

Algorithmically Insoluble Problems about Finitely Presented Solvable Groups, Lie and Associative Algebras, II

GILBERT BAUMSLAG,* DION GILDENHUYS,[†] AND RALPH STREBEL[‡]

**Department of Mathematics, CCNY, New York, New York 10031, USA;* [†]*Department of Mathematics and Statistics, McGill University, Montreal, Canada;* and [‡]*Department of Mathematics, E.T.H., Zurich, Switzerland*

Communicated by Marshall Hall

Received October 9, 1983

1. INTRODUCTION

1.1. In 1955 Novikov [11] constructed a finitely presented group with an insoluble word problem (cf. Miller [10] and also Boone [8]). Shortly afterwards, first Adyan [1-4] and then Rabin [13, 14] used this group of Novikov to prove that for every one of a host of group-theoretic properties, there is no algorithm whereby one can decide whether any finitely presented group has such a property. In particular, there is no algorithm whereby one can decide whether any finitely presented group is of order 1. Thus the isomorphism problem for finitely presented groups is algorithmically insoluble. These negative results were followed in 1959 by a number of similar ones concerned with elements and subgroups of finitely presented groups (Baumslag, Boone and Neumann [5]). Thus, for example, there is no algorithm whereby one can decide whether or not any element in a (suitably chosen) finitely presented group is a proper power.

In 1981 Harlampovich [9] constructed a finitely presented solvable group (of derived length 3) with an insoluble word problem. This then raised the possibility that many of the results cited above for finitely presented groups can be carried over to finitely presented solvable groups. It is not possible to carry over these results en masse to finitely presented solvable groups, since it is easy to decide whether any finitely presented solvable group is of order 1. Indeed there is an algorithm whereby one can determine whether any finitely presented solvable group is polycyclic (Baumslag, Cannonito and Miller [6]); again, no such algorithm exists for finitely presented groups as a whole (Adyan [2]). The methods employed previously cannot be applied to solvable groups because the constructions

used always produce non-cyclic free subgroups. Thus it is not clear how to exploit Harlampovich's example in order to prove further negative algorithmic results about finitely presented solvable groups.

In the first of this series of papers we constructed some new finitely presented solvable groups with insoluble word problem, which differ in several important respects from Harlampovich's group. These groups do lend themselves to the applications that we have been discussing. It is with these, for the most part easy, applications that this paper is concerned.

1.2. To begin with we shall prove:

THEOREM 1. *There is a recursive class of finitely presented solvable groups (of derived length 3) with insoluble isomorphism problem; that is to say there is no algorithm whereby one can determine whether or not any pair of groups in the class are isomorphic.*

Next we have:

THEOREM 2. *There is a recursive class of finitely presented solvable groups, each of which is either of derived length 3 or of derived length 4, such that there is no algorithm whereby one can decide whether any of these groups is of derived length 3.*

The upshot of Theorem 2 is that the information that a finitely presented group is solvable is insufficient for an algorithmic determination of its derived length. This answers a question raised by F. B. Cannonito a few years ago.

Another negative result is the following.

THEOREM 3. *There is a recursive class of finitely presented solvable groups of derived length 3, such that there is no algorithm whereby one can determine whether any group in the class is directly decomposable.*

The above theorems involve classes of solvable groups. Our final theorem is concerned with a single group.

THEOREM 4. *There is a finitely presented solvable group G of derived length 3, such that there is no algorithm whereby one can determine whether any word in the given generators represents*

- (i) *an element of the center of G ;*
- (ii) *an element that commutes with a given element of G ;*
- (iii) *an n th power, where $n > 1$ is an integer;*
- (iv) *a proper power.*

Furthermore, there is no algorithm whereby one can decide whether any given automorphism of G is either trivial or inner.

1.3. There are two simple constructions which we use in the proofs of the above theorems. The first is the so-called central product and the second is the standard wreath product. The rest of this paper is arranged as follows. Theorems 1 and 2 are proved in Section 2, Theorem 3 is proved in Section 3 and Theorem 4 is proved in Section 4.

It should be pointed out, in closing, that there are many algorithmic problems about finitely presented solvable groups that we have been unable to answer here (cf., e.g., [5, 14, 10]).

2. THE PROOFS OF THEOREMS 1 AND 2

2.1. *A Variation of Harlampovich's Example*

In the first of this series of papers we constructed an infinite family of finitely presented solvable groups with insoluble word problem [7]. It suffices for our needs here to concentrate on one such group U , say. U is a finitely presented solvable group of derived length 3 with the following properties. First of all there is a recursive set of words w_1, w_2, \dots (in the given generators of U) such that there is no algorithm whereby one can decide whether or not any of these words take on the value 1 in U . Second, each such word w_i represents an element in the center of U . Third, $w_i^p = 1$ in U , for $i = 1, 2, \dots$, where p is a fixed prime used initially in the definition of U . Finally, U can be decomposed into a semidirect product

$$U = P \rtimes A,$$

where P is a group of exponent dividing p^2 and A is torsion-free abelian. Thus the p -subgroups of U are all of exponent dividing p^2 .

We are now in a position to begin the proof of Theorem 1.

2.2. *The Proof of Theorem 1*

We shall make use here of the following group:

$$Q = \langle a, t; a^p = 1, t^p = 1, t^{-1}at = a^{1+p} \rangle.$$

Thus Q is a group of order p^5 , a is of order p^3 and t is of order p^2 . It is easy to check that $b = a^{p^2}$ is in the center of Q .

We now put

$$U_i = (U \times Q) / \text{gp}(\langle w_i, b^{-1} \rangle) \quad (i = 1, 2, \dots).$$

Here $U \times Q$ denotes the direct product of U and Q , whose elements are denoted by the pairs (u, q) ($u \in U, q \in Q$). Note that (w_i, b^{-1}) is central in $U \times Q$ and so $\text{gp}((w_i, b^{-1}))$ is normal in $U \times Q$. Observe that if $w_i \neq 1$, then w_i is of order p and U_i is the central product of U and Q with w_i identified with b . Therefore if $w_i \neq 1$, then the canonical maps of U and Q into U_i are injections. So if $w_i \neq 1$, then U_i contains a cyclic subgroup of order p^3 . Hence

$$U_i \cong U \times Q / \text{gp}(b) \quad \text{if and only if } w_i = 1.$$

This means that if there is an algorithm which decides whether or not any pair of the groups U_i are isomorphic, then there is an algorithm which decides whether or not any word w_i is equal to 1 in U . This proves Theorem 1.

2.3. *The Proof of Theorem 2*

Theorem 2 is proved in much the same way as Theorem 1. We, however, need to replace the group Q by another p -group, designed with the proof of Theorem 2 in mind. To this end let R be the group of all lower unitriangular 9×9 matrices over the field \mathbb{F}_p of p elements. It is easy to check that R is solvable of derived length 4. Moreover the third derived group R''' is generated by

$$c = 1 + e_{91},$$

where here 1 is the identity matrix and e_{91} is the 9×9 matrix with 1 in the $((9, 1)$ th place and 0's elsewhere. Thus R''' is actually the center of the group R .

Now, as before, let us put

$$V_i = (U \times R) / \text{gp}((w_i, c^{-1})) \quad (i = 1, 2, \dots).$$

Then V_i is of derived length 3 if and only if $w_i = 1$. This then proves Theorem 2.

3. THE PROOF OF THEOREM 3

3.1. *Decomposing Finitely Presented Solvable Groups*

We shall use the following notation here. $\zeta(G)$ denotes the center of the group G ; if x and y are elements of G , then we put

$$x^{-1}y^{-1}xy = [x, y], \quad x^{-1}yx = y^x.$$

Now let U be as before and let

$$W = U \wr T$$

be the standard wreath product of U by T , where T is a group of order p with generator t . We recall that W is generated by its subgroups U and T and that the conjugates

$$U(i) = t^{-i}Ut^i \quad (i = 0, 1, \dots, p-1)$$

of U by the powers of t generate their direct product. If $u \in U$, we put

$$u(i) = u^{t^i} \quad (i = 0, 1, \dots, p-1)$$

and define

$$\delta(u) = u(0)u(1) \cdots u(p-1).$$

Note that if $u \in \zeta(U)$, then $\delta(u) \in \zeta(W)$. So if

$$X = \langle x; x^{p^2} = 1 \rangle$$

is a cyclic group of order p^2 , then (see Section 2.1)

$$Y(i) = \text{gp}((\delta(w_i), x^{-i^{p^2}})) \quad (i = 1, 2, \dots).$$

is a central subgroup of the direct product $W \times X$ of W and X . We now put

$$W_i = (W \times X) / Y(i) \quad (i = 1, 2, \dots).$$

It is clear that if $w_i = 1$, then

$$W_i = W \times X / \text{gp}(x^{p^2})$$

is directly decomposable.

Our final objective is to prove that if $w_i \neq 1$, then W_i is directly indecomposable. The proof, although a little tedious, is easy enough.

Let us suppose then from now on that $w_i \neq 1$. We identify W and X with their canonical images in W_i and so view W_i as a group which is actually generated by W and X .

Next let us suppose that

$$W_i = E \times F,$$

where E and F are subgroups of W_i . We will prove that either E or F is the identity subgroup of W_i . To this end, put

$$S = \text{gp}(U(0), U(1), \dots, U(p-1), X).$$

Then every element $a \in W_i$ can be written in the form

$$a = t^m s \quad (s \in S).$$

Consider the direct decomposition of the element t in terms of an element of E and an element of F :

$$t = t^m r \cdot t^m s \quad (t^m r \in E, t^m s \in F, r, s \in S). \quad (1)$$

We may assume without loss of generality that $0 < m < p$. If $0 < n < p$ then $tr' \in E$ and $ts' \in F$ for some $r', s' \in S$. Now if $u \in U$, then

$$E \ni [te', u], \quad F \ni [ts', u].$$

In particular, if $u \in \zeta(U)$, $u \neq 1$, it follows that

$$1 \neq u(0)^{-1}u(1) \in E \cap F,$$

a contradiction. Thus $0 < n < p$ is impossible. Hence the decomposition (1) can be re-expressed as

$$t = tr \cdot r^{-1} \quad (tr \in E, r \in F, r \in S).$$

Clearly r centralises t . Hence

$$(tr)^p = t^p r^p = r^p \in E \cap F.$$

Therefore $r^p = 1$. Now E contains all elements of the form

$$[(tr)^i, u] = r^{-i}u(t)^{-1}r^i u(0).$$

If $u \in \zeta(U)$, it follows that

$$u(t)^{-1}u(0) \in E.$$

So

$$\delta(u)E = u(0)^p E.$$

One of the properties of the group U that we have not yet mentioned is that its center is of exponent p . Hence $u(0)^p = 1$. This means that

$$\delta(u) \in E \quad \text{if } u \in \zeta(U).$$

Suppose next that F contains a non-central element v , say. Since $[tr, v] = 1$ and $r^p = 1$, v must take the form

$$v = a(0) a(1)^r \cdots a(p-1)^{r^{p-1}} x' \quad (a \in U).$$

Since v is not central, $a \notin \zeta(U)$. Let b an element of U which does not commute with a . Now $E \ni [b, tr]$ and so

$$[[b, tr], v] = 1.$$

Since $[b, tr] = b(0)^{-1} \cdot r^{-1}b(1)r$ this implies that $[b, a] = 1$ after all. Therefore the elements of F are all of the form

$$\delta(u)x' \quad (u \in \zeta(U)).$$

Now

$$x^p = \delta(w_i) \in E.$$

Hence

$$(\delta(u)x')^p = (x^p)^l \in E \cap F.$$

Thus l is divisible by p and therefore

$$\delta(u)x' \in E.$$

This implies that $\delta(u)x' = 1$, i.e., that $F = 1$ as desired.

4. THE PROOF OF THEOREM 4

4.1. Problems about Elements and Automorphisms of Finitely Presented Solvable Groups

It follows easily from the methods developed in [7] that, for each prime p , there exists a finitely presented solvable group V_p , with the following properties. Firstly V_p is an extension of an abelian group of exponent p by a torsion-free metabelian group. Secondly, there exists a recursive set of words w_1, w_2, \dots , in the given generators of V_p , such that there is not algorithm whereby one can decide whether or not of these words takes on the value 1 in V_p . Thirdly, w_1, w_2, \dots represent central elements of V_p . Finally $w_i^p = 1$ in V_p , $i = 1, 2, \dots$.

Now suppose $n > 1$ is a given integer and that p is a prime divisor of n . Let Y be a group of order 2 with generator y and let Z be an infinite cyclic group with generator z . Furthermore, let $W = V_p \wr Y$ and let G be the direct product of W and Z :

$$G = W \times Z.$$

As in Section 3 we will view W and Z as subgroups of G .

Now $[w_i, y] = 1$ if and only if $w_i = 1$. Hence w_i is central in G if and only if $w_i = 1$. So we have proved both (i) and (ii) of Theorem 4. Next observe that $w_i z^n$ is an n th power if and only if $w_i = 1$. This proves (iii).

Similarly $w_i z^p$ is a proper power if and only if $w_i = 1$. This proves (iv). Finally observe that the automorphism φ_i of G defined by

$$\varphi_i: a \mapsto a \quad (a \in G), \quad z \mapsto w_i z \quad (i = 1, 2, \dots),$$

is inner if and only if $w_i = 1$. And φ_i is the identity automorphism if and only if $w_i = 1$. This then completes the proof of Theorem 4.

ACKNOWLEDGMENT

The first author thanks the N.S.F. for their support.

REFERENCES

1. S. I. ADYAN, Algorithmic unsolvability of problems of recognition of certain properties of groups, *Dokl. Akad. Nauk SSSR (N.S.)* **103** (1955), 533-535.
2. S. I. ADYAN, Unsolvability of some algorithmic problems in the theory of groups, *Trudy Moskov Math. Obshch.* **6** (1957), 231-298.
3. S. I. ADYAN, Finitely presented groups and algorithms, *Dokl. Akad. Nauk SSSR (N.S.)* **117** (1957), 9-12.
4. S. I. ADYAN, On algorithmic problems in effectively complete classes of groups, *Dokl. Akad. Nauk SSSR* **123** (1958), 13-16.
5. G. BAUMSLAG, W. W. BOONE, AND B. H. NEUMANN, Som unsolvable problems about elements and subgroups of groups, *Math. Scand.* **7** (1959), 191-201.
6. G. BAUMSLAG, B. CANNONITO, AND C. F. MILLER, Some recognizable properties of solvable groups, *Math. Z.* **178** (1981), 1-7.
7. G. BAUMSLAG, D. GILDENHUYIS, AND R. STREBEL, Algorithmically insoluble problems about finitely presented solvable groups and Lie algebras, *J. Pure and Applied Algebra* (1985), to appear.
8. W. W. BOONE, Certain simple, unsolvable problems of groups theory, V, VI, *Nederl. Akad. Wetensch. Proc. Ser. A* **60; Indag. Math.** **19** (1957), 22-27, 227-232.
9. O. G. HARLAMPOVICH, A finitely presented solvable group with insoluble equality problem, *Izv. Akad. Nauk Ser. Mat.* **45**, No. 4 (1981), 852-873.
10. C. F. MILLER, "On Group-Theoretic Decision Problems and Their Classification," *Annals of Mathematics Studies*, No. 68, Princeton Univ. Press, Princeton, N. J., 1971.
11. P. S. NOVIKOV, On algorithmic unsolvability of the problem of identity, *Doklady Akad. Nauk SSSR (N.S.)* **85** (1952), 709-712.
12. P. S. NOVIKOV, "On the Algorithmic Unsolvability of the Word Problem in Group Theory," *Trudy Mat. Inst. im. Steklov.* No. 44, Izdat. Akad. Nauk SSSR, Moscow, 1955.
13. M. O. RABIN, Recursive unsolvability of group theoretic problems, *Bull. Amer. Math. Soc.* **62** (1956), 396.
14. M. O. RABIN, Recursive unsolvability of group theoretic problems, *Ann. Of Math.* **67** (1958), 172-194.