КІБЕРНЕТИКА та КОМП'ЮТЕРНІ ТЕХНОЛОГІЇ

УДК 51.681.3 DOI:10.34229/2707-451X.21.1.2

С.Л. КРИВИЙ, Г.І. ГОГЕРЧАК

ЗАДАЧА ПРО МАТЕМАТИЧНИЙ СЕЙФ ТА ЇЇ РОЗВ'ЯЗАННЯ [1] (Ч. 2)

Дана стаття – продовження ч. 1 [1]. В цій частині роботи розглядаються застосування методів та алгоритмів, описаних в ч. 1 до розв'язання задачі про математичний сейф в різних варіаціях. Досліджені матричний та графовий варіанти математичного сейфа, розглянуті умови існування розв'язку, алгоритми розв'язання задачі для різних представлень та їх ефективність.

Ключові слова: *математичний сейф, скінченні комутативні кільця, скінченні поля.*

Вступ. Нагадаємо, що математичним сейфом називається система $Z=(z_1,z_2,\ldots,z_n)$ взаємнопов'язаних між собою засувів так, що коли виконується поворот ключа в одному із засувів, то такий же поворот виконується і у всіх засувах, які пов'язані з даним. При повороті ключа в даному засуві він і всі засуви, пов'язані з цим засувом, збільшують свою позицію на одиницю за моддулем k. Кожний із засувів може знаходитися в одній із декількох позицій. Всіх можливих позицій скінченне число: $0,1,\ldots,k-1$. Засув відкритий, якщо він знаходиться в позиції 0. В довільній іншій позиції засув вважається закритим. Сейф може задаватися двома способами за допомогою матриці (матричний сейф) і за допомогою графа (графовий сейф). Початкові позиції засувів сейфа Z при першому способі задання визначаються матрицею $B=\|b_{ij}\|$, де пов'язаними з засувом z_{ij} є засуви, які знаходяться в i-му рядку і j-му стовпчику, а при другому – позиціями засувів у вершинах, де пов'язаними з засувом у вершиі u є засуви, розміщені у суміжних вершинах з вершиною u.

Необхідно розв'язати таку задачу. Виходячи з початкових позицій сейфа, знайти таку послідовність засувів і число поворотів ключа в них, щоб сейф перейшов у положення відкритого, тобто коли всі засуви знаходяться в позиції 0. Як було показано в першій частині даної роботи [1], розв'язання задачі про матемематичний сейф зводиться до розв'язання системи лінійних рівнянь вигляду:

$$A\bar{x}+\bar{b}\equiv 0(\mathrm{mod}\ k). \qquad (1)$$

1. Розв'язання задачі про математичний сейф

Розглянемо задачу про математичний сейф та можливі її варіації над скінченними кільцями і полями [2]. Вибір області, над якою розглядається сейф, залежить від числа позицій засувів.

Випадок 1. Число позицій засувів p просте. Оскільки число позицій є простим числом, то задача про матричний сейф розглядається над полем лишків

[1] За фінансової підтримки НАН України (проект 0118U005227)

за модулем p. Побудова цього розв'язку зводиться до розв'язання системи лінійних рівнянь вигляду (1) і це розв'язання виконується TSS-методом. Нехай маємо сейф в полі F_3 з матрицею

$$B = \begin{pmatrix} 2 & 0 & 2 & 2 \\ 1 & 2 & 2 & 1 \end{pmatrix}.$$

Тоді $\bar{b} = (2,0,2,2,1,2,2,1)$ і система рівнянь $A\bar{x} + \bar{b} \equiv 0\,(mod\ 3)$ має вигляд:

$$A \cdot x + \bar{b} = \begin{cases} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 2 \\ 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 2 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 2 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 2 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 2 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \end{cases} \equiv 0\,(mod\ 3).$$

Застосовуючи TSS-алгоритм для розв'язання цієї системи, знаходимо розв'язок СЛНДР

$x = (0,2,2,0,0,2,0,0)$, тобто $x_{11} = 0, x_{12} = 2, x_{13} = 2, x_{14} = 0, x_{21} = 0, x_{22} = 2,\ x_{23} = 0, x_{24} = 0$.

Цьому розв'язку відповідають такі перетворення матриці B:

$$\begin{pmatrix} 2 & 0 & 2 & 2 \\ 1 & 2 & 2 & 1 \end{pmatrix} \to (x_{12} = 2) \begin{pmatrix} 1 & 2 & 1 & 1 \\ 1 & 1 & 2 & 1 \end{pmatrix} \to (x_{13} = 2) \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix} \to (x_{22} = 2) \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Отже, знайдена послідовність поворотів ключа відкриває сейф. Ця сама задача за модулем 13 має розв'язок $x_{11} = 8, x_{12} = 7, x_{13} = 7, x_{14} = 8, x_{21} = 7, x_{22} = 9, x_{23} = 7, x_{24} = 7,$ який відкриває сейф (в чому можна переконатися безпосередньою перевіркою).

Зауважимо, що в тому випадку коли число $m + n - 1$, де $m \times n$ розмірність матриці B, кратне модулю, а сума коефіцієнтів матриці B не кратна модулю, то задача про сейф не має розв'язку. Це випливає з теореми 3 (див. част. 1). Дійсно, якщо розв'язувати задачу про сейф з матрицею B за модулем 5

$$A \cdot x + b = \begin{cases} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 2 \\ 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 2 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 2 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 2 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 2 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \end{cases} \equiv 0\,(mod\ 5),$$

то задача не має розв'язку, оскільки $m + n - 1 = 2 + 4 - 1 = 5 \equiv 0\,(mod\ 5)$ (це означає, що останній рядок матриці A лінійно залежить від попередніх рядків), а сума елементів матриці B дорівнює 12 і не кратна 5.

Випадок 2. Число позицій засувів *k* складене. Тоді область над якою розглядається математичний сейф є кільце лишків Z_k. Нехай маємо сейф в кільці Z_{12} з матрицею

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

Тоді система (1) набуває вигляду:

$$\begin{cases} x_{11} + x_{12} + x_{13} + x_{21} + 4 = 0 \\ x_{11} + x_{12} + x_{13} + x_{22} + 5 = 0 \\ x_{11} + x_{12} + x_{13} + x_{23} + 2 = 0 \\ x_{11} + x_{21} + x_{22} + x_{23} + 1 = 0 \\ x_{12} + x_{21} + x_{22} + x_{23} + 3 = 0 \\ x_{13} + x_{21} + x_{22} + x_{23} + 1 = 0 \end{cases} (mod\ 12).$$

Застосовуючи *TSS*-алгоритм для розв'язання цієї системи в кільці Z_{12}, отримуємо такі розв'язки:

$$s_1 = (0,6,0,6,9,0,9),\ s_2 = (4,8,4,4,0,0,4).$$

З цих розв'язків потрібно отримати розв'язок, у якого остання координата дорівнює 1, що відповідає початковим позиціям засувів. Для цього розв'язуємо порівняння $9x + 4y \equiv 1(mod\ 12)$. Очевидним розв'язком цього порівняння є $x = 1, y = -2$ або з урахуванням доповнення $x = 1, y = 10$. Лінійна комбінація $s_1 + 10s_2$ дає розв'язок задачі про математичний сейф $z = (4,2,4,10,9,0)$. Дійсно,

$$\begin{pmatrix} 4 & 5 & 2 \\ 1 & 3 & 1 \end{pmatrix} \to (x_{11} = 4)\begin{pmatrix} 8 & 9 & 6 \\ 5 & 3 & 1 \end{pmatrix} \to (x_{12} = 2)\begin{pmatrix} 10 & 11 & 8 \\ 5 & 5 & 1 \end{pmatrix} \to (x_{13} = 4)\begin{pmatrix} 2 & 3 & 0 \\ 5 & 5 & 5 \end{pmatrix} \to$$

$$\to (x_{21} = 10)\begin{pmatrix} 0 & 3 & 0 \\ 3 & 3 & 3 \end{pmatrix} \to (x_{22} = 9)\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Випадок 3. Число позицій засувів $k = p^r$, де p – просте число. В цьому випадку областю стає поле F_{p^r}. Для цього поля математична постановка залишається незмінною, але всі операції здійснюються в полі F_{p^r}. Розглянемо задачу про математичний сейф в полі F_{2^2} (таблиці 1 і 2 операцій якого наведені нижче), оскільки всі викладки для більших значень p і r аналогічні [3].

ТАБЛИЦЯ 1

+	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

ТАБЛИЦЯ 2

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

Нехай матриця сейфа в полі F_{2^2} є така:

$$B = \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 1 \end{pmatrix}.$$

Тоді $\bar{b} = (1,2,3,0,1,1)$ і система $A\bar{x} + \bar{b} \equiv 0$ в полі F_{2^2} набуває вигляду:

$$A\bar{x} + \bar{b} = \begin{cases} 1 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 2 \\ 1 & 1 & 1 & 0 & 0 & 1 & 3 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{cases} \equiv 0.$$

Застосуємо *TSS*-алгоритм для розв'язання цієї системи в полі F_{2^2}. Оскільки доповнення 1 дорівнює 1 в полі F_{2^2}, то дістаємо такі розв'язки першого рівняння:

(1,0,0,0,0,0,1), (0,1,0,0,0,0,1), (0,0,1,0,0,0,1),

(0,0,0,1,0,0,1), (0,0,0,0,1,0,0), (0,0,0,0,0,1,0).

Значення лівої частини другого рівняння, знайдені за таблицями 1 і 2, які були наведені вище для поля F_{2^2}, дорівнюють: 3,3,3,2,1,0. За цими значеннями комбінуванням першого розв'язку з рештою, отримуємо розв'язки першого і другого рівняння системи:

(1,1,0,0,0,0,0), (1,0,1,0,0,0,0), (1,0,0,2,0,0,3), (1,0,0,0,3,0,1), (0,0,0,0,0,1,0).

Значення лівої частини третього рівняння, знайдені за цими ж таблицями, дорівнюють: 0,0,3,2,1. За цими значеннями комбінуванням останнього розв'язку з третім і четвертим, отримуємо розв'язки перших трьох рівнянь системи:

(1,1,0,0,0,0,0), (1,0,1,0,0,0,0), (1,0,0,2,0,3,3), (1,0,0,0,3,2,1).

Значення лівої частини четвертого рівняння дорівнюють: 1,1,0,0. За цими значеннями комбінуванням першого розв'язку з другим, отримуємо розв'язки перших чотирьох рівнянь системи:

(0,1,1,0,0,0,0), (1,0,0,2,0,3,3), (1,0,0,0,3,2,1).

Значення лівої частини п'ятого рівняння дорівнюють: 1,2,0. За цими значеннями дістаємо розв'язки перших п'яти рівнянь системи:

(1,2,2,2,0,3,3), (1,0,0,0,3,2,1).

Значення лівої частини шостого рівняння дорівнюють: 0,0. Це означає, що обидва вектори є розв'язками початкової системи. Другий розв'язок справді є розв'язком неоднорідної системи, а перший стає її розв'язком, якщо його помножити на 2 згідно таблиць 1 і 2 в полі F_{2^2}. В результаті знаходимо вектор (2,3,3,3,0,1) – другий розв'язок цієї системи.

Безпосередньою перевіркою переконуємося, що отримані розв'язки дійсно відкривають сейф. Для першого розв'язку маємо:

$$\begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 1 \end{pmatrix} \to (x_{11} = 1) \begin{pmatrix} 0 & 3 & 2 \\ 1 & 1 & 1 \end{pmatrix} \to (x_{22} = 3) \begin{pmatrix} 0 & 0 & 2 \\ 2 & 2 & 2 \end{pmatrix} \to (x_{23} = 2) \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Для другого розв'язку маємо:

$$\begin{pmatrix}1&2&3\\0&1&1\end{pmatrix}\to(x_{11}=2)\begin{pmatrix}3&0&1\\2&1&1\end{pmatrix}\to(x_{12}=3)\begin{pmatrix}0&3&2\\2&2&1\end{pmatrix}\to(x_{13}=3)\begin{pmatrix}3&0&1\\2&2&2\end{pmatrix}\to$$
$$\to(x_{21}=3)\begin{pmatrix}0&0&1\\1&1&1\end{pmatrix}\to(x_{23}=1)\begin{pmatrix}0&0&0\\0&0&0\end{pmatrix}.$$

Для існування розв'язку задачі про сейф в цьому полі, як і в попередньому випадку, повинна виконуватися умова: якщо $m+n-1\equiv 0\,(mod\ p)$, то $\sum_{i=1}^{mn-1} b_i \equiv b_{mn}\,(mod\ p)$, де сума обчислюється за таблицями поля F_{p^r}. Дійсно, якщо $m+n-1\equiv 0\,(mod\ p)$, то останнє рівняння цієї системи є сумою (лінійною комбінацією) попередніх рівнянь цієї системи, а звідси і випливає справедливість умови.

Наприклад, приведена вище задача про сейф, у якої останнє значення вільного члена дорівнює 2 (а не 1), не має розв'язку в полі F_{2^2} оскільки $m+n-1=1+1+1+1\equiv 0\,(mod\ 2)$ і $\sum_{i=1}^{5} b_i \equiv 1$, а останнє рівняння, яке є сумою попередніх п'яти рівнянь, дорівнює 2. Отримана суперечність говорить про несумісність системи (1). Справді, комбінація розв'язків

$$s_1=(1,2,2,2,0,3,3), s_2=(1,0,0,0,3,2,1)$$

для значень 2, 3 (результат підстановки в останнє рівняння) дає розв'язок $2s_1+s_2=(3,3,3,3,3,3,0)$, який не є розв'язком задачі.

2. Варіації задачі про математичний сейф

Випадок 1. Розглянемо матричний сейф в полі лишків F_k в такій постановці: сейф вважається відкритим не при нульових станах всіх засувів, а при певній комбінації цих засувів. Тоді система (1) набуває вигляду

$$A\bar{x}+\bar{b}\equiv\bar{c}\ (mod\ k), \tag{2}$$

де $\bar{c}$ позиції засувів, при яких сейф буде відкритим, а $\bar{b}$ – вектор початкових позицій засувів.

Очевидно, що дана задача зводиться до розглянутих вище випадків, оскільки система (2) редукується до СЛОДР

$$A\bar{x}+\bar{d}\equiv 0\,(mod\ k), \tag{3}$$

де $\bar{d}=\bar{b}-\bar{c}$.

Складність обчислення перебірним методом вектора $\bar{d}$, не знаючи потрібної комбінації позицій засувів, пропорціональна величині k^{mn}, де $m\times n$ – розмірність матриці A. При невеликих значеннях k,m,n обчислення вектора $\bar{d}$ не складає труднощів. Але коли модуль k досить велике число, то навіть при невеликих m і n складність обчислення стає великою. Наприклад, якщо $k=101, m=4,\ \ n=5$, то складність перебірного методу $P=101^{20}\approx 10^{41}\approx 2^{123}$. Це вже досить велика кількість комбінацій, яку необхідно в найгіршому випадку розглянути.

Нехай дана матриця сейфа

$$B=\begin{pmatrix}14&0&0\\0&0&0\\0&0&11\end{pmatrix},$$

а задача розв’язується в полі за модулем 17 з такою комбінацією, яка відкриває сейф,

$$c = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}.$$

Тоді СЛНДР $A\bar{x} + \bar{b} \equiv \bar{c}\ (mod\ 17)$ набуває вигляду:

$$\begin{cases} 1\ 1\ 1\ 1\ 0\ 0\ 1\ 0\ 0\ 14 = 1 \\ 1\ 1\ 1\ 0\ 1\ 0\ 0\ 1\ 0\ 0 = 2 \\ 1\ 1\ 1\ 0\ 0\ 1\ 0\ 0\ 1\ 0 = 3 \\ 1\ 0\ 0\ 1\ 1\ 1\ 1\ 0\ 0\ 0 = 4 \\ 0\ 1\ 0\ 1\ 1\ 1\ 0\ 1\ 0\ 0 = 5\ (mod\ 17). \\ 0\ 0\ 1\ 1\ 1\ 1\ 0\ 0\ 1\ 0 = 6 \\ 1\ 0\ 0\ 1\ 0\ 0\ 1\ 1\ 1\ 0 = 7 \\ 0\ 1\ 0\ 1\ 1\ 1\ 1\ 0\ 1\ 0 = 8 \\ 0\ 0\ 1\ 0\ 0\ 1\ 1\ 1\ 1\ 11 = 9 \end{cases}$$

Після перетворення цієї СЛНДР до СЛОДР, отримуємо

$$\begin{cases} 1\ 1\ 1\ 1\ 0\ 0\ 1\ 0\ 0\ 13 = 0 \\ 1\ 1\ 1\ 0\ 1\ 0\ 0\ 1\ 0\ 15 = 0 \\ 1\ 1\ 1\ 0\ 0\ 1\ 0\ 0\ 1\ 14 = 0 \\ 1\ 0\ 0\ 1\ 1\ 1\ 1\ 0\ 0\ 13 = 0 \\ 0\ 1\ 0\ 1\ 1\ 1\ 0\ 1\ 0\ 12 = 0\ (mod\ 17). \\ 0\ 0\ 1\ 1\ 1\ 1\ 0\ 0\ 1\ 11 = 0 \\ 1\ 0\ 0\ 1\ 0\ 0\ 1\ 1\ 1\ 10 = 0 \\ 0\ 1\ 0\ 1\ 1\ 1\ 1\ 0\ 1\ 9 = 0 \\ 0\ 0\ 1\ 0\ 0\ 1\ 1\ 1\ 1\ 2 = 0 \end{cases}$$

Розв’язком цієї системи є вектор $y = (3,13,5,1,13,,5,15,10,6,5)$. Для побудови розв’язку задачі про сейф необхідно розв'язати порівняння $5z \equiv 1\,(mod\ 17)$. Розв’язок цього порівняння $z = 7$. Помноживши вектор y на $z = 7,$ дістаємо розв'язок задачі про сейф: $x = (4,6,1,7,6,1,3,2,8)$. Дійсно,

$$\begin{pmatrix} 14 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 11 \end{pmatrix} \to (x_{11} = 4) \begin{pmatrix} 1 & 4 & 4 \\ 4 & 0 & 0 \\ 4 & 0 & 11 \end{pmatrix} \to (x_{12} = 6) \begin{pmatrix} 7 & 10 & 10 \\ 4 & 6 & 0 \\ 4 & 6 & 11 \end{pmatrix} \to (x_{13} = 1) \begin{pmatrix} 8 & 11 & 11 \\ 4 & 6 & 1 \\ 4 & 6 & 12 \end{pmatrix} \to$$

$$\to (x_{21} = 7) \begin{pmatrix} 15 & 11 & 11 \\ 11 & 13 & 8 \\ 11 & 6 & 12 \end{pmatrix} \to (x_{22} = 6) \begin{pmatrix} 15 & 0 & 11 \\ 0 & 2 & 14 \\ 11 & 12 & 12 \end{pmatrix} \to (x_{23} = 1) \begin{pmatrix} 15 & 0 & 12 \\ 1 & 3 & 15 \\ 11 & 12 & 13 \end{pmatrix} \to$$

$$\to (x_{31}=3)\begin{pmatrix}1 & 0 & 12\\ 4 & 3 & 15\\ 14 & 15 & 16\end{pmatrix}\to (x_{32}=2)\begin{pmatrix}1 & 2 & 12\\ 4 & 5 & 15\\ 16 & 0 & 1\end{pmatrix}\to (x_{33}=8)\begin{pmatrix}1 & 2 & 3\\ 4 & 5 & 6\\ 7 & 8 & 9\end{pmatrix}.$$

Випадок 2. Розглянемо задачу про сейф в полі F_{p^r}, який вважається відкритим при певній комбінації засувів.

Система (2) тепер розв'язується в полі F_{p^r}. Складність обчислення вектора $\bar{d}$, не знаючи потрібної комбінації позицій засувів, в найгіршому випадку пропорціональна величині $(p^r)^{mn} = p^{rmn}$, що вже при невеликих p,m,n,r складає великі труднощі обчислювального характеру. Наприклад, при $p=3, m=2, n=4, r=5$ отримуємо 3^{40} варіантів для аналізу (таблиці операцій 3 і 4 поля F_{3^2} відносно незвідного полінома x^2+x+2 над F_2 наведені нижче, де x позначений числом 3, $x+1$ – числом 4, $x+2$ – числом 5, $2x$ – числом 6, $2x+1$ – числом 7, $2x+2$ – числом 8).

ТАБЛИЦЯ 3

+	0	1	2	3	4	5	6	7	8
0	0	1	2	3	4	5	6	7	8
1	1	2	0	4	5	3	7	8	6
2	2	0	1	5	3	4	8	6	7
3	3	4	5	6	7	8	0	1	2
4	4	5	3	7	8	6	1	2	0
5	5	3	4	8	6	7	2	0	1
6	6	7	8	0	1	2	3	4	5
7	7	8	6	1	2	0	4	5	3
8	8	6	7	2	0	1	5	3	4

ТАБЛИЦЯ 4

*	0	1	2	3	4	5	6	7	8
0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8
2	0	2	1	6	8	7	3	5	4
3	0	3	6	7	1	4	5	8	2
4	0	4	8	1	5	6	2	3	7
5	0	5	7	4	6	2	8	1	3
6	0	6	3	5	2	8	7	4	1
7	0	7	5	8	3	1	4	2	6
8	0	8	4	2	7	3	1	6	5

Цю складність можна ще збільшити, якщо таблиці 3 і 4 поля F_{p^r} задавати з точністю до ізоморфізму. Такий варіант пошуку розв'язку за своєю складністю є гіршим за повний перебір розв'язків. В цьому випадку необхідно знайти ізоморфізм між таблицями 3 і 4 та таблицями 5 і 6, приведеними нижче, для поля F_{3^2}. Наприклад, перенумеруємо елементи цього поля таким чином: x позначимо числом 8, $x+1$ – числом 7, $x+2$ – числом 6, $2x$ – числом 5, $2x+1$ – числом 4, $2x+2$ – числом 3. Тоді таблиці 3 і 4 поля F_{3^2} набувають вигляду:

ТАБЛИЦЯ 5

+	0	1	2	8	7	6	5	4	3
0	0	1	2	8	7	6	5	4	3
1	1	2	0	7	6	8	4	3	5
2	2	0	1	6	8	7	3	5	4
8	8	7	6	5	4	3	0	1	2
7	7	6	8	4	3	5	1	2	0
6	6	8	7	3	5	4	2	0	1
5	5	4	3	0	1	2	8	7	6
4	4	3	5	1	2	0	7	6	8
3	3	5	4	2	0	1	6	8	7

ТАБЛИЦЯ 6

*	0	1	2	8	7	6	5	4	3
0	0	0	0	0	0	0	0	0	0
1	0	1	2	8	7	6	5	4	3
2	0	2	1	5	3	4	8	6	7
8	0	8	5	4	1	7	6	3	2
7	0	7	3	1	6	5	2	8	4
6	0	6	4	7	5	2	3	1	8
5	0	5	8	6	2	3	4	7	1
4	0	4	6	3	8	1	7	2	5
3	0	3	7	2	4	8	1	5	6

Навіть при $p = 3$ таких ізоморфізмів буде $(3^2 - 3)! = 6! = 720 \approx 3^6$.

Якщо в задачі, крім всього іншого, невідомий також і модуль поля, то задача ще більше ускладнюється. В цьому випадку необхідно знайти модуль поля і саме поле, що потребує додаткових часових і обчислювальних затрат.

Випадок 3. В цьому випадку розв'язки задачі про сейф шукаються в кільці лишків за модулем складеного числа *m* при заданій комбінації засувів, яка відкриває сейф.

Нехай задача про сейф розв'язується в кільці лишків за модулем 15 з матрицею

$$B = \begin{pmatrix} 14 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 11 \end{pmatrix}$$ і з такою комбінацією, яка відкриває сейф, $$c = \begin{pmatrix} 0 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 0 \end{pmatrix}.$$

Тоді СЛНДР $A\bar{x} + \bar{b} \equiv \bar{c}\ (mod\ 15)$ набуває вигляду:

$$\begin{cases} 1\ 1\ 1\ 1\ 0\ 0\ 1\ 0\ 0\ 14 = 0 \\ 1\ 1\ 1\ 0\ 1\ 0\ 0\ 1\ 0\ 2 = 2 \\ 1\ 1\ 1\ 0\ 0\ 1\ 0\ 0\ 1\ 3 = 3 \\ 1\ 0\ 0\ 1\ 1\ 1\ 1\ 0\ 0\ 4 = 4 \\ 0\ 1\ 0\ 1\ 1\ 1\ 0\ 1\ 0\ 5 = 5\ (mod\ 15). \\ 0\ 0\ 1\ 1\ 1\ 1\ 0\ 0\ 1\ 6 = 6 \\ 1\ 0\ 0\ 1\ 0\ 0\ 1\ 1\ 1\ 7 = 7 \\ 0\ 1\ 0\ 1\ 1\ 1\ 1\ 0\ 1\ 8 = 8 \\ 0\ 0\ 1\ 0\ 0\ 1\ 1\ 1\ 1\ 11 = 0 \end{cases}$$

Після перетворення цієї СЛНДР до СЛОДР, отримуємо

$$\begin{cases} 1\ 1\ 1\ 1\ 0\ 0\ 1\ 0\ 0\ 14 = 0 \\ 1\ 1\ 1\ 0\ 1\ 0\ 0\ 1\ 0\ 0 = 0 \\ 1\ 1\ 1\ 0\ 0\ 1\ 0\ 0\ 1\ 0 = 0 \\ 1\ 0\ 0\ 1\ 1\ 1\ 1\ 0\ 0\ 0 = 0 \\ 0\ 1\ 0\ 1\ 1\ 1\ 0\ 1\ 0\ 0 = 0\ (mod\ 15). \\ 0\ 0\ 1\ 1\ 1\ 1\ 0\ 0\ 1\ 0 = 0 \\ 1\ 0\ 0\ 1\ 0\ 0\ 1\ 1\ 1\ 0 = 0 \\ 0\ 1\ 0\ 1\ 1\ 1\ 1\ 0\ 1\ 0 = 0 \\ 0\ 0\ 1\ 0\ 0\ 1\ 1\ 1\ 1\ 11 = 0 \end{cases}$$

Розв'язком цієї системи є вектор $x = (5,13,0,13,5,7,0,7,5)$, який відкриває сейф. Дійсно,

$$\begin{pmatrix} 14 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 11 \end{pmatrix} \to (x_{11} = 5) \begin{pmatrix} 4 & 7 & 8 \\ 9 & 5 & 6 \\ 12 & 8 & 11 \end{pmatrix} \to (x_{12} = 13) \begin{pmatrix} 2 & 5 & 6 \\ 9 & 3 & 6 \\ 12 & 6 & 11 \end{pmatrix} \to$$

$$\to (x_{21}=13)\begin{pmatrix}0&5&6\\7&1&4\\10&6&11\end{pmatrix}\to (x_{22}=5)\begin{pmatrix}0&10&6\\12&6&9\\10&11&11\end{pmatrix}\to (x_{23}=7)\begin{pmatrix}0&10&13\\4&13&1\\10&11&3\end{pmatrix}\to$$

$$\to (x_{32}=7)\begin{pmatrix}0&2&13\\4&5&1\\2&3&10\end{pmatrix}\to (x_{33}=5)\begin{pmatrix}0&2&3\\4&5&6\\7&8&0\end{pmatrix}.$$

Випадок 4. Розв’язки задачі про сейф шукаються в кільці лишків за модулем складеного числа m при заданій комбінації засувів, яка відкриває сейф, і модифікованої матриці системи (2).

Нехай задача про сейф розв'язується в кільці за модулем 27 з матрицею

$$B=\begin{pmatrix}1&2&0\\0&0&0\\0&0&0\end{pmatrix}$$ і з такою комбінацією, яка відкриває сейф, $$c=\begin{pmatrix}1&2&3\\4&5&6\\7&8&9\end{pmatrix}.$$

Модифікована матриця A системи має вигляд:

$$\begin{vmatrix}1&1&1&3&0&0&2&0&0\\1&1&1&0&3&0&0&2&0\\1&1&1&0&0&3&0&0&2\\1&0&0&3&3&3&2&0&0\\0&1&0&3&3&3&0&2&0\\0&0&1&3&3&3&0&0&2\\1&0&0&3&0&0&2&2&2\\0&1&0&0&3&0&2&2&2\\0&0&1&0&0&3&2&2&2\end{vmatrix}.$$

Тоді СЛНДР $A\bar{x}+\bar{b}\equiv\bar{c}\ (mod\ 27)$ набуває вигляду:

$$A\bar{x}+\bar{b}=\bar{c}\begin{cases}1&1&1&3&0&0&2&0&0&1&=&1\\1&1&1&0&3&0&0&2&0&2&=&2\\1&1&1&0&0&3&0&0&2&0&=&3\\1&0&0&3&3&3&2&0&0&0&=&4\\0&1&0&3&3&3&0&2&0&0&=&5\\0&0&1&3&3&3&0&0&2&0&=&6\\1&0&0&3&0&0&2&2&2&0&=&7\\0&1&0&0&3&0&2&2&2&0&=&8\\0&0&1&0&0&3&2&2&2&0&=&9\end{cases}(mod\ 27).$$

Розв'язком цієї системи є вектор $x=(4,5,18,20,20,7,24,24,\ 24,18)$, який не відкриває сейф. Для того, щоб цей розв’язок відкривав сейф, необхідно його перетворити таким чином:

- перші три координати, які відповідають коефіцієнтам 1, залишаються незмінними;
- другі три координати, які відповідають коефіцієнтам 3, множаться на 3 за модулем 27;
- треті три координати, які відповідають коефіцієнтам 2, множаться на 2 за модулем 27.

В результаті дістаємо розв’язок $a=(4,5,18,6,6,21,21,21,9)$, який відкриває сейф. Дійсно,

$$\begin{pmatrix}1&2&0\\0&0&0\\0&0&0\end{pmatrix}\to(x_{11}=4)\begin{pmatrix}5&6&4\\4&0&0\\4&0&0\end{pmatrix}\to(x_{12}=5)\begin{pmatrix}10&11&9\\4&5&0\\4&5&0\end{pmatrix}\to(x_{13}=18)\begin{pmatrix}1&2&0\\4&5&18\\4&5&18\end{pmatrix}\to$$

$$\to(x_{21}=6)\begin{pmatrix}7&2&0\\10&11&24\\10&5&18\end{pmatrix}\to(x_{22}=6)\begin{pmatrix}7&8&0\\16&17&3\\10&11&18\end{pmatrix}\to(x_{23}=21)\begin{pmatrix}7&8&21\\10&11&24\\10&11&12\end{pmatrix}\to$$

$$\to(x_{31}=21)\begin{pmatrix}1&8&21\\4&11&24\\4&5&6\end{pmatrix}\to(x_{32}=21)\begin{pmatrix}1&2&21\\4&5&24\\25&26&0\end{pmatrix}\to(x_{33}=9)\begin{pmatrix}1&2&3\\4&5&6\\7&8&9\end{pmatrix}.$$

Нехай задача про сейф розв'язується, як і раніше, в кільці за модулем 27 з матрицею $B=\begin{pmatrix}6&6&0\\0&0&0\\0&0&0\end{pmatrix}$ і з такою комбінацією, яка відкриває сейф $c=\begin{pmatrix}0&0&6\\0&3&0\\0&3&0\end{pmatrix}$.

Крім того, матриця A системи має вигляд:

$$\begin{vmatrix}1&3&2&1&0&0&1&0&0\\1&3&2&0&3&0&0&3&0\\1&3&2&0&0&2&0&0&2\\1&0&0&1&3&2&1&0&0\\0&3&0&1&3&2&0&3&0\\0&0&2&1&3&2&0&0&2\\1&0&0&1&0&0&1&3&2\\0&3&0&0&3&0&1&3&2\\0&0&2&0&0&2&1&3&2\end{vmatrix}.$$

Тоді СЛНДР $A\bar{x}+\bar{b}\equiv\bar{c}\ (mod\ 27)$ набуває вигляду:

$$A\bar{x}+\bar{B}=\bar{c}\begin{cases}1&3&2&1&0&0&1&0&0&6&=&0\\1&3&2&0&3&0&0&3&0&6&=&0\\1&3&2&0&0&2&0&0&2&0&=&6\\1&0&0&1&3&2&1&0&0&0&=&0\\0&3&0&1&3&2&0&3&0&0&=&3\\0&0&2&1&3&2&0&0&2&0&=&0\\1&0&0&1&0&0&1&3&2&0&=&0\\0&3&0&0&3&0&1&3&2&0&=&3\\0&0&2&0&0&2&1&3&2&0&=&0\end{cases}(mod\ 27).$$

Розв'язком цієї системи є вектор $x = (0,19,24,12,13,9,12,13,9)$, який не відкриває сейф (в чому можно переконатися). Для того, щоб цей розв'язок відкривав сейф, необхідно його редукувати таким чином:

- перша, четверта і сьома координати, які відповідають коефіцієнту 1, залишаються незмінними;
- друга, п'ятая і восьма координати, які відповідають коефіцієнту 3, множаться на 3 за модулем 27;
- третя, шоста і дев'ята координати, які відповідають коефіцієнту 2, множаються на 2 за модулем 27.

В результаті дістаємо розв'язок $a = (0,3,21,12,12,18,12,12,18)$, який відкриває сейф. Дійсно,

$$\begin{pmatrix} 6 & 6 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \to (x_{12} = 3) \begin{pmatrix} 9 & 9 & 3 \\ 0 & 3 & 0 \\ 0 & 3 & 0 \end{pmatrix} \to (x_{13} = 21) \begin{pmatrix} 3 & 3 & 24 \\ 0 & 3 & 21 \\ 0 & 3 & 21 \end{pmatrix} \to (x_{21} = 12) \begin{pmatrix} 15 & 3 & 24 \\ 12 & 15 & 6 \\ 12 & 3 & 21 \end{pmatrix} \to$$

$$\to (x_{22} = 12) \begin{pmatrix} 15 & 15 & 24 \\ 24 & 0 & 18 \\ 12 & 15 & 21 \end{pmatrix} \to (x_{23} = 18) \begin{pmatrix} 15 & 15 & 15 \\ 15 & 18 & 9 \\ 12 & 15 & 12 \end{pmatrix} \to (x_{31} = 12) \begin{pmatrix} 0 & 15 & 15 \\ 0 & 18 & 9 \\ 24 & 0 & 24 \end{pmatrix} \to$$

$$\to (x_{32} = 12) \begin{pmatrix} 0 & 0 & 15 \\ 0 & 3 & 9 \\ 9 & 12 & 9 \end{pmatrix} \to (x_{33} = 18) \begin{pmatrix} 0 & 0 & 6 \\ 0 & 3 & 0 \\ 0 & 3 & 0 \end{pmatrix}.$$

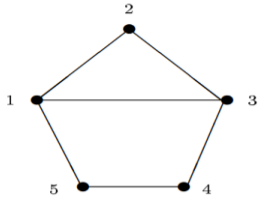
Система (2) буде несумісною, якщо хоча б по одному з модулів розкладу числа k вона несумісна, тобто не має розв'язків. Оцінки складності збільшуються, оскільки необхідно знайти матрицю A.

Якщо підсумувати сказане, то найбільш складною задачею про сейф при невідомому модулі і невідомій комбінації позицій засувів, яка відкриває сейф, є задача в полі F_{p^r} або в кільці Z_k.

3. Задання математичного сейфа за допомогою графа

Нагадаємо формулювання задачі про математичний сейф за допомогою графа. У вершинах графа $G = (V, E)$ знаходяться засуви, які можуть знаходитися в одній з позицій із множини $\{0,1,\ldots,k-1\}$. Якщо у вершині u засув знаходиться в позиції i, то поворот ключа в цій вершині переводить її засув в позицію $(i+1)\,(mod\ k)$ а також всі засуви вершин, які суміжні з вершиною u. Початкові позиції засувів у вершинах задаються вектором $\bar{b} = (b_1, b_2, \ldots, b_{|V|})$.

Розв'язання задачі виконується тими самими алгоритмами, що і при розв'язанні задачі на матрицях. Але при такому заданні структура матриці СЛНДР $A\bar{x} + \bar{b} \equiv \bar{c}\ (mod\ k)$ може бути, взагалі кажучи, довільною. Нехай дано граф, показаний на рисунку, і $\bar{b} = (1,2,1,1,3)$.



РИСУНОК

Будується СЛОДР $A\bar{x} + \bar{b} \equiv 0\,(mod\ k)$ для задачі про МС цього графа ($k = 5$):

$$A = \begin{cases} & 1 & 2 & 3 & 4 & 5 & \bar{b} \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 2 & 1 & 1 & 1 & 0 & 0 & 2 \\ 3 & 1 & 1 & 1 & 1 & 0 & 1 \\ 4 & 0 & 0 & 1 & 1 & 1 & 1 \\ 5 & 1 & 0 & 0 & 1 & 1 & 3 \end{cases} \equiv 0\,(mod\ 5).$$

Розв’язком даної СЛОДР є вектор $\bar{x} = (0,1,2,1,1)$

$$\begin{array}{c} 1\ 2\ 1\ 1\ 3, \\ \downarrow\ b_2 = 1 \\ 2\ 3\ 2\ 1\ 3, \\ \downarrow\ b_3 = 2 \\ 4\ 0\ 4\ 3\ 3, \\ \downarrow\ b_4 = 1 \\ 0\ 0\ 0\ 4\ 4, \\ \downarrow\ b_5 = 1 \\ 0\ 0\ 0\ 0\ 0. \end{array}$$

Таким чином сейф відкрито.

Висновки. Розглянуті варіації задачі про математичний сейф та способи її розв’язання. В залежності від області, над якою розглядається задача про математичний сейф, застосовуються різні варіації *TSS*-алгоритму для побудови базису множини всіх розв’язків системи $B\bar{x} + \bar{b} = \bar{c}$ та алгоритми побудови таблиць операцій відповідних областей. Області, над якими розв’язується задача про математичний сейф є скінченні поля, примарні кільця та загального вигляду асоціативно-комутативні кільця з одиницею. Алгоритми побудови таблиць операцій та алгоритми побудови базисних розв’язків мають поліноміальні оцінки складності (в кільцях за умови відомого розкладу на прості множники модуля).

Список літератури

1. Кривий С.Л., Гогерчак Г.І. Задача про математичний сейф та її розв’язання (Ч. 1). *Cybernetics and Computer Technologies*. 2020. 4. С. 24–35. https://doi.org/10.34229/2707-451X.20.4.2
2. Крывый С.Л. Численные методы решения задачи о математическом сейфе. *Кибернетика и системный анализ*. 2019. **55** (5). С.18–34.
3. Кострикин А.И. Введение в алгебру. М.: Наука, 1977. 495 с.

Одержано 06.12.2020

Кривий Сергій Лук’янович,
доктор фізико-математичних наук, професор, професор кафедри інтелектуальних програмних систем
Київського національного університету імені Тараса Шевченка, Київ,
https://orcid.org/0000-0003-4231-0691
sl.krivoi@gmail.com

Гогерчак Григорій Іванович,
аспірант факультету комп’ютерних наук та кібернетики
Київського національного університету імені Тараса Шевченка, Київ.
https://orcid.org/0000-0002-6898-2536
gogerchak.g@gmail.com

UDC 51.681.3

S. Kryvyi, H. Hoherchak

The Mathematical Safe Problem and Its Solution (P. 2)

Taras Shevchenko National University of Kyiv, Ukraine
Correspondence: sl.krivoi@gmail.com

Introduction. The problem of mathematical safe arises in the theory of computer games and cryptographic applications. The article considers numerous variations of the mathematical safe problem and examples of its solution using systems of linear Diophantine equations in finite rings and fields.

The purpose of the article. To present methods for solving the problem of a mathematical safe for its various variations, which are related both to the domain over which the problem is considered and to the structure of systems of linear equations over these domains. To consider the problem of a mathematical safe (in matrix and graph forms) in different variations over different finite domains and to demonstrate the work of methods for solving this problem and their efficiency (systems over finite simple fields, finite fields, ghost rings and finite associative-commutative rings).

Results. Examples of solving the problem of a mathematical safe, the conditions for the existence of solutions in different areas, over which this problem is considered. The choice of the appropriate area over which the problem of the mathematical safe is considered, and the appropriate algorithm for solving it depends on the number of positions of the latches of the safe. All these algorithms are accompanied by estimates of their time complexity, which were considered in the first part of this paper.

Conclusions. The considered methods and algorithms for solving linear equations and systems of linear equations in finite rings and fields allow to solve the problem of a mathematical safe in a large number of variations of its formulation (over finite prime field, finite field, primary associative-commutative ring and finite associative-commutative ring with unit).

Keywords: mathematical safe, finite rings, finite fields, method, algorithm.