УДК 519.1

А.Л. Гурин, И.С. Гращенко, Л.В. Савченко

ПАРАМЕТРИЧЕСКИЙ МЕТОД РЕШЕНИЯ ЗАДАЧ О МАТЕМАТИЧЕСКОМ СЕЙФЕ НА ГРАФАХ

Ключевые слова: математический сейф, система уравнений, модуль системы, вектор начального состояния сейфа, граф, параметрический метод.

Задаче о математическом сейфе и методам ее решения посвящена весьма обширная и разнообразная литература [1−9].

Математический сейф — это система взаимосвязанных определенным образом замков, которая задается как на графах, так и на матрицах, и такова, что при повороте ключом в одном замке, такой же поворот делается и в замках, связанных с ним. Здесь понятия ключа и замка употребляются в общепринятом смысле.

Как показали исследования, математический сейф лучше всего задавать с помощью ориентированного графа $Z=(z_1,\ z_2, ..., z_N)$, где замки являются вершинами, а дуги указывают на их взаимосвязь. Дуга $(z_i,\ z_j)$ указывает на то, что замок z_j связан с замком z_i и с любым поворотом ключа в замке z_i одновременно осуществляется поворот ключа и в замке z_j. Замок z_i является входным относительно замка z_j. Любой замок может находиться в одном из двух состояний — открытом или закрытом. Существуют замки, для открытия которых нужно некоторое количество поворотов ключа из множества (0, 1, 2, ..., K–1), где K — общее число состояний замка. Замок открыт, когда он находится в состоянии, равном нулю. В другом состоянии замок закрыт.

Необходимо решить следующую задачу. Исходя из начального состояния сейфа $\mathbf{b} = (b_1, b_2, ..., b_N)$, где $b_i \in$ (0, 1, 2, ..., K–1), найти такую последовательность замков и такое число поворотов ключа в них, чтобы сейф перешел в положение открытого, т.е. все замки находятся в состоянии, равном нулю.

Приведем математическую постановку такой задачи.

Пусть $x_j,\ j=1, 2, ..., N,$ — необходимое количество поворотов ключа в замке z_j, $z_1, z_2, ..., z_k$ — входные замки для замка z_j. Для каждого замка z_j должно выполняться основное уравнение, которое равносильно утверждению: сумма чисел поворотов входных замков для замка z_j, его числа поворотов x_j и его исходного состояния b_j должна быть равна 0 (mod K). Это утверждение запишем так:

$$\sum_{i=1}^{k} x_i + x_j + b_j = 0(\mathrm{mod}K),\quad j=1, 2, ..., N. \tag{1}$$

Рассмотрим один из новых методов решения задачи о математическом сейфе на графах определенной структуры, который назовем параметрическим. Суть его состоит в обозначении переменных, соответствующих некоторым вершинам графа, определенными параметрами, которыми выражаются все остальные неизвестные. Путем сравнения выбранных специальным образом неизвестных определяются указанные параметры, а затем и все неизвестные, т.е. решение задачи. В работе приводится описание метода на нескольких примерах.

Опишем сначала предлагаемый метод для простейшего графа типа «цепь», для которого достаточно одного параметра.

Рассмотрим сейф на графе в виде цепи (рис. 1).

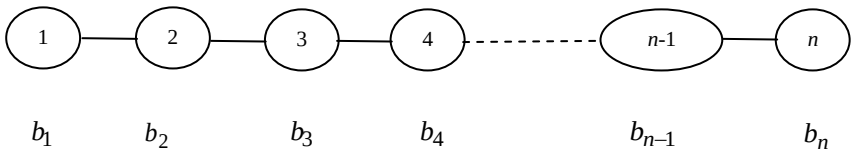

Рис. 1

Запишем для этого графа общую систему [1] при n = 7. Если перенести свободные члены в правую часть, то получим следующую систему:

$$\left.\begin{aligned}
x_1 + x_2 \;.\;.\;.\;.\;.\;. &\equiv -b_1\\
x_1 + x_2 + x_3 \;.\;.\;.\;.\;. &\equiv -b_2\\
x_2 + x_3 + x_4 \;.\;.\;.\;. &\equiv -b_3\\
x_3 + x_4 + x_5 \;.\;.\;. &\equiv -b_4\\
x_4 + x_5 + x_6 \;.\;. &\equiv -b_5\\
x_5 + x_6 + x_7 &\equiv -b_6\\
x_6 + x_7 &\equiv -b_7
\end{aligned}\right\} (\mathrm{mod} K). \qquad (2)$$

Обозначим $x_1 = \alpha$. Тогда $x_2 = -b_1 - \alpha$. Подставляя получаемые значения последовательно в уравнения системы, находим $x_3 = b_1 - b_2$, $x_4 = b_2 - b_3 + \alpha$, $x_5 = -b_1 + b_3 - b_4 - \alpha$, $x_6 = b_1 - b_2 + b_4 - b_5$, $x_7 = b_2 - b_3 + b_5 - b_6 + \alpha$. Если переменную x_7 определить из последнего уравнения, то $x_7 = -b_1 + b_2 - b_4 + b_5 - b_7$. Сравнивая оба значения x_7, получим значение параметра $\alpha = -b_1 + b_3 - b_4 + b_6 - b_7$, а затем — решение всей системы: $x_1 = -b_1 + b_3 - b_4 + b_6 - b_7$, $x_2 = -b_3 + b_4 - b_6 + b_7$, $x_3 = b_1 - b_2$, $x_4 = -b_1 + b_2 - b_4 + b_6 - b_7$, $x_5 = -b_6 + b_7$, $x_6 = b_1 - b_2 + b_4 - b_5$, $x_7 = -b_1 + b_2 - b_4 + b_5 - b_7$.

Рассмотрим пример для $\boldsymbol{b}$ = (3, 2, 1, 4, 3, 2, 4) при K = 5. Используя выражения для переменных x_i (i=1, 2, ..., 7), получим решение системы X = (2, 0, 1, 3, 2, 2, 4) (mod 5).

Проверим это решение.

b = (3, 2, 1, 4, 3, 2, 4), $x_1 = 2 \rightarrow$ (0, 4, 1, 4, 3, 2, 4), $x_3 = 1 \rightarrow$(0, 0, 2, 0, 3, 2, 4), $x_4 = 3 \rightarrow$(0, 0, 0, 3, 1, 2, 4), $x_5 = 2 \rightarrow$ (0, 0, 0, 0, 3, 4, 4), $x_6 = 2 \rightarrow$(0, 0, 0, 0, 0, 1, 1), $x_7 = 4 \rightarrow$ (0, 0, 0, 0, 0, 0, 0) (mod 5).

В связи с тем, что большинство уравнений системы (2) содержит три неизвестных, особое значение принимает число n относительно числа 3. Приведенное

решение получено для $n \equiv 1 \pmod 3$. По такой же схеме решается задача и для $n \equiv 0 \pmod 3$.

Для $n \equiv 2 \pmod 3$ при сравнении x_n параметр α исчезает и получаем соотношение

$$\sum_{i=0}^{\lfloor n/3 \rfloor} b_{3i+1} - \sum_{i=0}^{\lfloor n/3 \rfloor} b_{3i+2} = 0 \,(\mathrm{mod} K), \tag{3}$$

что является необходимым и достаточным условием решения задачи, а параметр α может принимать любое значение.

Рассмотрим сейф на графе типа «лесенки» (рис. 2) для $b = (1, 2, 3, 4, 4, 3, 2, 1)$.

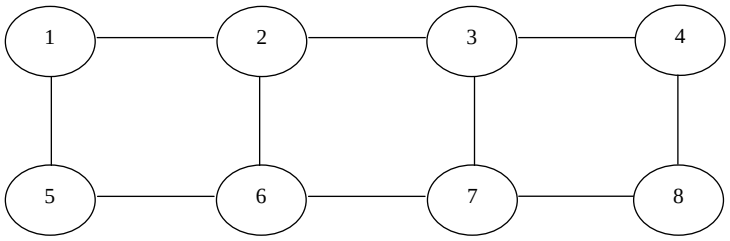

Рис. 2

Запишем для этого графа общую систему [1] при $n = 8$.

$$\left.\begin{array}{rrrrrrrrr}
x_1 + x_2 + . & & & x_5 & . & . & \equiv -1 \\
x_1 + x_2 + x_3 + . & & . & & x_6 & . & \equiv -2 \\
. & x_2 + x_3 + & .x_4 + & . & & x_7 & \equiv -3 \\
& & x_3 + & x_4 + . & & & x_8 & \equiv -4 \\
x_1 + & . & . & . & x_5 + & x_6 & . & . & \equiv -4 \\
. & x_2 + & . & . & x_5 + & x_6 + & x_7 & . & \equiv -3 \\
& & x_3 + . & & . & x_6 + & x_7 + & x_8 & \equiv -2 \\
& & & x_4 + . & & . & x_7 + & x_8 & \equiv -1
\end{array}\right\} (\mathrm{mod} K). \tag{4}$$

Обозначим $x_1 = \alpha$ и $x_5 = \beta$. Подставляя эти параметры в первое и пятое уравнения системы (4), находим значения $x_2 = -\alpha - \beta - 1$, $x_6 = -\alpha - \beta - 4$. Из второго уравнения находим $x_3 = \alpha + 2\beta + 3$, из шестого — $x_7 = 2\alpha + \beta + 2$, из третьего и седьмого — $x_4 = -2\alpha - 2\beta - 7$, $x_8 = -2\alpha - 2\beta - 3$.

Подставив эти значения в четвертое и восьмое уравнения системы (4), получим

$$\left.\begin{array}{l} 3\alpha + 2\beta = -3 \\ 2\alpha + 3\beta = -7 \end{array}\right\}. \tag{5}$$

Определитель этой системы равен пяти. Поэтому для $K \neq 5$ данная система имеет решение $\alpha = 1$, $\beta = -3$. Подставляя их в выражения неизвестных, получим решение $X = (1, 1, -2, -3, -3, -2, 1, 1)$.

Проверим это решение:

b = (1, 2, 3, 4, 4, 3, 2, 1), $x_1 = 1 \rightarrow$(2, 3, 3, 4, 5, 3, 2, 1), $x_2 = 1 \rightarrow$(3, 4, 4, 4, 5, 4, 2, 1), $x_3 = -2 \rightarrow$(3, 2, 2, 2, 5, 4, 0, 1), $x_4 = -3 \rightarrow$(3, 2, – 1, – 1, 5, 4, 0, – 2), $x_5 = -3 \rightarrow$ (0, 2, – 1, – 1, 2, 1, 0, – 2), $x_6 = -2 \rightarrow$(0, 0, – 1, – 1, 0, – 1, – 2, – 2), $x_7 = 1 \rightarrow$ (0, 0, 0, – 1, 0, 0, – 1, – 1), $x_8 = 1 \rightarrow$ (0, 0, 0, 0, 0, 0, 0, 0).

При $K = 5$ оба уравнения системы (4) преобразуются в одно $\alpha = (\beta - 1) \pmod 5$. Это означает, что при решении задачи параметру β можно назначать произвольное значение. Например, если $\beta = 1$, то $\alpha = 0$. Подставляя эти значения в найденные выше выражения для неизвестных, получим решение $X = (0, -2, 0, 1, 1, 0, -2, 0) \pmod 5$.

Проверим это решение:

b = (1, 2, 3, 4, 4, 3, 2, 1), $x_2 = -2 \rightarrow (-1, 0, 1, 4, 4, 1, 2, 1)$, $x_4 = 1 \rightarrow$ $\rightarrow (-1, 0, 2, 0, 4, 1, 2, 2)$, $x_5 = 1 \rightarrow (0, 0, 2, 0, 0, 2, 2, 2)$, $x_7 = -2 \rightarrow (0, 0, 0, 0, 0, 0, 0, 0) \pmod 5$. Такое же решение получено с помощью метода суммарных представлений [2] .

Рассмотрим сейф на графе типа «окошко» (рис. 3) для **b** = (1, 2, 3, 4, 5, 6, 3, 2, 1).

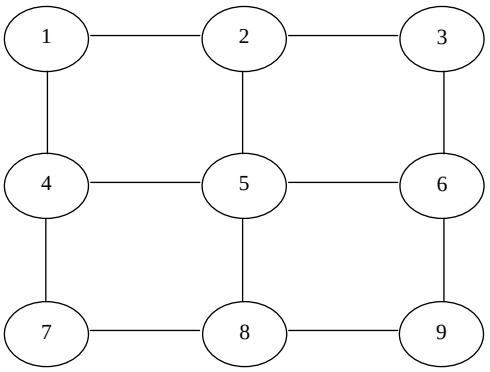

Рис. 3

Запишем для этого сейфа общую систему:

$$\left.\begin{array}{rl}
x_1 + x_2 + \ldots x_4 \ldots\ldots & \equiv -1 \\
x_1 + x_2 + x_3 + \ldots x_5 \ldots\ldots & \equiv -2 \\
\ldots x_2 + x_3 + \ldots \ldots x_6 \ldots\ldots & \equiv -3 \\
x_1 + \ldots \ldots x_4 + x_5 + \ldots x_7 \ldots\ldots & \equiv -4 \\
\ldots x_2 + \ldots x_4 + x_5 + x_6 + \ldots x_8 \ldots & \equiv -5 \\
\ldots \ldots x_3 + \ldots x_5 + x_6 + \ldots \ldots x_9 & \equiv -6 \\
\ldots \ldots \ldots x_4 + \ldots \ldots x_7 + x_8 \ldots & \equiv -3 \\
\ldots \ldots \ldots x_5 + \ldots x_7 + x_8 + x_9 & \equiv -2 \\
\ldots \ldots \ldots \ldots x_6 + \ldots x_8 + x_9 & \equiv -1
\end{array}\right\} (\text{mod } K). \qquad (6)$$

Обозначим $x_1 = \alpha$, $x_4 = \beta$, $x_7 = \chi$. Остальные переменные выразим этими параметрами, выбирая уравнения в порядке 1, 4, 7, 2, 5, 8. Получим $x_2 = -\alpha - \beta - 1$, $x_5 = -\alpha - \beta - \chi - 4$, $x_8 = -\beta - \chi - 3$, $x_3 = \alpha + 2\beta + \chi + 3$, $x_6 = 2\alpha + 2\beta + 2\chi + 3$, $x_9 = \alpha + 2\beta + \chi + 5$.

Подставив эти значения в третье, шестое и девятое уравнения системы (6), получим такую систему уравнений:

$$\left.\begin{array}{l}
2\alpha + 3\beta + 3\chi = -8 \\
3\alpha + 5\beta + 3\chi = -13 \\
3\alpha + 3\beta + 2\chi = -6
\end{array}\right\}. \qquad (7)$$

 ISSN 0572-2691

Определитель этой системы равен -7.

Если $K \neq 7$, то эта система решается в обычном порядке. Для нее детерминанты, определяющие α, β, χ, равны соответственно – 11, 23, 3. Например, для $K=5$ параметры имеют значения $\alpha = -2 \pmod 5$, $\beta = \chi = 1 \pmod 5$. Подставляя их в выражения неизвестных, получим решение задачи X =(–2, 0, –1, 1, 1, –2, 1, 0, 1) (mod 5).

Проверим это решение:

b = (1, 2, 3, 4, 5, 6, 3, 2, 1), $x_1 = -2 \rightarrow$ (– 1, 0, 3, 2, 5, 6, 3, 2, 1), $x_3 = -1 \rightarrow$ $\rightarrow$ (– 1, – 1, 2, 2, 5, 0, 3, 2, 1), $x_4 = 1 \rightarrow$ (0, – 1, 2, 3, 1, 0, – 1, 2, 1), $x_5 = 1 \rightarrow$ (0, 0, 2, – 1, 2, 1, – 1, 3, 1), $x_6 = -2 \rightarrow$ (0, 0, 0, – 1, 0, – 1, – 1, 3, – 1), $x_7 = 1 \rightarrow$ (0, 0, 0, 0, 0, – 1, 0, – 1, – 1), $x_9 = 1 \rightarrow$ (0, 0, 0, 0, 0, 0, 0, 0, 0) (mod 5).

При $K=7$ возникают определенные трудности. Обозначим $\sum_{i=1}^{9} x_i = S$. Образуем взвешенную сумму уравнений системы (6) с коэффициентами $d_1 = 3$, $d_2 = 2$, $d_3 = 3$, $d_4 = 2$, $d_5 = -1$, $d_6 = 2$, $d_7 = 3$, $d_8 = 2$, $d_9 = 3$. В результате получим $7S = -47$. Для $K=7$ это невозможно. Следовательно, система (6) не имеет решения. Поэтому необходимо заменить какое-то b_i, чтобы указанная сумма была кратна семи. Таким подходящим значением в системе (5) является $b_5 = 3$, что приведет к изменению значения x_6, которое станет равным $2\alpha + 2\beta + 2\chi + 5$. При этом система (6) получит другие правые части: – 10, – 15, – 8. Решая теперь эту систему, получим значения $\alpha = 1, \beta = -3, \chi = -1$. Подставляя их в выражения переменных, придем к решению X =(1, 1, – 3, – 3, – 1, – 1, – 1, 1, – 1) (mod 7).

Проверим это решение:

b = (1, 2, 3, 4, 3, 6, 3, 2, 1), $x_1 = 1 \rightarrow$ (2, 3, 3, 5, 3, 6, 3, 2, 1), $x_2 = 1 \rightarrow$ $\rightarrow$ (3, 4, 4, 5, 4, 6, 3, 2, 1), $x_3 = -3 \rightarrow$ (3, 1, 1, 5, 4, 3, 3, 2, 1), $x_4 = -3 \rightarrow$ $\rightarrow$ (0, 1, 1, 2, 1, 3, 0, 2, 1), $x_5 = -1 \rightarrow$ (0, 0, 1, 1, 0, 2, 0, 1, 1), $x_6 = -1 \rightarrow$ (0, 0, 0, 1, – 1, 1, 0, 1, 0), $x_7 = -1 \rightarrow$ (0, 0, 0, 0, – 1, 1, – 1, 0, 0), $x_8 = 1 \rightarrow$ (0, 0, 0, 0, 0, 1, 0, 1, 1), $x_9 = -1 \rightarrow$ (0, 0, 0, 0, 0, 0, 0, 0, 0) (mod 7).

На основании приведенных примеров можно сделать вывод, что параметрический метод достаточно эффективен и по трудоемкости сводится к решению системы линейных уравнений методом исключения, который, как известно, является полиномиальным. При этом число переменных уменьшается до количества, равного числу задаваемых параметров, которое интуитивно можно приравнять к ширине графа.

А.Л. Гурін, І.С. Гращенко, Л.В. Савченко

ПАРАМЕТРИЧНИЙ МЕТОД РОЗВ’ЯЗАННЯ ЗАДАЧ ПРО МАТЕМАТИЧНИЙ СЕЙФ НА ГРАФАХ

Розглядається параметричний метод розв’язання задачі про математичний сейф на деяких унікальних графах. Суть його полягає в позначені деяких змінних величин, що відповідають вершинам графа, визначеними параметрами, якими виражаються всі інші невідомі. Після порівняння невідомих, які вибрано спеціальним чином, визначаються вказані параметри шляхом розв’язання додаткової системи рівнянь відносно цих параметрів розмірності, рівній числу параметрів. Після розв’язання цієї системи рівнянь визначаються всі невідомі основної системи рівнянь, тобто розв’язок задачі. В даній роботі дається опис цього методу на спеціально підібраних прикладах. Метод продемонстровано для розв’язання задач про математичний сейф на прикладах таких графів, як «ланцюг», «драбинка», «віконце», які підтвердили його ефективність. Після кожного прикладу

проводиться покрокова перевірка розв'язку задачі для кожного замка, яка підтверджує, що сейф в дійсності стає відкритим, тобто сейф переходить в такий стан, коли всі його замки одночасно знаходяться в початковому стані, рівному нулю. При перевірці розв'язку задачі враховується той факт, що поворот ключа в будь-якому конкретному замку впливає на стан взаємопов'язаних з ним замків. Крім того, звернено увагу на виняткові випадки, коли розв'язку не існує. Вони виникають при деяких значеннях модуля основної системи рівнянь тоді, коли зважена сума рівнянь системи не кратна її модулю. В таких випадках для існування розв'язку здійснюється корекція початкового стану вектора **b** таким чином, щоб зважена сума рівнянь системи відповідала вказаному вище обмеженню. Потім задача розв'язується за загальною схемою методу.

Ключові слова: математичний сейф, система рівнянь, модуль системи, вектор початкового стану сейфа, граф, параметричний метод.

A.L. Gurin, I.S. Hrashchenko, L.V. Savchenko

PARAMETRIC METHOD OF SOLVING PROBLEMS OF MATHEMATICAL SAFE ON GRAPHS

We consider one method of solving the problem of mathematical safe on certain graphs called parametric. Its gist consist in denoting some variables, corresponding to graph vertices, by certain parameters. Other unknown variables are expressed through these parameters. Then unknown variables chosen in special way are compared and the mentioned parameters are found by solving additional system of equations for these parameters. Dimension of this system is equal to the number of parameters. Solution to the problem i.e. all unknown variables of the original system, are found by solving additional system of equations. In the paper this method is described on specially chosen examples. The method is demonstrated by solving the mathematical safe problem on the graphs of «chain», «ladder» and «window» types that showed its efficiency. Besides special attention is paid to special cases when solution does not exist. This occurs in the cases when the weighed sum of system equations is not divisable without remainder to its modulo. In such cases, to find solution the initial state of the vector **b** is corrected in such a way that the weighted sum of equations satisfies the above mentioned condition. Then solution of the problem is performed according to the general method scheme.

Keywords: mathematical safe, system of equations, module of the system, vector of the initial state of safe, graph, parametric method.

1. Donets G.A. Solution of safe problem on (0, 1)-matrices. *Cybernetics and Systems Analysis*. 2002. N 1. P. 98–105.
2. Чжань Бинь. Решение матричной задачи о математическом сейфе с различными замками. *Математические машины и системы.* 2006. № 4. С. 69–72.
3. Донец Г.А., Чжан Бинь. Задачи о математическом сейфе на графах. *Кибернетика и системный анализ.* 2006. № 5. С. 84–93.
4. Kryvyi S.L. Algorithms for solution of systems of linear Diophantine equations in residue fields. *Cybernetics and Systems Analysis.* 2007. **43**, N 2**.** P. 171−178.
5. Агаи Аг Гамиш Якуб, Донец Г.А. Задача о математическом сейфе на матрицах. *Теорія оптимальних рішень*. 2013. С. 124–130.
6. Kryvyi S.L. Solutin algoritms for systems of linear equations over residue rings. *Cybernetics and Systems Analysis.* 2016. **52**, N 5. P. 149−160.
7. Гурин А.Л., Донец А.Г. Задача о математическом сейфе из замков с двумя состояниями. *Международный научно-технический журнал «Проблемы управления и информатики»*. 2018. № 5. С. 33–41.
8. Гурин А.Л., Донец А.Г., Загороднюк С.П. Методы решения задач о математических сейфах на элементарных графах. *Международный научно-технический журнал «Проблемы управления и информатики»*. 2019. № 4. С. 36–48.
9. Кривий С.Л. Криптографічна система на основі абелевих груп та кілець. *Проблемы программирования.* 2020. № 2–3. С. 270–277.

Получено 31.03.2020
После доработки 15.09.2020