УДК 519.1

ЧЖАН БИНЬ

РЕШЕНИЕ МАТРИЧНОЙ ЗАДАЧИ О МАТЕМАТИЧЕСКОМ СЕЙФЕ С РАЗЛИЧНЫМИ ЗАМКАМИ

Abstract: *The mathematical safe problem in case of locks of various types is solved for the first time in this paper. Two theorems are proved, that allow to obtain solution to this problem for specific types of locks.*
Key words: *mathematical safe, set of locks, solution of comparison systems, final safe state, modulo residue class.*

Анотація: *Вперше досліджується матрична задача про математичний сейф з замками різних типів. Доводяться дві теореми, що дозволяє отримати розв'язок задачі для конкретних типів замків.*
Ключові слова: *математичний сейф, множина замків, розв'язок системи порівнянь, фінальний стан сейфа, клас лишків за модулем.*

Аннотация: *Впервые исследуется матричная задача о математическом сейфе с замками различных типов. Доказываются две теоремы, что позволяет получить решение задачи для конкретных типов замков.*
Ключевые слова: *математический сейф, множество замков, решение системы сравнений, финальное состояние сейфа, класс вычетов по модулю.*

1. Введение

Общая задача о математическом сейфе впервые была сформулирована в [1].

Задача. Математическим сейфом называется система $S\left(Z, b, \langle Z \rangle\right)$, состоящая из множества замков $Z = \{z_1, z_1, \ldots, z_N\}$, вектора состояний сейфа $b = (b_1, b_2, ..., b_N)$, где $b_i \in \{0,1,\ldots,k_i - 1\}$ – состояние i-го замка, и множества $\langle Z \rangle = \{Z_1, Z_2, ..., Z_N\}$, $z_l \in Z_l$, $Z_l \in 2^Z \left(1 \le i \le N\right)$. В результате одного поворота ключом по часовой стрелке в замке z_i все замки $z_j \in Z_l$ переходят из состояния b_j в состояние $(b_j + 1)\left(\mathrm{mod}\, k_j\right)$. Сейф считается открытым, если он находится в состоянии $\vec{b} = (0,0,\ldots,0) = b_{fin}$. Необходимо для каждого замка z_i найти такое количество поворотов x_i ключом, чтобы открыть сейф.

Вектор $\mathbf{X} = (x_1, x_2, \ldots, x_N)$ будем называть решением задачи о сейфе. Множество $\langle \mathbf{Z} \rangle$ называется множеством инцидентности. Его можно записать в виде матрицы инцидентности $\mathbf{A} = (a_{ij})$ размером $N \times N$, где на главной диагонали стоят нули, а $a_{ij} = 1$, если z_j принадлежит множеству $Z_i \left(1 \le i, j \le N\right)$, и нулю в противном случае.

Предполагается, что начальное положение сейфа $\vec{b}$ известно или, по крайней мере, его можно легко вычислить. Если $k_i = const$ для всех $1 \le i \le N$, то такие замки называются однотипными.

Рассмотрим сейф, у которого все замки расположены в виде прямоугольной таблицы размером $m \times n$. Для нее $N = mn$, $l = n(i-1) + j$ $(i = 1,2,...,m;\ \ j = 1,2,...,n)$. Обозначим Z_l – множество замков, объединяющее замки i-й строки и j-го столбца, и пусть все замки принадлежат двум типам, то есть $K = (k_1,\ k_2)$. В зависимости от значения параметра l любому

начальному состоянию сейфа соответствует матрица $B = (b_{ij})_{m,n}$, где $b_{ij} \in \{0,1,...,k_1 - 1\}$, или множеству $\{0,1,...,k_2 - 1\}$. Пусть $X = (x_{ij})_{m,n}$ – решение задачи, где x_{ij} равно числу поворотов ключа в замке z_l.

2. Решение задачи для двух замков со взаимно простыми k_1 и k_2

Здесь решается задача для сейфов, у которых первые p строк матрицы *B* представляют замки первого типа, а остальные строки – замки второго типа. По аналогии с вектором $\vec{b}$ введем соответствующий вектор-столбец $x = (x_1, x_2, ..., x_{mn})$, полученный из матрицы X путем последовательной записи строк.

Пусть $\Im_n$ – квадратная матрица порядка n, состоящая из единиц, а E_n – единичная матрица того же порядка. Тогда условием того, что элемент b_{ij} преобразуется матрицей X в нуль, представляется соотношениями

$$\sum_{k=1}^{n} x_{ik} + \sum_{\substack{k=1 \\ k \neq i}}^{m} x_{kj} + b_{ij} \equiv 0 (\mathrm{mod}\, k_1), \ (i = 1, 2, \ldots, p); \tag{1}$$

$$\sum_{k=1}^{n} x_{ik} + \sum_{\substack{k=1 \\ k \neq i}}^{m} x_{kj} + b_{ij} \equiv 0 (\mathrm{mod}\, k_2), \ (i = p+1, p+2, ..., m).$$

Если умножить первую часть (1) на k_2, а вторую часть – на k_1, то соотношения не изменятся, но теперь их можно записать в виде

$$A' x + b' \equiv 0 (\mathrm{mod}\, k_1 k_2), \tag{2}$$

где A' – квадратная матрица порядка $m \times n$, состоящая из m^2 подматриц.

$$A' = \begin{pmatrix} k_2\Im_n & k_2E_n & k_2E_n & \ldots & k_2E_n \\ k_2E_n & k_2\Im_n & k_2E_n & \ldots & k_2E_n \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ k_1E_n & k_1E_n & k_1E_n & \ldots & k_1E_n \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ k_1E_n & k_1E_n & k_1E_n & \ldots & k_1\Im_n \end{pmatrix}. \tag{3}$$

а $b' = (k_2b_1, \ k_2b_2, ..k_2b_p, \ k_1b_{p+1}, \ k_1b_{p+2}..., k_1b_N)$.

Теорема 1. Решение системы (1) удовлетворяет системе сравнений

$$Ax + b \equiv 0 (\mathrm{mod}\, k_1 k_2), \tag{4}$$

где $A = \begin{pmatrix} \Im_n & E_n & E_n & \ldots & E_n \\ E_n & \Im_n & E_n & \ldots & E_n \\ E_n & E_n & \Im_n & \ldots & E_n \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ E_n & E_n & E_n & \ldots & \Im_n \end{pmatrix}$. (5)

Доказательство. Для решения системы (1) необходимо найти ее обратную матрицу. Нетрудно удостовериться, что $\det A^{'} = k_2^{pn}\, k_1^{n(m-p)}\, \det A$. При подсчете миноров для обратных матриц можно заметить, что для $j \le p$ имеем $a_{ij}^{-1} = \left(a_{ij}^{'}\right)^{-1} / k_2$, а для $j \ge p$ имеет место $a_{ij}^{-1} = \left(a_{ij}^{'}\right)^{-/} / k_1$. Это приводит к равенству $A^{'-1} b^{'} = A^{-1} b$. Отсюда и вытекает справедливость теоремы, так как из двух систем получаем $x = -A^{-1} b = -A^{'-1} b^{'}$.

Таким образом, проблема сводится к отысканию обратной матрицы A^{-1}. В общем случае для произвольных m, n, k_1 и k_2 она может не существовать. Тогда система (1) может иметь решение, если начальное состояние удовлетворяет определенным ограничениям. Рассмотрим симметричную квадратную матрицу порядка n, зависящую от двух параметров $H(\alpha, \beta) = (\alpha - \beta) E_n + \beta \Im_n$.

Используем ее для построения квадратной матрицы порядка mn, зависящей от четырех параметров и состоящей из m^2 подматриц,

$$T_{m,n}(\alpha, \beta, \gamma, \delta) = \begin{pmatrix} H_n(\alpha, \beta) & H_n(\gamma, \delta) & \ldots & H_n(\gamma, \delta) \\ H_n(\gamma, \delta) & H_n(\alpha, \beta) & \ldots & H_n(\gamma, \delta) \\ \ldots & \ldots & \ldots & \ldots \\ H_n(\gamma, \delta) & H_n(\gamma, \delta) & \ldots & H_n(\alpha, \beta) \end{pmatrix}. \tag{6}$$

Из [2] следует, что $A^{-1} = T_{m,n}(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$, где

$$\left.\begin{aligned} \alpha_1 &\equiv \frac{1}{m-1} + \frac{1}{n-1} - 1 + \alpha_4 \\ \alpha_2 &\equiv \frac{1}{n-1} + \alpha_4,\ \alpha_3 \equiv \frac{1}{m-1} + \alpha_4 \\ \alpha_4 &\equiv -\left(\frac{1}{n-1} + \frac{1}{m-1}\right)\frac{1}{m+n-1} \end{aligned}\right\} (\mathrm{mod}\ k_1 k_2). \tag{7}$$

Отсюда вытекает **условие разрешимости системы (1):**

$$m \not\equiv 1 (\mathrm{mod}\, k_i);\quad n \not\equiv 1 (\mathrm{mod}\, k_i);\quad m + n \not\equiv 1 (\mathrm{mod}\, k_i), \text{ где } i = 1,2. \tag{8}$$

Пример 1. Пусть $m = 5$, $n = 3$, $k_1 = 3$, $k_2 = 5$, $p = 2$, а матрица B имеет вид

$B=\begin{pmatrix}0&1&0\\1&1&2\\1&4&0\\4&4&0\\0&3&3\end{pmatrix}$; вычислим дробные значения $\begin{cases}\dfrac{1}{m-1}=\dfrac{1}{4}\equiv 4(\mathrm{mod}\,3\cdot 5),\\ \dfrac{1}{n-1}=\dfrac{1}{2}\equiv 8(\mathrm{mod}\,3\cdot 5),\\ \dfrac{1}{m+n-1}=\dfrac{1}{7}\equiv 13(\mathrm{mod}\,3\cdot 5).\end{cases}$

Тогда, подставляя эти значения в (7), получаем $\alpha_4=9$, $\alpha_1=5$, $\alpha_2=2$, $\alpha_3=13$. Отсюда получаем обратную матрицу по (6) $A^{-1}=T_{5,3}(\alpha_1,\alpha_2,\alpha_3,\alpha_4)$. Подсчитаем $x=-A^{-1}b$=(7,10,11,-1,1,4,6,11,9,0,2,-3,2,4). Можно непосредственно убедиться, что это есть решение (1).

Теорема 2. Решение системы (1) для произвольного количества q типов замков удовлетворяет системе сравнений $Ax+b\equiv 0(\mathrm{mod}\,k_1k_2\cdots k_q)$, где A это (5), а $k_1,k_2,\cdots,k_q$ взаимно простые.

Доказательство проводится по той же схеме, что и теорема 1.

3. Выводы

Впервые предложена теория решения матричной задачи о математическом сейфе с различными типами замков. Предполагается, что количества состояний замков есть взаимно простые числа. Здесь не нашли решения случаи, когда не выполняется условие разрешимости системы (1), а также случаи, когда числа состояний замков являются составными. Все эти вопросы будут решены в последующих публикациях.

СПИСОК ЛИТЕРАТУРЫ

1. Donets G.A. Solution of one problem on a safe // The international conference on applied mathematics dedicated to the 65-th anniversary of B.N. Pshenichnyi. – Kyiv. – 2002. – June 25–28 – P. 39.
2. Донец Г.А. Решение задачи о сейфе на (0,1)–матрицах // Кибернетика и системный анализ. – 2002. – № 1. – С. 98 –105.