

УДК 519.1

А.Л. Гурін, А.Г. Донець, С.П. Загороднюк

МЕТОД СУМАРНИХ ПРЕДСТАВЛЕНЬ РОЗВ'ЯЗАННЯ ЗАДАЧ ПРО МАТЕМАТИЧНИЙ СЕЙФ НА МАТРИЦЯХ У СКІНЧЕННИХ ПОЛЯХ

Гурін Артем Леонідович

Національний технічний університет України «Київський політехнічний інститут
імені Ігоря Сікорського»,
orcid: 0000-0001-7429-2075

galtef.1@gmail.com

Донець Андрій Георгійович

Національний технічний університет України «Київський політехнічний інститут
імені Ігоря Сікорського»,
orcid: 0000-0002-8122-051X

ogurman72@gmail.com

Загороднюк Сергій Петрович

Київський національний університет імені Тараса Шевченка,
orcid:0000-0002-1063-1776

szagorodniuk@gmail.com

Розглядається один з існуючих методів розв'язання задачі про математичний сейф — метод сумарних представлень, розроблений для графів та матриць, теоретично описаний і обґрунтований у попередніх роботах. Ідея методу полягає у пошуку спеціального параметра S , який називається сумою невідомих, що представляють розв'язок вихідної системи рівнянь. В існуючому методі сумарних представлень на матрицях це досягається шляхом розв'язання спеціальної додаткової системи рівнянь, яка є зваженою сумою рівнянь вихідної системи з коефіцієнтами $d_i, i = 1, 2, \dots, n$, а сама сума рівна dS , де d — невідома константа. Дослідженнями обґрунтовано метод як інструмент розв'язку задач про математичний сейф, але метод чутливий до виняткових випадків, коли розв'язку не існує (значення параметра d кратне, де K — кількість станів кожного замка в сейфі), і потребує корекції початкових станів сейфу. Тому в даній статті пропонується метод сумарних представлень на матрицях, який дозволить отримати універсальний та стійкий метод розв'язку задач про математичний сейф довільного обсягу. Особливістю методу є «сегментація» висхідної системи рівнянь відносно змінних x_{ij} та введення оператора $\sigma_j = \sum_{i=1}^m x_{ij}$, який, на відміну від методу сума-

рних представлень розв'язання задачі про математичний сейф на гра-

© А.Л. ГУРІН, А.Г. ДОНЕЦЬ, С.П. ЗАГОРОДНЮК, 2023

*Міжнародний науково-технічний журнал
Проблеми керування та інформатики, 2023, № 4*

фах, є частковою сумою при фіксованому номері j . Завдяки введенню додаткового оператора σ_j отримаємо можливість розв'язку висхідної системи: $x_{ij} = s_i + \sigma_j + b_{ij}$. Метод продемонстровано на прикладі, який підтвердив його ефективність та якість. Проведено аналіз арифметичної складності алгоритму методу сумарних представлень у порівнянні з класичним методом Гаусса.

Ключові слова: математичний сейф, діофантова система рівнянь, вектор початкового стану сейфа, метод сумарних представлень, скінченні поля, скінченні кільця, оператор, арифметична складність.

Вперше метод сумарних представлень було розглянуто для розв'язання задач про математичний сейф на графах у статті [1].

Як відомо, завдання про математичний сейф формулюється за допомогою графів і матриць, а його розв'язання зводиться до розв'язку систем лінійних рівнянь у скінченних полях або скінченних кільцях [2], а також його варіації над цими областями.

Математичний сейф на матрицях представляється за допомогою матриці $B = (b_{ij})_{m,n}$, яка називається матрицею початкових станів замків, де кожний елемент відповідає одному замку і приймає одне з K значень $0, 1, \dots, K-1$. Один поворот ключем даного замка за годинниковою стрілкою призводить до збільшення стану замка на «+1», а проти годинникової стрілки — до зменшення на «-1». Замок вважається відкритим, якщо знаходиться в стані «0», в інших станах — закритий [3, 4]. Кожен поворот в даному замку призводить до такого ж повороту у суміжних замках, тобто таких, які знаходяться в одному рядку та стовпці. Задача полягає в тому, щоб для кожного ij -замка знайти таку кількість поворотів x_{ij} , після здійснення яких сейф стане відкритим, тобто $B_{fin} = (b_{ij} = 0)_{m,n}$, що відповідає одночасному відкриттю усіх замків. Для окремого обраного ij -замка це означає, що сума всіх x_{ij} обраного рядка та стовпця дорівнює $-b_{ij} \pmod{K}$.

Суть методу полягає у введенні спеціального оператора, який називається сумою невідомих S .

Запишемо систему рівнянь для першого рядка матриці B для кожного b_{1j} :

$$\left. \begin{aligned} x_{11} + x_{12} + \dots + x_{1n} + x_{21} + \dots + x_{m1} &= -b_{11} \\ x_{11} + x_{12} + \dots + x_{1n} + x_{22} + \dots + x_{m2} &= -b_{12} \\ \dots &= \dots \\ \underbrace{x_{11} + x_{12} + \dots + x_{1n}}_{S_1} + x_{2n} + \dots + x_{mn} &= -b_{1n} \end{aligned} \right\} \pmod{K}. \quad (1)$$

Позначимо $\sum_{j=1}^n x_{1j} = s_1$. Аналогічно $\sum_{j=1}^n x_{2j} = s_2, \dots, \sum_{j=1}^n x_{mj} = s_m$.

Додавши рівняння системи (1), отримаємо

$$ns_1 + s_2 + s_3 + \dots + s_m = -\sum_{j=1}^n b_{1j}.$$

Здійснюючи всі ті ж самі операції відносно інших рядків матриці B , отримаємо загальну систему лінійних діофантових рівнянь:

$$\left. \begin{aligned} ns_1 + s_2 + \dots + s_m &= -\sum_{j=1}^n b_{1j} \\ s_1 + ns_2 + \dots + s_m &= -\sum_{j=1}^n b_{2j} \\ \cdot &\quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ s_1 + s_2 + \dots + ns_m &= -\sum_{j=1}^n b_{mj} \end{aligned} \right\} (\text{mod } K). \quad (2)$$

Позначимо $s_1 + s_2 + \dots + s_m = S$. Додавши усі рівняння, отримаємо

$$(n+m-1) \cdot S = -\sum_{i=1}^m \sum_{j=1}^n b_{ij} \Rightarrow S = \frac{-\sum_{i=1}^m \sum_{j=1}^n b_{ij}}{n+m-1} (\text{mod } K). \quad (3)$$

Перейдемо до пошуку s_i із системи (2). Перше рівняння можна записати у

$$\text{вигляді } (n-1)s_1 + S = -\sum_{j=1}^n b_{1j} \Rightarrow s_1 = \frac{-\sum_{j=1}^n b_{1j} - S}{(n-1)} (\text{mod } K).$$

Аналогічні дії дозволяють знайти загальний вираз для пошуку s_i :

$$s_i = \frac{-\sum_{j=1}^n b_{ij} - S}{(n-1)} (\text{mod } K). \quad (4)$$

Позначимо $\sigma_j = \sum_{i=1}^m x_{ij}$. Після цього, якщо візьмемо перші рівняння із системи

типу (1) для кожного s_i , отримаємо

$$S + (m-1)\sigma_1 = -\sum_{i=1}^m b_{i1}.$$

Узагальнюючи для інших σ_j , беремо j -ті рівняння із системи (1), записані для s_i .

Отримаємо загальний вид

$$\sigma_j = \frac{-\sum_{i=1}^m b_{ij} - S}{(m-1)} (\text{mod } K). \quad (5)$$

Звідси маємо розв'язок висхідної системи (1): $x_{ij} = s_i + \sigma_j + b_{ij}$.

Розглянемо приклад задачі матриці у скінченному полі при $m = 3$, $n = 4$, $K = 7$, де матриця B має вигляд

$$B = \begin{vmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 2 & 2 & 2 & 2 \end{vmatrix}.$$

Запишемо для неї систему рівнянь:

$$\begin{aligned}
 x_{11} + x_{12} + x_{13} + x_{14} + x_{21} &+ x_{31} &= \\
 x_{11} + x_{12} + x_{13} + x_{14} &+ x_{22} &+ x_{32} &= \\
 x_{11} + x_{12} + x_{13} + x_{14} &+ x_{23} &+ x_{33} &= \\
 x_{11} + x_{12} + x_{13} + x_{14} &+ x_{24} &+ x_{34} &= \\
 x_{11} &+ x_{21} + x_{22} + x_{23} + x_{24} + x_{31} &= \\
 &x_{12} &+ x_{21} + x_{22} + x_{23} + x_{24} &+ x_{32} &= \\
 &&x_{13} &+ x_{21} + x_{22} + x_{23} + x_{24} &+ x_{33} &= \\
 &&&x_{14} + x_{21} + x_{22} + x_{23} + x_{24} &+ x_{34} &= \\
 x_{11} &+ x_{21} &+ x_{31} + x_{32} + x_{33} + x_{34} &= \\
 &x_{12} &+ x_{22} &+ x_{31} + x_{32} + x_{33} + x_{34} &= \\
 &&x_{13} &+ x_{23} &+ x_{31} + x_{32} + x_{33} + x_{34} &= \\
 &&&x_{14} &+ x_{24} + x_{31} + x_{32} + x_{33} + x_{34} &= \\
 &&&&&= -1 \\
 &&&&&= -2 \\
 &&&&&= -3 \\
 &&&&&= -4 \\
 &&&&&= -5 \\
 &&&&&= -6 \\
 &&&&&= -7 \\
 &&&&&= -8 \\
 &&&&&= -2 \\
 &&&&&= -2 \\
 &&&&&= -2 \\
 &&&&&= -2
 \end{aligned} \left. \vphantom{\begin{aligned} x_{11} + x_{12} + x_{13} + x_{14} + x_{21} &+ x_{31} &= \\ x_{11} + x_{12} + x_{13} + x_{14} &+ x_{22} &+ x_{32} &= \\ x_{11} + x_{12} + x_{13} + x_{14} &+ x_{23} &+ x_{33} &= \\ x_{11} + x_{12} + x_{13} + x_{14} &+ x_{24} &+ x_{34} &= \\ x_{11} &+ x_{21} + x_{22} + x_{23} + x_{24} + x_{31} &= \\ &x_{12} &+ x_{21} + x_{22} + x_{23} + x_{24} &+ x_{32} &= \\ &&x_{13} &+ x_{21} + x_{22} + x_{23} + x_{24} &+ x_{33} &= \\ &&&x_{14} + x_{21} + x_{22} + x_{23} + x_{24} &+ x_{34} &= \\ x_{11} &+ x_{21} &+ x_{31} + x_{32} + x_{33} + x_{34} &= \\ &x_{12} &+ x_{22} &+ x_{31} + x_{32} + x_{33} + x_{34} &= \\ &&x_{13} &+ x_{23} &+ x_{31} + x_{32} + x_{33} + x_{34} &= \\ &&&x_{14} &+ x_{24} + x_{31} + x_{32} + x_{33} + x_{34} &= \end{aligned}} \right\} (\text{mod } 7).$$

Позначимо відповідні суми $\sum_{j=1}^4 x_{1j} = s_1$, $\sum_{j=1}^4 x_{2j} = s_2$, $\sum_{j=1}^4 x_{3j} = s_3$.

Утворимо суми з 1-го по 4-е рівняння та відповідно — з 5-го по 8-е і з 9-го по 12-е. Отримаємо

$$\left. \begin{aligned} 4s_1 + s_2 + s_3 &= -10 \\ s_1 + 4s_2 + s_3 &= -26 \\ s_1 + s_2 + 4s_3 &= -8 \end{aligned} \right\} (\text{mod } 7). \quad (6)$$

Позначимо $s_1 + s_2 + s_3 = S$. Складемо усі три рівняння системи (6). Отримаємо $6S = -44(\bmod 7) = -2(\bmod 7) = 12(\bmod 7) \Rightarrow S = \frac{12}{6} = 2(\bmod 7)$. Візьмемо перше рівняння системи (6). Запишемо його як $3s_1 + S = -10(\bmod 7)$. Звідси $3s_1 = -10 - S(\bmod 7) = -12(\bmod 7) \Rightarrow s_1 = \frac{-12}{3} = -4(\bmod 7) = 3(\bmod 7)$.

Аналогічно з 2-го та 3-го рівнянь отримаємо:

$$3s_2 = -26 - S(\bmod 7) = -28(\bmod 7) \Rightarrow s_2 = 0(\bmod 7),$$

$$3s_3 = -8 - S(\bmod 7) = -10(\bmod 7) = -3(\bmod 7) \Rightarrow s_3 = \frac{-3}{3} = -1(\bmod 7).$$

Позначимо $x_{11} + x_{21} + x_{31} = \sigma_1$. Аналогічно $x_{12} + x_{22} + x_{32} = \sigma_2$, $x_{13} + x_{23} + x_{33} = \sigma_3$, $x_{14} + x_{24} + x_{34} = \sigma_4$. Візьмемо рівняння (1), (5), (9) та складемо. Отримаємо $S + 2\sigma_1 = -8(\bmod 7) \Rightarrow 2\sigma_1 = -8 - 2 \Rightarrow \sigma_1 = -5(\bmod 7) = 2(\bmod 7)$.

Тепер складемо рівняння (2), (6) та (10). Отримаємо $S + 2\sigma_2 = -10(\bmod 7) \Rightarrow 2\sigma_2 = -10 - 2 \Rightarrow \sigma_2 = -6(\bmod 7) = 1(\bmod 7)$.

Продовжимо: (3)+(7)+(11). Отримаємо $S + 2\sigma_3 = -12(\bmod 7) \Rightarrow 2\sigma_3 = -12 - 2 \Rightarrow \sigma_3 = -7(\bmod 7) = 0(\bmod 7)$.

Остаточно складемо (4)+(8)+(12). Отримаємо $S + 2\sigma_4 = -14(\bmod 7) \Rightarrow 2\sigma_4 = -14 - 2 \Rightarrow \sigma_4 = -8(\bmod 7) = -1(\bmod 7)$.

Запишемо рівняння для довільного b_{ij} . Отримаємо $s_i + \sigma_j - x_{ij} = -b_{ij}$. Звідси легко отримуємо розв'язок системи (1): $x_{ij} = s_i + \sigma_j + b_{ij}$. Відповідні значення є елементами матриці $X = (x_{ij})_{m,n}$.

$$\text{У підсумку отримаємо матрицю } X = \begin{pmatrix} -1 & -1 & -1 & -1 \\ 0 & 0 & 0 & 0 \\ 3 & 2 & 1 & 0 \end{pmatrix}.$$

$$\text{Перевіримо це рішення. Вихідна матриця } B = \begin{vmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 2 & 2 & 2 & 2 \end{vmatrix}:$$

$$x_{11} = -1 \rightarrow B = \begin{vmatrix} 0 & 1 & 2 & 3 \\ 4 & 6 & 0 & 8 \\ 1 & 2 & 2 & 2 \end{vmatrix}, \quad x_{12} = -1 \rightarrow B = \begin{vmatrix} -1 & 0 & 1 & 2 \\ 4 & 5 & 0 & 8 \\ 1 & 1 & 2 & 2 \end{vmatrix},$$

$$x_{13} = -1 \rightarrow B = \begin{vmatrix} -2 & -1 & 0 & 1 \\ 4 & 5 & 6 & 8 \\ 1 & 1 & 1 & 2 \end{vmatrix}, \quad x_{14} = -1 \rightarrow B = \begin{vmatrix} -3 & -2 & -1 & 0 \\ 4 & 5 & 6 & 0 \\ 1 & 1 & 1 & 1 \end{vmatrix},$$

$$x_{31} = 3 \rightarrow B = \begin{vmatrix} 0 & -2 & -1 & 0 \\ 0 & 5 & 6 & 0 \\ 4 & 4 & 4 & 4 \end{vmatrix}, \quad x_{32} = 2 \rightarrow B = \begin{vmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 6 & 0 \\ 6 & 6 & 6 & 6 \end{vmatrix}, \quad x_{33} = 1 \rightarrow B = \begin{vmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{vmatrix}.$$

Сейф відкритий.

Оскільки в роботі розглядаються системи рівнянь в полі лишків за модулем простого числа, то до такої системи рівнянь застосовний загальновідомий метод Гаусса скорочення числа невідомих. Проаналізуємо арифметичну складність алгоритму методу сумарних представлень і порівняємо його з методом Гаусса.

Відомо, що арифметична складність розв'язання системи лінійних однорідних діофантових рівнянь за методом Гаусса має складність $O(l^3(\log k)^2)$, де $l = \max(n, m)$.

Складність запропонованого методу сумарних представлень складається зі складності знаходження розв'язку висхідної системи (1) $x_{ij} = s_i + \sigma_j + b_{ij}$, яка складається зі складності знаходження розв'язку s_i та σ_j та оператора S . Арифметична складність знаходження значення S розраховується за формулою (3) та має значення $O(l(\log k))$, де $l = \max(n, m)$. Тоді складність знаходження оператора s_i відповідно до формули (4) є $O(l(\log k + 1)) \approx O(l(\log k))$, де $l = \max(n, m)$. Так само розрахуємо складність знаходження оператора σ_j , яка розраховується за формулою (5) та має значення $O(l^2(\log k + 1)^2) \approx O(l^2(\log^2 k))$, де $l = \max(n, m)$.

Відповідно, загальна арифметична складність знаходження розв'язку x_{ij} має величину $O(l^2(\log^2 k)) + O(l(\log k)) \approx O(l^2(\log^2 k))$, де $l = \max(n, m)$. Отже, метод сумарних представлень має переваги за арифметичною складністю відносно методу Гаусса. Це пояснюється тим, що метод сумарних представлень враховує специфіку задачі про математичний сейф. Також у подальшому запропонований метод можна модифікувати для розв'язання задачі про математичний сейф на матрицях у скінченних кільцях, де метод Гаусса не застосовний.

A. Gurin, A. Donets, S. Zahorodniyk

METHOD OF SUMMARIZED REPRESENTATIONS TO SOLVE THE MATHEMATICAL SAFE PROBLEM ON MATRICES IN FINITE FIELDS

Artem Gurin

National Technical University of Ukraine «Igor Sikorsky Kyiv Polytechnic Institute»,
galtef.1@gmail.com

Andriy Donets

National Technical University of Ukraine «Igor Sikorsky Kyiv Polytechnic Institute»,
ogurman72@gmail.com

Sergiy Zahorodniyk

Taras Shevchenko National University of Kyiv,
szahorodniuk@gmail.com

One of the existing methods of solving the problem of a mathematical safe is considered — the method of total representations, which was developed for graphs and matrices, theoretically described and substantiated in the cited previ-

ous works. The idea of the method is to find a special parameter S , called the sum of unknowns representing the solution of the original system of equations. In the existing method of total representations on matrices, this is achieved by solving a special additional system of equations, which is a weighted sum of equations of the original system with coefficients $d_i, i = 1, 2, \dots, n$, and the sum itself is equal to dS , d an unknown constant. Research justified the method as a tool for solving the problem about a mathematical safe, but the method is sensitive to exceptional cases when a solution does not exist (when the value of the parameter d is a multiple of K , here K is the number of states of each lock in the safe), and required correction of the initial states of the safe. Therefore, this article proposes a modification of the method of total representations on matrices, which will allow obtaining a universal and stable method of solving problems about a mathematical safe of arbitrary volume. The feature of the method that is, the modification consists in the «segmentation» of the ascending system of equations with respect to the variables x_{ij} , and the introduction of the

operator $\sigma_j = \sum_{i=1}^m x_{ij}$, which, unlike the «classical» method of total representations, is a partial sum, with a fixed number j . Thanks to the introduction of an additional operator σ_j , we will be able to solve the ascending system: $x_{ij} = s_i + \sigma_j + b_{ij}$. The method is demonstrated on an example that confirmed its effectiveness and quality. The analysis of the arithmetic complexity of the algorithm of the method of total representations in comparison with the classical Gaussian method was carried out.

Keywords: mathematical safe, Diophantine system of equations, vector of safe initial state, finite fields, finite rings, method of summarized representations, operator, arithmetic complexity.

ПОСИЛАННЯ

1. Гурин А.Л. Метод суммарных представлений для решения задач о математическом сейфе на графах. *Международный научно-технический журнал «Проблемы управления и информатики»*. 2019. № 6. С. 5–10.
2. Крытый С.Л. Алгоритмы решения систем диофантовых уравнений в кольцах вычетов. *Кибернетика и системный анализ*. 2007. № 6. С. 27–40.
3. 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.
4. Kryvyi S.L. Algorithms for solution of systems of linear diophantine equations in residue fields. *Cybernetics and Systems Analysis*. 2007. Vol. 43, N 2. P. 171–178.

Отримано 23.06.2023