A. A. Lorents

1963

SovietRxiv

Abstract

Full Text

A. A. Lorents

SOLUTION OF SYSTEMS OF EQUATIONS WITH ONE UNKNOWN IN FREE GROUPS

(Presented by Academician P. S. Novikov, 4 IX 1962)

In the present note we consider the question of an algorithm recognizing the solvability of systems of equations with one unknown in free groups. The first result in this direction was obtained by R. Lyndon in the paper ([2]). He succeeded in constructing the set of solutions of the equation

$$U(X) = 1$$

in a free group $\mathfrak{G}$ as the set of values of "parametric words" φ_i $(i = 1, \dots, n)$. Lyndon' s parametric words φ_i, representing solutions, were of a rather complicated nature, and the number of parameters on which φ_i depend turned out to be bounded only within each equation under consideration.

We have succeeded in reducing the number of parameters to two and in showing that the problem of solvability of systems of equations with one unknown in free groups (Lyndon did not explicitly consider this question) is equivalent to the solvability in nonnegative integers of systems of equations of the form

$$ax + by = c,$$

where a, b, c are integers.

By a system of equations in the free group $\mathfrak{G}$ with generators $G_1, G_2, \dots, \dots, G_r$ we mean a system of expressions

$$\begin{gathered} W_1(X) = 1, \\ \dots\dots \\ W_l(X) = 1, \end{gathered} \tag{1}$$

where $W_k(X)$ $(k = 1, 2, \dots, l)$ is an element of the free group $\mathfrak{G}_x{}^*$ with generators $G_1, G_2, \dots, G_r, X$, and $W_k(X) \notin \mathfrak{G}$.

Solutions of the system (1) are elements V of the group $\mathfrak{G}$ such that each word $W_k(V)$ $(k = 1, 2, \dots, l)$ is equal in $\mathfrak{G}$ to the empty word.

The left-hand sides of the equations of the system (1), obviously, can only be such words W from $\mathfrak{G}_x$ for which

$$W = A_0 X^{e_0} \dots A_{iX}^{e_i} \dots A_{tX}^{e_t} A_{t+1},$$

where $A_i \in \mathfrak{G}$ $(i = 0, 1, \dots, t+1)$, and the e_i take the values ± 1. It is easy to see that the equation

$$A_0 X^{e_0} \dots A_{iX}^{e_i} \dots A_{tX}^{e_t} A_{t+1} = 1$$

is equivalent to the equation

$$A'_0 X^{e_0} \dots A_{iX}^{e_i} \dots A_{tX}^{e_t} = 1,$$

where $A'_0 = A_{t+1} A_0$.

---

* By elements of the free group $\mathfrak{G}$ we mean words in the alphabet $\{G_1, G_2, \dots, \dots, G_r, G_1^{-1}, G_2^{-1}, \dots, G_r^{-1}\}$ in which G_i and G_i^{-1} do not stand next to each other $(i = 1, 2, \dots, r)$.

Definition 1. Let an equation be given

$$A_0 X^{e_0} \dots A_{iX}^{e_i} \dots A_{tX}^{e_t} = 1, \tag{2}$$

for which the element $V \in \mathfrak{G}$ is a solution. The V-eliminators of this equation will be all expressions of the form

$$(A_0,\ V^{e_0}),\quad (A_0,\ V^{e_0},\ A_1,\ V^{e_1}),\quad (V^{e_0},\ A_1,\ V^{e_1},\ A_2,\ V^{e_2}), \dots$$
$$\dots,\quad (V^{e_i-2},\ A_{i-1},\ V^{e_i-1},\ A_i,\ V^{e_i}), \dots,\quad (V^{e_t-2},\ A_{t-1},\ V^{e_t-1},\ A_t,\ V^{e_t}).$$

We shall agree to call the element V^{e_0} the middle term of the eliminators $(A_0,\ V^{e_0})$ and $(A_0,\ V^{e_0},\ A_1,\ V^{e_1})$, and the element V^{e_i-1} the middle term of the eliminator $(V^{e_i-2},\ A_{i-1},\ V^{e_i-1},\ A_i,\ V^{e_i})$ $(i = 2, 3, \dots, t)$.

Theorem 1. If an element V of the free group $\mathfrak{G}$ is a solution of equation (2) in the free group $\mathfrak{G}$, then among the V-eliminators of this equation there exists one in which the middle term is completely cancelled*, provided that the operation of multiplication is performed in the following order:

$$V^{e_i-2} A_{i-1} V^{e_i-1} A_{iV}^{e_i} = ((((V^{e_i-2} A_{i-1}) V^{e_i-1}) A_i) V^{e_i}).$$

To denote non-cancelling multiplication of A by B we shall use the notation $A \cdot B$ instead of AB. An element $S \in \mathfrak{G}$ will be called **cyclically reduced** if $SS = S \cdot S$. The empty word (or the identity of the group), which we denote by the symbol 1, is not considered a cyclically reduced element.

In what follows $[P^\partial]$ $(P \in \mathfrak{G})$ denotes the length of the word P, and $[P^\partial] = n$ if

$$P = G_{i_1}^{\varepsilon_1} \dots G_{i_n}^{\varepsilon_n}.$$

The length of the empty word is taken to be zero.

In Theorems 2 and 3 the letters S, T denote cyclically reduced elements.

Theorem 2. If a V-eliminator

$$(V^{e_j-1},\ A_j,\ V^{e_j},\ A_{j+1},\ V^{e_j+1})$$

of equation (2) is given, in which the term V^{e_j} is completely cancelled, then

$$V^{e_i} = A \cdot S^m \cdot B \cdot T^n \cdot C,$$

where

$$\max\{[S^\partial],\ [A^\partial],\ [B^\partial],\ [C^\partial],\ [T^\partial]\} \le 2\max\{[A_j^\partial],\ [A_{j+1}^\partial]\};$$

m, n are nonnegative integers.

Theorem 3. Let a system (1) of equations of the form (2) be given, where

$$W_k(X) = A_{0k}X^{e_{0k}} \dots A_{ik}X^{e_{ik}} \dots A_{t_{kk}}X^{e_{t_{kk}}},$$

and let

$$\min_{k=1,\dots,l}\ \max_{i=0,\dots,t_k}\ [A_{ik}^\partial] = \rho.$$

If V is a solution of the system (1), then

$$V = A \cdot S^m \cdot B \cdot T^n \cdot C,$$

where

$$\max\{[A^\partial],\ [B^\partial],\ [C^\partial],\ [S^\partial],\ [T^\partial]\} \le 2\rho \quad (A, B, C, S, T \in \mathfrak{G}).$$

---

* The middle term V^{e_i-1} is cancelled in the eliminator $(V^{e_i-2},\ A_{i-1},\ V^{e_i-1},\ A_i,\ V^{e_i})$ if the product $V^{e_i-2}A_{i-1}V^{e_i-1}A_{iV}^{e_i}$ annihilates its components.

In what follows, expressions of the form $A \cdot S^\mu \cdot B \cdot T^\nu \cdot C$ $(A, B, S, T \in \mathfrak{G};\ \mu$ and ν are variables that may take integer nonnegative values) will be called **parametric elements of the group $\mathfrak{G}$**.

It follows from Theorem 3 that the solutions of the system of equations (1) are the values of such parametric elements $A \cdot S^\mu \cdot B \cdot T^\nu \cdot C$ for which

$$\max\{[A^\partial], [B^\partial], [C^\partial], [S^\partial], [T^\partial]\} \le 2\rho.$$

An immediate consequence of this bound is that all solutions of the system of equations (1) are found among the values of a finite number of parametric elements of the group $\mathfrak{G}$. Therefore the problem of solvability of systems of equations with one unknown in free groups reduces to the analysis of equations that are obtained from the system (1) by substituting some parametric element $A \cdot S^{\mu} \cdot B \cdot T^{\nu} \cdot C$ in place of X (the substitution is made simultaneously everywhere that X occurs in the system (1)). A pair of integer nonnegative numbers m, n is regarded as a **solution** of the resulting **parametric equation** if, after replacing μ and ν by m and n, respectively, the product

$$A_0 (A \cdot S^m \cdot B \cdot T^n \cdot C)^{e_0} \dots A_i (A \cdot S^m \cdot B \cdot T^n \cdot C)^{e_i} \dots A_t (A \cdot S^m \cdot B \cdot T^n \cdot C)^{e_t}$$

is equal to the empty word. It is not hard to see that parametric equations can be put in the form

$$B_0 U_0^{\beta_0} \dots B_{iU} i^{\beta_i} \dots B_{tU} t^{\beta_t} B_{t+1} = 1,$$

where $\beta_i = \pm\mu$ or $\beta_i = \pm\nu$, $U_i = S$ or $U_i = T$, and, moreover, if $\beta_i = \pm\beta_j$, then $U_i = U_j$.

Theorem 4. *If a system of parametric equations in the free group* $\mathfrak{G}$ *is given*

$$\begin{gathered} W_1(\mu, \nu) = 1 \\ \dots\dots\dots \\ W_l(\mu, \nu) = 1 \end{gathered} \tag{3}$$

(μ, ν *are parameters), then one can construct one parametric equation in some free group* $\mathfrak{G}' \supset \mathfrak{G}$*, equivalent to the system (3).*

Definition 2. The expression

$$A_0 U_0^{\alpha_0} \dots A_{iU} i^{\alpha_i} \dots A_{tU} t^{\alpha_t} A_{t+1} = 1 \tag{4}$$

will be called a **reduced parametric equation** if it has the following properties:

1) A_i $(i = 0, 1, \dots, t+1)$ and U_i $(i = 0, 1, \dots, t)$ are fixed elements of the free group $\mathfrak{G}$, and all U_i are cyclically reduced.
2) If for U_i and U_j there exists an element $B \in \mathfrak{G}$ with the property

$$[B^{\partial}] < [U_j^{\partial}], \qquad U_i^{\pm[U_j^{\partial}]} \cdot B = B \cdot U_j^{\pm[U_i^{\partial}]},$$

then $U_i = U_j$.
3) A_i does not have $U_{i-1}^{\pm 1}$ as its beginning $(i = 1, 2, \dots, t+1)$.
4) A_i does not have $U_i^{\pm 1}$ as its end $(i = 0, 1, \dots, t)$.
5) $\alpha_i = c_i \mu_1 + d_i \mu_2 + e_i$, where c_i, d_i, e_i are given integers $(i = 0, 1, \dots, t)$.

A pair of integer nonnegative numbers m_1, m_2 will be called a **solution** of the equa-

solutions (4), if

$$A_0 U_0^{\alpha'_0} \dots A_i U_i^{\alpha'_i} \dots A_t U_t^{\alpha'_t} A_{t+1} = 1^*,$$

where $\alpha'_i = c_i m_1 + d_i m_2 + e_i$ $(i = 0, 1, \dots, t)$.

Theorem 5. For any system of equations with one unknown in a free group $\mathfrak{G}$, one can construct a finite number of parametric elements $\varphi_1, \dots, \varphi_s$ such that:

a) all solutions of the system are contained among the values of $\varphi_1, \dots, \varphi_s$;

b) if

$$W(X) = 1 \tag{5}$$

is some equation with one unknown in the free group $\mathfrak{G}$, and

$$W(\mu, \nu) = 1 \tag{6}$$

is the parametric equation obtained from (5) by substituting one of the φ_i in place of X, then equation (6) is equivalent to some reduced parametric equation.

Theorem 5 reduces the decidability problem for the system (1) to the analysis of reduced parametric equations.

Definition 3. Denote by

$$V_1(X),\, V_2(X), \dots, V_m(X); \quad V_1^*(Y),\, V_2^*(Y), \dots, V_n^*(Y)$$

equations whose solutions may be vectors

$$Z = \{\zeta_1, \zeta_2, \dots, \zeta_s\}$$

with integral nonnegative coordinates ζ_k $(k = 1, 2, \dots, s)$. Consider two **disjunctive systems of equations****

$$V_1(X) \vee V_2(X) \vee \dots \vee V_m(X), \tag{7}$$

$$V_1^*(Y) \vee V_2^*(Y) \vee \dots \vee V_m^*(Y). \tag{8}$$

The vectors $X = \{\xi_1, \xi_2, \dots, \xi_s\}$ and $Y = \{\eta_1, \eta_2, \dots, \eta_s\}$ will respectively be solutions of the systems (7) and (8), if X satisfies at least one $V_i(X)$ ($i = 1, 2, \dots, m$), and Y–$V_j^*(Y)$ ($j = 1, 2, \dots, n$).

We shall call the systems (7) and (8) **equivalent** if every solution of the system (7) is also a solution of the system (8) and, conversely, every solution of the system (8) is a solution of the system (7).

Theorem 6. Every disjunctive system of reduced parametric equations is equivalent to some disjunctive system of Diophantine equations of the form

$$c\mu_1 + d\mu_2 + e = 0.$$

Received
24 VIII 1962

REFERENCES

1. R. C. Lyndon, Trans. Am. Math. Soc., **96**, 518 (1960).

2. R. C. Lyndon, Trans. Am. Math. Soc., **96**, 445 (1960).

* An equation of the form $A = 1$ ($A \in \mathfrak{G}$) will also be considered by us as a reduced parametric equation.

** A single equation is also regarded by us as a disjunctive system.

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