ON REPRESENTATIONS OF SETS OF SOLUTIONS OF SYSTEMS OF EQUATIONS WITH ONE UNKNOWN IN A FREE GROUP

MATHEMATICS

1968

SovietRxiv

Abstract

Full Text

UDC 519.4

MATHEMATICS

A. A. LORENTS

ON REPRESENTATIONS OF SETS OF SOLUTIONS OF SYSTEMS OF EQUATIONS WITH ONE UNKNOWN IN A FREE GROUP

(Presented by Academician P. S. Novikov on March 20, 1967)

The present note is devoted to the investigation of structural properties of sets of solutions of systems of equations with one unknown in a free group. All concepts which are not defined here but are needed for understanding the note may be found in ([1]).

The first result concerning the problem of an effective description of the set of solutions of a system of equations with one unknown in a free group was obtained by R. Lyndon ([2,3]). Although he did not explicitly consider systems of several equations, nevertheless his results remain valid for systems with any number of members. The next step was made by the author in ([1]), where it was shown that the set of solutions of a system of equations with one unknown in a free group is representable by a finite number of parametric words (for details see ([2])) of the form $AS^{\mu}BT^{\nu}C$, $AS^{\mu}BT^{\mu}C$ (A, S, B, T, C are elements of the free group; μ, ν are parameters taking arbitrary natural values).

Using the latter, one can prove a more precise result.

Theorem 1. *If a system of equations with one unknown in a free group is soluble, then the set of its solutions is representable by a finite number of parametric words of the form $AB^{\mu}C$ (A, B, C are elements of the free group; μ is an integer parameter).*

We note that in parametric words of the form $AB^{\mu}C$ the element B may be the identity of the group. Equations can easily be constructed which require, for the representation of the set of their solutions, only one parametric word. Such, for example, are the equations

$$AX^{-1} = 1, \tag{1}$$

$$AXA^{-1}X^{-1} = 1, \tag{2}$$

where A is an element of the free group distinct from the identity of the group. Equation (1) has the unique solution $X = A$, whereas equation (2) has infinitely many solutions. Attempts to construct examples of another kind, i.e. equations or systems of them requiring, for the representation of the set of their solutions, more than one parametric word, encountered difficulties. Therefore one might have supposed that there are no systems of equations with one unknown in a free group requiring, for the representation of the set of their solutions, more than one parametric word of the form $AB^{\mu}C$. A careful analysis, however, showed the untenability of such a supposition.

Theorem 2. *Whatever the natural number n, in the free group $\mathfrak{G}$ with generators G_1, G_2 one can construct an equation with one unknown having a finite number $m \geq n$ of solutions.*

The proof of Theorem 2 is contained in Lemmas 1 and 2, for the formulation of which one definition is necessary.

Definition 1. We shall consider functions $\varphi(X)$ in the group $\mathfrak{G}$, defined by elements of the free group $\mathfrak{G}_X$ with generators G_1, G_2, X,

i.e., forms of the type $A_0 X^{e_0} A_1 X^{e_1} \dots A_{nX}^{e_n} A_{n+1}$, where A_i $(i = 0, 1, \dots, n+1)$ are elements of the group $\mathfrak{G}$, and e_i $(i = 0, 1, \dots, n)$ are numbers equal to ± 1. According to what has been said, the notation

$$\varphi(X) = A_0 X^{e_0} A_1 X^{e_1} \dots A_{nX}^{e_n} A_{n+1}$$

means that the function $\varphi(X)$ assumes the value

$$\varphi(U) = \left(\prod_{i=0}^{n} (A_{iU}^{e_i}) \right) A_{n+1}$$

when the argument has the value $X = U$, where $U \in \mathfrak{G}$.

Define the class of functions Φ as follows.

I. The function

$$\varphi(X) = G_2^{-1} X G_2 G_1 X^{-1} G_2^{-1} X^{-1} G_2 X G_2 G_1^{-1} G_2^{-1} G_1$$
$$X^{-1} G_2^{-1} X G_2 X G_1^{-1} G_2^{-1} X^{-1} G_2^2 G_1 G_2^{-1}$$

belongs to the class $\Phi_{\mathfrak{G}}$.

II. If the function

$$\varphi(X) = A_0 X^{e_0} A_1 X^{e_1} \dots A_{nX}^{e_n} A_{n+1}$$

belongs to the class $\Phi_{\mathfrak{G}}$, and B^{-1} is some value of this function different from G_1, then the function

$$\varphi'(X) = A_0 X^{e_0} A_1 X^{e_1} \ldots A^{e_n}_{nX} A_{n+1} B G_1 A^{-1}_{n+1} \\ X^{-e_n} A^{-1}_n \ldots X^{-e_1} A^{-1}_1 X^{-e_0} A^{-1}_0 B^{-1}$$

also belongs to the class $\Phi_{\mathfrak{G}}$.

Lemma 1. For each function $\varphi(X) \in \Phi_{\mathfrak{G}}$ there are only finitely many values $m \geq 3$ of the argument X for which $\varphi(X)$ assumes the value G_1.

Lemma 2. If $\varphi(X) \in \Phi_{\mathfrak{G}}$ is such that the word $X G_2 G_1 X^{-1} G_2^{-1} X^{-1} G_2 X$ enters into its defining form exactly n times, then there are $\log_2 n + 3$ distinct values of the argument X for which the function $\varphi(X)$ assumes the value G_1.

We note that the function $\varphi(X) = G_2^{-1} X G_2 G_1 X^{-1} G_2^{-1} X^{-1} G_2 X$ assumes the value G_1 only for $X = 1$ and $X = G_1$.

Theorem 3. Whatever natural number $n \geq 1$ is given, in some free group one can construct an equation with one unknown such that:

I. The set of solutions of this equation is representable by n parametric words of the form A^μ with $A \neq 1$.

II. No system of parametric words of the form $AB^\mu C$, containing fewer than n members, is a representation of its set of solutions.

This theorem is a simple consequence of Lemma 3, whose formulation requires one auxiliary notion.

Definition 2. Suppose that a free group $\mathfrak{G}'$ of rank $n \geq 2$ is given. Define in this group a class of equations as follows:

I. The class $J_{\mathfrak{G}'}$ contains any equation of the form

$$G_i^{-2} X G^{-1}_{iX} G_j^{-1} X G_j^2 X^{-1} G_j^{-1} X G_i^{-1} X^{-1} G_i^2 X$$

$$G_i^{-1} X^{-1} G_{jXG} j^{-2} X^{-1} G^{-1}_{jXG_{iX}} = 1, \tag{3}$$

where G_i, G_j are distinct free generators of the group $\mathfrak{G}'$.

II. Suppose that the equation

$$w(X) = 1 \tag{4}$$

belongs to the class $J_{\mathfrak{G}'}$; then, if G_j^{-2} is the first coefficient in order of equation (4), and the free generator G_i of the group $\mathfrak{G}'$ does not ⋯

is a coefficient of this equation, then the class $J_{\mathfrak{G}'}$ also contains the equation

$$G_i^{-2}XG_{iX}^{-1}G_{jw}(X)G_j^{-1}XG_i^{-1}X^{-1}G_i^2X$$
$$G_i^{-1}X^{-1}G_j(w(X))^{-1}G_{iX}^{-1}=1. \tag{5}$$

Lemma 3. *For any natural number m $(2\leq m\leq n)$, in the class of equations $J_{\mathfrak{G}'}$ one can specify an equation whose set of solutions is representable by a system of parametric words $G_1^\mu, G_2^\mu, \dots, G_m^\mu$.*

A modification of the construction of the class of equations $J_{\mathfrak{G}'}$ makes it possible to avoid increasing the rank of the group $\mathfrak{G}'$ depending on the given number of parametric words. But this strengthening has so far been obtained only at the cost of weakening Theorem 3 in other respects.

Theorem 3′. *For any natural number $n\geq 1$, in a free group $\mathfrak{G}$ of rank 2 one can construct an equation with one unknown which requires, for the representation of the set of its solutions, no fewer than n parametric words of the form $AB^\mu C$ with $B\neq 1$.*

The results obtained suggest the following hypothesis: if an equation with one unknown in a free group is solvable, then its set of solutions is representable either by parametric words of the form $AB^\mu C$ with $B\neq 1$, or by parametric words of the same form with $B=1$. The following theorem shows that the proposed uniformity does not occur.

Theorem 4. *For any pair of natural numbers m, n $(m>0,\ n>0)$, one can construct, in some free group, an equation*

$$w(X)=1 \tag{6}$$

with one unknown such that:

I. The set of solutions of equation (6) is representable by a finite system of parametric words of the form $AB^\mu C$, containing: a) exactly m such words with $B\neq 1$; b) no fewer than n parametric words with $B=1$.

II. Any system of parametric words of the form $AB^\mu C$ containing fewer than m such words with $B\neq 1$, or fewer than n parametric words with $B=1$, is not a representation of the set of solutions of equation (6).

We indicate the construction of the equations referred to in Theorem 4. Denote by $\mathfrak{G}^*$ the free group with generators G_1, G_2, G_3, relative to which the free group $\mathfrak{G}$ with generators G_1, G_2 is a subgroup. Suppose that the form $A_0X^{e_0}A_1X^{e_1}\dots A_{tX}^{e_t}A_{t+1}$ defines a function $\varphi(X)\in\Phi_{\mathfrak{G}}$ taking the value G_1 for $n>0$ values of the argument X. It is easy to show that one can find an element $C\in\mathfrak{G}$ such that $S=CG_1^{-1}A_0\neq 1$, $T=A_{t+1}C^{-1}\neq 1$, and moreover S, T are cyclically reduced. The equation

$$G_3^2XG_3X^{-1}SX^{e_0}A_1X^{e_1}\dots A_{tX}^{e_t}TXG_3^{-1}X^{-1}G_3^2X$$

$$G_3^{-1}X^{-1}T^{-1}X^{-e_t}A_t^{-1}\dots X^{-e_1}A_1^{-1}X^{-e_0}S^{-1}XG_3X^{-1}=1$$

will be the desired one for $m=1$.

The corresponding equations for $m>1$ can be constructed by the inductive method of Definition 2.

It should be noted that the equations whose existence is asserted in Theorem 4 can already be constructed in a free group of rank 2. An example of this kind is the equation

$$G_2^{-1}XG_2G_1X^{-1}G_2^{-1}X^{-1}G_2X^2G_1^{-1}X^{-1}=1. \tag{7}$$

Institute of Electronics
and Computer Engineering
Academy of Sciences of the Latvian SSR

Received
9 III 1967

REFERENCES

1. A. A. Lorents, DAN, 148, No. 6, 1253 (1963).
2. R. C. Lyndon, Trans. Am. Math. Soc., 96, 518 (1960).
3. R. C. Lyndon, Trans. Am. Math. Soc., 96, 445 (1960).

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