Теорія оптимальних рішень

УДК 519.8

УДК 519.8

АГАИ АГ ГАМИШ ЯКУБ, Г.А. ДОНЕЦ

ЗАДАЧА О МАТЕМАТИЧЕСКОМ СЕЙФЕ НА МАТРИЦАХ

В работах [1, 2] дано общее определение математического сейфа, и изучались сейфы, заданные на графах, ориентированных или неориентированных. Из общего определения математического сейфа следует, что любой из них можно задать с помощью матрицы смежностей некоторого графа. Однако существуют математические сейфы со своей спецификой, позволяющей их задавать с помощью матриц.

Существует реальная интерпретация задачи: на двери сейфа расположены в виде матрицы скважины одинаковых замков. Известны состояния каждого замка – он открыт или закрыт. Если вставить ключ в одну из скважин и сделать один поворот, то такой же поворот будет сделан и во всех замках той же строки и того же столбца. Необходимо найти такую последовательность замочных скважин, чтобы поворотами в них ключа открыть сейф. Это произойдет при всех открытых замках.

Рассмотрим в общем случае сейф, определенный в [2], 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 имеют произвольное число состояний и принадлежат одному типу, т. е. $k_l = K$. Любому начальному состоянию сейфа $\vec{b}$ соответствует матрица $B = (b_{ij})_{m,n}$,

Рассматривается задача о математическом сейфе, заданная на матрице. Исследуется сейф с однотипными замками. Находятся необходимые условия существования решения задачи для простого числа состояний замков.

где $b_{ij} \in \{0,1,\ldots,K-1\}$. Необходимо найти такую последовательность замков и соответствующее количество поворотов в них, чтобы «открыть сейф», т. е. перейти в состояние сейфа $B_{fin} = (b_{ij} = 0)_{m,n}$. Пусть $X = (x_{ij})_{m,n}$ – решение задачи, где x_{ij} равно числу поворотов ключа в замке z_l. Тогда условием того, что элемент b_{ij} преобразуется матрицей X в нуль, представляется соотношением

$$\sum_{k=1}^{n} x_{ik} + \sum_{\substack{k=1 \\ k \neq i}}^{m} x_{kj} + b_{ij} \equiv 0 (\mathrm{mod}\, K), \text{ где } i = 1, 2, ..., m;\ j = 1, 2, ..., n. \qquad (1)$$

Обозначим $\vec{x} = \left(x_{11}, x_{12}, ..., x_{1n}, x_{21}, x_{22}, ..., x_{2n}, ..., x_{m,n-1}, x_{mn}\right)$ вектор-столбец, полученный из матрицы X последовательной записью ее строк.

Аналогично из матрицы *B* получим вектор-столбец $\vec{b}$. Кроме того, пусть $\Im_n$ – матрица размера *n*×*n*, состоящая из единиц, E_n – единичная матрица того же размера, а I_n – вектор-строка из *n* единиц. Тогда условие преобразования (1) для всей матрицы *B* запишем в виде системы уравнений

$$A\vec{x} \equiv \vec{b} (\mathrm{mod}\, K), \qquad (2)$$

где матрица *A* размера *mn*× *mn* состоит из m^2 клеток:

$$A = \begin{pmatrix} \Im_n & E_n & E_n & .. & .. & E_n \\ E_n & \Im_n & E_n & .. & .. & E_n \\ E_n & E_n & \Im_n & .. & .. & E_n \\ .. & .. & .. & .. & .. & .. \\ E_n & E_n & E_n & .. & .. & \Im_n \end{pmatrix}. \qquad (3)$$

Эту задачу легко можно свести к решению системы линейных диофантовых уравнений, если добавить в правые части (2) слагаемые $Ky_i, (i = 1, 2, ..., mn)$, используя известные методы. Однако специфика задачи позволяет находить ее решение непосредственно, так как матрица *A* имеет стандартный вид и не зависит от значений матрицы *B*. Ее ранг и определитель зависят только от значений m и n.

Поскольку матрица *A* симметрическая, то в дальнейшем все рассуждения относительно строк матрицы справедливы и для одноименных столбцов и строк и наоборот.

Если ранг матрицы *A* равен *mn*, то решение системы (2) имеет вид

$$\vec{x} = -A^{-1}\vec{b} (\mathrm{mod}\, K). \qquad (4)$$

Таким образом, проблема сводится к отысканию обратной матрицы A^{-1}.

В зависимости от конкретных значений m, n и K возникают различные по сложности решения задачи. Их можно разделить на три таких вида в зависимости от типа замков: 1) замки с двумя состояниями; 2) однотипные замки с произвольным числом состояний; 3) произвольные замки.

Решение задачи для замков с двумя состояниями в полном объеме получено в [3]. Здесь исследуется второй случай.

Если $K > 2$, то проблема нахождения обратной матрицы наталкивается на ряд существенных препятствий. Исследуем сначала вопрос о ее структуре.

Рассмотрим симметричную квадратную матрицу порядка n, зависящую от двух параметров $H_n(\alpha,\beta)=(\alpha-\beta)E_n+\beta\Im_n$.

$$H_n(\alpha,\beta)=\begin{pmatrix} \alpha & \beta & \beta & \dots & \beta \\ \beta & \alpha & \beta & \dots & \beta \\ \beta & \beta & \alpha & \dots & \beta \\ \dots & \dots & \dots & \dots & \dots \\ \beta & \beta & \beta & \dots & \alpha \end{pmatrix}. \qquad (5)$$

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

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

Матрицы такого типа будем называть T-матрицами. В этих обозначениях единичная матрица и матрица A также являются T-матрицами, а именно $E_{mn}=T_{m,n}(1,0,0,0)$, а $A=T_{mn}(1,1,1,0)$. Если можно вместо элементов подставлять подматрицы, то T-матрицы можно представлять в виде $T_{m,n}=H_m(H_n(\alpha,\beta),H_n(\gamma,\delta))$.

Лемма 1. Результатом умножения двух T-матриц будет также T-матрица.

Для доказательства рассмотрим две T-матрицы $T_{m,n}(\alpha_1,\alpha_2,\alpha_3,\alpha_4)$, $T_{m,n}(\beta_1,\beta_2,\beta_3,\beta_4)$ и перемножим их. Ввиду симметричности матриц элементами c_{ij} матрицы $\boldsymbol{C}$, полученной в результате их умножения, будут равны скалярному произведению i-й строки первой и j-й строки второй матриц. В зависимости от значений i и j эти произведения можно разбить на 4 группы.

а) $i = j$. Тогда получаются диагональные элементы матрицы $\boldsymbol{C}$

$$c_{ii} = \alpha_1\beta_1 + (n-1)\alpha_2\beta_2 + (m-1)\alpha_3\beta_3 + (m-1)(n-1)\alpha_4\beta_4. \qquad (7)$$

Очевидно, что таких элементов ровно mn.

б) $i \neq j$; $kn+1 \le i,\ j \le (k+1)n,\ k \ge 0$. В результате получаются недиагональные элементы типа β диагональных подматриц $H_n(\alpha,\beta)$.

$$c_{ij} = \alpha_1\beta_2 + \alpha_2\beta_1 + (n-2)\alpha_2\beta_2 + (m-1)(\alpha_3\beta_4 + \alpha_4\beta_3) + (m-1)(n-1)\alpha_4\beta_4. \qquad (8)$$

Для фиксированного k таких элементов будет $n(n–1)$, а всего mn $(n-1)$.

в) $|i-j| \equiv 0 \pmod n$, $i \neq j$. В результате получаются диагональные элементы типа γ подматриц $H_n(\gamma,\delta)$

$$c_{ij} = \alpha_1\beta_3 + \alpha_3\beta_1 + (n-1)(\alpha_2\beta_4 + \alpha_4\beta_2) + (m-2)\alpha_3\beta_3 + (m-2)(n-1)\alpha_4\beta_4. \qquad (9)$$

Каждой строке первой матрицы соответствует $(m-1)$ строка второй матрицы, поэтому таких элементов будет mn $(m-1)$.

г) $i \neq j \pmod n$, $kn+1 \le i \le (k+1)n$, $nl+1 \le j \le (l+1)n, k \neq l$, $k \ge 0, l \ge 0$.

В результате получаются недиагональные элементы типа δ подматриц $H_n(\gamma,\delta)$

$$c_{ij} = \alpha_1\beta_4 + \alpha_4\beta_1 + \alpha_2\beta_3 + \alpha_3\beta_2 + (n-2)(\alpha_2\beta_4 + \alpha_4\beta_2) + (m-2)(\alpha_3\beta_4 + \alpha_4\beta_3) + (m-2)(n-2)\alpha_4\beta_4. \qquad (10)$$

Если зафиксировать одну строку первой матрицы, то ей будут соответствовать $n-1$ строк в $m-1$ подматрицах второй матрицы, т. е. будет $mn(m-1)(n-1)$ элементов. Если просуммировать число элементов этих четырех групп, то получим число m^2n^2. Это означает, что в результате умножения других элементов не образуется, что и доказывает справедливость леммы.

Будем искать обратную матрицу A^{-1} системы (2) в виде T-матрицы $A^{-1} = T_{m,n}(\alpha_1,\alpha_2,\alpha_3,\alpha_4)$. Так как $AA^{-1} = E_{mn}$, то подставляя соответствующие значения в (7 – 10), получаем систему уравнений

$$\left.\begin{array}{llll} \alpha_1 + (n-1)\alpha_2 + (m-1)\alpha_3 & & & \equiv 1 \\ \alpha_1 + (n-1)\alpha_2 & & + (m-1)\alpha_4 & \equiv 0 \\ \alpha_1 & + (m-1)\alpha_3 & + (n-1)\alpha_4 & \equiv 0 \\ + \alpha_2 & + \alpha_3 & + (m+n-3)\alpha_4 & \equiv 0 \end{array}\right\} (\mathrm{mod}\, K). \qquad (11)$$

Матрица этой системы имеет вид

$$S = \begin{pmatrix} 1 & n-1 & m-1 & 0 \\ 1 & n-1 & 0 & m-1 \\ 1 & 0 & m-1 & n-1 \\ 0 & 1 & 1 & m+n-3 \end{pmatrix}. \qquad (12)$$

Нетрудно подсчитать, что $\det S \equiv -(m-1)(n-1)(m+n-1)(\mathrm{mod}\, K)$.

Отсюда получаем необходимое условие разрешимости системы (2):

$$m \neq 1(\mathrm{mod}\ K);\ n \neq 1(\mathrm{mod}\ k);\ m+n \neq 1(\mathrm{mod}\ K). \qquad (13)$$

В дальнейшем будем часто использовать дробные выражения типа *p/q*, под которыми подразумеваются целое число *t*, являющееся корнем (если он существует) уравнения

$$qt \equiv p(\mathrm{mod}\, K). \qquad (14)$$

В результате решения системы (12) получаются следующие значения корней:

$$\left.\begin{aligned} \alpha_1 &\equiv -1-(m+n-2)^2/\det S, \\ \alpha_2 &\equiv [-m(m+n-3)+2n-3]/\det S, \\ \alpha_3 &\equiv [2m-3-n(m+n-3)]/\det S, \\ \alpha_4 &\equiv (m+n-2)/\det S \end{aligned}\right\} (\mathrm{mod}\, K).$$

В результате упрощений получаем окончательно

$$\left.\begin{aligned} \alpha_1 &\equiv \frac{1}{m-1}+\frac{1}{n-1}-1+\alpha_4 \\ \alpha_2 &\equiv \frac{1}{n-1}+\alpha_4 \\ \alpha_3 &\equiv \frac{1}{m-1}+\alpha_4 \\ \alpha_4 &\equiv -\left(\frac{1}{n-1}+\frac{1}{m-1}\right)\frac{1}{m+n-1} \end{aligned}\right\} (\mathrm{mod}\, K). \qquad (15)$$

Пример 1. Пусть $K = 7$, $n = 4$, $m = 3$, а матрица (вектор) начального состояния сейфа

$$B = \begin{pmatrix} 0 & 3 & 1 & 0 \\ 5 & 6 & 0 & 2 \\ 3 & 3 & 5 & 1 \end{pmatrix};\ \vec{b}^T = (0,3,1,0,5,6,0,1,3,3,5,1).$$

Матрица **A** имеет вид

$$A=\begin{pmatrix}
1&1&1&1&1&0&0&0&1&0&0&0\\
1&1&1&1&0&1&0&0&0&1&0&0\\
1&1&1&1&0&0&1&0&0&0&1&0\\
1&1&1&1&0&0&0&1&0&0&0&1\\
1&0&0&0&1&1&1&1&1&0&0&0\\
0&1&0&0&1&1&1&1&0&1&0&0\\
0&0&1&0&1&1&1&1&0&0&1&0\\
0&0&0&1&1&1&1&1&0&0&0&1\\
1&0&0&0&1&0&0&0&1&1&1&1\\
0&1&0&0&0&1&0&0&1&1&1&1\\
0&0&1&0&0&0&1&0&1&1&1&1\\
0&0&0&1&0&0&0&1&1&1&1&1
\end{pmatrix}.$$

Вычислим дробные значения:

$$\frac{1}{m-1}=\frac{1}{2}\equiv t_1\,(\mathrm{mod}\,7),\ \ t_1\equiv 4\,(\mathrm{mod}\,7);$$

$$\frac{1}{n-1}=\frac{1}{3}\equiv t_2\,(\mathrm{mod}\,7),\ \ t_2\equiv 5\,(\mathrm{mod}\,7);$$

$$\frac{1}{m+n-1}=\frac{1}{6}\equiv t_3\,(\mathrm{mod}\,7),\ \ t_3\equiv 6\,(\mathrm{mod}\,7).$$

Вычислим по (15) элементы обратной матрицы:

$$\alpha_4=-(4+5)\cdot 6\equiv 2\,(\mathrm{mod}\,7);\ \ \alpha_1=4+5-1+2\equiv 3\,(\mathrm{mod}\,7);$$

$$\alpha_2=5+2\equiv 0\,(\mathrm{mod}\,7);\ \alpha_3=4+2\equiv 6\,(\mathrm{mod}\,7).$$

Отсюда обратная матрица

$$A^{-1}=\begin{pmatrix}
3&0&0&0&6&2&2&2&6&2&2&2\\
0&3&0&0&2&6&2&2&2&6&2&2\\
0&0&3&0&2&2&6&2&2&2&6&2\\
0&0&0&3&2&2&2&6&2&2&2&6\\
6&2&2&2&3&0&0&0&6&2&2&2\\
2&6&2&2&0&3&0&0&2&6&2&2\\
2&2&6&2&0&0&3&0&2&2&6&2\\
2&2&2&6&0&0&0&3&2&2&2&6\\
6&2&2&2&6&2&2&2&3&0&0&0\\
2&6&2&2&2&6&2&2&0&3&0&0\\
2&2&6&2&2&2&6&2&0&0&3&0\\
2&2&2&6&2&2&2&6&0&0&0&3
\end{pmatrix}.$$

$$\vec{x}^T = \left(-A^{-1}\vec{b}\right)^T \equiv (2, 3, 4, 1, 4, 3, 0, 0, 0, 5, 3, 4);$$

$$X = \begin{pmatrix} 2 & 3 & 4 & 1 \\ 4 & 3 & 0 & 0 \\ 0 & 5 & 3 & 4 \end{pmatrix}.$$

Матрица X определяет количество поворотов ключа для каждого замка сейфа, которые приведут к открытию сейфа. Рассмотрим эту последовательность преобразований матрицы B, в которой очередной элемент (замок) преобразования, а также соответствующие строка и столбец выделены параллельными линиями.

$$B = \left(\begin{array}{\overset{+2}{c}|ccc} 0 & 3 & 1 & 0 \\ \hline 5 & 6 & 0 & 2 \\ 3 & 3 & 5 & 1 \end{array}\right) \to \left(\begin{array}{\overset{+3}{c}|ccc} 2 & 5 & 3 & 2 \\ \hline 0 & 6 & 0 & 2 \\ 5 & 3 & 5 & 1 \end{array}\right) \to \left(\begin{array}{\overset{+4}{c}|ccc} 5 & 1 & 6 & 5 \\ \hline 0 & 2 & 0 & 2 \\ 5 & 6 & 5 & 1 \end{array}\right) \to$$

$$\to \left(\begin{array}{ccc|\overset{+1}{c}} 2 & 5 & 3 & 2 \\ 0 & 2 & 4 & 2 \\ 5 & 6 & 2 & 1 \end{array}\right) \to \left(\begin{array}{\overset{+4}{c}|ccc} 3 & 6 & 4 & 3 \\ \hline 0 & 2 & 4 & 3 \\ \hline 5 & 6 & 2 & 2 \end{array}\right) \to \left(\begin{array}{\overset{+3}{c}|ccc} 0 & 6 & 4 & 3 \\ \hline 4 & 6 & 1 & 0 \\ \hline 2 & 6 & 2 & 2 \end{array}\right) \to$$

$$\to \left(\begin{array}{\overset{+5}{c}|ccc} 0 & 2 & 4 & 3 \\ \hline 0 & 2 & 4 & 3 \\ \hline 2 & 2 & 2 & 2 \end{array}\right) \to \left(\begin{array}{\overset{+3}{c}|ccc} 0 & 0 & 4 & 3 \\ \hline 0 & 0 & 4 & 3 \\ \hline 0 & 0 & 0 & 0 \end{array}\right) \to \left(\begin{array}{\overset{-3}{c}|ccc} 0 & 0 & 0 & 3 \\ \hline 0 & 0 & 0 & 3 \\ \hline 3 & 3 & 3 & 3 \end{array}\right) \to \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} = B_{fin}.$$

Агаі Аг Гаміш Якуб, *Г.О. Донець*

ЗАДАЧА ПРО МАТЕМАТИЧНИЙ СЕЙФ НА МАТРИЦЯХ

Розглядається задача про математичний сейф, заданий на матриці. Досліджується сейф з однотиповими замками. Знаходяться умови існування розв'язку задачі для простого числа станів замків.

Aghaei Agh Ghamish Yaghoub, *G.A. Donets*

THE TASK ABOUT THE MATHEMATICAL SAFE ON MATRICES

The task about the mathematical safe, set on a matrix is considered. The safe with the same type of locks is researched. We have found the necessary conditions of the solution of the task for a prime number of states of the lock.

1. *Донец Г.А., Чжан Бинь.* Постановка и решение некоторых задач о математическом сейфе // Кибернетика и системный анализ.– 2006. – № 3. – С. 3 –14.
2. *Донец Г.А., Чжан Бинь.* Задачи о математическом сейфе на графах // Кибернетика и системный анализ. – 2006. – № 5. – С. 84 –93.
3. *Донец Г.А.* Решение задачи о сейфе на (0,1)-матрицах // Кибернетика и системный анализ. – 2002. – № 1. – С. 98 –105.

Получено 03.04.2013