J. Group Theory **24** (2021), 445–452
DOI 10.1515/jgth-2020-0030

Obstruction to a Higman embedding theorem for residually finite groups with solvable word problem

Emmanuel Rauzy*

Communicated by Pavel A. Zalesskii

Abstract. We prove that, for a finitely generated residually finite group, having solvable word problem is not a sufficient condition to be a subgroup of a finitely presented residually finite group. The obstruction is given by a residually finite group with solvable word problem for which there is no effective method that allows, given some non-identity element, to find a morphism onto a finite group in which this element has a non-trivial image. We also prove that the depth function of this group grows faster than any recursive function.

Introduction

It is well known that there can be no Higman embedding theorem for recursively presented finitely generated residually finite groups, that is to say, not all finitely generated recursively presented residually finite groups embed into finitely presented residually finite groups. Indeed, a theorem of McKinsey [3, 9, 11] states that all finitely presented residually finite groups have solvable word problem, while on the other hand several recursively presented residually finite groups are known that fail to have solvable word problem: for instance, one example was constructed by Meskin in [10], and one by Dyson in [4].

It was unknown whether or not the condition of having solvable word problem is sufficient for such embeddings to exist. For instance, in the article [7], the authors ask whether "unsolvability of the word problem is the only obstacle" to embed recursively presented residually finite groups into finitely presented residually finite groups. We answer that question negatively.

Theorem 1. *There exists a finitely generated residually finite group with solvable word problem, that does not embed in any finitely presented residually finite group.*

Call a group G *effectively residually finite* if there is an algorithm that takes a word w on the generators of G as input and, if $w \neq e$ in G, produces a morphism φ from G to a finite group F that satisfies $\varphi(w) \neq e$. What we actually prove here is the following theorem.

Theorem 2. *There exists a finitely generated residually finite group with solvable word problem, that is not effectively residually finite.*

Theorem 1 then follows from the following facts.

Fact 3. *A finitely presented residually finite group is effectively residually finite.*

Fact 4. *A finitely generated subgroup of an effectively residually finite group is itself effectively residually finite.*

Fact 3 follows from McKinsey's algorithm. It comes from the fact that a finitely presented group has computable finite quotients; see [12]. Fact 4 is straightforward.

In the first section, Dyson's groups are introduced, and they are used to reduce the proof of Theorem 2 to a problem about subsets of $\mathbb{Z}$. In the second section, this problem is solved. In the last section, we show that the group constructed in order to prove Theorem 2 has a depth function that grows faster than any recursive function.

Following [4], throughout, recursively presented groups will be called re groups (for recursively enumerable), and groups in which there is an algorithm that recognizes non-trivial elements will be called co-re groups. A group has solvable word problem if and only if it is re and co-re.

1 Dyson's groups

The author already used Dyson's groups to investigate the property of having computable finite quotients [12]. What we construct here is a strengthening of the result obtained in that article; we will include here all definitions but omit the proofs that already appear there.

Dyson's groups are amalgamated products of two lamplighter groups.

The lamplighter group L is the wreath product of $\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z}$, noted $\mathbb{Z} \wr \mathbb{Z}/2\mathbb{Z}$, which is by definition the semi-direct product $\mathbb{Z} \ltimes \bigoplus_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$, where $\mathbb{Z}$ acts on $\bigoplus_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$ by permuting the indices. It admits the following presentation:

$$\langle a, \varepsilon \mid \varepsilon^2,\ [\varepsilon, a^i \varepsilon a^{-i}],\ i \in \mathbb{Z}\rangle.$$

The element $a^i \varepsilon a^{-i}$ of L corresponds to the element of $\bigoplus_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$ with only one non-zero coordinate in position $i \in \mathbb{Z}$. We call it u_i. Consider another copy $\hat{L}$ of the lamplighter group; with an isomorphism, we write $g \mapsto \hat{g}$. For each subset $\mathcal{A}$ of $\mathbb{Z}$, define $L(\mathcal{A})$ to be the amalgamated product of L and $\hat{L}$, with $u_i = a^i \varepsilon a^{-i}$ identified with $\hat{u}_i = \hat{a}^i \hat{\varepsilon} \hat{a}^{-i}$ for each i in $\mathcal{A}$. It has the following presentation:

$$\langle a, \hat{a}, \varepsilon, \hat{\varepsilon} \mid \varepsilon^2,\ \hat{\varepsilon}^2,\ [\varepsilon, a^i \varepsilon a^{-i}],\ [\hat{\varepsilon}, \hat{a}^i \hat{\varepsilon} \hat{a}^{-i}],\ i \in \mathbb{Z},\ a^j \varepsilon a^{-j} = \hat{a}^j \hat{\varepsilon} \hat{a}^{-j},\ j \in \mathcal{A}\rangle$$

Whether the group $L(\mathcal{A})$ is residually finite depends on whether the set $\mathcal{A}$ is closed in the profinite topology on $\mathbb{Z}$. The profinite topology on a group G, which we denote by $\mathcal{PT}(G)$, is the topology defined by taking cosets of finite index normal subgroups as a basis for the open sets. Thus a subset $\mathcal{A}$ of $\mathbb{Z}$ is open in $\mathcal{PT}(\mathbb{Z})$ if and only if, for every n in $\mathcal{A}$, there exists an integer p such that $n + p\mathbb{Z} \subseteq \mathcal{A}$. The profinite topology on $\mathbb{Z}$ was rediscovered in 1955 by Furstenberg in [5] (the profinite topology on an arbitrary group was defined in 1950 in [6]), where it is used to give an elegant proof of the existence of infinitely many primes, and it was proven in [8] that this topology comes from a metric, which is given by the following formula:

$$\|x\| = \frac{1}{\sup\{n : 1|x, 2|x, 3|x, \ldots, n|x\}}, \quad d(x, y) = \|x - y\|.$$

The norm $\|x\|$ is thus the reciprocal of the greatest integer n with the property that $1, 2, \ldots, n$ all divide x. A sequence converges to 0 in that topology if and only if, for any integer k, there exists a point beyond which k divides all terms of the sequence. For instance, $n!$ goes to 0 as n goes to infinity. Define a function θ on the natural numbers by $\theta(n) = \operatorname{lcm}\{1, 2, 3, \ldots, n\}$. $\theta(n)$ is the smallest non-zero natural number such that $\|\theta(n)\| \leq \frac{1}{n}$. The closed ball of radius $\frac{1}{n}$ and centered in x, which is the set $\left\{y \in \mathbb{Z},\ d(x, y) \leq \frac{1}{n}\right\}$, is simply the set $x + \theta(n)\mathbb{Z}$. It is in fact also open. Call $\overline{B}(x, r)$ the closed ball centered in x and of radius r, and $B(x, r)$ the corresponding open ball (but note that the latter is not the interior of the former). The distance d is in fact ultrametric: for x, y and z integers, one has $d(x, z) \leq \max(d(x, y), d(y, z))$. This implies that each point of a ball can be taken as its center, and thus that if two balls intersect, one is contained in the other.

Of course, the distance d is effective: d is a recursive function. This implies that both the closed and open balls of $\mathcal{PT}(\mathbb{Z})$ are recursive sets.

Call an open set O *effectively open* (in $\mathcal{PT}(\mathbb{Z})$) if there is an effective procedure that, given any number n in O, computes some integer p such that $n + p\mathbb{Z}$ is contained in O. A set is *effectively closed* if its complement is effectively open.

We can now state the properties of the group $L(\mathcal{A})$ that will allow us to prove Theorem 2.

Proposition 5. *Let $\mathcal{A}$ be a subset of $\mathbb{Z}$.*

(1) $L(\mathcal{A})$ *is re, co-re or has solvable word problem if and only if $\mathcal{A}$ is respectively re, co-re or recursive.*

(2) $L(\mathcal{A})$ *is residually finite if and only if $\mathcal{A}$ is closed in $\mathcal{PT}(\mathbb{Z})$.*

(3) $L(\mathcal{A})$ *is effectively residually finite if and only if $\mathcal{A}$ is co-re and effectively closed in $\mathcal{PT}(\mathbb{Z})$.*

(1) and (2) were proved by Dyson in [4]. See also [12]. We prove here only the third point.

Proof. Suppose first that $L(\mathcal{A})$ is effectively residually finite. Then $L(\mathcal{A})$ is co-re, and by (1), $\mathcal{A}$ is co-re as well. Let x be an integer in the complement of $\mathcal{A}$ such that $u_x\hat{u}_x^{-1} \neq 1$ in $L(\mathcal{A})$. By our hypothesis, we can effectively find a morphism φ from $L(\mathcal{A})$ to a finite group F, with $\varphi(u_x\hat{u}_x^{-1}) \neq 1$ in F. Call N the product of the orders of the images of a and $\hat{a}$ in F. We then claim that $\mathcal{A} \cap (x + N\mathbb{Z}) = \varnothing$. Indeed, if it were not the case, there would exist an integer k such that $x + kN \in \mathcal{A}$, that is to say, such that $u_{x+kN} = \hat{u}_{x+kN}$ in $L(\mathcal{A})$. But then, this would imply

$$\begin{aligned}\varphi(u_x) &= \varphi(a)^{kN}\varphi(u_x)\varphi(a)^{-kN} = \varphi(a^{kN}u_xa^{-kN})\\ &= \varphi(u_{x+kN}) = \varphi(\hat{u}_{x+kN}).\end{aligned}$$

Because it can similarly be proved that $\varphi(\hat{u}_x) = \varphi(\hat{u}_{x+kN})$, this contradicts the assumption that $\varphi(u_x\hat{u}_x^{-1}) \neq 1$. Thus $\mathcal{A}$ does not meet $x + N\mathbb{Z}$.

The proof of the converse follows closely the proof of (2) given in [12] (which differs from the original proof of Dyson), as one only needs to see that the hypothesis that $\mathcal{A}$ is effectively closed in $\mathcal{PT}(\mathbb{Z})$ is enough to effectively carry out that proof. As we actually only use the first implication of (3) in the proof of Theorem 2, no further details are given here. □

From Proposition 5, to prove Theorem 2, it suffices to build $\mathcal{A}$ with the following properties: $\mathcal{A}$ is recursive, $\mathcal{A}$ is closed, but not effectively so.

2 Construction in $\mathbb{Z}$

Lemma 6. *There exists a recursive subset $\mathcal{A}$ of $\mathbb{Z}$, closed in $\mathcal{PT}(\mathbb{Z})$, but not effectively so.*

Proof. We construct a set $\mathcal{B}$, which will be the complement of the announced $\mathcal{A}$. Thus it has to be recursive and open but not effectively open.

Call p_n the n-th prime number. Define a sequence $(t_n)_{n\geq 0}$ by $t_n = p_1 \dots p_n$. This sequence is defined so that p_k divides t_n if and only if $k \geq n$. Note also that t_n divides t_{n+1}.

Consider an effective enumeration of all Turing machines: M_1 is the first machine, M_2 is the second, ... We will build $\mathcal{B}$ as a disjoint union of open sets X_n, each X_n being a neighborhood of t_n defined thanks to a run of the n-th Turing machine M_n. If this machine does not halt, X_n is a closed ball centered at t_n of radius $\frac{1}{t_{n+1}}$. If it halts, it is a finite union of balls, one of which is centered at t_n, the radius of which depends of the number of steps needed for M_n to halt. Thanks to this, information of the form "X_n contains a ball of radius r centered in t_n" will translate into "if M_n halts, it does so in less than N steps", where N can be computed from r.

Initialize $X_n = \{t_n\}$. Call $r_n = \frac{1}{t_{n+1}}$ and $m = \theta(t_{n+1})$ so that the closed ball $\overline{B}(t_n, r_n)$ is the set $t_n + m\mathbb{Z}$. Start a run of the machine M_n.

After each computation step of M_n, note k the number of steps already done in the computation and add, to X_n, $t_n + km$, $t_n - km$, as well as open balls centered in those numbers that are contained in $\overline{B}(t_n, r_n)$ and do not contain t_n. That is, we replace X_n by

$$X_n \cup B\Big(t_n + km, \frac{1}{2}d(t_n, t_n + km)\Big) \cup B\Big(t_n - km, \frac{1}{2}d(t_n, t_n - km)\Big).$$

Because the distance d is ultrametric, both balls $B(t_n + km, \frac{1}{2}d(t_n, t_n + km))$ and $B(t_n - km, \frac{1}{2}d(t_n, t_n - km))$ are contained in $\overline{B}(t_n, r_n)$.

If, at some point, the machine M_n halts, X_n consists of t_n and of finitely many open balls centered at points $t_n \pm km$. By construction, a point from $X_n \setminus \{t_n\}$ is at distance at least $\inf_k \big\{\frac{1}{2}d(t_n, t_n \pm km)\big\}$ from t_n. This infimum can be computed; call it r. Then compute the smallest natural number y such that $d(t_n, y) < r$, and call r' the distance $d(t_n, y)$. We then add to X_n the ball $B(u_n, r')$. This implies that X_n cannot contain any ball of center t_n and of radius strictly greater than r' because it does not contain y. In particular, any ball centered in t_n that contains one of the elements of the form $t_n \pm km$ that were added to X_n is not contained in X_n.

Of course, if the machine M_n does not halt, X_n will be the whole ball $\overline{B}(t_n, r_n)$.

This ends the definition of X_n, and $\mathcal{B}$ is defined as the union $\bigcup X_n$. This union is disjoint because, by the choice of the radius r_n, any element of X_n is divisible by p_n, but none is divisible by p_{n+1}. We now prove that $\mathcal{B}$ defined this way satisfies all three properties that appear in the statement of this lemma.

$\mathcal{B}$ is clearly open, because each X_n is open, whether or not the machine M_n halts.

$\mathcal{B}$ is a recursive set. It is obviously recursively enumerable because it was defined by an effective enumeration. To see that it is also co-re, let x be an integer; we want to decide whether x belongs to $\mathcal{B}$. By looking at the prime decomposition of x, one can find up to one n such that x might belong to X_n. Because X_n is always contained in $\overline{B}(t_n, r_n)$, if $d(t_n, x) > r_n$, x cannot be in X_n. Otherwise, it belongs to $\overline{B}(t_n, r_n) = t_n + m\mathbb{Z}$, and we can find k such that $x = t_n + km$. Then, if a run of M_n lasts more then k steps, automatically, x will belong to X_n. On the other hand, if M_n stops in less than k steps, X_n can be determined explicitly as a finite union of open balls, and thus the question of whether x belongs to X_n can be settled. Because the problem "does M_n halt in more then k steps" is a computable one, in either case, we will be able to determine whether or not x belongs to $\mathcal{B}$.

Finally, $\mathcal{B}$ is not effectively open. Suppose we have an algorithm that gives, for x in $\mathcal{B}$, an integer k such that $x + k\mathbb{Z}$ is contained in $\mathcal{B}$. Applying it to t_n, we can find a radius r such that $B(t_n, r)$ is contained in $\mathcal{B}$. We will show that this information implies a new information of the form: if the machine M_n halts, then it halts in less than N steps. This would of course allow one to solve the halting problem; thus such an algorithm does not exist.

Indeed, we have seen that if M_n halts in N steps, X_n cannot contain any ball centered in t_n that contains an element of the form $t_n \pm km$, with $k \leq N$. Turning this around, computing N such that $t_n + mN$ belongs to $B(t_n, r)$ (for instance, $N = \theta(\lceil \frac{1}{r} \rceil + 1)$), the information "$B(t_n, r)$ is contained in $\mathcal{B}$" implies that either M_n does not halt, or it halts in less then N steps.

This ends the proof of Lemma 6. □

What we do not know yet is whether the condition of being recursively presented and effectively residually finite, which is necessary to be a subgroup of a finitely presented residually finite group, is also sufficient. For instance, the strictly stronger condition of having computable finite quotients is not known to be unnecessary (see [12]).

3 Non-recursive depth function

In [1], Bou-Rabee introduced the *residual finiteness growth function*, or *depth function*, ρ_G, of a residually finite group G. To a natural number n, ρ_G associates the smallest number k such that, for any non-trivial element of length at most n in G, there exists a finite quotient of G of order at most k such that the image of this element in that quotient is non-trivial.

A finitely generated subgroup H of a finitely generated residually finite group G must have a depth function ρ_H that grows more slowly than that of G (see [1]). Because it is easy to see that a finitely presented residually finite group always has a recursive growth function, a subgroup of a finitely presented residually finite group must have its depth function bounded above by a recursive function. Note that, in [7], it was shown that finitely presented residually finite groups can have arbitrarily large recursive depth function. It was also known that the depth function of a residually finite group could grow arbitrarily fast (see [2]).

Note that an effectively residually finite group with solvable word problem always has its depth function bounded above by a recursive function.

Proposition 7. *Let $\mathcal{A}$ be the subset of $\mathbb{Z}$ given in Lemma* 6. *The depth function $\rho_{L(\mathcal{A})}$ of $L(\mathcal{A})$ cannot be smaller than a recursive function.*

Proof. Suppose there exists a recursive function f such that $\rho_{L(\mathcal{A})} \leq f$. Then, for each n which is not in $\mathcal{A}$, $u_n \hat{u}_n^{-1}$ is a non-identity element of $L(\mathcal{A})$, and thus it has a non-trivial image in a finite quotient F of size at most $f(4n+2)$ (because u_n and $\hat{u}_n$ are of word length $2n+1$). Now the orders of a and $\hat{a}$ in F both divide $f(4n+2)!$; thus F is a quotient of the quotient of $L(\mathcal{A})$ given by adding to it the two relations

$$a^{f(4n+2)!} = e \quad \text{and} \quad \hat{a}^{f(4n+2)!} = e$$

$$(\text{i.e. } \langle L(\mathcal{A}) \mid a^{f(4n+2)!}, \hat{a}^{f(4n+2)!} \rangle).$$

Thus, in this group as well, $u_n \hat{u}_n^{-1}$ is a non-identity element, and we know that this implies that $n + f(4n+2)!\,\mathbb{Z}$ does not meet $\mathcal{A}$ (see the proof of Proposition 5). This shows that $\mathcal{A}$ is effectively closed, contradicting our hypothesis. □

Bibliography

[1] K. Bou-Rabee, Quantifying residual finiteness, *J. Algebra* **323** (2010), no. 3, 729–737.

[2] K. Bou-Rabee and B. Seward, Arbitrarily large residual finiteness growth, *J. Reine Angew. Math.* **710** (2016), 199–204.

[3] V. H. Dyson, The word problem and residually finite groups, *Notices Amer. Math. Soc.* **11** (1964), 616–617.

[4] V. H. Dyson, A family of groups with nice word problems, *J. Aust. Math. Soc.* **17** (1974), 414–425.

[5] H. Furstenberg, On the infinitude of primes, *Amer. Math. Monthly* **62** (1955), 353.

[6] M. Hall, Jr., A topology for free groups and related groups, *Ann. of Math. (2)* **52** (1950), 127–139.

[7] O. Kharlampovich, A. Myasnikov and M. Sapir, Algorithmically complex residually finite groups, *Bull. Math. Sci.* **7** (2017), no. 2, 309–352.

[8] R. L. Lovas and I. Mezo, On an exotic topology of the integers, preprint (2010), `https://arxiv.org/abs/1008.0713`.

[9] J. C. C. McKinsey, The decision problem for some classes of sentences without quantifiers, *J. Symbolic Logic* **8** (1943), 61–76.

[10] S. Meskin, A finitely generated residually finite group with an unsolvable word problem, *Proc. Amer. Math. Soc.* **43** (1974), 8–10.

[11] A. W. O. Mostowski, On the decidability of some problems in special classes of groups, *Fund. Math.* **59** (1966), 123–135.

[12] E. Rauzy, Computability of finite quotients of finitely generated groups, preprint (2020), `https://arxiv.org/abs/2002.02541`.

Received February 22, 2020; revised September 16, 2020.

Author information

Corresponding author:
Emmanuel Rauzy, Institut Mathématique Jussieu-Paris Rive Gauche,
Université de Paris, UFR de Mathématiques, Bâtiment Sophie Germain,
8 place Aurélie Nemours, 75013 Paris, France.
E-mail: `emmanuel.rauzy.14@normalesup.org`