УДК 519.1

А.Л. Гурин

МЕТОД СУММАРНЫХ ПРЕДСТАВЛЕНИЙ ДЛЯ РЕШЕНИЯ ЗАДАЧ О МАТЕМАТИЧЕСКОМ СЕЙФЕ НА ГРАФАХ

Ключевые слова: математический сейф, система уравнений, вектор начального состояния сейфа, неориентированный граф, метод суммарных представлений.

Метод суммарных представлений впервые рассмотрен в [1], где использовался на чисто интуитивном уровне. В данной работе дается теоретическое обоснование этого метода.

Как известно, задача о математическом сейфе формулируется с помощью графов и матриц, а ее решение сводится к решению систем линейных уравнений в конечных полях [2] или конечных кольцах [3]. Вершины графов изобразим в виде кружочков, внутри которых указан номер вершины. Для каждого математического сейфа существует начальное состояние, которое задается вектором $\boldsymbol{b}$ = $= (b_1, b_2, ..., b_n)$, где $0 \le b_i \le k_i - 1$. Число состояний i -го замка обозначим k_i. Рассмотрим случай, когда все $k_i = K$. Такой сейф называется сейфом с однотипными замками. Задача состоит в следующем: исходя из начального состояния сейфа найти такой вектор $\boldsymbol{x} = (x_1,\ x_2, ..., x_n)$, чтобы после осуществления x_i поворотов в соответствующих замках сейф перешел в состояние bfin = $(b_i = 0)_n$. Предлагаемый метод рассмотрим на неориентированных графах, представляющих сейфы с однотипными замками. В общем случае решение задачи сводится к решению системы

$$A\,\boldsymbol{x} + \boldsymbol{b} \equiv 0 \,(\mathrm{mod}\, K), \tag{1}$$

где A — матрица инцидентности графа.

Суть метода состоит во введении специального параметра, который называется суммой неизвестных $S = \sum_{i=1}^{n} x_i$. Некоторые графы позволяют представлять переменные системы через этот параметр. Суммируя эти переменные, получаем уравнение относительно него. Решив данное уравнение, получим значение этого параметра и значения всех переменных.

Основная проблема заключается в нахождении данного параметра. Для его нахождения в системе (1) умножим i-е уравнение на такой множитель d_i, $i = 1, 2, ..., n,$ чтобы сумма всех уравнений дала в левой части вектор $(dx_1,\ dx_2,\ ...,\ dx_n)$, где d — какая-то константа. Отсюда получаем равенство

$dS = -\sum_{i=1}^{n} d_i b_i$ и легко находим S . Но для этого необходимо найти d_i и d . В силу последнего построения они удовлетворяют системе уравнений

$$AD \equiv \overline{d} \text{ (mod } K), \qquad (2)$$

где $D=(d_1, d_2, ..., d_n)$, а $\overline{d} = (d, d, \ ..., d)$. Для различных графов система (2) решается по-разному. При этом используются специфические свойства графов, такие как симметрия, связность и т.п. Учет специфики структуры графов облегчает нахождение этих параметров.

Пример 1. Рассмотрим граф на рис. 1, где K = 7, $\boldsymbol{b}$ = (1, 2, 3, 4, 5, 6, 7, 8).

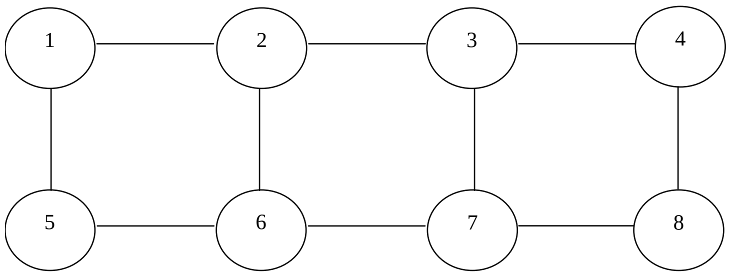

Рис. 1

Запишем для этого графа системы (1) и (2) в виде систем (3) и (4).

$$\left.\begin{array}{l}
x_1 + x_2 + x_5 \equiv -1 \\
x_1 + x_2 + x_3 + x_6 \equiv -2 \\
x_2 + x_3 + x_4 + x_7 \equiv -3 \\
x_3 + x_4 + x_8 \equiv -4 \\
x_1 + x_5 + x_6 \equiv -5 \\
x_2 + x_5 + x_6 + x_7 \equiv -6 \\
x_3 + x_6 + x_7 + x_8 \equiv -7 \\
x_4 + x_7 + x_8 \equiv -8
\end{array}\right\} (\text{ mod} K), \qquad (3)$$

$$\left.\begin{array}{l}
d_1 + d_2 + d_5 \equiv d \\
d_1 + d_2 + d_3 + d_6 \equiv d \\
d_2 + d_3 + d_4 + d_7 \equiv d \\
d_3 + d_4 + d_8 \equiv d \\
d_1 + d_5 + d_6 \equiv d \\
d_2 + d_5 + d_6 + d_7 \equiv d \\
d_3 + d_6 + d_7 + d_8 \equiv d \\
d_4 + d_7 + d_8 \equiv d
\end{array}\right\} (\text{ mod} K). \qquad (4)$$

Сравнивая в ситеме (4) четвертое и восьмое уравнения, получим равенство $d_3 = d_7$. По аналогии с этим из первого и пятого уравнений следует $d_2 = d_6$, из третьего и седьмого — $d_4 = d_8$, из второго и шестого — $d_1 = d_5$.

Таким образом, получаем $d_1 = d_4 = d_5 = d_8$, а $d_2 = d_3 = d_6 = d_7$.

Сравнивая первое и второе уравнения из (4), получим $d_5 = 2d_2$. Пусть $d_2 = 1$. Тогда $d_3 = d_6 = d_7 = 1$, $d_1 = d_4 = d_5 = d_8 = 2$. Значит, $d = 5$. Отсюда $5S =$ $= -\sum_{i=1}^{n} d_i b_i = -54$ = 2(mod 7), а S = 6 (mod 7).

Найдем x_i, $i = 1, 2, \ldots, n$, из системы (3), используя представления переменных через параметр S. Складывая четвертое и шестое уравнения, получим $S - x_1 = -10$. Значит, $x_1 = S + 10$ = 16 = 2(mod 7). Аналогично из второго и восьмого уравнений получим x_5 = 2(mod 7), из первого и седьмого — x_4 = 0(mod 7), из третьего и пятого — x_8 = 0(mod 7). Подставляя полученные значения в уравнения системы (3), получим x_2 = 2(mod 7), x_3 = 0(mod 7), x_6 = –2(mod 7), x_7 = – 1(mod 7). В результате находим общее решение $\boldsymbol{x}$ = (2, 2, 3, 0, 2, – 2, –1, 0)(mod 7).

Проверим это решение:

$$\boldsymbol{b} = (1, 2, 3, 4, 5, 6, 7, 8),\ x_1 = 2 \to (3, 4, 3, 4, 0, 6, 7, 8),$$

$$x_2 = 2 \to (5, 6, 5, 4, 0, 8, 7, 8),\ x_3 = 3 \to (5, 9, 8, 0, 0, 8, 10, 8),$$

$$x_5 = 2 \to (0, 9, 8, 0, 2, 10, 10, 8),\ x_6 = -2 \to (0, 0, 8, 0, 0, 8, 8, 8),$$

$$x_7 = -1 \to (0,0,0,0,0,0,0,0) \pmod 7.$$

Здесь возникают трудности, если K = 5. Тогда уравнение $5S = -\sum_{i=1}^{n} d_i b_i =$ $= -54$ (mod 5) не имеет решения. Чтобы оно имело решение, необходимо скорректировать начальное состояние сейфа. Положим $b_7 = 7$. Тогда $5S = -55$ (mod 5), отсюда $S = -1$(mod 5). Произведя те же операции, что и выше, с уравнениями из системы (4), но по модулю 5, получим общее решение $\boldsymbol{x}$ = (0, 0, – 3, 2, – 1, 1, – 2, 2)(mod 5).

Проверим это решение:

$$\boldsymbol{b} = (1, 2, 3, 4, 5, 7, 7, 8),\ x_3 = -3 \to (1, -1, 0, 1, 5, 7, 4, 8),$$

$$x_4 = 2 \to (1, -1, 2, 3, 5, 7, 4, 0),\ x_5 = -1 \to (0, -1, 2, 3, 4, 6, 4, 0),$$

$$x_6 = 1 \to (0, 0, 2, 3, 0, 7, 5, 0),\ x_7 = -2 \to (0, 0, 0, 3, 0, 0, 3, -2),$$

$$x_8 = 2 \to (0, 0, 0, 0, 0, 0, 0, 0) \pmod 5.$$

Пример 2. Рассмотрим граф на рис. 2, где K = 5, $\boldsymbol{b}$ = (1, 2, 3, 4, 5, 6, 3, 2, 1).

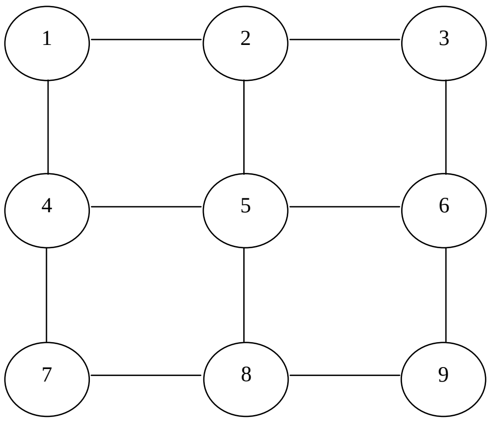

Рис. 2

Запишем для этого сейфа общую систему.

$$\left.\begin{array}{l}
x_1+x_2+\;.\;\;x_4\;\;.\;\;.\;\;.\;\;.\;\;.\;\;\equiv -1\\
x_1+x_2+x_3+\;.\;\;x_5\;\;.\;\;.\;\;.\;\;.\;\;\equiv -2\\
.\;\;x_2+x_3+\;.\;\;.\;\;x_6\;\;.\;\;.\;\;.\;\;\equiv -3\\
x_1+\;.\;\;.\;\;x_4+x_5+\;.\;\;x_7\;\;.\;\;.\;\;\equiv -4\\
x_2+\;.\;\;x_4+x_5+x_6+\;.\;\;x_8\;\;.\;\;\equiv -5\\
.\;\;.\;\;x_3+\;.\;\;x_5+x_6+\;.\;\;.\;\;x_9\;\equiv -6\\
.\;\;.\;\;.\;\;x_4+\;.\;\;.\;\;x_7+x_8\;\;.\;\;\equiv -3\\
.\;\;.\;\;.\;\;x_5+\;.\;\;x_7+x_8+x_9\equiv -2\\
.\;\;.\;\;.\;\;.\;\;.\;\;x_6+\;.\;\;x_8+x_9\equiv -1
\end{array}\right\}(\bmod 5). \qquad (5)$$

$$\left.\begin{array}{l}
d_1+d_2+\;.\;\;d_4\;\;.\;\;.\;\;.\;\;.\;\;.\;\;\equiv d\\
d_1+d_2+d_3+\;.\;\;d_5\;\;.\;\;.\;\;.\;\;.\;\;\equiv d\\
.\;\;d_2+d_3+\;.\;\;.\;\;d_6\;\;.\;\;.\;\;.\;\;\equiv d\\
d_1+\;.\;\;.\;\;d_4+d_5+\;.\;\;d_7\;\;.\;\;.\;\;\equiv d\\
d_2+\;.\;\;d_4+d_5+d_6+\;.\;\;d_8\;\;.\;\;\equiv d\\
.\;\;.\;\;d_3+\;.\;\;d_5+d_6+\;.\;\;.\;\;d_9\;\equiv d\\
.\;\;.\;\;.\;\;d_4+\;.\;\;.\;\;d_7+d_8\;\;.\;\;\equiv d\\
.\;\;.\;\;.\;\;d_5+\;.\;\;d_7+d_8+d_9\equiv d\\
.\;\;.\;\;.\;\;.\;\;.\;\;d_6+\;.\;\;d_8+d_9\equiv d
\end{array}\right\}(\bmod 5). \qquad (6)$$

В силу симметрии графа очевидно, что $d_1=d_3=d_7=d_9$, а $d_2=d_4=d_6=d_8$. Решая в системе (6) совместно второе и пятое уравнения, получим соотношение $2d_1=3d_2$. Следовательно, отсюда самым простейшим решением есть $d_1=3$, $d_2=2$. Таким образом, $d=7$, а $d_5=-1$. Просуммировав все уравнения в системе (6), получим $7S=-\sum\limits_{i=1}^{n} d_i b_i=-47$ (mod 5) = 3(mod 5). Отсюда $S=-1$(mod 5).

Переходим к поиску переменных системы (5) с помощью данного параметра. Складывая первое, третье и восьмое уравнения, получаем в левой части $S+x_2$, а в правой части — число – 1 –3 –2 = – 6. Отсюда $x_2=-6+1=-5=0$ (mod 5). Аналогично из первого, шестого и седьмого уравнений получим $x_4=1$ (mod 5), из третьего, четвертого и девятого уравнений — $x_6=-2$ (mod 5), из второго, седьмого и девятого — $x_8=0$ (mod 5). Подставляя полученные значения в первое, третье, седьмое и девятое уравнения, получаем $x_1=-2$ (mod 5), $x_3=-1$ (mod 5), $x_7=1$ (mod 5), $x_9=1$ (mod 5). Из пятого уравнения — $x_5=1$ (mod 5). Таким образом, общее решение имеет вид $\boldsymbol{x}$ = (–2, 0, –1, 1, 1, –2, 1, 0, 1)(mod 5).

Проверим это решение:

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

Возникает проблема при K = 7. Тогда уравнение $7S = -47\,(\mathrm{mod}\ 7)$ не имеет решения, следовательно, в данном примере задача не имеет решения. Для того чтобы она имела решение, необходимо откорректировать начальное состояние сейфа. Положим $b_7 = 2$, $b_8 = 1$. Тогда $7S = -\sum_{i=1}^{n} d_i b_i = -42\,(\mathrm{mod}\ 7)$ = 3(mod7). Отсюда $S = 1\,(\mathrm{mod}\ 7)$. Произведя те же операции, что и выше, с уравнениями из системы (4), но по модулю 7, получим общее решение $\boldsymbol{x}$ = (1, 1, – 3, – 3, – 2, – 1, 0, 1, 0)(mod 7). Легко проверить, что оно в действительности является решением.

Как показали приведенные примеры, метод суммарных представлений является универсальным для решения задач о математических сейфах на неориентированных графах. Исключение — случай, когда d кратное K. Тогда для существования решения необходимо откорректировать начальное состояние сейфа таким образом, чтобы $-\sum_{i=1}^{n} d_i b_i$ была кратной K. В результате задача решается по общим правилам метода.

А.Л. Гурін

МЕТОД СУМАРНИХ ПРЕДСТАВЛЕНЬ ДЛЯ РОЗВ'ЯЗКУ ЗАДАЧ ПРО МАТЕМАТИЧНИЙ СЕЙФ НА ГРАФАХ

Розглянуто один із заявлених в попередніх роботах методів — метод сумарних представлень, який використано на чисто інтуїтивному рівні, та дано його теоретичне обгрунтування. Суть методу полягає у пошуку спеціального параметра S, який називається сумою невідомих, що представляють розв'язок вихідної системи рівнянь. Деякі графи за своєю структурою дозволяють виразити змінні системи через цей параметр. Отже, проблема полягає в знаходженні значення цього параметра. Як показали проведені теоретичні дослідження, це досягається шляхом розв'язання спеціальної додаткової системи рівнянь, яка є зваженою сумою рівнянь вихідної системи з коефіцієнтами d_i, $i = 1, 2, \ldots, n$, а сама сума дорівнює dS, де d — невідома константа. Розв'язавши цю додаткову систему рівнянь, отримаємо значення d_i, $i = 1, 2, \ldots, n, d$ та S, а разом з тим і значення всіх змінних основної системи. Метод продемонстровано на двох прикладах, які підтвердили його ефективність. Крім того, в обох прикладах звернено увагу на виняткові випадки, коли розв'язку не існує. Вони виникають тоді, коли значення параметра d кратне K, де K — кількість станів кожного замка в сейфі. У таких випадках для існування розв'язку здійснюється корекція початкових станів сейфа b_i, $i = 1, 2, \ldots, n$, таким чином, щоб $-\sum_{i=1}^{n} d_i b_i$ була кратною K. Потім задача розв'язується за загальною схемою методу.

Ключові слова: математичний сейф, система рівнянь, вектор початкового стану сейфа, неорієнтований граф, метод сумарних представлень.

A.L.Gurin

METHOD OF SUMMARIZED REPRESENTATIONS TO SOLVE THE MATHEMATICAL SAFE PROBLEM ON THE GRAPHS

We explore one of the methods, first formulated in our previous papers, namely, the method of summarized representations which was used in these papers on merely intuitive level. In this paper, theoretical substantiation of the method is given. The gist of the method consists in search of special parameter S, called the sum of unknowns, representing the solution of original system of equations. Some graphs in design are susceptible to express unknowns of the system through the above mentioned parameter. In such cases, the problem reduces to evaluation of the parameter value. The in-depth analysis of the problem at hand shows that this can be achieved by solving special auxiliary system of equations. The latter presents itself as the weighted sum of original equations, namely, the sum of original system of equations multiplied by coefficients $d_i, i = 1, 2, ..., n$. It should be noted that the above mentioned sum equals dS with d being an unknown constant. Upon solving the auxiliary system of equations we obtain the values of d_i, $i = 1, 2, ..., n, d$, and S, as well as the values of all original system variables. The method is demonstrated on two examples confirming its efficiency. In both examples special attention is given to the particular case of solution nonexistence. This is the case when d is K-fold, where K is the number of states in each safe lock. For the solution to exist the initial safe state is adjusted in such a way that the sum $-\sum_{i=1}^{n} d_i b_i$ becomes K-fold (b_i, $i = 1, 2, ..., n$, are the safe states). Then the problem is solved using the general scheme of the method.

Keywords: mathematical safe, vector of safe initial state, nonoriented graph, method of summarized representations.

1. Донец Г.А., Гурин А.Л., Загороднюк С.П. Методы решения задач о математическом сейфе на элементарных графах. *Международный научно-технический журнал «Проблемы управления и информатики»*. 2019. № 4. С. 36–47.
2. Kryvyi S.L. Algorithms for solution of systems of linear Diophantine equations in residue fields. *Cybernetics and Systems Analysis*. 2007. **43**(2). P. 171−178.
3. Kryvyi S.L. Solutin algoritms for systems of linear equations over residue rings. *Cybernetics and Systems Analysis*. 2016. **52**(5). P. 149−160.

Получено 06.09.2019