FINITELY PRESENTED GROUPS AND ALGORITHMS

1957

SovietRxiv

Abstract

Full Text

MATHEMATICS

S. I. Adian

FINITELY PRESENTED GROUPS AND ALGORITHMS

(Presented by Academician I. M. Vinogradov on 7 V 1957)

A group F is called **finitely presented** if it can be given by a finite number of generators and defining relations. A group property α is called **invariant** if, whenever it holds in a group F, it also holds in every group F_1 isomorphic to the group F.

In ([3]) the impossibility of recognition algorithms was proved for certain classes of invariant properties of finitely presented groups. A. A. Markov proved the impossibility of recognition algorithms for a very broad class of properties of associative calculi ([2]). The first part of the present work is a continuation of ([3]). A theorem is proved analogous to A. A. Markov' s theorem for associative calculi.

Theorem 1. *Let α be some invariant group property. If there exist both a finitely presented group F_1 possessing the property α, and a finitely presented group F_2 which is not embeddable in any finitely presented group with this property, then no algorithm is possible which determines, for every finitely presented group F, whether or not it possesses the property α.*

In ([1]) P. S. Novikov constructed a finitely presented group with an unsolvable identity problem. Let this group, which we denote by F_0, be given by generators $a_1, a_2, \dots, a_n$ and defining relations*

$$A_i = A_i'. \tag{1}$$

In the proof of Theorem 1 the following fact is used: the group F_0 has no torsion (the latter is not proved in ([1]), but can be proved without particular difficulty on the basis of ([1])).

The following lemma is almost obvious.

Lemma 1. *Every finitely presented group F_2 is isomorphically embedded in a finitely presented group F_2' given by a system of generators all of which have infinite order.*

Let the group F_2', into which the finitely presented group F_2 satisfying the condition of Theorem 1 is isomorphically embedded, be given by generators

$b_1, b_2, \dots, b_m$ and defining relations

$$B_j = B'_j. \tag{2}$$

By F we denote the free product

$$F = F_0 * F'_2 * F_3,$$

where F_3 is the free group with one generator p.

---

* In specifying a finitely presented group we shall always write out only the positive alphabet and the nontrivial defining relations, i.e. relations which do not hold in the free group.

The group F is defined by the generators

$$a_1,\ a_2, \dots,\ a_n,\ b_1,\ b_2, \dots,\ b_m,\ p \tag{3}$$

and by the defining relations (1) and (2).

We shall call two letters of the alphabet (3) **of the same type** if either both are generators of the group F_0, or both are generators of the group F'_2. Otherwise they are called **of different types**.

Lemma 2. *Any two letters of different types in the alphabet of the group F are free generators of the subgroup generated by them in F.*

Lemma 3. *The alphabet of the group F can be arranged in a sequence with repetitions*

$$e_1, e_2, e_3, \dots, e_k, \tag{4}$$

having the following properties: 1) the collection of letters standing in (4) in odd positions up to e_{k-2} constitutes the whole alphabet (3); 2) the letters e_i and e_{i+2} are of different types, and the letters e_k and e_{k-1} are of different types and are distinct from the letter p.

The defining relations of the group F may be written in the alphabet (4). In doing so it will be necessary to add a number of relations of the form $e_i = e_j$, which will reflect the repetition of letters in (4).

Let the defining relations of the group F in the alphabet (4) be

$$C_\nu = D_\nu. \tag{5}$$

Consider an arbitrary word A of the group F containing neither the letters p nor p^{-1}. To each word of this kind we shall assign a finitely defined group, which we shall denote by F_{qA}.

The positive alphabet of the group F_{qA} is obtained by adjoining to the alphabet (4) k new letters $q_1, q_2, \dots, q_k$. As defining relations of the group F_{qA} we take all relations (5), adding to them the following relations:

$$q_i q_{i+1} = q_{i+1} e_i \quad (i = 1, 2, \dots, k-1); \tag{6}$$

$$e_{2j-1} q_{2j-1} = q_{2j-1} E \quad \left(j = 1, 2, \dots, \left[\frac{k-1}{2} \right] \right); \tag{7}$$

$$e_k q_k E = q_k e_k q_k^{-1}. \tag{8}$$

Main lemma. *If $A = 1$ in the group F, then the corresponding group F_{qA} is trivial. If the word A has infinite order in the group F, then the group F is a subgroup of the group F_{qA}.*

The first part of this lemma is easily proved on the basis of relations (6), (7), (8) and Lemma 3. The proof of the second part is difficult and constitutes the main difficulty of the present work.

Using the main lemma, it is not hard to prove Theorem 1.

To each word A of the group F_0 we assign the finitely defined group

$$F'_{qA} = F_{qA} * F_1,$$

where F_{qA} is the group constructed above from the word A; F_1 is a finitely defined group with property α, whose existence is guaranteed by Theorem 1.

We have obtained a certain class of finitely defined groups. If $A = 1$ in F_0, then $A = 1$ in F, and, by the main lemma, the group F_{qA} is trivial. Then F'_{qA} is isomorphic to the group F_1, and the invariant property α is satisfied in the group F'_{qA}.

Suppose $A \neq 1$ in F_0. Then the word A has infinite order in F_0, since F_0 is a torsion-free group. Consequently, the word A has infinite order in F. By the main lemma, the group F is a subgroup of the group F_{qA}, and therefore also of the group F'_{qA}. The group F has a subgroup F'_2, po-

the latter in turn contains the subgroup F_2. Since, by the hypothesis of Theorem 1, the group F_2 cannot be embedded in any finitely presented group with property α, the group F'_{qA} does not have property α. By virtue of the undecidability of the identity problem in the group F_0, there is no algorithm which, for each group F'_{qA}, determines whether or not property α holds in it. Theorem 1 is proved.

The condition of Theorem 1 cannot be weakened by replacing the requirement that there exist a finitely presented group not embeddable in any finitely presented group with property α by the requirement that there exist a finitely presented group not having property α. Indeed, there exist both finitely presented groups that coincide with their commutator subgroup and finitely presented groups that do not coincide with their commutator subgroup. At the same time, there is an algorithm which determines, for an arbitrary finitely presented group, whether it coincides with its commutator subgroup or not. This is an algorithm solving the identity problem for commutative groups.

We note that this same algorithm makes it possible, for an arbitrary finitely presented solvable (or arbitrary nilpotent) group, to determine whether it is the trivial group or not. This is all the more interesting because the identity problem for solvable groups has not been solved.

Each invariant property α singles out a class of finitely presented groups possessing property α. We shall call such a class a **class of α-groups**. A class of finitely presented groups α will be called **complete** if every finitely presented group is isomorphic to some subgroup of some group from the class α. Theorem 1 may be formulated in the following way.

Theorem $1'$**.** *If α is a nonempty and incomplete class of finitely presented groups, then there is no algorithm which determines, for an arbitrary finitely presented group, whether it belongs to the class α or not.*

Incompleteness of the class α is not a necessary condition, for there exist infinitely many complete classes of groups with an undecidable membership recognition problem. For example, the class of finitely presented groups decomposable into a direct product of k groups, or decomposable into a free product of k groups, and so on. The completeness of these classes is obvious.

The second part of the paper is devoted to proving the completeness of certain classes of finitely presented groups. From everything said above about the class of groups coinciding with their commutator subgroup, it follows that this class is complete. Let us note at once that every complete class contains a group with an undecidable identity problem.

As was proved in ([3]), there is no algorithm which, for any finitely presented group, determines whether it is simple or not. If, however, it is known in advance that the group is simple, then an algorithm solving the identity problem in it is constructed very simply.* Hence it follows that the class of simple groups is incomplete in the sense defined above.

In order that a finitely presented group F be simple, it is necessary and sufficient that adding to the defining relations of the group F any relation $A = B$ not holding in F should turn the group F into the trivial group.

Consider a finite system of words

$$L_1, L_2, \dots, L_r, \tag{9}$$

formed from the letters $x_1, x_2, \dots, x_s, x_1^{-1}, x_2^{-1}, \dots, x_s^{-1}$. A finitely presented group F will be called **conditionally trivial with respect to the system of defining relations**

$$L_i \equiv 1 \quad (i = 1, 2, \dots, r), \tag{10}$$

* This algorithm was communicated to the author by A. V. Kuznetsov.

if the addition to the defining relations of the group F of any one of the identical relations (10) turns the group F into the trivial one. In an analogous way one can define conditionally finite groups, conditionally abelian groups, etc. If a class of α-groups contains the trivial group, then the class of conditionally α-groups contains the entire class of conditionally trivial groups.

An identical relation is called nontrivial if it is not satisfied in the free group.

Theorem 2. *Whatever finite system of nontrivial identities (10) is taken, the class of conditionally trivial groups with respect to this system of identities is complete.*

Above we established that any finitely defined group can be embedded isomorphically in a group of type F_{qA}. For this it is sufficient that the word A contain no letters p and p^{-1} and have infinite order in the group F.

To prove Theorem 2 it is sufficient to choose such a word A_0 that would have infinite order in the group F and would become the identity upon the addition of any one of the identical relations (10).

The elements a_1 and b_1 are free generators of the subgroup F' of the group F generated by them. Consequently, the group F' contains free subgroups of any finite rank. Take a subgroup F'' of the group F' of rank $s + 1$. Let its free generators be $E_1, E_2, \dots, E_s, E_{s+1}$. Substitute in the words (9), in place of the letters $x_1, x_2, \dots, x_s, x_1^{-1}, x_2^{-1}, \dots, x_s^{-1}$, respectively, the words $E_1, E_2, \dots, E_s, E_1^{-1}, E_2^{-1}, \dots, E_s^{-1}$. Denote the words thereby obtained by $L'_1, L'_2, \dots, L'_r$.

Since all the identical relations (10) are, by assumption, nontrivial, not one of the words L'_i $(i = 1, 2, \dots, r)$ is equal to 1 in the group F''. The word

$$A_0 = [\dots[[E_{s+1}L'_1, L'_2], L'_3], \dots L'_r] \tag{11}$$

is also not equal to 1 in F'', for in a free group two elements will not be permutable if they are both not equal to the identity and are not equal to one another. Since the group F'' is free, the word A_0 has infinite order in F'', and hence also in the group F. At the same time A_0 becomes the identity upon the addition of any one of the identical relations (11). Theorem 2 is proved.

Theorem 3. *The class of finitely defined groups given by finite systems of mutually conjugate generators is complete.*

Since all generators of the group F_{qA} are conjugate to the word A, for the proof of Theorem 3 it is sufficient to take $A = a_1$.

Mathematical Institute named after V. A. Steklov
Academy of Sciences of the USSR

Received
25 IV 1957

CITED LITERATURE

1. P. S. Novikov, *Trudy Mat. inst. im. V. A. Steklova*, **44** (1955).

2. A. A. Markov, *Trudy Mat. inst. im. V. A. Steklova*, **42** (1954).

3. S. I. Adyan, DAN, **103**, No. 4 (1955).

Note: Figure translations are in progress. See original paper for figures.