PROCEEDINGS OF THE YEREVAN STATE UNIVERSITY

Physical and Mathematical Sciences 2015, № 2, p. 62–65

C O M M U N I C A T I O N

M a t h e m a t i c s

GENERAL SOLUTION OF QUADRATIC EQUATIONS IN FREE GROUPS

G. S. MAKANIN[1], A. Sh. MALKHASYAN[2] *

[1] *Steklov Institute of Mathematics of RAS, Russian Federation*

[2] *Chair of Discrete Mathematics and Theoretical Informatics YSU, Armenia*

The general solution of quadratic equations in free group using an automat, specified by the certain oriented graph is presented.

MSC2010: 20F28; 20E36.

***Keywords*:** quadratic equation, free group, equation in free semigroup.

Introduction. The article is devoted to the study of equations in free group and to methods of description of the general solution.

Let F be a free group on the alphabet $a_1, a_2, \dots, a_n$ of generators.

The equation with m unknowns in the free group is an equality of the form

$$B_1 x_{j_1}^{\varepsilon_1}\, B_2 x_{j_2}^{\varepsilon_2} \dots\, B_k x_{j_k}^{\varepsilon_k} = 1, \tag{1}$$

where $x_{j_s} \in \{x_1, \dots, x_m\}$, $\varepsilon_s = \pm 1$, and B_s are words in a group alphabet $a_1, a_2, \dots, a_n$. The degree of equation is the maximal number of occurrence of an unknown. The equation of first degree is called linear and the equation of the second degree is called quadratic.

The tuple of words

$$X_1, \dots, X_m$$

in the group alphabet $a_1, a_2, \dots, a_n$ is called the solution of equation, if the equality $B_1 X_{j_1}^{\varepsilon_1} B_2 X_{j_2}^{\varepsilon_2} \dots B_k X_{j_k}^{\varepsilon_k} = 1$ holds in the group F. An algorithm, identifying solvability of every equation in free group, was suggested in [1], while the problem of description of the general solution stays open. There are many results devoted to the problem of description of the general solution of the equations in free groups. In particular, we would like to mention the following articles [2–7]. In the present article the general solution of quadratic equation in free group will be given. Let us remind

* E-mail: amalkhasyan@mail.ru

some notation and results from [1]. The free semigroup P with alphabet of generators $a_1,a_2,\ldots,a_n,a_1^{-1},a_2^{-1},\ldots,a_n^{-1}$ is called a double-alphabet semigroup, and an equality of words in this semigroup is called the equality in double-alphabet. The system of equality

$$\varphi_i(a_1,a_2,\ldots,a_n,a_1^{-1},a_2^{-1},\ldots,a_n^{-1},z_1,z_2,\ldots,z_q,z_1^{-1},z_2^{-1},\ldots,z_q^{-1}) = \qquad (2)$$
$$= \psi(a_1,a_2,\ldots,a_n,a_1^{-1},a_2^{-1},\ldots,a_n^{-1},z_1,z_2,\ldots,z_q,z_1^{-1},z_2^{-1},\ldots,z_q^{-1}),$$

$i=1,\ldots,p$, will be called a system of equations in the double-alphabet, and a number of occurrences of the letters from the set

$$a_1,a_2,\ldots,a_n,a_1^{-1},a_2^{-1},\ldots,a_n^{-1}, z_1,z_2,\ldots,z_q,z_1^{-1},z_2^{-1},\ldots,z_q^{-1}$$

is called the length of its record. The tuple of irreducible words

$$Z_1,Z_2,\ldots,Z_q$$

(that do not contain subwords like $a_ia_i^{-1},a_i^{-1}a_i$) is called a solution of the system of equations, if we get graphical equalities after substitutions of Z_i in z_i.

Here we will prove Lemma 1 for quadratic equations an analogue of which was proved in [1].

Lemma 1. For each quadratic equation in free group we can form a finite list of systems of quadratic equations in double-alphabet, such that the list of systems has a solution, if and only if any one of the systems of equations has a solution.

Proof. Let the list of words

$$X_1,\ldots,X_m$$

be the solution of Eq. (1) and, consequently, the word $B_1X_{j_1}^{\varepsilon_1}B_2X_{j_1}^{\varepsilon_2}...B_kX_{j_1}^{\varepsilon_k}$ is reduced to empty word of group F. Every component of solution has the form

$$X_i = C_{i,1}Z_{j_1}^{\delta_1}\ldots C_{i,l}Z_{j_l}^{\delta_l}C_{i,l+1}, \qquad (3)$$

where $i=1,\ldots,m$, $\delta_s=\pm1$.

The words $C_{i,s}$ can be reduced with subwords of B_k. The words $Z_{j_s}^{\delta_s}$ can be reduced with subwords $Z_{j_k}^{-\delta_k}$ of other components of solution of Eq. (1). Let us denote in words X_i each of entry of subwords Z_q by an unknown z_q. Write down the equations like (2) obtained by equating of words formed from different entries of words X_i. It is obvious, that each solution of system of Eq. (2) turns out to a solution of Eq. (1). It is easy to notice that by substituting the components of solutions

$$Z_1,Z_2,\ldots,Z_q$$

in the system (1) instead of proper variables we get that the tuple of words

$$\varphi_i(a_1,a_2,\ldots,a_n,a_1^{-1},a_2^{-1},\ldots,a_n^{-1},Z_1,Z_2,\ldots,Z_q,Z_1^{-1},Z_2^{-1},\ldots,Z_q^{-1}),\ i=1,..,n, \qquad (4)$$

is a solution of the Eq. (1). The number of systems like (2) is limited by the meaning of certain recursive function depends on the length of the record of Eq. (1). The number of equations in each system is no more than number of entries of unknowns in (1). In addition, each of the formed systems of equations in double-alphabet contains no more than two entries of unkowns z_i, i.e. that is quadratic. $\square$

Let's consider the system of equations like (2) in double-alphabet and consider a certain of equation of this system, for instant

$\varphi_1(a_1,a_2,\ldots,a_n,a_1^{-1},a_2^{-1},\ldots,a_n^{-1},z_1,z_2,\ldots,z_q,z_1^{-1},z_2^{-1},\ldots,z_q^{-1}) =$
$= \phi_1(a_1,a_2,\ldots,a_n,a_1^{-1},a_2^{-1},\ldots,a_n^{-1},z_1,z_2,\ldots,z_q,z_1^{-1},z_2^{-1},\ldots,z_q^{-1}).$

If the system of equation has a solution, then it will turn out the considered equation, after substitution of the component of solution

$$Z_1,Z_2,\ldots,Z_q$$

in the system (2) instead of unknowns.

The following cases are possible.

1. The beginnings of right and left parts of the first equation are a coefficients. In this case this beginnings will be reduced. In result we get the system of equations with a shorter length of recording form which is equivalent to the given system.

2. At the beginning of the left and right parts of the first equation recorded is z_i, A. After replacing z_i by Az_i, or by D, where D is a subword of word A, the system will stay quadratic, and the length of its record does not exceed the length of record of this system.

3. At the beginning of the left and right parts of the first equation recorded is z_i, z_j. After replacing z_j by z_iz_j or z_i by z_jz_i, the system will stay quadratic, and the length of its record does not exceed the length of record of this system.

Let us notice, that if the system of equations is obtained from a system like (2) with the help of above mentioned transformations, the solution

$$U_1,U_2,\ldots,U_q$$

of the system will be obtained from the solution

$$Z_1,Z_2,\ldots,Z_q$$

of the system (2) with substitution of Z_k by U_k, if $i \neq k$; and Z_i by U_iU_j in case 3 and substitution of Z_k by D in case 2.

Let us mark as $\sum_1$ the system of Eq. (2), and mark as $\sum_2,\sum_3\ldots$ the systems of equations formed from (2) by the all possible transformations 1.,2.,3. The same should be done with each of the systems and will continue this process on each of systems. As a result of transformations 1.,2.,3., the length of record of system of equations $\sum_i$ does not increase. The quantity of systems of equation will be limited with the meaning of certain recursive function, which is dependent from the length of recording $\sum_1$.

Let us consider the graph Γ, the vertices of which are marked by the systems of quadratic equations $\sum_1$, $\sum_2$, $\sum_3,\ldots$, in the dual alphabet, obtained from the system of the Eq. (2). Take an oriented edge from the vertex $\sum_i$ to the vertex $\sum_j$, if the system $\sum_j$ is obtained from $\sum_i$ by means of one of transformations of three types. Let us call the graph Γ a graph of the system.

From all above follows.

Lemma 2. The system of Eq. (4) has the solution, if and only if in the graph Γ of the system $\sum_1$ there is a path, connecting the vertex $\sum_1$ with a vertex with zero length of record.

Further, let (1) be a quadratic equation in free group F with the alphabet $a_1, a_2, \ldots, a_n$. For this equation, according to Lemma 1, a finite list of systems of equations in double-alphabet is constructed. From these systems are considered only those, which graphs have a vertex marked by the system with the empty length of record.

For each of such systems of equations in double-alphabet, its graph has an initial vertex, marked by this system and a finite vertex, marked by a system with zero length of record.

By the parametric word in the alphabet $a_1, a_2, \ldots, a_n, a_1^{-1}, a_2^{-1}, \ldots, a_n^{-1}$ with the set of parameters $z_1, z_2, \ldots, z_q, z_1^{-1}, z_2^{-1}, \ldots, z_q^{-1}$ we will call an irreducible word in joint alphabet

$$a_1, a_2, \ldots, a_n, a_1^{-1}, a_2^{-1}, \ldots, a_n^{-1}, z_1, z_2, \ldots, z_q, z_1^{-1}, z_2^{-1}, \ldots, z_q^{-1}.$$

We call value of a parametric word, the word obtained after substitution in place of z_j any words in the alphabet

$$a_1, a_2, \ldots, a_n, a_1^{-1}, a_2^{-1}, \ldots, a_n^{-1}.$$

Now we will consider various (all possible) oriented ways in each of these graphs, starting in initial and ending in conclusive vertices of this graph. Let us consider all the parametric words, which can be obtained from transformation corresponding edges of the given path. Let us call them graph-derived words.

We get the following theorem:

Theorem. The general solution of the quadratic equation in free group is the set of values of all graph-derived words.

Received 08.05.2015

REFERENCES

1. **Makanin G.S.** Equations in a Free Group. // Izv. Akad. Nauk SSSR. Ser. Matematika, 1982, v. 46, № 6, p. 1199–1273 (in Russian).
2. **Khmelevskii Yu.I.** Systems of Equations in a Free Group. I. // Izv. Akad. Nauk SSSR. Ser. Matematika, 1971, v. 35, № 6, p. 1237–1268 (in Russian).
3. **Grigorchuk R.I., Kurchanov P.F.** On Quadratic Equations in Free Groups. // Proceedings of the International Conference on Algebra. Novosibirsk, Part 1, Contemp. Math., v. 131; Amer. Math. Soc., Providence, RI, 1992, p. 159–171.
4. **Razborov A.A.** On Systems of Equations in a Free Group. // Izv. Akad. Nauk SSSR. Ser. Matematika, 1984, v. 48, № 4, p. 779–832 (in Russian).
5. **Lyndon R.C.** Equations in Free Group. // Trans. Amer. Math. Soc, 1960, v. 96, p. 445–457.
6. **Durnev V.G., Zetkina O.V.** On Equations in Free Groups with Constraints on the Solution. // Chebyshevskii Sb., 2012, v. 13, № 1, p. 63–80 (in Russian).
7. **Malkhasyan A.Sh.** On the Solvability of Equations in Subgroups of Free Groups. // Proceedings of All-Union Symposium on Group Theory. M., 1986, p. 96 (in Russian).