

А. МАРКОВ

## ОБ ОДНОЙ НЕРАЗРЕШИМОЙ ПРОБЛЕМЕ, КАСАЮЩЕЙСЯ МАТРИЦ

(Представлено академиком И. М. Виноградовым 17 IV 1951)

1. Будем рассматривать квадратные целочисленные матрицы конечного порядка. Будем их называть просто матрицами.

2. Пусть  $U_1, \dots, U_q$  — матрицы порядка  $n$ . Будем говорить о матрице  $U$  порядка  $n$ , что она представима через  $U_1, \dots, U_q$ , если существуют целое положительное число  $\lambda$  и целые числа  $i_1, \dots, i_\lambda$  ( $1 \leq i_v \leq q$ ) такие, что

$$U = \prod_{v=1}^{\lambda} U_{i_v}.$$

3. В связи с понятием представимости естественно возникают следующие проблемы.

Общая проблема представимости. Дано целое положительное число  $n$ ; требуется указать алгоритм, посредством которого можно было бы узнавать для любой системы матриц  $U, U_1, \dots, U_q$  порядка  $n$ , представима ли матрица  $U$  через  $U_1, \dots, U_q$ .

Частная проблема представимости. Даны матрицы  $U_1, \dots, U_q$  порядка  $n$ ; требуется указать алгоритм, посредством которого можно было бы узнавать для любой матрицы  $U$  того же порядка, представима ли она через  $U_1, \dots, U_q$ .

В общей проблеме представимости число  $n$  играет роль параметра. Каждому значению  $n$  соответствует своя алгоритмическая проблема. В частной проблеме представимости роль параметра играет система матриц  $U_1, \dots, U_q$  порядка  $n$ . Всякому выбору такой системы соответствует своя алгоритмическая проблема.

Термин «алгоритм» мы применяем в этих проблемах в современном точном смысле.

4. При всяком  $n \geq 6$  может быть так указана система матриц  $U_1, \dots, U_q$  порядка  $n$ , что частная проблема представимости будет неразрешима для этой системы матриц: искомый в проблеме алгоритм не будет возможен. Число  $q$  матриц  $U_1, \dots, U_q$  может быть взято независимым от  $n$  (в частности, можно взять  $q = 102$ ).

Отсюда непосредственно следует, что общая проблема представимости неразрешима при  $n \geq 6$ .

5. Наметим вкратце доказательство формулированного результата. Определим матрицы  $A_1$  и  $A_2$  2-го порядка, положив

$$A_1 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \quad A_2 = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}.$$

Как было ранее указано <sup>(2)</sup>, возможно так задать матрицы  $S, Z_i, Z'_i$  ( $i = 1, \dots, p$ ), представимые через  $A_1$  и  $A_2$ , что не будет возможен алгоритм, посредством которого можно было бы узнавать для

любой матрицы  $Q$ , представимой через  $A_1$  и  $A_2$ , осуществляется ли равенство

$$C \prod_{v=1}^{\lambda} Z_{i_v} = \left( \prod_{v=1}^{\lambda} Z'_{i_v} \right) Q \quad (1)$$

при каком-нибудь выборе целого положительного числа  $\lambda$  и целых положительных чисел  $i_1, \dots, i_\lambda$ , не превосходящих  $p$ . (Исходя из конкретной ассоциативной системы с неразрешимой проблемой тождества <sup>(1)</sup>, удается осуществить указанное построение матриц при  $p = 99$ .)

6. В дальнейшем  $I_h$  означает единичную матрицу  $h$ -го порядка,  $O_h$  — нулевую матрицу  $h$ -го порядка, знак  $+$  — прямое сложение матриц. Положим  $D = C + I_2$ ,  $X_i = Z_i + Z'_i$  ( $i = 1, \dots, p$ ),  $B_j = A_j + A_j$  ( $j = 1, 2$ ).

Как нетрудно видеть, равенство (1) тогда и только тогда имеет место для матрицы  $Q$ , представимой через  $A_1$  и  $A_2$ , когда матрица 4-го порядка  $D \left( \prod_{v=1}^{\lambda} X_{i_v} \right) (I_2 + Q)$  представима через  $B_1$  и  $B_2$ . А это, ввиду унимодулярности всякой такой матрицы  $Q$ , имеет место тогда и только тогда, когда матрица 4-го порядка  $(I_2 + Q)^{-1}$  может быть представлена в виде

$$\left( \prod_{p=1}^{\sigma} B_{j_p}^{-1} \right) D \prod_{v=1}^{\lambda} X_{i_v} \quad \text{с } \sigma, \lambda > 0 \quad (j_1, \dots, j_\sigma = 1, 2; i_1, \dots, i_\lambda = 1, \dots, p). \quad (2)$$

Следовательно, невозможен алгоритм, посредством которого можно было бы узнавать для любой матрицы 4-го порядка, может ли она быть представлена в виде (2) с  $\sigma, \lambda > 0$ .

7. Введем теперь матрицы 2-го порядка  $E_1 = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ ,  $E_2 = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$ . Как нетрудно видеть,

$$E_i^\nu = E_i \quad (i = 1, 2; \nu = 1, 2, \dots), \quad (3)$$

$$E_1 E_2 = E_2 E_1 = O_2. \quad (4)$$

Для любой матрицы  $N = \begin{bmatrix} N_{11} & N_{12} \\ N_{21} & N_{22} \end{bmatrix}$  2-го порядка имеем

$$E_1 N = \begin{bmatrix} N_{11} & N_{12} \\ 0 & 0 \end{bmatrix}, \quad E_2 N = \begin{bmatrix} 0 & 0 \\ N_{21} & N_{22} \end{bmatrix}, \quad N E_1 = \begin{bmatrix} N_{11} & 0 \\ N_{21} & 0 \end{bmatrix}, \quad N E_2 = \begin{bmatrix} 0 & N_{12} \\ 0 & N_{22} \end{bmatrix}. \quad (5)$$

Введем еще матрицы 2-го порядка

$$F = \begin{bmatrix} 0 & 0 \\ 2 & 0 \end{bmatrix}, \quad G = \begin{bmatrix} 2 & 0 \\ 2 & 2 \end{bmatrix}. \quad (6)$$

Согласно (3) и (5)

$$E_2^\sigma G E_1^\lambda = F \quad (\sigma, \lambda = 1, 2, \dots). \quad (7)$$

8. Условимся обозначать через  $\Delta U$  общий наибольший делитель коэффициентов матрицы  $U$ . Имеем

$$\Delta F = \Delta G = 2. \quad (8)$$

В силу билинейности закона умножения матриц, для любой системы матриц  $U_1, \dots, U_s$  одного и того же порядка имеет место делимость

$$\prod_{i=1}^s \Delta U_i \mid \Delta \prod_{i=1}^s U_i. \quad (9)$$

9. Положим теперь

$$X_{p+1} = D, \quad (10)$$

$$X_{p+1+j} = B_j^{-1} \quad (j = 1, 2), \quad (11)$$

$$Y_i = E_1 \quad (i = 1, \dots, p), \quad Y_{p+1} = G, \quad Y_i = E_2 \quad (i = p+2, p+3). \quad (12)$$

Так как матрицы 4-го порядка  $X_i$  ( $i = 1, \dots, p$ ) были уже введены ранее, имеем теперь систему матриц 4-го порядка  $X_i$  и матриц 2-го порядка  $Y_i$  с  $i = 1, \dots, p+3$ . Положим

$$U_i = X_i + Y_i \quad (i = 1, \dots, p+3), \quad (13)$$

определяя этим систему матриц  $U_i$  ( $i = 1, \dots, p+3$ ) 6-го порядка. Мы покажем, что для этой системы матриц неразрешима частная проблема представимости. Согласно предыдущему, для этого достаточно доказать следующую лемму.

*Матрица  $W$  4-го порядка тогда и только тогда может быть представлена в виде (2) с  $\sigma, \lambda > 0$  ( $j_1, \dots, j_\sigma = 1, 2$ ;  $i_1, \dots, i_\lambda = 1, \dots, p$ ), когда матрица  $W + F$  представима через  $U_1, \dots, U_{p+3}$ .*

Докажем эту лемму.

10. Допустим сперва, что

$$W = \left( \prod_{\rho=1}^{\sigma} B_{j_\rho}^{-1} \right) D \prod_{\nu=1}^{\lambda} X_{i_\nu}, \quad (14)$$

где  $\sigma, \lambda > 0$ ;  $j_1, \dots, j_\sigma = 1, 2$ ;  $i_1, \dots, i_\lambda = 1, \dots, p$ .

Согласно (10), (11) и (14)

$$W = \prod_{\rho=1}^{\sigma+1+\lambda} X_{h_\rho}, \quad (15)$$

где

$$\begin{aligned} h_\rho &= p+1+j_\rho \quad (\rho = 1, \dots, \sigma), \quad h_{\sigma+1} = p+1, \\ h_\rho &= i_{\rho-\sigma-1}, \quad (\rho = \sigma+2, \dots, \sigma+1+\lambda). \end{aligned} \quad (16)$$

С другой стороны, согласно (7), (12) и (16),

$$F = \prod_{\rho=1}^{\sigma+1+\lambda} Y_{h_\rho}. \quad (17)$$

В силу (13), (15) и (17),

$$W + F = \prod_{\rho=1}^{\mu} U_{h_\rho}, \quad (18)$$

где  $\mu = \sigma+1+\lambda$ . Следовательно, матрица  $W + F$  представима в этом случае через матрицы  $U_1, \dots, U_{p+3}$ .

11. Допустим теперь, что матрица  $W + F$  представима через матрицы  $U_1, \dots, U_{p+3}$ , т. е. что для некоторого целого положительного  $\mu$

и некоторых  $h_1, \dots, h_\mu = 1, \dots, p+3$  имеет место равенство (18). Покажем, что тогда матрица  $W$  может быть представлена в виде (9) с  $\sigma, \lambda > 0, j_1, \dots, j_\sigma = 1, 2; i_1, \dots, i_\lambda = 1, \dots, p$ .

Согласно (13) и (18)

$$W = \prod_{\rho=1}^{\mu} X_{h_\rho} \quad (19)$$

$$F = \prod_{\rho=1}^{\mu} Y_{h_\rho}. \quad (20)$$

Согласно (12), каждая из матриц  $Y_{h_\rho}$  равна  $E_1, E_2$  или  $G$ . Но, в силу (3), (4) и (6), матрица  $F$  не представима через  $E_1$  и  $E_2$ . Поэтому, согласно (20), существует  $\rho$ , для которого  $Y_{h_\rho} = G$ . С другой стороны, не может быть более одного такого  $\rho$ , так как иначе, согласно (20), (8) и (9), выходило бы, что 2 делится на 4. Обозначим через  $\tau$  единственное значение  $\rho$ , для которого  $Y_{h_\rho} = G$ . Имеем  $Y_{h_\tau} = G$ , тогда как  $Y_{h_\rho} = E_1$  или  $E_2$  при  $\rho \neq \tau$ .

Равенства (4), (6) и (20) показывают далее, что не может быть  $\nu$  и  $\rho$ , удовлетворяющих условиям:  $\nu < \tau, \rho < \tau, Y_{h_\nu} = E_1, Y_{h_\rho} = E_2$ . Не может быть также  $\nu$  и  $\rho$ , удовлетворяющих условиям:  $\nu > \tau, \rho > \tau, Y_{h_\nu} = E_1, Y_{h_\rho} = E_2$ . Таким образом, либо для всех рассматриваемых  $\rho < \tau$  имеем  $Y_{h_\rho} = E_1$ , либо для всех таких  $\rho$  имеем  $Y_{h_\rho} = E_2$ . Совершенно так же обстоит дело для  $\rho > \tau$ .

Мы видим далее, что не может существовать  $\rho$ , меньших  $\tau$  и таких, что  $Y_{h_\rho} = E_1$ . Иначе мы имели бы  $Y_{h_1} = E_1$  и, согласно (20), матрица  $F$  представлялась бы в виде  $E_1 N$ , что невозможно в силу (5) и (6). Аналогичным образом не может быть  $\rho$ , больших  $\tau$  и таких, что  $Y_{h_\rho} = E_2$ . Следовательно,  $Y_{h_\rho} = E_2$  для всех рассматриваемых  $\rho$ , меньших  $\tau$ , и  $Y_{h_\rho} = E_1$  для всех рассматриваемых  $\rho$ , больших  $\tau$ . В силу этого, сообразно тому, имеем ли мы  $1 = \tau = \mu, 1 = \tau < \mu, 1 < \tau = \mu$  или  $1 < \tau < \mu$ , правая часть равенства (20) равна, согласно (3), одной из матриц:  $G, GE_1, E_2 G, E_2 G E_1$ . Но из этих четырех матриц лишь последняя равна  $F$ . Следовательно,  $1 < \tau < \mu$ .

Положим  $\sigma = \tau - 1, \lambda = \mu - \tau$ . Имеем  $\sigma, \lambda > 0, \tau = \sigma + 1, \mu = \sigma + 1 + \lambda$  и, согласно вышесказанному,  $Y_{h_\rho} = E_2$  при  $\rho = 1, \dots, \sigma; Y_{h_{\sigma+1}} = G, Y_{h_\rho} = E_1$  при  $\rho = \sigma + 2, \dots, \sigma + 1 + \lambda$ . В силу (12) отсюда следует, что  $h_\rho > p + 1$  при  $\rho = 1, \dots, \sigma; h_{\sigma+1} = p + 1$  и  $h_\rho \leq p$  при  $\rho = \sigma + 2, \dots, \sigma + 1 + \lambda$ . Положим  $j_\rho = h_\rho - p - 1$  ( $\rho = 1, \dots, \sigma$ ),  $i_\nu = h_{\sigma+1+\nu}$  ( $\nu = 1, \dots, \lambda$ ). Имеем  $j_\rho = 1, 2$  ( $\rho = 1, \dots, \sigma$ ),  $i_\nu = 1, \dots, p$  ( $\nu = 1, \dots, \lambda$ ). Согласно (11),  $X_{h_\rho} = X_{p+1+j_\rho} = B_{j_\rho}^{-1}$  ( $\rho = 1, \dots, \sigma$ ); согласно (10),  $X_{h_{\sigma+1}} = X_{p+1} = D$ . Мы заключаем поэтому из (19), что имеет место равенство (14), что и требовалось доказать.

12. Мы доказали таким образом наш основной результат для  $n = 6$  при  $q = p + 3$ . Переход к любому  $n > 6$  легко выполняется хотя бы путем прямого сложения построенных для  $n = 6$  матриц  $U_1, \dots, U_q$  с матрицей  $O_{n-6}$ . Число  $q$  остается при этом неизменным. (Так как можно обойтись с  $p = 99$ , в качестве  $q$  можно взять 102. По всей вероятности, можно обойтись и значительно меньшим числом матриц.)

Ленинградское отделение  
Математического института им. В. А. Стеклова  
Академии наук СССР

Поступило  
16 IV 1951

#### ЦИТИРОВАННАЯ ЛИТЕРАТУРА

<sup>1</sup> А. Марков, ДАН, 58, № 3 (1947). <sup>2</sup> А. Марков, ДАН, 57, № 6 (1947).