ON ISOMORPHISM TO A FREE GROUP AND BEYOND

VLADIMIR SHPILRAIN

Abstract. The isomorphism problem for infinite finitely presented groups is probably the hardest among standard algorithmic problems in group theory. It has been completely solved only in the classes of nilpotent groups, hyperbolic groups, and limit groups. In this short paper, we address the problem of isomorphism to particular groups, including free groups and subgroups of limit groups.

In memory of Ben Fine

1. Introduction

The isomorphism problem has been completely solved in the class of finitely generated nilpotent groups in [8].

Later, it was solved in the class of hyperbolic groups [15] (torsion-free case), [5] (general case), although it is difficult (if at all possible) to "computerize" these algorithms, i.e., to code them in one of the known programming languages.

Then, the isomorphism problem was also solved in the class of limit groups (a.k.a. fully residually free groups) [4].

In the class of finitely generated one-relator groups, although the isomorphism problem is still open in general, it has been settled for "most" one-relator groups (in a precise formal sense) in [9]. More specifically, for any $r \geq 2$, there is a subset $\mathcal{G}$ of elements of the free group F_r such that: (1) $\mathcal{G}$ has asymptotic density 1 in F_r; (2) it is algorithmically possible to find out whether or not a given element $u \in F_r$ is in $\mathcal{G}$; (3) for any two elements $u, v \in \mathcal{G}$, it is algorithmically possible to find out whether or not two one-relator groups (with the relators u and v, respectively) are isomorphic.

The "next in line" class of groups where the isomorphism problem may be solvable is the class of finitely presented metabelian groups (see [3], Problem (M1)), where "most" algorithmic problems have solutions by now [2].

We note that the isomorphism problem has a reasonable chance to be solvable only in classes of groups where all groups have solvable word problem. This rules out, for example, the class of finitely presented solvable groups of derived length ≥ 3 since this class has groups with unsolvable word problem [10].

In this paper, we address an apparently easier problem of isomorphism to a particular group. Using a simple trick, we establish here the following result that appears to be useful in some situations.

Proposition 1. *Let G be a group with n given generators. Suppose that G has solvable word problem. Let H be a finitely presented group, and suppose either G or H is Hopfian. If one can decide whether or not there is an epimorphism from G onto H and find it as an explicit map on the generators in case it exists, then one can decide whether or not G is isomorphic to H.*

Recall that a group is *Hopfian* if any *onto* endomorphism of this group is also one-to-one, i.e., is an automorphism. Note that in Proposition 1 we do not require that H has solvable word problem or that G is finitely presented.

Our main goal actually was to address the problem of isomorphism to the (absolutely) free group F_n of rank n. There is a classical result of Adyan [1] saying that given an arbitrary (finitely presented) group B, there is no algorithm that would decide, given any (finitely presented) group G, whether or not G is isomorphic to B. However, if we require solvability of the word problem in G, then the problem of isomorphism of G to the free group F_n becomes algorithmically solvable:

Theorem 1. *Let G be a finitely presented group with m generators and an algorithm for solving the word problem in G. Then it is algorithmically possible to find out whether or not G is isomorphic to a free group of rank $n \le m$.*

There is a "detour" that leads to this result, see [7, Corollary 4.3]. Specifically, there is an algorithm that, given a finitely presented group G with solvable word problem, decides whether or not G is a limit group [6]. If not, then G cannot be isomorphic to a free group because any finitely generated free group is a limit group. If G is a limit group, then one can use an algorithm, due to [4], that decides if there is an isomorphism between two limit groups.

Our proof is more straightforward, but it still uses a "big gun", namely Razborov's work on solving (systems of) equations in a free group.

It appears that solvability of equations in groups should inevitably be an important ingredient in any solution of the isomorphism problem for infinite groups. However, this is typically not enough. In our proof of Theorem 1, we actually establish an isomorphism (or non-isomorphism) of the group G to a subgroup of a given fixed finitely generated free group, and then we use the fact that every nontrivial subgroup of a free group is itself free. This is not the case with hyperbolic groups, say; moreover, a finitely generated subgroup of a hyperbolic group may not even be finitely presented, and this makes our method inapplicable in that situation. One class of groups where our method does work is the class of limit groups since every finitely generated subgroup of a limit group is a finitely presented limit group. Also, finitely generated limit groups are Hopfian because they are residually free and therefore residually finite. The following result may be of interest:

Theorem 2. *Let G be a finitely presented group with a given algorithm for solving the word problem in G. Let H be a limit group with a given algorithm for solving the word problem in H. Then it is algorithmically possible to find out whether or not G can be embedded in H.*

2. Proof of Proposition 1

Let $g_1, \ldots, g_n$ be the given generators of the group G, and $h_1, \ldots, h_n$ generators of the group H. Needless to say, if there is no epimorphism from G onto H, then G and H are not isomorphic.

Now suppose the map $\varphi : g_i \to h_i$ can be extended to an epimorphism from G onto H. Then run two algorithms in parallel:

1. Algorithm $\mathcal{A}$ will detect non-isomorphism by looking for an element in the kernel of φ. To that effect, it goes over nontrivial elements of G one at a time (this is possible since the word problem in G is solvable) and checks if φ takes them to the trivial element of H.

Here the reader may say: wait, you do not require that the word problem in H is solvable. Indeed, but here we only need the "yes" part of the word problem (i.e., detecting that the element is trivial), and this part works in any recursively presented group. Specifically, to detect that $w = 1$ one can go over all finite products of conjugates of defining relators and (graphically) compare them to w.

We note that if the kernel of φ is nontrivial, then H is isomorphic to a proper factor group of G and therefore cannot be isomorphic to G since we assumed that either G or H was Hopfian.

2. Algorithm $\mathcal{B}$ will detect isomorphism by looking for a map ψ, given on the generators h_i of H, such that $\psi(\varphi(g_i)) = g_i$ for all generators g_i of the group G. To that effect, $\mathcal{B}$ will go over n-tuples $(y_1, \ldots, y_n)$ of elements of G, one at a time, and define ψ by $\psi(h_i) = y_i$.

First check if ψ is a homomorphism by computing $\psi(r_j)$ for every defining relator r_j of the group H and checking if $\psi(r_j) = 1$. This is possible since G has solvable word problem, although we do not really need this because again, here we only need the "yes" part of the word problem.

If ψ is a homomorphism, then just check if $\psi(\varphi(g_i)) = g_i$ for all g_i, again using the "yes" part of the word problem in G. If H is isomorphic to G, then eventually a map ψ like that will be found.

Eventually one of the algorithms, $\mathcal{A}$ or $\mathcal{B}$, will stop and give an answer. □

We note that the only place in the proof where we used solvability of the word problem in G was where we were trying to detect non-isomorphism by looking for a nontrivial element in the kernel of φ.

3. Proof of Theorem 1

Let $g_1, \ldots, g_m$ be the given generators of the group G, and let $r_1, \ldots, r_s$ be all defining relators of G. Let F_n be a free group of rank n, and let $\alpha : g_i \to x_i$ for some $x_i \in F_n$, $i = 1, \ldots, m$. This map extends to a homomorphism $\alpha : G \to F_n$ if and only if $\alpha(r_j) = 1$ for all $j = 1, \ldots, s$. This translates into a system of s equations in the group F_n.

First, we will run Razborov's algorithm $\mathcal{R}$ [14] to see if this system of equations has a solution tuple $(a_1, \ldots, a_m)$ that generates a free subgroup of rank $r \geq n$ in F_n; in other words, if there is an epimorphism of G onto a free group of rank $r \geq n$. Denote this free group by H_r (recall that every nontrivial subgroup of a free group is free). If the system has no such solutions, then G is not isomorphic to a free group of rank n.

If there is an epimorphism of G onto H_r, then there is also an epimorphism of G onto a free group of rank n, denote this group by H_n. To find an explicit epimorphism of G onto H_n (as a map on the generators), one can first find generators of H_n and an epimorphism of H_r onto H_n by using Nielsen reduction, see e.g. [13].

After one finds an epimorphism of G onto H_n, Proposition 1 applies (since any finitely generated free group is Hopfian), and this completes the proof. □

We note that Razborov's results [14] were crucial for this proof. We also note that we used not only an algorithm for solving systems of equations in a free group, but also the fact (due to [14] as well) that it is algorithmically possible to find a subgroup of F_n of the maximum rank generated by a solution tuple of the given system of equations.

4. Proof of Theorem 2

For the most part, the proof is similar to that of Theorem 1. Again, let $g_1, \ldots, g_m$ be the given generators of the group G, and Let $r_1, \ldots, r_s$ be all defining relators of G. Let $\alpha : g_i \to x_i$ for some $x_i \in H$. This map extends to a homomorphism $\alpha : G \to H$ if and only if $\alpha(r_i) = 1$ for all $i = 1, \ldots, s$. This translates into a system of s equations in the group H.

There are known algorithms for solving systems of equations in limit groups (see e.g. [11]). Moreover, the results of [11] imply that in a limit group H, different m-tuples of solutions of a system of equations generate only finitely many subgroups H_i of the group H up to isomorphism, and a (finite) presentation of each subgroup H_i can be algorithmically computed according to [12, Theorem 30].

We will therefore first run an algorithm from [11] to see if the system of equations mentioned in the first paragraph of this section has solutions. If not, then G cannot be embedded in H. If it does have solutions, then we find generating m-tuples $(h_{i1}, \ldots, h_{im})$ of subgroups H_i. Then, using an algorithm from [11], we find (finitely many) defining relations for each subgroup H_i representing an isomorphism class mentioned in the previous paragraph.

Thus, if G can be embedded in H, it should be isomorphic to one of the subgroups H_i. Suppose there are k of them. We will then run k algorithms $\mathcal{C}_i$ in parallel, where each $\mathcal{C}_i$, in turn, is a pair of algorithms $(\mathcal{A}_i, \mathcal{B}_i)$ running in parallel.

As in the proof of Theorem 1, algorithm $\mathcal{A}_i$ will detect non-isomorphism by looking for a nontrivial element in the kernel of $\varphi : g_j \to h_{ij}$. If the kernel is nontrivial, then the subgroup H_i is isomorphic to a proper factor group of the group G and therefore cannot be isomorphic to G itself because all finitely generated subgroups of a limit group are Hopfian.

At the same time, algorithm $\mathcal{B}_i$ will detect isomorphism of the subgroup H_i to the group G by looking for a map ψ, given on the generators h_{ij} of H_i, such that $\psi(\varphi(g_i)) = g_i$ for all generators g_i of the group G. This is done the same way as in the proof of Theorem 1, but there is one more ingredient needed here. To check if ψ is a homomorphism, we see if ψ takes each defining relation of H_i to the identity element of G.

Eventually one of the algorithms, $\mathcal{A}$ or $\mathcal{B}$, will stop and give an answer about isomorphism (or non-isomorphism) of H_i to G.

Acknowledgement. I am grateful to Olga Kharlampovich and Alexei Myasnikov for useful discussions on equations in groups and on various properties of limit groups.

References

[1] S. I. Adyan, *Algorithmic unsolvability of problems of recognition of certain properties of groups*, Dokl. Akad. Nauk SSSR **103** (1955), 533–535.

[2] G. Baumslag, F. Cannonito, D. Robinson, *The algorithmic theory of finitely generated metabelian groups*, Trans. Amer. Math. Soc. **344** (1994), 629–648.

[3] G. Baumslag, A. G. Myasnikov, V. Shpilrain, *Open problems in combinatorial group theory. Second edition*, Contemp. Math., Amer. Math. Soc. **296** (2002), 1–38.

[4] I. Bumagin, O. Kharlampovich, A. Miasnikov, *The isomorphism problem for finitely generated fully residually free groups*, J. Pure Appl. Algebra **208** (2007), 961–977.

[5] F. Dahmani, V. Guirardel, *The isomorphism problem for all hyperbolic groups*, Geom. Funct. Anal. **21** (2011), 223–300.

[6] D. Groves, *Limit groups for relatively hyperbolic groups, I: The basic tools*, Algebr. Geom. Topol. **9** (2009), 1423–1466.

[7] D. Groves, H. Wilton, *Enumerating limit groups*, Groups Geom. Dyn. **3** (2009), 389–399.

[8] F. Grunewald, D. Segal, *Some general algorithms II. Nilpotent groups*, Ann. of Math. **112** (1980), 585–617.

[9] I. Kapovich, P. Schupp, V. Shpilrain, *Generic properties of Whitehead's algorithm and isomorphism rigidity of random one-relator groups*, Pacific J. Math. **223** (2006), 113–140.

[10] O. G. Kharlampovich, *A finitely presented solvable group with unsolvable word problem.* (Russian) Izv. Akad. Nauk SSSR Ser. Mat. **45** (1981), 852–873.

[11] O. G. Kharlampovich, A. Myasnikov, V. N. Remeslennikov, D. Serbin, *Subgroups of fully residually free groups: algorithmic problems*, in: Group theory, statistics, and cryptography, Contemp. Math. Amer. Math. Soc. **360** (2004), 63–101.

[12] O. G. Kharlampovich, A. Myasnikov, *Elementary theory of free non-abelian groups*, J. Algebra **302** (2006), 451–552.

[13] R. Lyndon, P. Schupp, *Combinatorial Group Theory*, (Reprint of the 1977 edition). In *Classics in Mathematics*, Springer-Verlag, Berlin (2001).

[14] A. A. Razborov, *Systems of equations in a free group*, Izv. Akad. Nauk SSSR Ser. Mat. **48** (1984), 779–832.

[15] Z. Sela, *The isomorphism problem for hyperbolic groups. I*, Ann. of Math. **141** (1995), 217–283.

Department of Mathematics, The City College of New York, New York, NY 10031
Email address: shpilrain@yahoo.com