_H y\} \leq F_n \times F_n$. It is straightforward to verify that

$$A = \langle (1, R_1), \dots, (1, R_m), (s_1, s_1), \dots, (s_n, s_n) \rangle$$

(and so it is finitely generated), and that $MP(A, F_n \times F_n)$ is solvable if and only if $WP(H)$ is solvable. Since there exist 2-generated groups with unsolvable word problem, it follows that $F_2 \times F_2$ contains finitely generated subgroups $A \leq F_2 \times F_2$ with unsolvable $MP(A, F_2 \times F_2)$. From all this, we deduce the following.

Proposition 5.4. *Let F be a finitely generated group such that $F_2 \times F_2$ embeds in $\text{Aut}(F)$ in such a way that the image intersects trivially with $\text{Stab}^*(z)$, for some $z \in F$. Then, $\text{Aut}(F)$ contains an orbit undecidable subgroup; in other words, there exist F -by-free groups with unsolvable conjugacy problem.*

Consider the particular case of the free group of rank three, $F_3 = \langle q, a, b \mid \rangle$, and the following copy of $F_2 \times F_2$ inside $\text{Aut}(F_3)$. For every $u, v \in \langle a, b \rangle \leq F_3$, consider the automorphism ${}_u\theta_v: F_3 \rightarrow F_3, q \mapsto uqv, a \mapsto a, b \mapsto b$. Clearly, ${}_{u_1}\theta_{1u_2}\theta_1 = {}_{u_1u_2}\theta_1$ and ${}_{1\theta_{v_1}}\theta_{v_2} = {}_{1\theta_{v_2v_1}}$, which means that

$$F_2 \simeq \{ {}_u\theta_1 \mid u \in \langle a, b \rangle \} \leq \text{Aut}(F_3) \quad \text{and} \quad F_2 \simeq F_2^{\text{op}} \simeq \{ {}_1\theta_v \mid v \in \langle a, b \rangle \} \leq \text{Aut}(F_3).$$

Furthermore, it is also clear that ${}_u\theta_1$ and ${}_1\theta_v$ do commute, ${}_u\theta_1{}_1\theta_v = {}_u\theta_v = {}_1\theta_{vu}\theta_1$. So,

$$B = \langle {}_{a^{-1}}\theta_1, {}_{b^{-1}}\theta_1, {}_1\theta_a, {}_1\theta_b \rangle = \{ {}_u\theta_v \mid u, v \in \langle a, b \rangle \} \leq \text{Aut}(F_3)$$

is a subgroup of $\text{Aut}(F_3)$ isomorphic to $F_2 \times F_2$. In order to apply Proposition 5.3, let us consider $z = qaqbq \in F_3$. We claim that $B \cap \text{Stab}^*(z) = \{\text{Id}\}$. In fact, suppose $u, v \in \langle a, b \rangle$ are such that $(z)_u\theta_v = uqvauqvbuqv$ is conjugate to $z = qaqbq$ in F_3 . Since both words have exactly three occurrences of q , they must agree up to cyclic reordering. That is, $q(vau)q(vbu)q(vu)$ equals either $qaqbq$, or qbq^2a , or q^2aqb . From this, one can straightforwardly deduce that $u = v = 1$ in all three cases. Thus, ${}_u\theta_v = \text{Id}$ proving the claim.

Now, let $H = \langle a, b \mid R_1, \dots, R_{12} \rangle$ be the above example of a group with two generators, twelve relations, and unsolvable word problem. By Mihailova result and Proposition 5.3,

$$A \cdot \text{Inn}(F_3) = \langle {}_1\theta_{R_1}, \dots, {}_1\theta_{R_{12}}, {}_{a^{-1}}\theta_a, {}_{b^{-1}}\theta_b \rangle \cdot \text{Inn}(F_3) \leq \text{Aut}(F_3)$$

is orbit undecidable. Hence, by equation (4.2), the F_3 -by- F_{14} group determined by the fourteen automorphisms ${}_1\theta_{R_1}, \dots, {}_1\theta_{R_{12}}, {}_{a^{-1}}\theta_a, {}_{b^{-1}}\theta_b \in \text{Aut}(F_3)$, namely

$$G = \langle q, a, b, d_1, d_2, t_1, \dots, t_{12} \mid t_i^{-1}qt_i = qR_i, d_1^{-1}qd_1 = a^{-1}qa, d_2^{-1}qd_2 = b^{-1}qb, t_i^{-1}at_i = a, \\ d_1^{-1}ad_1 = a, d_2^{-1}ad_2 = a, t_i^{-1}bt_i = b, d_1^{-1}bd_1 = b, d_2^{-1}bd_2 = b \rangle$$

has unsolvable conjugacy problem. This is precisely Miller's group $G(H)$ associated to $H = \langle a, b \mid R_1, \dots, R_{12} \rangle$, recovering the original Miller's construction. Note that this reasoning provides an alternative proof for Miller's Theorem 5.1.

However, adopting this more general point of view, one can look at other subgroups of $\text{Aut}(F_3)$ isomorphic to $F_2 \times F_2$; for each such subgroup $B \leq \text{Aut}(F_3)$, we can replicate the construction finding many other free-by-free groups with unsolvable conjugacy problem (brothers, in this sense, of Miller's examples). Or, even more interestingly, one can replicate this construction over an arbitrary group F (not necessarily free) with the only condition that $\text{Aut}(F)$ contains a copy of $F_2 \times F_2$ (plus the technical condition of existence of that element $z \in F$). This provides lots of new examples of orbit undecidable subgroups of $\text{Aut}(F)$, which correspond to lots of new extensions of F with unsolvable conjugacy problem. Some of the results in the literature in this line are reviewed in the following sections.

6 Extensions of free groups

Following the idea at the end of Section 4, let us particularize Theorem 4.1 to groups F for which we know a solution to its twisted conjugacy problem, in order to find certain extensions of F having solvable conjugacy problem, and others having unsolvable conjugacy problem. Of course, the first non-trivial examples of groups with solvable TCP are free groups (see Theorem 3.2).

Let us take F in Theorem 4.1 to be free, say $F = F_n$, and H to be free as well, say F_m (the reader could easily extend the following results to H being torsion-free hyperbolic, since these groups also satisfy condition (iii) from Theorem 4.1, see [2, Section 4.2]). As we observed in Section 3, Brinkmann's Theorem 3.3 can be rephrased by saying that cyclic subgroups of $\text{Aut}(F_n)$ are orbit decidable up to conjugacy; hence,

Corollary 6.1 (Brinkmann–Bogopolski–Martino–Maslakova–Ventura [1, 8]). *Free-by-cyclic groups have solvable conjugacy problem.*

The classical Whitehead Theorem 2.1 leads us to

Corollary 6.2 (Bogopolski–Martino–Ventura [2]). *Let F_n be a finitely generated free group. If ϕ_1, \dots, ϕ_m generate $\text{Aut}(F_n)$, then the F_n -by- F_m group $G = F_n \rtimes_{\phi_1, \dots, \phi_m} F_m$ has solvable conjugacy problem.*

It is not known, in general, whether orbit decidability goes down to finite index subgroups. But, in [2], it was proved to do so at least for the special case of the free group and for the full automorphism group,

Theorem 6.3 (Bogopolski–Martino–Ventura [2]). *Let F_n be a finitely generated free group. Any finite index subgroup of $\text{Aut}(F_n)$ is orbit decidable up to conjugacy.*

Hence,

Corollary 6.4 (Bogopolski–Martino–Ventura [2]). *Let F_n be a finitely generated free group. If ϕ_1, \dots, ϕ_m generate a finite index subgroup of $\text{Aut}(F_n)$, then the F_n -by- F_m group $G = F_n \rtimes_{\phi_1, \dots, \phi_m} F_m$ has solvable conjugacy problem.*

Since $\text{Out}(F_2) \simeq \text{GL}_2(\mathbb{Z})$ is virtually free, the case of rank two is very special:

Theorem 6.5 (Bogopolski–Martino–Ventura, [2]). *Let F_2 be the free group of rank two. Then every finitely generated subgroup of $\text{Aut}(F_2)$ is orbit decidable up to conjugacy.*

And, hence,

Corollary 6.6 (Bogopolski–Martino–Ventura, [2]). *Every F_2 -by-free group has solvable conjugacy problem.*

In [2, Section 6.2.] the reader can find more interesting examples of orbit decidable subgroups in $\text{Aut}(F_n)$, this time coming from a more geometric context, together with the corresponding free extensions with solvable conjugacy problem.

7 Extensions of free abelian groups

Let us take now F in Theorem 4.1 to be free abelian, say $F = \mathbb{Z}^n$, and H to be free, say F_m (the reader could easily extend the following results to H being torsion-free hyperbolic, like in the previous section). Of course we can, because $\text{TCP}(\mathbb{Z}^n)$ is solvable as reducible to the compatibility of a system of linear equations. Note that, in this case, orbit decidability/undecidability is going to concern subgroups of $\text{Aut}(\mathbb{Z}^n) \simeq \text{GL}_n(\mathbb{Z})$, i.e., groups of invertible integral $n \times n$ matrices. Note also that orbit decidability and orbit decidability up to conjugacy do coincide in this context because the base group is abelian.

To start with, and as explained above, Kannan–Lipton gave a polynomial time algorithm in 1986, see [17], to solve the orbit decidability problem for cyclic subgroups of $\text{GL}_n(\mathbb{Q})$ (they call its rational version *the orbit problem*).

Theorem 7.1 (Kannan–Lipton [17]). *Cyclic subgroups of $GL_n(\mathbb{Q})$ are orbit decidable.*

The corresponding consequence is

Corollary 7.2. *All \mathbb{Z}^n -by- \mathbb{Z} groups have solvable conjugacy problem.*

It should be mentioned that this was already known since \mathbb{Z}^n -by- \mathbb{Z} groups are clearly polycyclic, and an old result due to V. N. Remeslennikov established that polycyclic groups are conjugacy separable and, as a consequence, have solvable conjugacy problem.

Moreover, this result was used in [2] to prove a more general fact about orbit decidability in $GL_n(\mathbb{Z})$. J. Tits [30] proved the deep and remarkable fact that every finitely generated subgroup of $GL_n(\mathbb{Z})$ is either virtually solvable or it contains a non-abelian free subgroup. It turns out that all subgroups of the first kind are orbit decidable, so forcing orbit undecidable subgroups of $GL_n(\mathbb{Z})$ (if any) to contain non-abelian free subgroups:

Theorem 7.3 (Bogopolski–Martino–Ventura [2]). *Any virtually solvable subgroup of $GL_n(\mathbb{Z})$ is orbit decidable.*

Corollary 7.4 (Bogopolski–Martino–Ventura [2]). *Let $A_1, \dots, A_m \in GL_n(\mathbb{Z})$. If $\langle A_1, \dots, A_m \rangle \leq GL_n(\mathbb{Z})$ is virtually solvable, then the \mathbb{Z}^n -by- F_m group $G = \mathbb{Z}^n \rtimes_{A_1, \dots, A_m} F_m$ has solvable conjugacy problem.*

Following the same route as for free groups, the folklore Observation 2.9, tells us that

Corollary 7.5 (Bogopolski–Martino–Ventura [2]). *Let $A_1, \dots, A_m \in GL_n(\mathbb{Z})$. If $\langle A_1, \dots, A_m \rangle = GL_n(\mathbb{Z})$, then the \mathbb{Z}^n -by- F_m group $G = \mathbb{Z}^n \rtimes_{A_1, \dots, A_m} F_m$ has solvable conjugacy problem.*

And orbit decidability also goes down to finite index subgroups for free abelian groups, at least in the case of the whole linear group:

Theorem 7.6 (Bogopolski–Martino–Ventura [2]). *Any finite index subgroup of $GL_n(\mathbb{Z})$ is orbit decidable.*

Consequently,

Corollary 7.7 (Bogopolski–Martino–Ventura [2]). *Let $A_1, \dots, A_m \in GL_n(\mathbb{Z})$. If $\langle A_1, \dots, A_m \rangle$ has finite index in $GL_n(\mathbb{Z})$, then the \mathbb{Z}^n -by- F_m group $\mathbb{Z}^n \rtimes_{A_1, \dots, A_m} F_m$ has solvable conjugacy problem.*

Finally, the rank two case is again special:

Theorem 7.8 (Bogopolski–Martino–Ventura [2]). *Every finitely generated subgroup of $GL_2(\mathbb{Z})$ is orbit decidable.*

And hence,

Corollary 7.9 (Bogopolski–Martino–Ventura [2]). *All \mathbb{Z}^2 -by-free groups have solvable conjugacy problem.*

It is interesting to consider now the negative situation: are there orbit undecidable subgroups of $GL_n(\mathbb{Z})$? In other words, are there \mathbb{Z}^n -by-free groups with unsolvable conjugacy problem? Such groups, if they exist, would be a kind of Miller-type groups but with the base group being abelian.

Of course, in dimension $n = 2$ there are none, by the two previous results. However, Bogopolski–Martino–Ventura constructed such examples in dimensions 4 and above. Their existence is a direct consequence of Proposition 5.4: it is well known that F_2 embeds in $GL_2(\mathbb{Z})$ (in fact, $GL_2(\mathbb{Z})$ is virtually free), and so $F_2 \times F_2$ embeds in $GL_2(\mathbb{Z}) \times GL_2(\mathbb{Z}) \leq GL_4(\mathbb{Z}) \leq GL_n(\mathbb{Z})$ for $n \geq 4$; it is easy to find such an embedding admitting a vector $v \in \mathbb{Z}^4$ whose stabilizer intersects trivially with its image and so, by Proposition 5.4, one deduces the existence of orbit undecidable subgroups of $GL_n(\mathbb{Z})$ and, consequently, the existence of \mathbb{Z}^4 -by-free groups with unsolvable conjugacy problem:

Theorem 7.10 (Bogopolski–Martino–Ventura [2]). *For $n \geq 4$, $GL_n(\mathbb{Z})$ contains finitely generated orbit undecidable subgroups.*

Corollary 7.11 (Bogopolski–Martino–Ventura [2]). *There exist \mathbb{Z}^4 -by-free groups with unsolvable conjugacy problem.*

These groups are the first known examples of free abelian-by-free groups with unsolvable conjugacy problem. While having a quite different structure from Miller's examples, they are clearly reminiscent to them, but with a free abelian base group.

At this point it is worth mentioning the intriguing case of dimension 3, in which none of the above arguments work. The crucial fact in the proof of Theorem 7.8 is $GL_2(\mathbb{Z})$ being virtually free, while $GL_3(\mathbb{Z})$ is clearly not; on the other hand, the crucial fact in the proof of Theorem 7.10 is $F_2 \times F_2$ being a subgroup of $GL_n(\mathbb{Z})$ for $n \geq 4$, while it is known not to embed in $GL_3(\mathbb{Z})$. Hence, the two above arguments fail dramatically in the case of dimension 3 and, as far as we know, the question remains open.

Question 7.12. Do there exist finitely generated orbit undecidable subgroups of $GL_3(\mathbb{Z})$? In other words, do there exist \mathbb{Z}^3 -by-free groups with unsolvable conjugacy problem?

The examples of finitely generated orbit undecidable subgroups Γ of $GL_n(\mathbb{Z})$ provided by Theorem 7.10 are not finitely presented because they are build using Mihailova's construction. By modifying a little bit that construction, and at the cost of increasing the dimension by two extra units, Sunić–Ventura found in [29], for $n \geq 6$, new examples of finitely generated orbit undecidable subgroups $\Gamma \leq GL_n(\mathbb{Z})$ which are, additionally, free.

Proposition 7.13 (Sunić–Ventura [29]). *The group $Aut(F_d)$, for $d \geq 5$, and the group $GL_d(\mathbb{Z})$, for $d \geq 6$, both contain finitely generated, orbit undecidable, free subgroups.*

Question 7.14. Do $Aut(F_3)$, $Aut(F_4)$, $GL_3(\mathbb{Z})$, $GL_4(\mathbb{Z})$ and $GL_5(\mathbb{Z})$ contain finitely generated, orbit undecidable, free subgroups?

As an interesting side application of these last results, Sunić–Ventura constructed in [29] the first known examples of automaton groups with unsolvable conjugacy problem. Automaton groups are defined as those subgroups of the automorphism group of a regular rooted infinite tree generated by finite self-similar sets; many papers have been published these last years developing this new an interesting area (see [29] for a quick introduction and references). The word problem, for example, is solvable for all groups in this class, with a rather straightforward exponential time algorithm (several alternative better algorithms are known, working in polynomial time for certain specific subclasses). The question on solvability of the conjugacy problem was explicitly raised for the class of automaton groups by Grigorchuk–Nekrashevych–Sushchanskiĭ in [15], and solved in the negative direction by Sunić–Ventura in [29]:

Theorem 7.15 (Sunić–Ventura [29]). *There exist automaton groups with unsolvable conjugacy problem.*

The strategy followed was to observe that the implication to the right in Theorem 4.1 uses no hypothesis at all: in any short exact sequence, orbit decidability of the action subgroup is a subproblem of the conjugacy problem of the extension group. In particular,

Observation 7.16. *Let H be a finitely generated group, and let Γ be a finitely generated subgroup of $Aut(H)$. If $\Gamma \leq Aut(H)$ is orbit undecidable, then $H \rtimes \Gamma$ has unsolvable conjugacy problem.*

Then, the central part in [29] was dedicated to prove that $\mathbb{Z}^d \rtimes \Gamma$ is an automaton group for every finitely generated subgroup $\Gamma \leq GL_d(\mathbb{Z})$, using techniques from Brunner–Sidki. Now Corollary 7.11 completed the proof.

8 Extensions of other groups

In the recent paper [14], González-Meneses and Ventura consider the braid group B_n and solve $TCP(B_n)$. With a first superficial look, it may seem an easy problem because it is well known that $Out(B_n) \simeq C_2$, with the non-trivial element represented by the automorphism $\alpha: B_n \rightarrow B_n$ which inverts all generators, $\sigma_i \mapsto \sigma_i^{-1}$. However, the conjugacy problem twisted by this α (namely, solving the equation $(x\alpha)^{-1}ux = v$ for $x \in B_n$) becomes a quite delicate combinatorial problem about palindromic braids, see [14] for details.

Theorem 8.1 (González-Meneses–Ventura [14]). *The twisted conjugacy problem is solvable in the braid group.*

After that, the natural thing to do was to look at short exact sequences with $F = B_n$, and to study the conjugacy problem for extensions of B_n by free (or by torsion-free hyperbolic) groups, via Theorem 4.1. The result was fully positive, like in $GL_2(\mathbb{Z})$ or $Aut(F_2)$:

Theorem 8.2 (González-Meneses–Ventura [14]). *Every finitely generated subgroup $A \leq Aut(B_n)$ is orbit decidable.*

Corollary 8.3 (González-Meneses–Ventura [14]). *Every braid-by-free group $B_n \rtimes F_m$ has solvable conjugacy problem.*

Another successful situation was Thompson’s group F . Burillo–Matucci–Ventura, in the recent preprint [9], followed a similar project and solved the twisted conjugacy problem for this particular group $TCP(F)$.

Theorem 8.4. *Thompson’s group F has solvable twisted conjugacy problem.*

Here, the situation is different from the braid group since $Out(F)$ is quite big. However, it has been possible to solve the twisted conjugacy problem because, due to a result by M. Brin [7] saying that every automorphism of Thompson’s group F looks like a conjugation by an element from some extension of F . Thompson’s group F can be viewed as the subgroup of $PL_2(\mathbb{R})$ (this is the group of all piecewise-linear orientation preserving homeomorphisms of \mathbb{R} with a discrete set of breakpoints at dyadic rational points and such that all slopes are powers of 2) formed by all those elements f which, additionally, are eventually integral translations, i.e., which satisfy $f(t) = t + m_-$ and $f(t) = t + m_+$, respectively, for $t \ll 0$ and for $t \gg 0$. In this setting, one can look at the intermediate group $EP_2(\mathbb{R})$ of those elements $f \in PL_2(\mathbb{R})$ which are eventually periodic (i.e., such that $f(t - 1) = f(t) - 1$ for $t \ll 0$, and $f(t + 1) = f(t) + 1$ for $t \gg 0$). If we expand this last subgroup by forgetting the condition of orientation preserving (i.e., allowing decreasing maps), we get the group $\widetilde{EP}_2(\mathbb{R})$ which happens to be isomorphic to the automorphism group $Aut(F)$ of Thompson’s group F :

Theorem 8.5 (Brin [7]). *For Thompson’s group F , the map*

$$\begin{aligned} \widetilde{EP}_2 &\rightarrow Aut(F), & \tau &\mapsto \gamma_\tau : F \rightarrow F, \\ & & g &\mapsto \tau^{-1}g\tau, \end{aligned}$$

is well defined and it is a group isomorphism, so

$$Aut(F) \simeq \widetilde{EP}_2.$$

Furthermore, given $\varphi \in Aut(F)$ by the images of the standard generators, one can algorithmically compute the (unique) $\tau \in \widetilde{EP}_2$ such that $\varphi(g) = \tau^{-1}g\tau$ for all $g \in F$.

The good point of this result is that then, given an automorphism $\gamma_\tau \in Aut(F)$, the equation corresponding to the γ_τ -twisted conjugacy problem, namely $(x\gamma_\tau)^{-1}ux = v$, becomes the much simpler one $(\tau^{-1}x\tau)^{-1}ux = v$, i.e., $x^{-1}(\tau u)x = (\tau v)$. Hence, the twisted conjugacy problem for F reduces to the conjugacy problem in \widetilde{EP}_2 , allowing only conjugators from F . After dealing with non-easy technical problems of dynamic nature, Burillo–Matucci–Ventura overcame them, solving the twisted conjugacy problem for Thompson’s group F , see [9] for details.

The question about orbit decidability seems a bit more complicated. In [9] the authors were only able to prove that the full automorphism group $Aut(F)$ (as well as the subgroup of positive automorphisms $Aut_+(F)$) is orbit decidable assuming that a certain conjecture is true: the solvability of the simultaneous conjugacy problem for F . Partial results have been obtained by Bleak, Kassabov and Matucci on this matter, but the problem in general is still open, and so is the orbit decidability of $Aut(F)$.

On the other hand, Burillo–Matucci–Ventura proved in [9] that $F_2 \times F_2$ embeds in $Aut(F)$ and so, using Proposition 5.4, got the corresponding negative result:

Theorem 8.6. *There are extensions of Thompson’s group F by finitely generated free groups, with unsolvable conjugacy problem.*

To conclude this section, we refer the reader to a paragraph written in the introduction of [2]:

“In light of Theorem 4.1, it becomes interesting, first, to collect groups F where the twisted conjugacy problem can be solved. And then, for every such group F , to study the property of orbit decidability for subgroups of $\text{Aut}(F)$: every orbit decidable (undecidable) subgroup of $\text{Aut}(F)$ will correspond to extensions of F having solvable (unsolvable) conjugacy problem”.

We interpret this as an invitation to the (algorithmic oriented) reader to push this same project further into his/her own area of expertise: choose your favorite group G , and try to solve $\text{TCP}(G)$. This will not be a very interesting result by itself (it is just a technical variation of $\text{CP}(G)$), but it will pave the way, via Theorem 4.1, to study the CP in a vast collection of extensions of G : you will have chances to prove results of the type “all G -by-free groups have solvable CP”, or “there exists a G -by-free group with unsolvable CP”.

9 Variations on orbit decidability

The definition of orbit decidability admits variations, pointing to deeper algorithmic problems. We present here one of these possible variations that we find interesting. It is not totally clear, by the moment, whether is it related to some algebraic problem, like standard orbit decidability is related to the CP via Theorem 4.1. Even if it is not, the problems it provides are interesting enough by themselves.

Definition 9.1. Let G be a group, and $A \leq \text{Aut}(G)$. We say that A is (m -)subgroup orbit decidable, (m -)SOD for short, if there is an algorithm which, given $g, h_1, \dots, h_m \in G$, decides whether $g\alpha \in H = \langle h_1, \dots, h_m \rangle \leq G$ for some $\alpha \in A$.

Since in F_n , as well as in \mathbb{Z}^n , roots of elements are well defined and must be preserved by automorphisms (i.e., $x\alpha = y$ implies $\hat{x}\alpha = \hat{y}$), it is easy to see that, for every A , solvability of $\text{OD}(A)$ implies solvability of 1-SOD(A). However, m -SOD(A) for $m \geq 2$ looks like a much more complicated problem, even over the free abelian group.

Over the free group F_n , at least two special instances of this problem are solved in the literature. Silva–Weil solved in [28] the problem $\text{SOD}(\text{Aut}(F_2))$: given an element x and a subgroup H of the rank two free group F_2 , one can algorithmically decide whether $x\alpha \in H$ for some $\alpha \in \text{Aut}(F_2)$. Clifford–Goldstein [11] gave a complicated algorithm solving the particular case of $\text{SOD}(\text{Aut}(F_n))$ where the given input x is a primitive element: there is an algorithm deciding whether a given subgroup $H \leq F_n$ contains a primitive element of F_n . The rest of the problem $\text{SOD}(\text{Aut}(F_n))$ remains open, and nothing is known for other subgroups $A \leq \text{Aut}(F_n)$.

Over the free abelian group \mathbb{Z}^n , $\text{SOD}(\text{GL}_n(\mathbb{Z}))$ is an exercise (just a matter of greatest common divisors of the entries of the involved vectors). But, for a fixed given matrix $A \in \text{GL}_n(\mathbb{Z})$, the problem $\text{SOD}(\langle A \rangle)$ is much more interesting: after projectivizing \mathbb{Z}^n , the automorphism $A: \mathbb{Z}^n \rightarrow \mathbb{Z}^n$ induces a map $\varphi: \mathbb{P}^{n-1}(\mathbb{Z}) \rightarrow \mathbb{P}^{n-1}(\mathbb{Z})$ and $\text{SOD}(\langle A \rangle)$ becomes the problem of deciding whether a given orbit of φ intersects a given (projective) linear variety in $\mathbb{P}^{n-1}(\mathbb{Z})$ (for $n = 2$, this problem becomes a nice exercise in linear algebra, involving the eigenvalues of A).

Funding: The author acknowledges partial support from the Spanish Government through grant number MTM2011-25955.

References

- [1] O. Bogopolski, A. Martino, O. Maslakova and E. Ventura, Free-by-cyclic groups have solvable conjugacy problem, *Bull. Lond. Math. Soc.* **38** (2006), no. 5, 787–794.
- [2] O. Bogopolski, A. Martino and E. Ventura, Orbit decidability and the conjugacy problem for some extensions of groups, *Trans. Amer. Math. Soc.* **362** (2010), 2003–2036.

- [3] O. Bogopolski and O. Maslakova, A basis of the fixed point group of an automorphism of a free group, preprint (2012), versions 1 to 6, <http://arxiv.org/abs/1204.6728>.
- [4] O. Bogopolski and E. Ventura, On endomorphisms of torsion-free hyperbolic groups, *Internat. J. Algebra Comput.* **21** (2011), no. 8, 1415–1446.
- [5] V. V. Borisov, Simple examples of groups with unsolvable word problem (in Russian), *Mat. Zametki* **6** (1969), 521–532; translation in *Math. Notes* **6** (1969), 768–775.
- [6] M. Bridson and D. Groves, The quadratic isoperimetric inequality for mapping tori of free group automorphisms, *Mem. Amer. Math. Soc.* **203** (2010), no. 955.
- [7] M. G. Brin, The chameleon groups of Richard J. Thompson: Automorphisms and dynamics, *Publ. Math. Inst. Hautes Études Sci.* **84** (1997), 5–33.
- [8] P. Brinkmann, [Detecting automorphic orbits in free groups](#), *J. Algebra* **324** (2010), 1083–1097.
- [9] J. Burillo, F. Matucci and E. Ventura, The conjugacy problem for extensions of Thompson’s group, *Israel J. Math.*, to appear.
- [10] L. Ciobanu and A. Houcine, The monomorphism problem in free groups, *Arch. Math. (Basel)* **94** (2010), no. 5, 423–434.
- [11] A. Clifford and R. Goldstein, Subgroups of free groups and primitive elements, *J. Group Theory* **13** (2010), no. 4, 601–611.
- [12] F. Dahmani and V. Guirardel, The isomorphism problem for all hyperbolic groups, *Geom. Funct. Anal.* **21** (2011), no. 2, 223–300.
- [13] S. M. Gersten, On Whitehead’s algorithm, *Bull. Amer. Math. Soc. (N.S.)* **10** (1984), no. 2, 281–284.
- [14] J. González-Meneses and E. Ventura, Twisted conjugacy in the braid group, *Israel J. Math.*, to appear.
- [15] R. I. Grigorchuk, V. V. Nekrashevich and V. I. Sushchanskiĭ, Automata, dynamical systems, and groups, *Tr. Mat. Inst. Steklova* **231** (2000), 134–214.
- [16] G. Higman, B. H. Neumann and H. Neumann, Embedding theorem for groups, *J. Lond. Math. Soc.* **24** (1950), 247–254.
- [17] R. Kannan and R. Lipton, Polynomial-time algorithm for the orbit problem, *J. ACM* **33** (1986), no. 4, 808–821.
- [18] O. Kharlampovich and E. Ventura, A Whitehead algorithm for toral relatively hyperbolic groups, *Internat. J. Algebra Comput.* **22** (8) (2012), Article ID 1240004.
- [19] G. Levitt and K. Vogtmann, A Whitehead algorithm for surface groups, *Topology* **39** (2000), 1239–1251.
- [20] R. Lyndon and P. Schupp, *Combinatorial Group Theory*, Springer-Verlag, Berlin, 1977.
- [21] G. Makanin, Equations in free groups (in Russian), *Izv. Akad. Nauk SSSR Ser. Mat.* **46** (1982), 1190–1273.
- [22] O. Maslakova, Fixed point subgroup of an automorphism of a free group (in Russian), *Algebra Logika* **42** (2003), no. 4, 422–472.
- [23] J. McCool, A presentation for the automorphism group of a free group of finite rank, *J. Lond. Math. Soc. (2)* **8** (1974), 259–266.
- [24] K. A. Mihailova, The occurrence problem for direct products of groups, *Dokl. Acad. Nauk SSSR* **119** (1958), 1103–1105.
- [25] C. F. Miller III, *On Group-Theoretic Decision Problems and Their Classification*, Ann. of Math. Stud. 68, Princeton University Press, Princeton, 1971.
- [26] A. Ol’shanskii and M. Sapir, Groups with small Dehn functions and bipartite chord diagrams, *Geom. Funct. Anal.* **16** (2006), no. 6, 1324–1376.
- [27] V. N. Remeslennikov, Conjugacy in polycyclic groups (in Russian), *Algebra Logika* **8** (1969), 712–725; translation in *Algebra Logic* **8** (1969), 404–411.
- [28] P. Silva and P. Weil, Automorphic orbits in free groups: Words versus subgroups, *Internat. J. Algebra Comput.* **20** (2010), no. 4, 561–590.
- [29] Z. Sunić and E. Ventura, The conjugacy problem in automaton groups is not solvable, *J. Algebra* **364** (2012), 148–154.
- [30] J. Tits, [Free subgroups in linear groups](#), *J. Algebra* **20** (1972), 250–270.
- [31] J. H. C. Whitehead, On certain sets of elements in a free group, *Proc. Lond. Math. Soc. (2)* **41** (1936), 48–56.
- [32] J. H. C. Whitehead, On equivalent sets of elements in a free group, *Ann. of Math. (2)* **37** (1936), 782–800.

Received September 17, 2014.