Доклады Академии наук СССР
1955. Том 103, № 5

МАТЕМАТИКА

С. И. АДЯН

О ПРОБЛЕМЕ ДЕЛИМОСТИ В ПОЛУГРУППАХ

(Представлено академиком И. М. Виноградовым 6 V 1955)

Ассоциативная система называется полугруппой, если в ней выполнено правило сокращения. Каждая полугруппа определяется заданием определенного алфавита

$$a_1, a_2, \ldots, a_n \tag{1}$$

и системы определяющих соотношений

$$A_i = B_i. \tag{2}$$

Буквы, входящие в алфавит полугруппы, будем называть также образующими полугруппы.

Проблема правой (левой) делимости для полугруппы $\mathfrak{A}$, определенной алфавитом (1) и соотношениями (2), состоит в следующем: указать алгоритм, посредством которого можно было бы для любых двух слов Q и R в $\mathfrak{A}$ узнавать, существует ли слово X в $\mathfrak{A}$ такое, что соотношение $XQ = R$ (соответственно, $QX = R$) выполнено в полугруппе $\mathfrak{A}$.

Полугруппа $\mathfrak{A}$ называется полугруппой с единицей, если в ней есть элемент E, удовлетворяющий равенству

$$XE = X,$$

где X — произвольный элемент полугруппы $\mathfrak{A}$. Единицу полугруппы будем обозначать через 1.

Если полугруппа $\mathfrak{A}$, определенная алфавитом (1) и соотношениями (2), не содержит единицы, то полугруппой с единицей, определенной алфавитом (1) и соотношениями (2), назовем полугруппу $\mathfrak{A}_1$, получающуюся из $\mathfrak{A}$ присоединением к ней единицы.

Если в полугруппе $\mathfrak{A}$ с единицей существует правый обратный элемент для элемента A (т. е. такое X, что $AX = 1$), то он же является левым обратным элементом для A.

Проблема существования обратного элемента для полугруппы $\mathfrak{A}$ с единицей, заданной при помощи образующих и определяющих соотношений, состоит в следующем: найти алгоритм, посредством которого можно было бы для любого слова A в $\mathfrak{A}$ узнавать, существует ли слово X такое, что соотношение $AX = 1$ выполнено в полугруппе $\mathfrak{A}$.

А. А. Марков построил ассоциативную систему с неразрешимой проблемой делимости.

В настоящей заметке излагаются без подробного доказательства следующие результаты.

Теорема 1. *Существует полугруппа, заданная конечным числом образующих и определяющих соотношений, для которой проблема делимости неразрешима.*

Теорема 2. *Невозможно построить полугруппу с конечным числом образующих и определяющих соотношений, для которой была бы неразрешима проблема существования обратного элемента.*

Теорема 3. *Невозможен общий алгоритм для всех полугрупп с единицей, задаваемых конечным числом образующих и определяющих соотношений, решающий в каждой из них проблему существования обратного элемента.*

Теорема 4. *Существует полугруппа, эффективно задаваемая счетным числом образующих и определяющих соотношений, для которой неразрешима проблема существования обратного элемента.*

n°1. П. С. Новиков построил группу с конечным числом образующих и определяющих соотношений, в которой неразрешима проблема тождества слов ([1]). Обозначим эту группу П. С. Новикова через $\mathfrak{A}_0$. Он доказал, что невозможен алгоритм, выясняющий, какие из слов вида XpX^+ (где p — опорная буква группы $\mathfrak{A}_0$; X — произвольное слово из положительных букв левого алфавита; X^+ — соответствующее слово из букв правого алфавита) равны в группе $\mathfrak{A}_0$, какие нет ([1]). В дальнейшем, говоря о словах вида XpX^+, будем подразумевать именно такие слова с указанным ограничением на X и X^+. Обозначим через $\mathfrak{A}_1$ полугруппу с единицей, определяемую тем же положительным алфавитом и системой определяющих соотношений, что и группа $\mathfrak{A}_0$.

Легко заметить, что теоремы 1 и 2 главы VI работы ([1]) содержат в себе доказательство следующего утверждения: *если слова вида XpX^+ равны в группе $\mathfrak{A}_0$, то они равны и в полугруппе $\mathfrak{A}_1$*. С другой стороны, очевидно, что, если слова такого вида равны в полугруппе $\mathfrak{A}_1$, то они равны и в группе $\mathfrak{A}_0$. Так доказывается

Лемма 1. *Для того чтобы два слова вида XpX^+ были равны в полугруппе $\mathfrak{A}_1$, необходимо и достаточно, чтобы они равнялись друг другу в группе $\mathfrak{A}_0$.*

Отсюда следует, что в полугруппе $\mathfrak{A}_1$ неразрешима проблема тождества слов. Пользуясь тем, что группа $\mathfrak{A}_0$ является центрально-симметрической группой с правильной проходной буквой p, нетрудно доказать, что верна следующая лемма:

Лемма 2. *Для того чтобы два слова вида XpX^+ делились справа (слева) друг на друга в полугруппе $\mathfrak{A}_1$, необходимо и достаточно, чтобы они равнялись друг другу в группе $\mathfrak{A}_0$.*

Из этой леммы следует неразрешимость проблемы правой (левой) делимости для полугруппы $\mathfrak{A}_1$.

n°2. Пусть $\mathfrak{A}$ — полугруппа с единицей, заданная образующими (1) и соотношениями (2).

Лемма 3. *Для того чтобы в полугруппе $\mathfrak{A}$ слово*

$$A = a_{i_1} a_{i_2} \dots a_{i_k} \tag{3}$$

имело обратный элемент, необходимо и достаточно, чтобы каждая образующая, входящая в запись (3) *слова A, также имела в $\mathfrak{A}$ обратный элемент.*

Необходимость. Пусть $AX_0 = 1$ в $\mathfrak{A}$. Покажем, что для a_{i_t} $(1 \leqslant t \leqslant k)$ в полугруппе $\mathfrak{A}$ есть обратный элемент X_t. Таким элементом будет

$$X_t = a_{i_{t+1}} a_{i_t} \dots a_{i_k} X_0 a_{i_1} \dots a_{i_{t-1}}.$$

Выполнив в равенстве

$$a_{i_1} \dots a_{i_{t-1}} a_{i_t} a_{i_{t+1}} \dots a_{i_k} X_0 a_{i_1} \dots a_{i_{t-1}} = a_{i_1} \dots a_{i_{t-1}}$$

все сокращения слева, мы найдем, что $a_{i_t} X_t = 1$ в $\mathfrak{A}$.

Достаточность. Допустим, что обратным элементом для каждого a_{i_t} является X_t, т. е. $a_{i_t}X_t = 1$ в $\mathfrak{A}$. Тогда имеем в $\mathfrak{A}$ равенство

$$AX_kX_{k-1}\ldots X_1 = 1,$$

т. е. слово $X_kX_{k-1}\ldots X_1$ будет обратным для A.

Докажем теперь теорему 2. Если бы для конкретной полугруппы $\mathfrak{A}$ с конечным числом образующих и определяющих соотношений была доказана неразрешимость проблемы существования обратного элемента, то этим было бы опровергнуто утверждение: для каждой образующей полугруппы $\mathfrak{A}$ разрешим вопрос о существовании в $\mathfrak{A}$ обратного элемента для нее. Это же означало бы, что в конструктивной математике опровергнут закон исключенного третьего, что невозможно.

n°3. Пусть полугруппа $\mathfrak{A}_1$, о которой шла речь в n°1, задается образующими

$$a_1a_2\ldots a_m \tag{4}$$

и определяющими соотношениями

$$C_l = D_l. \tag{5}$$

Для доказательства теоремы 3 построим систему полугрупп, для которой уже невозможен общий алгоритм, решающий в каждой из этих групп проблему существования обратного элемента. Пусть (A, B) — произвольная пара слов полугруппы $\mathfrak{A}_1$ вида XpX_1. Каждой такой паре слов соотнесем полугруппу с единицей, которую обозначим через $\mathfrak{A}_{7,A,B}$. Алфавит полугруппы $\mathfrak{A}_{q,A,B}$ получается добавлением к (4) одной новой буквы q. Система определяющих соотношений получается добавлением к соотношениям (5) одного соотношения

$$p^2qB = qA, \tag{6}$$

где p — опорная буква группы $\mathfrak{A}_0$.

На основе свойств центрально-симметрической группы $\mathfrak{A}_0$ доказывается:

Лемма 4. *Для того чтобы в полугруппе $\mathfrak{A}_{7,A,B}$ для буквы p существовал обратный элемент, необходимо и достаточно, чтобы выполнялось равенство $A = B$ в группе $\mathfrak{A}_0$.*

Из этой леммы следует верность теоремы 3.

n°4. Упорядочим все пары (A, B) слов вида XpX^+ полугруппы $\mathfrak{A}$ в последовательность

$$(A_1B_1);\ (A_2B_2);\ \ldots;\ (A_j,\ B_j);\ \ldots \tag{7}$$

Полугруппа $\mathfrak{B}_1$, существование которой утверждается в теореме 4, строится следующим образом. В качестве образующих $\mathfrak{B}_1$ берем счетную последовательность букв

$$b_1,\ b_2,\ \ldots,\ b_i,\ \ldots \tag{8}$$

Система определяющих соотношений составляется объединением счетного числа подсистем

$$S_1,\ S_2,\ \ldots,\ S_j,\ \ldots \tag{9}$$

Здесь каждое S_i есть конечная система соотношений, которая строится по индексу i следующим образом: находим в (7) пару (A_i, B_i), записываем по этой паре систему определяющих соотношений полугруппы $\mathfrak{A}_{q,A_i,B_i}$, заменяя в них образующие полугруппы $\mathfrak{A}_{q,A_i,B_i}$ буквами

$$b_{(i-1)(m+1)+1},\ b_{(i-1)(m+1)+2},\ \ldots,\ b_{i(m+1)}, \tag{10}$$

взятыми из (8), причем соблюдается требование, чтобы роль буквы p (опорной буквы группы $\mathfrak{A}_0$) в соотношениях системы S_i играла буква $b_{i\,(m+1)}$.

Короче говоря, полугруппа $\mathfrak{B}_1$ будет свободным произведением полугрупп $\mathfrak{A}_{q,\,A_i,\,B_i}$, взятых для каждой пары (A_i, B_i) из последовательности (7). Поэтому вопрос о существовании обратного элемента для $b_{i\,(m+1)}$ в полугруппе $\mathfrak{B}_1$ эквивалентен вопросу о существовании обратного элемента для буквы p в полугруппе $\mathfrak{A}_{q,\,A_i,\,B_i}$, который, в силу леммы 4, эквивалентен вопросу о верности равенства $A_i = B_i$ в группе $\mathfrak{A}_0$. Таким образом, невозможен алгоритм, решающий проблему существования обратного элемента для образующих полугруппы $\mathfrak{B}_1$. Этим доказана теорема 4.

Московский государственный
педагогический институт
им. В. И. Ленина

Поступило
28 IV 1955

ЦИТИРОВАННАЯ ЛИТЕРАТУРА

[1] П. С. Новиков, Тр. Матем. инст. им. В. А. Стеклова, 44 (1955). [2] А. А. Марков, ДАН, 58, № 3 (1947).