V. S. Guba, Equivalence of infinite systems of equations in free groups and semigroups to finite subsystems, *Mat. Zametki*, 1986, Volume 40, Issue 3, 321–324

МАТЕМАТИЧЕСКИЕ ЗАМЕТКИ

т. 40, № 3 (1986)

ЭКВИВАЛЕНТНОСТЬ БЕСКОНЕЧНЫХ СИСТЕМ УРАВНЕНИЙ В СВОБОДНЫХ ГРУППАХ И ПОЛУГРУППАХ КОНЕЧНЫМ ПОДСИСТЕМАМ

В. С. Губа

В настоящей работе доказана гипотеза А. Эренфойхта, состоящая в следующем: (*) *всякое множество слов* L *над некоторым конечным алфавитом* A *содержит конечное подмножество* F (*«тестовое множество»*) *такое, что для любой пары* (g, h) *гомоморфизмов свободной полугруппы* $\Pi(A)$ *с базисом* A, *в произвольную свободную полугруппу* $g(x) = h(x)$ *для всех* x *из* L, *если и только если* $g(x) = h(x)$ *для всех* x *из* F (*см. по этому поводу* [1, 2]).

Сначала мы докажем основную теорему, представляющую самостоятельный интерес.

ТЕОРЕМА. *Всякая система уравнений в свободной группе (в свободной полугруппе) от конечного числа неизвестных над произвольным алфавитом эквивалентна конечной подсистеме.*

Напомним, что уравнением в свободной группе

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

от неизвестных $x_1, \ldots, x_n$ над групповым алфавитом A называется выражение вида (1), где $w(x_1, \ldots, x_n)$ — групповое слово над $X \bigcup A$, где $X = \{x_1^{\pm 1}, \ldots, x_n^{\pm 1}\}$; $X \bigcap A = \varnothing$.

Решение уравнения (1) — это набор слов $(X_1, \ldots, X_n)$ над A таких, что $w(X_1, \ldots, X_n)$ равно 1 в свободной группе, порожденной A.

Аналогично уравнением в свободной полугруппе

$$v(x_1, \ldots, x_n) = w(x_1, \ldots, x_n) \qquad (2)$$

от неизвестных $x_1, \ldots, x_n$ над полугрупповым алфавитом A называется выражение вида (2), где $v(x_1, \ldots, x_n)$ и $w(x_1, \ldots, x_n)$ — слова над $X \cup A$, где $X = \{x_1, \ldots, x_n\}$; $X \cap A = \varnothing$. Решение уравнения (2) — это набор $(X_1, \ldots, X_n)$ слов над A таких, что слова $v(X_1, \ldots, X_n)$ и $w(X_1, \ldots, X_n)$ графически равны.

Прежде чем доказать теорему, покажем, что из нее следует (*). Пусть B — фиксированный конечный алфавит; $\Pi(B)$ — свободная полугруппа слов над B; $L \subseteq \Pi(B)$. Пусть также B' — биективная копия алфавита B. Каждому слову $b_{i_1}b_{i_2} \ldots b_{i_r} \in L$ сопоставим уравнение

$$b_{i_1}b_{i_2} \ldots b_{i_r} = b'_{i_1}b'_{i_2} \ldots b'_{i_r} \qquad (3)$$

от неизвестных $b_1, b'_1, b_2, b'_2, \ldots, b_m, b'_m$, где $m = |B|$, над счетным алфавитом C. Пара гомоморфизмов (g, h) из $\Pi(B)$ в $\Pi(C)$ удовлетворяет условию $g(b_{i_1} \ldots b_{i_r}) = h(b_{i_1} \ldots b_{i_r})$, если и только если $R = (g(b_1), h(b_1), \ldots, g(b_m), h(b_m))$ — решение уравнения (3). Таким образом, условие «$g(x) = h(x)$ для всех $x \in L$» означает, что R — решение системы, состоящей из уравнений вида (3), соответствующих словам из L. Пользуясь теоремой, выбираем конечную подсистему, что дает нам искомое конечное подмножество в L.

Приступим к доказательству теоремы. Докажем сначала ее частный случай, когда рассматриваются уравнения в свободной группе, а алфавит A есть $\{a_1^{\pm 1}, a_2^{\pm 1}\}$.

По теореме Санова [3, с. 129] подгруппа в $SL_2(\mathbf{Z})$, порожденная матрицами $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ и $\begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$, есть свободная группа F_2. Таким образом, гомоморфизм θ: $F_2 \to SL_2(\mathbf{Z})$, определяемый условиями $\theta(a_1) = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$, $\theta(a_2) = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$, есть изоморфное вложение. Пусть $(X_1, \ldots, X_n)$ — набор слов из F_2; обозначим $\theta(X_j) = \begin{pmatrix} P_j & Q_j \\ R_j & S_j \end{pmatrix}$. Очевидно, $\theta(X_j^{-1}) = \begin{pmatrix} S_j & -Q_j \\ -R_j & P_j \end{pmatrix}$. Ясно, что $w(X_1, \ldots, X_n) = 1$

в $F_2 \Leftrightarrow w(\theta X_1, \ldots, \theta X_n) = E$ в $SL_2(\mathbf{Z})$. Последнее означает, что набор $(P_1, Q_1, R_1, S_1, \ldots, P_n, Q_n, R_n, S_n)$ является решением системы из четырех диофантовых уравнений, получаемых перемножением матриц, из которых состоит произведение $w(\theta X_1, \ldots, \theta X_n)$, и приравниванием полученной в результате матрицы к единичной. По этой причине, если $M_j = \begin{pmatrix} P_j & Q_j \\ R_j & S_j \end{pmatrix}$, $j = \overline{1, n}$,— набор из n матриц, лежащих в $\theta(F_2)$, компоненты которых удовлетворяют указанной четверке диофантовых уравнений, то их прообразы $X_j = \theta^{-1}(M_j)$ образуют решение уравнения $w(x_1, \ldots, x_n) = 1$.

Пусть теперь $w_i(x_1, \ldots, x_n) = 1$, $i \in I$,— система уравнений в свободной группе над A. Каждому $i \in I$ сопоставим указанным выше образом четверку диофантовых уравнений (уравнения из одной такой четверки будем называть связанными). Полученная система диофантовых уравнений эквивалентна конечной. Действительно, пусть $\Phi_{ik}(p_1, q_1, r_1, s_1, \ldots, p_n, q_n, r_n, s_n) = 0$, где $k = 1, 2, 3, 4$, $i \in I$,— данная система. Идеал в $\mathbf{Z}[p_1, q_1, \ldots, r_n, s_n]$, порожденный всеми Φ_{ik}, конечно порожден по теореме Гильберта о базисе [4, с. 169]. Поэтому можно выделить конечное число многочленов среди Φ_{ik}, которые порождают этот идеал. Далее добавим, если это необходимо, к каждому выделенному уравнению $\Phi_{ik} = 0$ все связанные с ним. Полученная конечная система эквивалентна исходной; она состоит из уравнений $\Phi_{ik} = 0$, где $k = 1, 2, 3, 4$. $i \in I_0$, $|I_0| < \infty$. «Переводим» ее опять в систему уравнений в свободной группе $w_i(x_1, \ldots, x_n) = 1$, $i \in I_0$. Она эквивалентна первоначальной. Действительно, если $(X_1, \ldots, X_n)$ — ее решение, то компоненты матриц $\theta(X_1), \ldots, \theta(X_n)$ образуют решение конечной системы диофантовых уравнений, а потому и всей системы диофантовых уравнений. По сказанному выше, их прообразы образуют решение исходной системы $w_i(x_1, \ldots, x_n) = 1$, $i \in I$, что и требовалось доказать.

Теперь распространим этот результат на случай, когда алфавит A конечен или счетен. Поскольку существует вложение свободной группы F с базисом A в F_2 [3, с. 128], мы можем рассматривать систему Σ уравнений над A как систему Σ' уравнений над $\{a_1^{\pm 1}, a_2^{\pm 1}\}$. Множество решений Σ над А есть пересечение множества решений Σ' над $\{a_1^{\pm 1}, a_2^{\pm 1}\}$ с n-й прямой степенью F. Сводя Σ' к конечной подсистеме Σ_0' и переходя к подсистеме Σ_0 в Σ, получим систему, эквивалентную Σ, так как множество решений Σ_0 также есть пересечение множества решений Σ_0' с F^n.

Теперь пусть А — алфавит любой мощности, а $w_i(x_1, \ldots, x_n) = 1$, $i \in I$,— система Σ уравнений над А. Предположим, что она не эквивалентна никакой конечной подсистеме. Пусть $i_1 \in I$ — произвольный элемент; так как Σ не эквивалентна системе Σ_1, состоящей из уравнения $w_{i_1} = 1$, то существует решение $R_1 = (X_1^{(1)}, \ldots, X_n^{(1)})$ системы Σ_1, которое не есть решение Σ. Пусть $i_2 \in I$ таково, что R_1 не есть решение $w_{i_2} = 1$. Образуем систему Σ_2, добавляя к Σ_1 уравнение $w_{i_2} = 1$. Опять-таки, существует решение $R_2 = (X_1^{(2)}, \ldots, X_n^{(2)})$ системы Σ_2, которое не есть решение Σ; выбираем $i_3 \in I$ такое, что R_2 не есть решение $w_{i_3} = 1$ и т. д. Получаем счетную систему уравнений $\Sigma_\omega = \bigcup_{l=1}^{\infty} \Sigma_k$. Множество букв из А, входящих в запись хотя бы одного из уравнений из Σ_ω или же хотя бы одного из слов $X_j^{(k)}$, $j = \overline{1, n}$, образует не более чем счетный подалфавит A_0. Система Σ_ω, как система над A_0, не эквивалентна никакой конечной подсистеме: если она эквивалентна, скажем, Σ_s, то получается противоречие, т. к. R_s есть решение Σ_s, но не решение Σ_{s+1}. Итак, групповой вариант теоремы доказан.

Полугрупповой вариант легко следует из группового. Именно, пусть Σ — система уравнений $v_i(x_1, \ldots, x_n) = w_i(x_1, \ldots, x_n)$, $i \in I$, над А. Рассмотрим систему групповых уравнений:

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

(над $A^{\pm 1}$). Сведем ее к конечной ($i \in I_0$, $|I_0| < \infty$). Тогда подсистема в Σ, определяемая I_0, очевидным образом эквивалентна исходной. Теорема полностью доказана.

Московский государственный университет им. М. В. Ломоносова

Поступило 09.04.85

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

[1] Albert J. On the Ehrenfeucht conjecture on test sets and its dial version // Lect. Notes Computer Sci. 1984. V. 176. P. 176—184.

[2] Culic II, Homomorphisms: decidability, equality and test sets // Formal language theory. Perspectives and open problems/ Ed. R. Book. New York: Academic Press, 1980.

[3] Каргаполов М. И., Мерзляков Ю. И. Основы теории групп. М.: Наука, 1982.

[4] Ленг С. Алгебра. М.: Мир. 1968.