КІБЕРНЕТИКА

УДК 004.822

С.Л. КРИВИЙ
Київський національний університет імені Тараса Шевченка, Київ, Україна,
e-mail: *sl.krivoi@gmail.com*.

АЛГОРИТМ РОЗВ'ЯЗАННЯ ЛІНІЙНИХ РІВНЯНЬ В АСОЦІАТИВНИХ КІЛЬЦЯХ З ОДИНИЦЕЮ

Анотація. Запропоновано алгоритми розв'язання лінійних рівнянь та систем таких рівнянь в асоціативних некомутативних кільцях з одиницею за умови, що всі коефіцієнти в рівняннях є дільниками одиниці. Наведено основні поняття теорії кілець та приклади роботи запропонованих алгоритмів. Складність роботи алгоритмів залежить від властивостей елементів кільця, над яким розглядаються рівняння та системи рівнянь.

Ключові слова: лінійне рівняння, некомутативне кільце, дільник одиниці, алгоритм.

ВСТУП

У практичних задачах часто виникає необхідність розв'язувати лінійні рівняння в різних дискретних областях, які можуть бути як скінченними, так і нескінченними. Однією з таких областей є кільця. Прикладом скінченного кільця є кільце лишків Z_n за модулем n, а прикладом нескінченного кільця — кільце Z цілих чисел. Ці кільця належать до групи асоціативно-комутативних кілець з одиницею. Алгоритми розв'язання лінійних рівнянь і систем лінійних рівнянь для цих кілець розглянуто в роботах [1, 2].

У цій статті розглядаються асоціативні некомутативні кільця з одиницею і метод розв'язання системи лінійних рівнянь над такими кільцями.

1. НЕОБХІДНІ ОЗНАЧЕННЯ

Кільцем називається алгебра $K = (A, \{+, \cdot\})$, яка відносно операції додавання $(+)$ складає Абелеву групу, відносно операції множення $(\cdot)$ є групоїдом, а операції додавання і множення зв'язані законами дистрибутивності: $\forall a, b, c \in K$

$$a(b+c) = ab + ac \text{ і } (b+c)a = ba + ca.$$

Групоїд називається мультиплікативним групоїдом кільця, а Абелева група — адитивною групою кільця.

Кільце K називається асоціативним кільцем з одиницею (АК1), якщо його групоїд є напівгрупою з одиницею (моноїдом). Нуль адитивної групи називається нулем кільця, а одиниця мультиплікативної напівгрупи — одиницею кільця. Для цих елементів виконуються тотожності

$$(\forall a \in K)\ 0 \cdot a = a \cdot 0 = 0,\ 1 \cdot a = a \cdot 1 = a\,.$$

Нехай K — асоціативне кільце з одиницею. Якщо в K для елементів $a, b \in K \setminus \{0\}$ виконується рівність $ab = 0$, то a називається лівим дільником нуля,

а b — правим дільником нуля. Елемент $a \in K$ називається лівим (правим) дільником одиниці (або лівим оберненим (правим оберненим)), якщо в кільці існує такий елемент b, що $ab = 1$ ($ba = 1$). Зазначимо, що множина дільників одиниці складає групу, яка називається мультиплікативною групою кільця [3, 4].

Наведемо деякі властивості дільників нуля і одиниці. Дільник одиниці не може бути дільником нуля. Дійсно, нехай $a, b, c \in K \setminus \{0\}$ і $ab = 0$, $ca = 1$, тоді з виразу $ab = 0$ випливає $cab = 1 \cdot b = b = 0$, що суперечить початковим умовам. Дільники одиниці комутують між собою. Дійсно, із виразу $ab = 1$ випливає $aba = a$ або $a(ba - 1) = 0$, звідси отримуємо $ba = 1$ з урахуванням того, що $a \neq 0$ і a — дільник одиниці. До того ж сума (різниця) дільників нуля може бути дільником одиниці і навпаки, сума (різниця) дільників одиниці може бути дільником нуля. Ці властивості операцій додавання і віднімання означають, що множина дільників нуля не є ідеалом у такому кільці.

2. ЛІНІЙНІ РІВНЯННЯ НАД АК

Оскільки кільце K не комутативне, то системи лінійних рівнянь (СЛР) можуть бути правими:

$$S_r = \begin{cases} a_{11}x_1 + \ldots + a_{1q}x_q = b_1, \\ a_{21}x_1 + \ldots + a_{2q}x_q = b_2, \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ a_{p1}x_1 + \ldots + a_{pq}x_q = b_p \end{cases}$$

і лівими:

$$S_l = \begin{cases} x_1a_{11} + \ldots + x_qa_{1q} = b_1, \\ x_1a_{21} + \ldots + x_qa_{2q} = b_2, \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ x_1a_{p1} + \ldots + x_qa_{pq} = b_p, \end{cases}$$

де $a_{ij},\ b_j \in K,\ i = 1, 2, \ldots, p,\ j = 1, 2, \ldots, q$.

2.1. Лінійне рівняння над АК1. Нехай лінійне рівняння (ЛР) має вигляд

$$L(x) = a_1x_1 + \ldots + a_qx_q = b, \tag{1}$$

де $a_i, b \in K, i = 1, 2, \ldots, q$.

Розглянемо випадок, коли всі a_i і b — дільники одиниці. За цих умов ЛР (1) можна легко розв'язати. Нехай $a_i \neq 0$ — дільник одиниці. Тоді існує елемент $c_i \in K$ такий, що $a_ic_i = 1$. Звідси отримуємо розв'язок ЛР (1):

$$\bar{x}_i = (0, \ldots, c_ib, 0, \ldots, 0).$$

Дійсно, вектор $\bar{x}_i = (0, \ldots, 0, c_ib, 0, \ldots, 0)$, де $a_ic_i = 1$, задовольняє ЛР (1):

$$L(\bar{x}_i) = a_ic_ib = 1 \cdot b = b.$$

Розглянемо однорідне ЛР, яке відповідає неоднорідному ЛР (1), тобто

$$\bar{L}(x) = a_1x_1 + \ldots + a_qx_q = 0. \tag{2}$$

Враховуючи умови, для цього рівняння легко побудувати розв'язки, а саме вектори вигляду

$$x_1^0 = (c_1, -c_2, \ldots, 0),\ x_2^0 = (c_1, 0, -c_3, \ldots, 0), \ldots,\ x_{q-1}^0 = (c_1, 0, \ldots, -c_q),$$

де c_i — праві обернені до a_i, тобто $a_ic_i = 1,\ i = 1, 2, \ldots, q$. Наприклад, для x_1^0 матимемо

$$L(x_1^0) = a_1c_1 - a_2c_2 = 1 - 1 = 0.$$

Зауважимо, що ліве ЛР

$$\overline{L}(x) = x_1 a_1 + x_2 a_2 + \ldots + x_q a_q = 0 \qquad (3)$$

буде мати ті ж розв'язки, що й праве. Дійсно, на підставі властивості комутативності дільників одиниці отримуємо

$$\overline{L}(x_i^0) = c_1 a_1 - c_i a_i = 1 - 1 = 0,$$

де $i = 1, 2, \ldots, q$, $x_i^0 = (c_1 \ldots, -c_i, 0, \ldots, 0)$.

Має місце твердження.

Лема 1. Множина векторів x_i^0, $i = 1, 2, \ldots, q$, є базисом множини розв'язків ЛР (2).

Доведення. Нехай $u = (u_1, u_2, \ldots, u_q)$ — довільний розв'язок ЛР (2), тобто

$$L(x) = a_1 u_1 + a_2 u_2 + \ldots + a_q u_q = 0.$$

Розглянемо вектор

$$u - x_1^0 a_2 u_2 - x_2^0 a_3 u_3 - \ldots - x_{q-1}^0 a_q u_q =$$

$$= (u_1 - c_1 (a_2 u_2 + a_3 u_3 + \ldots + a_q u_q), u_2 - c_2 a_2 u_2, \ldots, u_q - c_q u_q) =$$

$$= (u_1 - c_1 a_1 u_1, u_2 - u_2, \ldots, u_q - u_q) = (u_1 - u_1, u_2 - u_2, \ldots, -u_q - u_q) = (0, 0, \ldots, 0)$$

з урахуванням комутативності дільників одиниці і того, що вектор u — розв'язок ЛР (2). Звідси знаходимо

$$u = x_1^0 a_2 u_2 + x_2^0 a_3 u_3 + \ldots + x_{q-1}^0 a_q u_q,$$

тобто отримаємо зображення вектора u у вигляді лінійної комбінації векторів x_i^0, $i = 1, 2, \ldots, q-1$, що й потрібно було показати.

Доведемо лінійну незалежність векторів x_i^0, $i = 1, 2, \ldots, q-1$. Припустимо, що ці вектори лінійно залежні, тобто

$$x_1^0 d_1 + x_2^0 d_2 + \ldots + x_{q-1}^0 d_{q-1} = 0.$$

Тоді в координатній формі ця рівність набуває вигляду

$$(c_1 (d_1 + d_2 + \ldots + d_{q-1}), -c_2 d_1, -c_3 d_2, \ldots, -c_q d_{q-1}) = 0.$$

Оскільки всі c_i — дільники одиниці, то вони не можуть бути дільниками нуля, тоді з виразу $c_{i+1} d_i = 0$ випливає, що $d_i = 0$ для всіх $i = 1, 2, \ldots, q-1$.

Покажемо тепер єдиність зображення розв'язку u, використовуючи вектори x_i^0, $i = 1, 2, \ldots, q-1$. Припустимо, що існує два зображення вектора u у вигляді лінійних комбінацій:

$$u = x_1^0 d_1 + x_2^0 d_2 + \ldots + x_{q-1}^0 d_{q-1}$$

і

$$u = x_1^0 f_1 + x_2^0 f_2 + \ldots + x_{q-1}^0 f_{q-1}.$$

Звідси отримуємо

$$u - u = x_1^0 (d_1 - f_1) + x_2^0 (d_2 - f_2) + \ldots + x_{q-1}^0 (d_{q-1} - f_{q-1}) = 0.$$

Але вектори x_i^0 лінійно незалежні, тому ця рівність виконується лише тоді, коли всі коефіцієнти дорівнюють нулю, а звідси матимемо $d_i = f_i$ для всіх $i = 1, 2, \ldots, q-1$.

Розглянемо приклад, коли сума (різниця) декількох коефіцієнтів ЛР (2) є дільником нуля. Не обмежуючи загальності, нехай $a_1 + a_3 + a_5 = c$, де c — дільник нуля. Тоді існує такий елемент $d \in K$, що $cd = 0$, і тоді вектор $x = (d, 0, d, 0, d, 0, \dots, 0)$ є розв'язком ЛР (2). Дійсно, $a_1 d + a_3 d + a_5 d = (a_1 + a_3 + a_5)d = cd = 0$. Покажемо, що цей розв'язок також є лінійною комбінацією базисних векторів x_i^0, $i = 1, \dots, q-1$. Побудуємо вектори $s_1 = x_1^0 - x_2^0 = (0, -c_2, c_3, 0, 0, 0, 0, \dots, 0)$, $s_2 = x_1^0 - x_4^0 = (0, -c_2, 0, 0, c_5, 0, \dots, 0)$, тоді наведена далі лінійна комбінація буде шуканим зображенням вектора x:

$$x_1^0 a_1 d - s_1 a_3 d - s_2 a_5 d = (d, -c_2 a_1 d - c_2 a_3 d - c_2 a_5 d, d, 0, d, 0, \dots, 0) =$$

$$= (d, 0, d, 0, d, 0, \dots, 0) = x,$$

оскільки $-c_2 a_1 d - c_2 a_3 d - c_2 a_5 d = -c_2 (a_1 + a_3 + a_5)d = -c_2 cd = -c_2 0 = 0$. ■

Наслідок 1. 1. Загальний розв'язок ЛР (1) має вигляд $x = x_1 + \sum_i x_i^0 d_i$, де x_1 — частинний розв'язок ЛР (1), x_i^0 — базисний розв'язок ЛР (2), $d_i \in K$ — довільні.

2. Якщо вектор v — розв'язок ЛР (3), то він має зображення

$$v = u_2 a_2 x_1^0 + u_3 a_3 x_2^0 + \dots + u_q a_q x_{q-1}^0.$$

Доведення. 1. Дійсно, якщо v_1, v_2 — розв'язок ЛР (1), то $v_1 - v_2$ — розв'язок ЛР (2) і з урахуванням леми 1 маємо $v_1 - v_2 = \sum_i x_i^0 d_i$ або $v_1 = v_2 + \sum_i x_i^0 d_i$.

2. Перевіряється безпосередньо. ■

Приклад 1. Знайти над кільцем K раціональних матриць (матриці з раціональними коефіцієнтами) розміру 2×2 загальний розв'язок ЛР

$$L(x) = A_1 x_1 + A_2 x_2 + A_3 x_3 + A_4 x_4 = B,$$

де коефіцієнти рівняння і вільний член мають вигляд

$$A_1 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},\ A_2 = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix},\ A_3 = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix},\ A_4 = \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix},\ B = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}.$$

Розв'язання. У такому кільці дільниками одиниці є невироджені матриці, а дільниками нуля — вироджені матриці. Згідно з результатами обчислення детермінантів коефіцієнтів цього ЛР знаходимо $D(A_1) = -2$, $D(A_2) = 2$, $D(A_3) = 1$, $D(A_4) = -1$. Будуємо обернені матриці для дільників одиниці:

$$A_1^{-1} = \begin{pmatrix} 1/2 & 1/2 \\ 1/2 & -1/2 \end{pmatrix},\ A_2^{-1} = \begin{pmatrix} 1/2 & 1/2 \\ -1/2 & 1/2 \end{pmatrix},\ A_3^{-1} = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix},\ A_4^{-1} = \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}.$$

Вибираємо, наприклад, дільник одиниці A_1 і отримуємо частинний розв'язок ЛР:

$$x_1 = A_1^{-1} B = \begin{pmatrix} 1/2 & 1/2 \\ 1/2 & -1/2 \end{pmatrix} \cdot \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Будуємо базисні розв'язки однорідного ЛР, яке відповідає розглядуваному неоднорідному ЛР:

$$x_1^0 = (A_1^{-1}, -A_2^{-1}, 0, 0),\ x_2^0 = (A_1^{-1}, 0, -A_3^{-1}, 0),\ x_3^0 = (A_1^{-1}, 0, 0, -A_4^{-1}).$$

Отже, загальний розв'язок початкового ЛР набуває вигляду

$$x = x_1 + x_1^0 d_1 + x_2^0 d_2 + x_3^0 d_3,$$

де $d_1, d_2, d_3 \in K$ — довільні 2×2-матриці.

Нехай, наприклад, d_1 і d_2 — одиничні матриці, тоді

$$x = \left[\left(\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, 0, 0, 0\right) + \left(\begin{pmatrix} 1/2 & 1/2 \\ 1/2 & -1/2 \end{pmatrix}, \begin{pmatrix} -1/2 & -1/2 \\ 1/2 & -1/2 \end{pmatrix}, 0, 0\right) + \right.$$

$$\left. + \left(\begin{pmatrix} 1/2 & 1/2 \\ 1/2 & -1/2 \end{pmatrix}, 0, \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}, 0\right)\right] =$$

$$= \left[\begin{pmatrix} 2 & 1 \\ 1 & -2 \end{pmatrix}, \begin{pmatrix} -1/2 & -1/2 \\ 1/2 & -1/2 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}, 0\right],$$

$$L(x) = \begin{pmatrix} 3 & -1 \\ 1 & 3 \end{pmatrix} + \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} + \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} = B.$$

Зауважимо, що $A_1 + A_2 = C$, де $C = \begin{pmatrix} 2 & 0 \\ 2 & 0 \end{pmatrix}$, тобто сума двох дільників одиниці є дільником нуля. Тоді розв'язком однорідного ЛР є вектор $x = (d, d, 0, 0)$, де d — така матриця, що $Cd = 0$. Зображення вектора x у базисі розв'язків цього ЛР матиме вигляд

$$x = x_1^0 A_1 d = (d, -A_2^{-1} A_1 d, 0, 0) = (d, d, 0, 0),$$

оскільки $-A_2^{-1} A_1 = d$. Дійсно, із рівності $A_1 + A_2 = C$ матимемо $A_1 d + A_2 d = 0$, звідси випливає, що $-A_2^{-1} A_1 d = d$. Кінець прикладу.

Зазначимо, що коли в ЛР всі коефіцієнти a_i — дільники одиниці, а b — дільник нуля, то справджується лема 1 і наслідок з неї, хоча частинний розв'язок тепер буде дільником нуля. Дійсно, довільний розв'язок вигляду

$$\bar{x}_i = (0, \ldots, 0, c_i b, 0, \ldots, 0)$$

має координату $c_i b$, яка є дільником нуля. Отже, загальний розв'язок ЛР (1) набуває вигляду $x = x_1 + \sum\limits_i x_i^0 d_i$, де x_1 — частинний розв'язок ЛР (1), x_i^0 — базисний розв'язок ЛР (2), $d_i \in K$ — довільні.

Розглянемо ЛР, де всі коефіцієнти і вільний член є дільниками одиниці, а один із коефіцієнтів a_i — дільник нуля. У цьому разі до базисних розв'язків однорідного ЛР, яке відповідає неоднорідному ЛР, додається розв'язок

$$x = (0, \ldots, 0, d_i, 0, \ldots, 0),$$

де $a_i d_i = 0$.

Приклад 2. Знайти над кільцем K раціональних матриць розміру 2×2 загальний розв'язок ЛР

$$L(x) = A_1 x_1 + A_2 x_2 + A_3 x_3 + A_4 x_4 = B,$$

де коефіцієнти рівняння і вільний член мають вигляд

$$A_1 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},\ A_2 = \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix},\ A_3 = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix},\ A_4 = \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix},\ B = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}.$$

Розв'язання. Обчислюємо детермінанти коефіцієнтів розглядуваного ЛР: $D(A_1) = -2$, $D(A_2) = 0$, $D(A_3) = 1$, $D(A_4) = -1$. Обернені матриці для дільників одиниці побудовано в прикладі 1.

Вибираємо, наприклад, дільник одиниці A_1 і отримуємо частинний розв'язок ЛР

$$x_1 = A_1^{-1}B = \begin{pmatrix} 1/2 & 1/2 \\ 1/2 & -1/2 \end{pmatrix} \cdot \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Будуємо базисні розв'язки однорідного ЛР, яке відповідає розглядуваному неоднорідному ЛР:

$$x_1^0 = (A_1^{-1}, 0, -A_3^{-1}, 0),\ x_2^0 = (A_1^{-1}, 0, 0, -A_4^{-1}),\ x_3^0 = (0, A_2^0, 0, 0),$$

де $A_2^0 = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$ — матриця, отримана з рівняння $A_2 \cdot A_2^0 = 0$ (зауважимо, що матриця A_2^0 не єдина, в цьому випадку таких матриць може бути нескінченно багато, наприклад $A_2^0 = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 2 & 0 \end{pmatrix}, \begin{pmatrix} 3 & 0 \\ 3 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}$ і т.д.). Тоді загальний розв'язок ЛР матиме вигляд

$$x = x_1 + x_1^0 d_1 + x_2^0 d_2 + x_3^0 d_3,$$

де $d_1,\ d_2,\ d_3 \in K$ — довільні 2×2-матриці.

Нехай, наприклад, d_1 і d_2 — одиничні матриці, тоді

$$x = \left(\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, 0, 0, 0 \right) + \left(\begin{pmatrix} 1/2 & 1/2 \\ 1/2 & -1/2 \end{pmatrix}, 0, \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}, 0 \right) +$$

$$+ \left(\begin{pmatrix} 1/2 & 1/2 \\ 1/2 & -1/2 \end{pmatrix}, 0, 0, \begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix} \right) + \left(0, \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, 0, 0 \right) =$$

$$= \left(\begin{pmatrix} 2 & 1 \\ 1 & -2 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}, \begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix} \right),$$

$$L(x) = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 2 & 1 \\ 1 & -2 \end{pmatrix} + \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} + \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix} +$$

$$+ \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix} \cdot \begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 3 & -1 \\ 1 & 3 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} + \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} = B.$$

Кінець прикладу.

2.2. Системи лінійних рівнянь над АК1. Із наведеного вище випливає, що коли всі коефіцієнти ЛР є дільниками одиниці, то загальний розв'язок такого ЛР можна знайти, використовуючи наведений вище спосіб. Розглянемо праву СЛР

$$S_r = \begin{cases} a_{11}x_1 + \ldots + a_{1q}x_q = b_1, \\ a_{21}x_1 + \ldots + a_{2q}x_q = b_2, \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ a_{p1}x_1 + \ldots + a_{pq}x_q = b_p, \end{cases}$$

де $a_{ij}, b_j \in K,\ i = 1, 2, \ldots, p,\ j = 1, 2, \ldots, q.$

Системи лінійних однорідних рівнянь (СЛОР). Розглянемо спочатку СЛОР вигляду

$$S_2 = \begin{cases} a_{11}x_1 + \ldots + a_{1q}x_q = 0, \\ a_{21}x_1 + \ldots + a_{2q}x_q = 0, \end{cases}$$

де всі коефіцієнти в рівняннях є дільниками одиниці, $a_{ij}, b_j \in K,\ i = 1, 2,$ $j = 1, 2, \ldots, q$.

Побудуємо для першого рівняння цієї СЛОР базис множини розв'язків $B_1 = \{e_1, e_2, \ldots, e_{q-1}\}$ та обчислимо значення $d_i = L_2(e_i),\ i = 1, 2, \ldots, q-1$. Припус-

тимо, що всі d_i — дільники одиниці і розглянемо рівняння

$$d_1 y_1 + d_2 y_2 + \ldots + d_{q-1} y_{q-1} = 0. \qquad (4)$$

Знайдемо його базисні розв'язки $g_1, g_2, \ldots, g_{q-2}$. Нехай $g_i = (c_{i1}, c_{i2}, \ldots, c_{iq-1})$, побудуємо лінійну комбінацію вигляду $u_i = e_1 c_{i1} + e_2 c_{i2} + \ldots + e_{q-1} c_{iq-1}$.

Лема 2. Множина векторів $\{u_i\}$, $i = 1, 2, \ldots, q-2$, є базисом множини розв'язків СЛОР S_2.

Доведення. Нехай $v = (v_1, v_2, \ldots, v_q)$ — довільний розв'язок СЛОР S_2. Згідно з лемою 1 матимемо

$$v = e_1 b_1 + e_2 b_2 + \ldots + e_{q-1} b_{q-1}, \text{ де } e_i \in B_1.$$

Тоді

$$L_2(v) = L_2(e_1) b_1 + L_2(e_2) b_2 + \ldots + L_2(e_{q-1}) b_{q-1} =$$

$$= d_1 b_1 + d_2 b_2 + \ldots + d_{q-1} b_{q-1} = 0,$$

а це означає, що вектор $b = (b_1, b_2, \ldots, b_{q-1})$ є розв'язком ЛР (4), тобто $b = g_1 a_1 + g_2 a_2 + \ldots + g_{q-2} a_{q-2}$ або

$$v = e_1 b_1 + e_2 b_2 + \ldots + e_{q-1} b_{q-1} = u_1 a_1 + u_2 a_2 + \ldots + u_{q-2} a_{q-2}. \blacksquare$$

Отже, якщо всі коефіцієнти СЛОР — дільники одиниці і всі коефіцієнти проміжного ЛР (4) — теж дільники одиниці, то базис множини її розв'язків можна знайти наведеним методом за умови алгоритмічної розв'язуваності задачі обчислення обернених елементів у кільці K.

Повернемося тепер до загального випадку СЛОР, всі коефіцієнти якої є дільниками одиниці і всі проміжні ЛР вигляду (4) мають коефіцієнти — дільники одиниці. Тоді для такої СЛОР справедливе твердження.

Теорема 1. Якщо проблема побудови обернених елементів у кільці K розв'язувана, всі коефіцієнти СЛОР і коефіцієнти проміжних ЛР вигляду (4) — це дільники одиниці, то множину базисних розв'язків СЛОР S_o можна визначити наведеним вище способом.

Доведення здійснюється індукцією за кількістю рівнянь в СЛОР:

$$S_o = \begin{cases} L_1(x) = a_{11} x_1 + \ldots + a_{1q} x_q = 0, \\ L_2(x) = a_{21} x_1 + \ldots + a_{2q} x_q = 0, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ L_p(x) = a_{p1} x_1 + \ldots + a_{pq} x_q = 0, \end{cases}$$

де $a_{ij} \in K$, $i = 1, 2, \ldots, p$, $j = 1, 2, \ldots, q$.

Базис індукції має місце на підставі лем 1 і 2.

Крок індукції. Нехай твердження теореми справедливе для СЛОР з $p-1$ рівнянням. Покажемо, що воно справджується і для СЛОР з p рівняннями.

Нехай $u_1, u_2, \ldots, u_k$ — базис множини розв'язків підсистеми, що складається з перших $p-1$ рівнянь, v — довільний розв'язок СЛОР S_o; тоді $u = u_1 d_1 + u_2 d_2 + \ldots + u_k d_k$, $L_p(u_1) = b_1$, $L_p(u_2) = b_2, \ldots$, $L_p(u_k) = b_k$. Повторюємо викладки з доведення леми 2 і отримаємо справедливість твердження теореми. $\blacksquare$

Приклад 3. Розглянемо СЛОР

$$S_2 = \begin{cases} L_1(x) = A_{11} x_1 + A_{12} x_2 + A_{13} x_3 + A_{14} x_4 = 0, \\ L_2(x) = A_{21} x_1 + A_{22} x_2 + A_{23} x_3 + A_{24} x_4 = 0, \end{cases}$$

де K — кільце квадратних матриць A_{ij} розміру 2×2 над полем раціональних

чисел Q, $i=1,2$, $j=1,2,3,4$. Матриці-коефіцієнти в СЛОР мають вигляд

$$A_{11}=\begin{pmatrix}1 & 2\\ -1 & 1\end{pmatrix},\ A_{12}=\begin{pmatrix}0 & 1\\ 1 & -1\end{pmatrix},\ A_{13}=\begin{pmatrix}-2 & -1\\ 1 & 1\end{pmatrix},\ A_{14}=\begin{pmatrix}2 & 1\\ -1 & 0\end{pmatrix}$$

(детермінанти цих матриць дорівнюють відповідно $2,-1,-1,1$, тобто всі матриці невироджені і тому є дільниками одиниці в кільці таких матриць);

$$A_{21}=\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix},\ A_{22}=\begin{pmatrix}1 & -1\\ -1 & 1\end{pmatrix},\ A_{23}=\begin{pmatrix}-1 & 1\\ -1 & 0\end{pmatrix},\ A_{24}=\begin{pmatrix}1 & 1\\ 0 & -1\end{pmatrix}$$

(детермінанти цих матриць дорівнюють відповідно $-2,0,1,-1$, тобто друга матриця є дільником нуля, а перша, третя і четверта — дільники одиниці).

Обернені матриці матимуть вигляд:

$$A_{11}^{-1}=\begin{pmatrix}0 & -1\\ 1/2 & 1/2\end{pmatrix},\ A_{12}^{-1}=\begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix},\ A_{13}^{-1}=\begin{pmatrix}-1 & -1\\ 1 & 2\end{pmatrix},\ A_{14}^{-1}=\begin{pmatrix}0 & -1\\ 1 & 2\end{pmatrix},$$

$$A_{21}^{-1}=\begin{pmatrix}1/2 & 1/2\\ 1/2 & -1/2\end{pmatrix},\ A_{23}^{-1}=\begin{pmatrix}0 & -1\\ 1 & -1\end{pmatrix},\ A_{24}^{-1}=\begin{pmatrix}1 & 1\\ 0 & -1\end{pmatrix}.$$

Тоді базисними розв'язками першого рівняння є вектори

$$e_1=(A_{11}^{-1},-A_{12}^{-1},0,0),\ e_2=(A_{11}^{-1},0,-A_{13}^{-1},0),\ e_3=(A_{11}^{-1},0,0,-A_{14}^{-1}).$$

Обчислимо значення $L_2(x_i^0)$:

$$L_2(e_1)=A_{21}\cdot A_{11}^{-1}-A_{22}\cdot A_{12}^{-1}=$$

$$=\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\cdot\begin{pmatrix}0 & -1\\ 1/2 & 1/2\end{pmatrix}-\begin{pmatrix}1 & -1\\ -1 & 1\end{pmatrix}\cdot\begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix}=\begin{pmatrix}1/2 & -3/2\\ -1/2 & -1/2\end{pmatrix}=B_1,$$

$$L_2(e_2)=A_{21}\cdot A_{11}^{-1}-A_{23}\cdot A_{13}^{-1}=\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\cdot\begin{pmatrix}0 & -1\\ 1/2 & 1/2\end{pmatrix}-$$

$$-\begin{pmatrix}-1 & 1\\ -1 & 0\end{pmatrix}\cdot\begin{pmatrix}-1 & -1\\ 1 & 2\end{pmatrix}=\begin{pmatrix}-3/2 & -7/2\\ -3/2 & -5/2\end{pmatrix}=B_2,$$

$$L_2(e_3)=A_{21}\cdot A_{11}^{-1}-A_{24}\cdot A_{14}^{-1}=\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\cdot\begin{pmatrix}0 & -1\\ 1/2 & 1/2\end{pmatrix}-$$

$$-\begin{pmatrix}1 & 1\\ 0 & -1\end{pmatrix}\cdot\begin{pmatrix}0 & -1\\ 1 & 2\end{pmatrix}=\begin{pmatrix}-1/2 & -3/2\\ 1/2 & 1/2\end{pmatrix}=B_3.$$

Оскільки детермінанти всіх матриць B_1, B_2, B_3 відмінні від нуля (і дорівнюють відповідно $-1,-2/3,1/2$), отримуємо такі обернені матриці:

$$B_1^{-1}=\begin{pmatrix}1/2 & -3/2\\ -1/2 & -1/2\end{pmatrix},\ B_2^{-1}=\begin{pmatrix}5/3 & -7/3\\ -1 & 1\end{pmatrix},\ B_3^{-1}=\begin{pmatrix}1 & 3\\ -1 & -1\end{pmatrix}.$$

Розв'язуємо рівняння $B_1y_1+B_2y_2+B_3y_3=0$ і знаходимо такі розв'язки:

$$y_1^0=(B_1^{-1},-B_2^{-1},0),\ y_2^0=(B_1^{-1},0,-B_3^{-1}).$$

Будуємо базис множини розв'язків СЛОР S_o:

$$u_1=e_1y_1^0+e_2y_2^0=(A_{11}^{-1}B_1^{-1}-A_{11}^{-1}B_2^{-1},-A_{12}^{-1}B_1^{-1},A_{13}^{-1}B_2^{-1},0),$$

$$u_2=e_1y_1^0+e_3y_2^0=(A_{11}^{-1}B_1^{-1}-A_{11}^{-1}B_3^{-1},-A_{12}^{-1}B_1^{-1},0,A_{14}^{-1}B_3^{-1}).$$

Перевіримо отримані розв'язки. Для першого рівняння системи після підстановки отримуємо

$$L_1(u_1) = A_{11}A_{11}^{-1}(B_1^{-1} - B_2^{-1}) - A_{12}A_{12}^{-1}B_1^{-1} + A_{13}A_{13}^{-1}B_2^{-1} + 0 =$$
$$= B_1^{-1} - B_2^{-1} - B_1^{-1} + B_2^{-1} = 0;$$
$$L_1(u_2) = A_{11}A_{11}^{-1}(B_1^{-1} - B_3^{-1}) - A_{12}A_{12}^{-1}B_1^{-1} + 0 + A_{14}A_{14}^{-1}B_3^{-1} =$$
$$= B_1^{-1} - B_3^{-1} - B_1^{-1} + B_3^{-1} = 0.$$

Виконаємо перевірку для другого рівняння системи. Для цього обчислимо матриці

$$A_{11}^{-1}(B_1^{-1} - B_2^{-1}) = \begin{pmatrix} 0 & -1 \\ 1/2 & 1/2 \end{pmatrix} \cdot \begin{pmatrix} -7/6 & 5/6 \\ 1/2 & -3/2 \end{pmatrix} = \begin{pmatrix} -1/2 & 3/2 \\ -1/3 & -1/3 \end{pmatrix},$$

$$-A_{12}^{-1}B_1^{-1} = -\begin{pmatrix} 1 & 1 \\ 1 & -0 \end{pmatrix} \cdot \begin{pmatrix} 1/2 & -3/2 \\ -1/2 & -1/2 \end{pmatrix} = \begin{pmatrix} 0 & 2 \\ 1/2 & -3/2 \end{pmatrix},$$

$$A_{13}^{-1}B_2^{-1} = \begin{pmatrix} -1 & -1 \\ 1 & 2 \end{pmatrix} \cdot \begin{pmatrix} 5/3 & -7/3 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} -2/3 & 4/3 \\ -1/3 & -1/3 \end{pmatrix}.$$

Потім знаходимо

$$A_{21}A_{11}^{-1}(B_1^{-1} - B_2^{-1}) = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 1/2 & 3/2 \\ -1/3 & -1/3 \end{pmatrix} = \begin{pmatrix} -5/6 & 7/6 \\ -1/6 & 11/6 \end{pmatrix},$$

$$A_{22}(-A_{12}^{-1}B_1^{-1}) = \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 2 \\ -1/2 & 3/2 \end{pmatrix} = \begin{pmatrix} 1/2 & 1/2 \\ -1/2 & -1/2 \end{pmatrix},$$

$$A_{23}A_{13}^{-1}B_2^{-1} = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix} \cdot \begin{pmatrix} -2/3 & 4/3 \\ -1/3 & -1/3 \end{pmatrix} = \begin{pmatrix} 1/3 & -5/3 \\ 2/3 & -4/3 \end{pmatrix}.$$

Тепер перевіряємо

$$L_2(u_1) = \begin{pmatrix} -5/6 & 7/6 \\ -1/6 & 11/6 \end{pmatrix} + \begin{pmatrix} 1/2 & 1/2 \\ -1/2 & -1/2 \end{pmatrix} + \begin{pmatrix} 2/6 & -10/6 \\ 4/6 & -8/6 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Аналогічно перевіряють другий розв'язок. Кінець прикладу.

Системи лінійних неоднорідних рівнянь (СЛНР). Нехай задано неоднорідну СЛР

$$S_r = \begin{cases} a_{11}x_1 + \ldots + a_{1q}x_q = b_1, \\ a_{21}x_1 + \ldots + a_{2q}x_q = b_2, \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ a_{p1}x_1 + \ldots + a_{pq}x_q = b_p. \end{cases}$$

Перетворимо її до вигляду однорідної СЛР, використовуючи додатковий невідомий x_0 при вільних членах:

$$S_r^1 = \begin{cases} a_{11}x_1 + \ldots + a_{1q}x_q - b_1x_0 = 0, \\ a_{21}x_1 + \ldots + a_{2q}x_q - b_2x_0 = 0, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{p1}x_1 + \ldots + a_{pq}x_q - b_px_0 = 0. \end{cases}$$

Побудуємо базис множини розв'язків цієї СЛОР, вважаючи, що коефіцієнти задовольняють умови теореми 1:

$$B = \{e_1, e_2, \ldots, e_k\}.$$

У цьому базисі потрібно знайти такий розв'язок СЛНР, у якого остання координата (що відповідає невідомому x_0) дорівнює одиниці. Для цього знайдемо у множині B розв'язок, остання координата якого є дільником одиниці. Помножимо отриманий розв'язок на елемент, обернений до цієї останньої координати, яку вилучаємо (оскільки вона після множення на обернений елемент дорівнює 1) і одержимо частинний розв'язок початкової СЛНР. Вилучаючи також з множини B останню нульову координату в базисних елементах, матимемо базисні розв'язки СЛОР, яка відповідає початковій СЛНР. Якщо такого розв'язку в множині B немає, то початкова СЛНР несумісна.

Часова складність запропонованого методу розв'язання залежить від складності знаходження обернених елементів в кільці і складності реалізації операцій множення і додавання у ньому. Наприклад, якщо розглядають кільце квадратних матриць над полем раціональних чисел, то в цьому кільці складності побудови обернених елементів, як і виконання операцій кільця, мають поліноміальні оцінки [5].

Отже, запропонований метод у повному обсязі застосовний для кілець з діленням, які називаються тілами. У цих кільцях мультиплікативна напівгрупа є групою і тому всі елементи мають обернені. А це означає, що для таких кілець умови теорем 1 і 2 автоматично виконуються.

ВИСНОВКИ

Запропоновано метод розв'язання систем лінійних рівнянь над асоціативним некомутативним кільцем з одиницею. Показано, яким чином будують базис множини розв'язків таких систем над кільцями, які не є комутативними. Часова складність методу залежить від складності реалізації операцій кільця і складності операції знаходження обернених елементів у такому кільці. Метод можна застосовувати у повному обсязі для кілець з діленням.

СПИСОК ЛІТЕРАТУРИ

1. Крывый С.Л. Алгоритмы решения систем линейных диофантовых уравнений в кольце вычетов. *Кибернетика и системный анализ.* 2007. № 6. С. 27–40.
2. Крывый С.Л. Алгоритмы построения базиса множества решений систем линейных диофантовых уравнений в кольце целых чисел. *Кибернетика и системный анализ*. 2009. № 6. С. 36–41.
3. Кострикин А.И. Введение в алгебру (Часть 2). Москва: Физматлит, 2004. 272 с.
4. Скобелев В.В. Автоматы на алгебраических структурах. Модели и методы исследования. Донецк: ИПМ НАНУ, 2013. 307 с.
5. Bockmayr A., Weispfenning V. Solving numerical constraints. *Handbook of Automated Reasoning*. 2001. Ch. 12. P. 753–842.

S. Kryvyi

ALGORITHMS FOR SOLVIG LINEAR EQUATIONS OVER ASSOCIATIVE RINGS WITH UNITY ELEMENT

Abstract. The author proposes algorithms for solving linear equations and systems of such equations in associative non-commutative rings with unity under the condition that all the coefficients in the equations are divisors of unity. The basic concepts of ring theory and examples of operation of the proposed algorithms are provided. The complexity of the algorithms depends on the properties of elements of the ring over which the equations and systems of equations are considered.

Keywords: linear equation, non-commutative ring, divisor of unit, algorithm.

Надійшла до редакції 14.05.2021