EQUIVALENCE OF INFINITE SYSTEMS OF EQUATIONS IN FREE GROUPS AND SEMIGROUPS TO FINITE SUBSYSTEMS

V. S. Guba

In the present work the conjection of A. Ehrenfeucht is proved. This consists of the following: (*) every set of words L over some finite alphabet A contains a finite subset F ("test set") such that, for any pair (g, h) of homomorphisms, from the free semigroup $\Pi(A)$ with basis A into an arbitrary free semigroup, $g(x) = h(x)$ for all x from L if and only if $g(x) = h(x)$ for all x from F (see, in this regard, [1, 2]).

We shall first prove a basic theorem which has independent interest.

THEOREM. Every system of equations in a free group (in a free semigroup) from a finite number of unknowns over an arbitrary alphabet is equivalent to a finite subsystem.

We recall that an expression of the form

$$w(x_1, \ldots, x_n) = 1 \tag{1}$$

in unknowns $x_1, \ldots, x_n$ over the group alphabet A is called an equation in the free group, where $w(x_1, \ldots, x_n)$ is a group word over $X \cup A$, $X = \{x_1^{\pm 1}, \ldots, x_n^{\pm 1}\}$, and $X \cap A = \phi$.

A solution of Eq. (1) is a collection of words $(X_1, \ldots, X_n)$ over A such that $w(X_1, \ldots, X_n)$ equals 1 in the free group generated by A.

Analogously, an expression of the form

$$v(x_1, \ldots, x_n) = w(x_1, \ldots, x_n) \tag{2}$$

in unknowns $x_1, \ldots, x_n$ over a semigroup alphabet A, is called an equation in the free semigroup, where $v(x_1, \ldots, x_n)$ and $w(x_1, \ldots, x_n)$ are words over $X \cup A$, $X = \{x_1, \ldots, x_n\}$, and $X \cap A = \emptyset$. A solution of Eq. (2) is a collection $(X_1, \ldots, X_n)$ of words over A such that the words $v(X_1, \ldots, X_n)$ and $w(X_1, \ldots, X_n)$ are graphically equal.

Before proving the theorem, we shall show that (*) follows from it. Let B be a fixed finite alphabet, $\Pi(B)$ be the free semigroup of words over B, and $L \subset \Pi(B)$. Also, let B' be a bijective copy of the alphabet B. To each word $b_{i_1}, b_{i_2}, \ldots, b_{i_r} \in L$ we associate the equation

$$b_{i_1} b_{i_2} \ldots b_{i_r} = b'_{i_1} b'_{i_2} \ldots b'_{i_r} \tag{3}$$

in the unknowns $b_1, b_1', b_2, b_2', \ldots, b_m, b_m'$, where $m = |B|$, over a countable alphabet C. A pair of homomorphisms (g, h) from $\Pi(B)$ to $\Pi(C)$ satisfies the condition $g(b_{i_1}, \ldots, b_{i_r}) = h(b_{i_1}, \ldots, b_{i_r})$ if and only if $R = (g(b_1), h(b_1), \ldots, g(b_m), h(b_m))$ is a solution of Eq. (3). Thus, the condition "$g(x) = h(x)$ for all $x \in L$" means that R is a solution of the system which consists of the equations of form (3) corresponding to words from L. Using the theorem we choose a finite subsystem that gives us the desired subsystem in L.

We now proceed to the proof of the theorem. We shall first prove it in the special case when the equations considered are in the free group where the alphabet A is $\{a_1^{\pm 1}, a_2^{\pm 1}\}$.

By Sanov's theorem [3, p. 129], the subgroup in $SL_2(\mathbf{Z})$ generated by the matrices $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$ is the free group F_2. Thus, the homomorphism $\theta: F_2 \to SL_2(Z)$, defined by the conditions $\theta(a_1) = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \theta(a_2) = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$ is an isomorphic imbedding. Let $(X_1, \ldots, X_n)$ be a collection of words from F_2. We denote $\theta(X_j) = \begin{pmatrix} P_j & Q_j \\ R_j & S_j \end{pmatrix}$. It is obvious that $\theta(X_j^{-1}) = \begin{pmatrix} S_j & -Q_j \\ -R_j & P_j \end{pmatrix}$.

M. V. Lomonosov Moscow State University. Translated from Matematicheskie Zametki, Vol. 40, No. 3, pp. 321-324, September, 1986. Original article submitted April 9, 1985.

0001-4346/86/4034-0688$12.50

It is clear that $w(X_1, \ldots, X_n) = 1$ in $F_2 \Leftrightarrow w(\theta X_1, \ldots, \theta X_n) = E$ in $SL_2(\mathbf{Z})$. The latter means that the collection $(P_1, Q_1, R_1, S_1, \ldots, P_n, Q_n, R_n, S_n)$ is a solution of the system of four Diophantine equations which are obtained by multiplying the matrices which form the product $w(\theta X_1, \ldots, \theta X_n)$ and by then equating the resulting matrix to the identity matrix.

For this reason, if $M_j = \begin{pmatrix} P_j & Q_j \\ R_j & S_j \end{pmatrix}$, $j = \overline{1, n}$ is a collection of n matrices lying in $\theta(F_2)$, the components of which satisfy the indicated four Diophantine equations, then their inverse images $X_j = \theta^{-1}(M_j)$ form a solution of the equation $w(x_1, \ldots, x_n) = 1$.

Now let $w_i(x_1, \ldots, x_n) = 1$, $i \in I$, be a system of equations in the free group over A. To each $i \in I$ we associate in the manner indicated above four Diophantine equations (we shall refer to the equations from one such set of four as connected). The system of Diophantine equations obtained is equivalent to a finite one. Actually, let $\Phi_{ik}(p_1, q_1, r_1, s_1, \ldots, p_n, q_n, r_n, s_n) = 0$, where $k = 1, 2, 3, 4$, $i \in I$, be the given system. The ideal in $\mathbf{Z}[p_1, q_1, \ldots, r_n, s_n]$, which is generated by all the Φ_{ik}, is finitely generated by the Hilbert basis theorem [4]. It is therefore possible to select a finite number of polynomials among the Φ_{ik} which generate this ideal. If necessary, we also add to each chosen equation $\Phi_{ik} = 0$ all those that are connected with it. The finite system obtained is equivalent to the initial one. It consists of the equations $\Phi_{ik} = 0$, where $k = 1, 2, 3, 4$, $i \in I$, $|I_0| < \infty$. We "translate" it again into a system of equations in the free group $w_i(x_1, \ldots, x_n) = 1$, $i \in I_0$. This is equivalent to the original system. Actually, if $(X_1, \ldots, X_n)$ is its solution, then the components of the matrices $\theta(X_1), \ldots, \theta(X_n)$ form a solution to the finite system of Diophantine equations and, therefore, also to the whole system of Diophantine equations. By what was said above, their inverse images form a solution to the initial system $w_i(x_1, \ldots, x_n) = 1$, $i \in I$, which is what was to be proved.

We now extend this result to the case when the alphabet A is finite or countable. Since there exists an imbedding of the free group F with basis A into F_2 [3, p. 128], we can consider a system Σ of equations over A as a system Σ' of equations over $\{a_0^{\pm 1}, a_2^{\pm 1}\}$. The set of equations of Σ over A is the intersection of the set of solutions of Σ' over $\{a_0^{\pm 1}, a_2^{\pm 1}\}$ with the n-th direct power of F. Reducing Σ' to a finite subsystem Σ_0' and passing to a subsystem Σ_0 in Σ we obtain a system equivalent to Σ, since the set of solutions of is also the intersection of the set of solutions of Σ_0' with F^n.

Now let A be an alphabet of any cardinality, and $w_i(x_1, \ldots, x_n) = 1$, $i \in I$, be a system Σ of equations over A. We assume that it is not equivalent to any finite subsystem. Let $i_1 \in I$ be an arbitrary element. Since Σ is not equivalent to the system Σ_1 consisting of the equation $w_{i_1} = 1$, there exists a solution $R_1 = (X_1^{(1)}, \ldots, X_n^{(1)})$ of the system Σ_1 which is not a solution of Σ. Let $i_2 \in I$ be such that R_1 is not a solution of $w_{i_2} = 1$. We form a system Σ_2, adding to Σ_1 the equation $w_{i_2} = 1$. But, again, there exists a solution $R_2 = (X_1^{(2)}, \ldots, X_n^{(2)})$ of the system Σ_2 which is not a solution of Σ. We choose $i_3 \in I$ such that R_2 is not a solution of $w_{i_3} = 1$, and so forth. We thus obtain a countable system of equations $\Sigma_\omega = \bigcup_{k=1}^{\infty} \Sigma_k$. The set of letters from A which enter in the list of even one of the equations from Σ_ω or even one of the words $X_j^{(k)}$, $j = \overline{1, n}$, forms a not greater than countable subalphabet A_0. The system Σ_ω, as a system over A_0, is not equivalent to any finite subsystem: if it is equivalent, say, to Σ_s, then a contradiction is obtained, since R_s is a solution to Σ_s, but not a solution to Σ_{s+1}. Thus, the group variant of the theorem is proved.

The semigroup variant follows easily from the group one. Namely, let Σ be a system of equations $v_i(x_1, \ldots, x_n) = w_i(x_1, \ldots, x_n)$, $i \in I$, over A. We consider the system of group equations

$$v_i(x_1, \ldots, x_n) \cdot w_i^{-1}(x_1, \ldots, x_n) = 1, \quad i \in I$$

(over $A^{\pm 1}$). We reduce it to a finite one ($i \in I_0$, $|I_0| < \infty$). Then the subsystem in Σ defined by I_0 is equivalent in an obvious way to the initial one. This completes the proof of the theorem.

LITERATURE CITED

1. J. Albert, "On the Ehrenfeucht conjecture on test sets and its dual version," Lect. Notes Comput. Sci., 176, 176-184 (1984).

2. II Culic, "Homomorphisms: decidability, equality, and test sets," in: Formal Language Theory: Perspectives and Open Problems, R. Book (ed.), Academic Press, New York (1980).
3. M. I. Kargapolov and Yu. I. Merzlyakov, Basic Theory of Groups [in Russian], Nauka, Moscow (1982).
4. S. A. Lang, Algebra, Addison-Wesley (1965).

THE NUMBER OF SOLUTIONS OF A SYSTEM OF A LINEAR EQUATION AND A QUADRATIC EQUATION IN GALOIS FIELDS OF CHARACTERISTIC 2

B. Zh. Kamaletdinov

Let GF(q), $q = p^w$, be a Galois field of characteristic p. In the present note, we determine the number of solutions of a system of a linear equation and a nondegenerate quadratic equation over $\mathcal{F} = GF(q)$, $q = 2^n$, where n is a natural number. The proposed results, together with those obtained in [1, 2] for fields of characteristic $p > 2$, completely solve the problem of determination of the number of general solutions of a system of a linear equation and a quadratic equation in a field of arbitrary characteristic.

Let $e(x)$, $x \in \mathcal{F}$, be a character of the additive group $\mathcal{F}$ in the field of real numbers. Obviously, $e(x) = (-1)^{\operatorname{tr} x}$, where

$$\operatorname{tr} x = \sum_{i=0}^{n-1} x^{2^i}$$

is the trace of $x \in \mathcal{F}$ in GF(2). As we know [3, p. 191],

$$\sum_{x \in \mathcal{F}} e(ax) = q\delta(a), \quad a \in \mathcal{F}, \tag{1}$$

where $\delta(a)$ is the delta function on $\mathcal{F}$ defined as

$$\delta(a) = \begin{cases} 1, & a = 0, \\ 0, & a \neq 0. \end{cases} \tag{2}$$

We also know (see, e.g., [4, p. 59]) that an arbitrary nondegenerate form

$$f(y_0, y_1, \ldots, y_{m-1}) = \sum_{j=0}^{m-1} \sum_{i \leq j} \alpha_{ij} y_i y_j, \quad \alpha_{ij} \in \mathcal{F},$$

can be reduced to one of the following two canonical forms $f_k(x_0, x_1, \ldots, x_{m-1})$:

$$f_k(x_0, x_1, \ldots, x_{m-1}) = \begin{cases} \beta(x_0^2 + x_1^2) + \sum_{i=0}^{l-1} x_{2i} x_{2i+1}, & m = 2l, \quad l \geqslant 1, \\ x_0^2 + \sum_{i=1}^{l} x_{2i-1} x_{2i}, & m = 2l+1, \quad l \geqslant 1, \end{cases}$$

where β is equal to zero or to one of the values of β' for which the quadratic form $\beta' x_0^2 + \beta' x_1^2 + x_0 x_1$ is irreducible in $\mathcal{F}$. This means that an arbitrary system of a linear equation and a quadratic equation can be expressed as

$$\begin{cases} \sum_{i=0}^{2l-1} \gamma_i x_i = a, \\ \beta(x_0^2 + x_1^2) + \sum_{i=0}^{l-1} x_{2i} x_{2i+1} = b \end{cases} \tag{3}$$

or as

V. I. Ul'yanov (Lenin) Leningrad Electrotechnical Institute. Translated from Matematicheskie Zametki, Vol. 40, No. 3, pp. 325-330, September, 1986. Original article submitted June 3, 1985.

 0001-4346/86/4034-0690$12.50