Доклады Академии Наук СССР
1947. Том LVII, № 6

МАТЕМАТИКА

А. МАРКОВ

О НЕКОТОРЫХ НЕРАЗРЕШИМЫХ ПРОБЛЕМАХ, КАСАЮЩИХСЯ МАТРИЦ

(Представлено академиком И. М. Виноградовым 8 V 1947)

1. Будем рассматривать квадратные матрицы порядка n с целыми коэффициентами, где n — фиксированное натуральное число. Такие матрицы будем называть n-матрицами. n-матрица с определителем, равным 1, называется унимодулярной. Множество унимодулярных n-матриц мы называем полугруппой, если произведение любых двух матриц, принадлежащих этому множеству, также принадлежит ему.

Для всякого множества унимодулярных n-матриц существуют полугруппы, содержащие это множество, и среди них имеется единственная наименьшая, о которой мы говорим, что она порождается данным множеством матриц. Полугруппу, порождаемую конечным множеством матриц $\{X_1, \ldots, X_p\}$, мы обозначаем символом $S(X_1, \ldots, X_p)$. Это, очевидно, есть совокупность матриц вида

$$\prod_{k=1}^{m} X_{i_k}, \tag{1}$$

где m — целое положительное число, i_k $(k=1, \ldots, m)$ — целые положительные числа, не превосходящие p.

Для любых двух конечных множеств унимодулярных n-матриц $\{X_1, \ldots, X_p\}$ и $\{Y_1, \ldots, Y_q\}$ естественно поставить вопрос о том, имеют ли порождаемые ими полугруппы $S(X_1, \ldots, X_p)$ и $S(Y_1, \ldots, Y_q)$ хотя бы один общий элемент. Естественно, далее, поставить проблему о разыскании алгорифма, посредством которого можно было бы для любых двух данных конечных множеств унимодулярных n-матриц $\{X_1, \ldots, X_p\}$ и $\{Y_1, \ldots, Y_q\}$ узнавать, имеют ли полугруппы $S(X_1, \ldots, X_p)$ и $S(Y_1, \ldots, Y_q)$ хотя бы один общий элемент. Число n при этом фиксировано. Термин „алгорифм“ применяется здесь в смысле Church'а — Kleene'а — Turing'а.

Теорема 1. *При $n \geqslant 4$ только что формулированная проблема неразрешима: искомый алгорифм невозможен при таком n.*

Дополнение. При всяком $n \geqslant 4$ могут быть так заданы числа p, q и унимодулярные n-матрицы $X_2, \ldots, X_p, Y_1, \ldots, Y_q$, что будет неразрешима и более частная проблема о разыскании алгорифма, посредством которого можно было бы для любой унимодулярной n-матрицы X_1 узнавать, имеют ли полугруппы $S(X_1, \ldots, X_p)$ и $S(Y_1, \ldots, Y_q)$ хотя бы один общий элемент. Числа p и q можно при этом задать независимо от n и, в частности, положить $q=2$.

2. Непустое множество n-матриц мы называем решеткой, если разность любых двух матриц, принадлежащих этому множеству, принадлежит ему.

Для всякого множества n-матриц существуют содержащие его решетки и среди них имеется единственная наименьшая, о которой мы говорим, что она порождается данным множеством матриц. Решетку, порождаемую конечным множеством матриц $\{X_1, \ldots, X_p\}$, мы обозначаем символом $L(X_1, \ldots, X_p)$. Это, очевидно, есть совокупность матриц вида

$$\sum_{i=1}^{p} \lambda_i X_i,$$

где λ_i $(i=1, \ldots, p)$ — целые числа.

Для любого конечного множества унимодулярных n-матриц $\{X_1, \ldots, X_p\}$ и любого конечного множества n-матриц $\{Y_1, \ldots, Y_q\}$ возникает вопрос о том, имеет ли полугруппа $S(X_1, \ldots, X_p)$ общий элемент с решеткой $L(Y_1, \ldots, Y_q)$. Естественно, далее, поставить проблему о рзыскании алгорифма, посредством которого можно было бы для любого конечного множества унимодулярных n-матриц $\{X_1, \ldots, X_p\}$ и любого конечного множества n-матриц $\{Y_1, \ldots, Y_q\}$ узнавать, имеет ли полугруппа $S(X_1, \ldots, X_p)$ общий элемент с решеткой $L(Y_1, \ldots, Y_q)$.

Теорема 2. *При $n \geqslant 4$ только что формулированная проблема неразрешима: искомый алгорифм невозможен при таком n.*

Дополнение 1. При всяком $n \geqslant 4$ могут быть так заданы числа p, q, унимодулярные n-матрицы $X_2, \ldots, X_p$ и n-матрицы $Y_1, \ldots, Y_q$, что будет неразрешима и более частная проблема о разыскании алгорифма, посредством которого можно было бы для любой унимодулярной n-матрицы X_1 узнавать, имеет ли полугруппа $S(X_1, \ldots, X_p)$ общий элемент с решеткой $L(Y_1, \ldots, Y_q)$. Числа p и q можно при этом задать независимо от n и, в частности, положить $q=5$. При $n=4$ годится и $q=4$.

Дополнение 2. При всяком $n \geqslant 4$ могут быть так заданы числа p, q и унимодулярные n-матрицы $X_1, \ldots, X_p$, что будет неразрешима проблема о разыскании алгорифма, посредством которого можно было бы для любых n-матриц $Y_1, \ldots, Y_q$ узнавать, имеет ли полугруппа $S(X_1, \ldots, X_p)$ общий элемент с решеткой $L(Y_1, \ldots, Y_q)$. Числа p и q можно при этом задать независимо от n и, в частности, положить $q=5$. При $n=4$ годится и $q=4$.

3. Доказательства этих результатов основаны на следующей теореме Post'a [1].

Пусть A_0 — алфавит, состоящий из букв a, b. Невозможен алгорифм, посредством которого можно было бы для любой конечной системы пар слов G_i, G_i' $(i=1, \ldots, p)$ в A_0 узнавать, осуществляется ли равенство

$$G_{i_1} \ldots G_{i_m} = G'_{i_1} \ldots G'_{i_m} \tag{2}$$

при каком-нибудь выборе целого положительного числа m и целых положительных чисел $i_1, \ldots, i_m$, не превосходящих p.

Из приведенного Post'ом доказательства этой теоремы легко усмотреть, что она может быть дополнена следующим образом.

Число p и слова $G_2, \ldots, G_p, G_1', \ldots, G_p'$ в A_0 могут быть так выбраны, что не будет возможен алгорифм, посредством которого можно было бы для любого слова G_1 в A_0 узнавать, осуществляется ли равенство (2) при каком-нибудь выборе целого положительного числа m и целых положительных чисел $i_1, \ldots, i_m$, не превосходящих p.

Из того же доказательства усматривается, что имеет место и следующая теорема.

Число p и слова H, G_i, G_i' $(i=1, \ldots, p)$ в A_0 могут быть выбраны так, что не будет возможен алгорифм, посредством которого можно было бы для любого слова R в A_0 узнавать, осуществляется ли равенство

$$HG_{i_1}\ldots G_{i_m}=G'_{i_1}\ldots G'_{i_m}R$$

при каком-нибудь выборе целого положительного числа m и целых положительных чисел $i_1,\ldots,i_m$, не превосходящих p.

4. Переход от этих результатов Post'a к вышеприведенным теоремам о матричных полугруппах осуществляется с помощью построения той или иной свободной полугруппы 2-матриц с двумя производящими элементами. Такие полугруппы известны. Например, матрицы

$$A=\begin{bmatrix}1&1\\0&1\end{bmatrix},\quad B=\begin{bmatrix}1&0\\1&1\end{bmatrix}$$

порождают свободную полугруппу; иначе говоря, всякая матрица представимая в виде произведения положительных степеней матриц A и B, представляется так единственным образом ([2]). Это дает возможность перевести результаты Post'a на матричный язык. В частности, первый из них дает следующую лемму.

Невозможен алгорифм, посредством которого можно было бы для любой конечной системы пар 2-матриц Z_i, Z_i' $(i=1,\ldots,p)$ из полугруппы $S(A,B)$ узнавать, осуществляется ли равенство

$$\prod_{k=1}^{m} Z_{i_k}=\prod_{k=1}^{m} Z'_{i_k} \tag{3}$$

при каком-нибудь выборе целого положительного числа m и целых положительных чисел $i_1,\ldots,i_m$, не превосходящих p.

Аналогичные леммы получаются из других цитированных результатов Post'a.

5. Рассмотрение системы пар 2-матриц Z_i, Z_i' $(i=1,\ldots,p)$ сводится к рассмотрению системы 4-матриц

$$X_i=Z_i \dot{+} Z_i' \quad (i=1,\ldots,p), \tag{4}$$

где $\dot{+}$ есть знак прямого сложения. Равенство (3) имеет место тогда и только тогда, когда матрица (1) с так определенными X имеет вид $Z\dot{+}Z'$ где Z есть 2-матрица. Если при этом Z_i, Z_i' принадлежит полугруппе $S(A,B)$, то и Z принадлежит этой полугруппе. Но совокупность матриц вида $Z\dot{+}Z$, где Z принадлежит $S(A,B)$, есть, очевидно, полугруппа $S(A\dot{+}A,\ B\dot{+}B)$. Таким образом, равенство (3) осуществляется для матриц Z_i, Z_i' $(i=1,\ldots,p)$ из $S(A,B)$ при некотором выборе целого положительного числа m и целых положительных чисел $i_1,\ldots,i_m$ в том и только в том случае, когда полугруппа $S(X_1,\ldots,X_p)$ имеет общий элемент с полугруппой $S(A\dot{+}A,\ B\dot{+}B)$.

В силу этого дополнение к теореме Post'a в матричной формулировке дает теорему 1 и дополнение к ней для частного случая $n=4$. Мы усматриваем при этом, что можно положить $q=2$, $Y_i=A\dot{+}A$, $Y_2=B\dot{+}B$. Переход к случаю любого $n>4$ в дополнении к теореме 1 осуществляется посредством прямого сложения построенных для $n=4$ матриц $X_2,\ldots,X_p$, Y_1, Y_2 с матрицей I_{n-4}, где I_h означает единичную h-матрицу.

6. Положим

$$E_{11}=\begin{bmatrix}1&0\\0&0\end{bmatrix},\quad E_{12}=\begin{bmatrix}0&1\\0&0\end{bmatrix},\quad E_{21}=\begin{bmatrix}0&0\\1&0\end{bmatrix},\quad E_{22}=\begin{bmatrix}0&0\\0&1\end{bmatrix},$$

$$F_{rs}=E_{rs}\dot{+}E_{rs} \quad (r,\ s=1,\ 2).$$

Матрицы вида $Z \dotplus Z$, где Z есть 2-матрица, очевидно, образуют решетку $L(F_{11}, F_{12}, F_{21}, F_{22})$. Следовательно, равенство (3) осуществляется для матриц $Z_i\, Z_i'$ ($i=1,\ldots,p$) из полугруппы $S(A, B)$ при некотором выборе целого положительного числа m и целых положительных чисел $i_1,\ldots,i_m$ в том и только в том случае, когда полугруппа $S(X_1,\ldots,X_p)$ имеет общий элемент с решеткой $L(F_{11},F_{12},F_{21},F_{22})$.

В силу этого дополнение к теореме Post'a в матричной формулировке дает теорему 2 и дополнение 1 к этой теореме для частного случая $n=4$. Мы видим что здесь можно положить $p=4$, $Y_1=F_{11}$, $Y_2=F_{12}$, $Y_3=F_{21}$, $Y_4=F_{22}$. Переход к любому $n>4$ в дополнении 1 осуществляется посредством прямого сложения построенных для $n=4$ матриц $X_2,\ldots,X_p$ с I_{n-4}, матриц Y_1,Y_2,Y_3,Y_4 с 0_{n-4} и присоединения новой матрицы $Y_5=I_n$. При этом p не меняется, а q увеличивается на 1. 0_h означает здесь нулевую h-матрицу. При $n=4$ можно, конечно, также положить $q=5$ и присоедиинить матрицу $Y_5=I_4$.

7. Чтобы доказать дополнение 2 к теореме 2, зададим матрицы C, Z_i, Z_i' ($i=1,\ldots,p$) из $S(A, B)$ таким образом, что не будет возможен алгорифм, посредством которого можно было бы для любой матрицы Q из S (A, B) узнавать, осуществляется ли равенство

$$C \prod_{k=1}^{m} Z_{i_k} = \left(\prod_{k=1}^{m} Z'_{i_k}\right) Q \tag{5}$$

при каком-нибудь выборе целого положительного числа m и целых положительных чисел $i_1,\ldots,i_m$, не превосходящих p. Задать так эти матрицы возможно, согласно цитированному выше результату Post'a, переведенному на матричный язык.

Определим матрицы $X_1,\ldots,X_p$ равенством (4) и положим

$$D = C \dotplus I_2.$$

Равенство (5) окажется тогда равносильным тому, что матрица

$$D\left(\prod_{k=1}^{m} X_{i_k}\right) W,$$

где $W = I_2 \dotplus Q$, принадлежит решетке $L(F_{11}, F_{12}, F_{21}, F_{22})$, а это равносильно тому, что матрица (1) принадлежит решетке

$$L(D^{-1}F_{11}W^{-1},\ D^{-1}F_{12}W^{-1},\ D^{-1}F_{21}W^{-1},\ D^{-1}F_{22}W^{-1}). \tag{6}$$

Следовательно, невозможен алгорифм, посредством которого можно было бы для любой унимодулярной 4-матрицы W узнавать, имеет ли решетка (6) общие элементы с полугруппой $S(X_1,\ldots,X_p)$. Тем более невозможен алгорифм, посредством которого можно было бы для любых 4-матриц Y_1, Y_2, Y_3, Y_4 узнавать, имеет ли решетка $L(Y_1, Y_2, Y_3, Y_4)$ общие элементы с полугруппой $S(X_1,\ldots,X_p)$. Этим доказано дополнение 2 для $n=4$. Переход к любому $n>4$ очевиден.

Поступило
8 V 1947

ЦИТИРОВАННАЯ ЛИТЕРАТУРА

[1] E. L. Post, Bull. Am. Math. Soc., 52, 4, 246 (1946). [2] J. Nielsen, Danske Vidensk. Selsk. Math.-Fys. Medd., 5, 12 (1924).