

КАНОНІЧНІ ТА МАТРИЧНІ ЗАДАННЯ КВАЗІГРУП ЧЕТВЕРТОГО ПОРЯДКУ

Квазігрупа називається луною, якщо вона має нейтральний елемент. При позначенні його через 0, її називаємо 0-луною. 0-лун четвертого порядку є 4, одна з них група Кляйна, інші три ізоморфні циклічній групі. Отримані результати: 1) кожна квазігрупа четвертого порядку має єдиний канонічний розклад точно над однією із цих чотирьох 0-лун; 2) кожна квазігрупа 4-го порядку має єдиний матричний канонічний розклад або над циклічною групою, або над групою Кляйна; 3) наведені формули та приклади їх використання.

Ключові слова: квазігрупа, луна, канонічний розклад, матриця, ізоморфізм, група Кляйна, циклічна група.

Вступ. Під час застосування квазігруп та їхніх парастрофних перетворень у криптографії, для генерації псевдовипадкових чисел, побудови нелінійних S-блоків для блокових шифрів, динамічного змішування бітів у поточкових шифрах, для побудови цифрових підписів тощо необхідно задавати квазігрупи у зручному вигляді. Добре відоме задання квазігрупи через задану операцію у вигляді таблиці Келі, результат внутрішньої частини якої є латинським квадратом [13]. Аналітичне задання квазігруп через перестановки або набір тотожностей чи рівнянь формує їх поліноміальне задання [9] у вигляді канонічного розкладу. Канонічне подання квазігруп у вигляді булевих функцій [10, 12], заданих векторами чи матрицями, найкраще підходить для криптографії.

Ця проблема стала предметом дослідження низки статей [3, 4, 9–12, 15]. Але навіть на чотириелементному носії вона залишалась нерозв'язаною для задання всіх квазігруп четвертого порядку, а запропоновані підходи лише частково давали відповідь на поставлені задачі [1, 3, 4, 7, 11].

Головною ідеєю цієї статті є використання того факту, що четвертого порядку існує лише дві неізоморфні луни – четвертна група Кляйна $Z_2^2 := Z_2 \times Z_2$ та циклічна група Z_4 . Отже, кожна квазігрупа четвертого порядку ізотопна точно одній з цих груп. А це дає можливість застосувати теорію ізоотопів груп, розроблену в працях [5, 6] для групових ізоотопів довільного носія та уточнену в публікаціях [1, 6, 4, 8, 16].

Основна мета цього дослідження – оформити просте задання квазігруп четвертого порядку у вигляді канонічного розкладу, тобто такого, який завжди існує та єдиний. Аналітичне задання квазігрупових операцій для програмної реалізації криптографічних систем та протоколів забезпечує мінімальні обсяг оперативної пам'яті та апаратні витрати на реалізацію спеціалізованих обчислювачів.

1. Допоміжні поняття та результати. Нехай $(\circ)$ – бінарна операція, яка визначена на множині Q . Пару $(Q; \circ)$ називають *квазігрупою*, якщо для всіх a і b із Q кожне з рівнянь

$$x \circ a = b, \quad a \circ y = b$$

має єдиний розв'язок. У цьому випадку множину Q називають *носієм*, а операцію $(\circ)$ – *оборотною* або *квазігруповою*. Множину всіх оборотних операцій носія Q позначатимемо через $\Delta(Q)$ або Δ , якщо відомий носій.

✉ fmsokha@ukr.net

Квазігрупу називають *лупою* або *0-лупою*, якщо вона має *нейтральний елемент*, тобто такий елемент 0 , що $0 \circ x = x \circ 0 = x$ для всіх $x \in Q$. Множину всіх 0-луп позначатимемо через $\Lambda_0(Q)$ або Λ_0 . Перетворення α носія Q називають *унітарним* у лупі $(Q; \circ, 0)$, якщо $\alpha(0) = 0$.

Інакше кажучи, $(Q; \circ)$ є квазігрупою, якщо для кожного $a \in Q$ *лівий* L_a і *правий* R_a *зсуви*, що визначають з рівностей $L_a(x) := a \circ x$, $R_a(x) := x \circ a$, є підстановками носія Q . Легко перевірити, що квазігрупа є групою тоді і тільки тоді, коли вона асоціативна.

1.1. Ізотопія. Дві квазігрупи $(A; *)$ та $(B; \triangleleft)$ називають *ізотопними*, якщо існують такі бієкції α, β, γ із множини A на множину B , що

$$\alpha(x) \triangleleft \beta(y) = \gamma(x * y)$$

для всіх $x, y \in A$, трійку (α, β, γ) називають *ізотопізмом*. Ізотопію називають *головною*, якщо $\gamma = \text{id}$, а квазігрупи – *ізоморфними*, коли $\alpha = \beta = \gamma$. І відношення ізотопії, і відношення ізоморфізму є відношеннями еквівалентності, тому їм відповідають розбиття множини всіх оборотних операцій, що визначені на одному й тому ж носії. Кожен групоїд, будучи ізотопним деякій квазігрупі, також є квазігрупою. Кожна квазігрупа ізотопна лупі з наперед заданим нейтральним елементом. Відмітимо відомий результат, який подано в зручному вигляді.

Твердження 1. Нехай $(Q; \cdot)$ – квазігрупа, $a \in Q$ і $b := L_a^{-1}(a)$, тоді $(Q; \circ, a)$ є лупою, де $x \circ y := R_b^{-1}(x) \cdot L_a^{-1}(y)$.

Доведення. Справді, $x \circ a = R_b^{-1}(x) \cdot L_a^{-1}(a) = R_b^{-1}(x) \cdot b = x$. Оскільки $R_b^{-1}(a) = a$, то $a \circ y = R_b^{-1}(a) \cdot L_a^{-1}(y) = a \cdot L_a^{-1}(y) = y$. $\diamond$

1.2. Канонічні розклади. Розглянемо квазігрупи на скінченних носіях. Якщо носій має m елементів, то його занумеруємо першими m числами розширеного натурального ряду і позначимо Z_m :

$$Z_m := \{0, 1, 2, \dots, m-2, m-1\}.$$

Нехай $(+)$ – позначає додавання, а $(\cdot)$ – множення за модулем m і $Z_m := (Z_m; +, \cdot)$ є кільцем лишків за модулем m . Адитивну групу кільця лишків за модулем m також позначатимемо $Z_m := (Z_m; +)$, якщо це не призведе до непорозуміння.

Означення 1. Нехай $(Q; \circ)$ – квазігрупа і $x \circ y = t(x, y)$ для всіх $x, y \in Q$, де $t(x, y)$ – деякий терм, який назовемо *розкладом квазігрупи* $(Q; \circ)$. Розклад назовемо *канонічним*, якщо він завжди існує та єдиний.

Означення 2. Нехай $(Z_m; *)$ – довільна скінченна квазігрупа. Розклад

$$x * y = \alpha(x) \circ \beta(y) \tag{1}$$

назовемо *лівим 0-канонічним*, якщо $(Z_m; \circ, 0)$ – лупа з нейтральним елементом 0 , а α, β – підстановки носія, причому $\alpha(0) = 0$. Ізотопізм $(\alpha, \beta, \text{id})$ назовемо *0-канонічним*.

Теорема 1. Кожна квазігрупа має 0-канонічний розклад.

Доведення. Нехай $(Z_m; *)$ – довільна скінченна квазігрупа. Покладемо $\alpha := R_0$, $\beta := L_b$, де $b := L_0^{-1}(0)$. З твердження 1, якщо $a = 0$, маємо рівність

$$x \circ y := \alpha^{-1}(x) * \beta^{-1}(y),$$

з якої випливає, що $(Z_m; \circ, 0)$ – лупа з нейтральним елементом 0 та виконується рівність $\alpha(0) = 0$. Тому, замінивши x на $\alpha(x)$ та y – на $\beta(y)$, отримаємо розклад

$$x * y := \alpha(x) \circ \beta(y).$$

Залишилось довести єдиність. Припустимо існування лупи $(Z_m; *, 0)$ та підстановок γ, δ з умовами $\gamma(0) = 0$ та $x * y := \gamma(x) * \delta(y)$. Отже,

$$\alpha(x) \circ \beta(y) = \gamma(x) * \delta(y)$$

для всіх $x, y \in Q$. Покладемо в цій рівності $x = 0$, отримаємо $\beta = \delta$, а при $y = \beta^{-1}(0)$ маємо $\alpha = \gamma$, тому $(\circ) = (*)$. $\diamond$

Нехай Q – довільна множина, Δ – множина оборотних операцій з носієм Q , $\Delta_0(f)$ – множина оборотних операцій, які канонічно ізотопні 0-лупі f .

Наслідок 1. Нуль-канонічний розклад e -лупи $(\bullet)$ такий: $x \bullet y = x \circ L_e^{-1}(y)$.

Доведення. Нехай $(\bullet) \in \Delta_0(\circ)$ і нехай

$$x \bullet y = \alpha(x) \circ \beta(y) -$$

0-канонічний розклад лупи $(Q; \bullet, e)$. Оскільки 0 є нейтральним елементом для $(\circ)$, а e – для $\alpha(0) = 0$, то при $x = 0$ та $y = e$ маємо $0 \bullet e = \alpha(0) \circ \beta(e)$, тобто $\beta(e) = 0$. Тому, якщо $y = e$, отримуємо:

$$x \bullet e = \alpha(x) \circ \beta(e), \quad x = \alpha(x) \circ 0, \quad \alpha(x) = x, \quad \alpha = \text{id}.$$

А при $x = e$ маємо $\beta = L_e^{-1}$. $\diamond$

Наслідок 2. Нуль-канонічна ізотопія утворює розбиття множини Δ , причому кожний клас розбиття містить точно одну 0-лупу.

Доведення. В теоремі 1 доведено, що кожна квазігрупа має 0-канонічний розклад і він єдиний, тому множини $\Delta_0(f)$ неперехресні, а їх об'єднання становить всю множину квазігруп Δ , що визначені на фіксованому носії, тобто канонічна ізотопія є розбиттям множини Δ . З наслідку 1, якщо $e = 0$, випливає єдиність 0-лупи в кожній множині $\Delta_0(f)$. $\diamond$

Наслідок 3. Кількість квазігруп m -го порядку, які канонічно ізотопні одній 0-лупі, дорівнює $(m-1)! \cdot m!$.

Доведення. З теоремі 1 випливає, що кожна квазігрупу над фіксованою лупою порядку m взаємно однозначно визначає канонічний ізотопізм, який має два параметри: α та β (канонічний розклад (1)). Параметр α набуває $(m-1)!$ значень, оскільки $\alpha(0) = 0$, а параметр β – $m!$ значень. Тому всього таких пар параметрів $(m-1)! \cdot m!$, тоді й квазігруп стільки ж. $\diamond$

Наслідок 4. Кількість квазігруп m -го порядку

$$(m-1)! \cdot m! \cdot m_0,$$

де m_0 – кількість 0-луп порядку m .

Доведення. Доведення безпосередньо випливає із наслідку 3. $\diamond$

Легко перевірити істинність такого твердження.

Твердження 2. ([5,6]). Трійка (α, β, γ) бієкцій $A \rightarrow B$ є ізотопізмом лупи $(A; \cdot, e)$ на комутативну групу $(B; +, 0)$ тоді і тільки тоді, коли існу-

ють такі елементи $a, b \in B$ та ізоморфізм ϕ лупи $(A; \cdot, e)$ на $(B; +, 0)$, що $\alpha = L_a \phi$, $\beta = L_b \phi$, $\gamma = L_{a+b} \phi$, де $L_c(x) := c + x$, $a, b, c \in B$.

Доведення. Нехай трійка (α, β, γ) є ізотопізмом лупи $(A; \cdot, e)$ на комутативну групу $(B; +, 0)$, тобто виконується тотожна рівність

$$\alpha(x) + \beta(y) = \gamma(x \cdot y). \quad (2)$$

Визначимо такі елементи і перетворення:

$$a := \alpha(e), \quad b := \beta(e), \quad \phi_1 := L_a^{-1} \alpha, \quad \phi_2 := L_b^{-1} \beta, \quad \phi := L_{a+b}^{-1} \gamma.$$

Звідси $\alpha = L_a \phi_1$, $\beta = L_b \phi_2$, $\gamma = L_{a+b} \phi$. Тоді рівність (2) запишемо у вигляді

$$a + \phi_1(x) + b + \phi_2(y) = a + b + \phi(x \cdot y).$$

Скоротивши, отримаємо рівносильну рівність

$$\phi_1(x) + \phi_2(y) = \phi(x \cdot y),$$

в яку покладемо по черзі $x = e$ та $y = e$. Оскільки $\phi_1(e) = \phi_2(e) = 0$, то $\phi_1 = \phi_2 = \phi$. $\diamond$

Звідси, зокрема, випливає, що ізотопні комутативні групи ізоморфні.

2. **Лупи третього порядку.** Розглянемо 0-лупу третього порядку (перша таблиця Келі з (3)). Враховуючи, що в рядках і стовпцях всі елементи різні, отримуємо однозначне заповнення таблиці: $1 + 2 = 0$, $1 + 1 = 2$, $2 + 1 = 0$, $2 + 2 = 1$ (друга таблиця Келі з (3)):

$$\begin{array}{|c|c|c|c|} \hline + & 0 & 1 & 2 \\ \hline 0 & 0 & 1 & 2 \\ \hline 1 & 1 & & \\ \hline 2 & 2 & & \\ \hline \end{array} \quad \begin{array}{|c|c|c|c|} \hline + & 0 & 1 & 2 \\ \hline 0 & 0 & 1 & 2 \\ \hline 1 & 1 & 2 & 0 \\ \hline 2 & 2 & 0 & 1 \\ \hline \end{array}. \quad (3)$$

Оскільки 0-лупу визначають однозначно, то це і є адитивна група за модулем 3 Z_3 . Отже, всі квазігрупи третього порядку 0-канонічно ізотопні групі Z_3 .

Теорема 2. Третього порядку є 12 квазігруп. Загальний 0-канонічний розклад оберотної операції $(*)$ такий:

$$x * y = \alpha(x) + \beta(y), \text{ де } \alpha \in \{1, (12)\}, \beta \in S_3 = \{1, (01), (02), (12), (012), (021)\}.$$

Доведення. Очевидне.

3. **Лупи четвертого порядку.** З огляду на програмування та природність задання операцій елементи носія $Z_4 := \{0, 1, 2, 3\}$ зручно подавати у двійковій системі числення:

$$Z_2^2 := \{00, 01, 10, 11\}.$$

Знайдемо задання всіх оборотних операцій у зручному для програмування вигляді. Але спочатку опишемо всі квазігрупи на носіїв Z_4 .

3.1. **Циклічна група та група Кляйна.** На чотириелементній множині природно виникають дві групи.

- **Циклічна** – адитивна група кільця лишків Z_4 за модулем 4. Елементи носія Z_2^2 розглядаємо як числа двійкової системи числення, а їх дода-

вання здійснюємо за модулем 4. Операцію позначатимемо $(+)$, а групу – $(Z_2^2; +; \bar{0})$, де $\bar{0} := 00$ – нейтральний її елемент.

- Група Кляйна – це адитивна група кільця $Z_2 \times Z_2$. Елементи носія Z_2^2 – пари чисел 0 та 1, а їх додавання здійснюємо покомпонентно у двійковій системі числення. Наприклад, $11 = (1,1)$, $10 = (1,0)$ і тоді їх сума є покомпонентним додаванням за модулем 2:

$$11 \oplus 10 = (1,1) \oplus (1,0) = (1+1, 1+0) = (0,1) = 01.$$

Операцію позначатимемо $(\oplus)$, а групу – $(Z_2^2; \oplus; \bar{0})$, де $\bar{0} := 00$ – нейтральний елемент цієї групи.

Ці групи неізоморфні, оскільки в групі Кляйна виконується тотожність $2x = 0$, а в циклічній групі – ні: $1+1=2$. Отже, для цих операцій на носіїв Z_2^2 маємо такі таблиці Келі:

+	00	01	10	11
00	00	01	10	11
01	01	10	11	00
10	10	11	00	01
11	11	00	01	10

+	00	01	10	11
00	00	01	10	11
01	01	00	11	10
10	10	11	00	01
11	11	10	01	00

(4)

3.2. Квазігрупи четвертого порядку на носіїв Z_4 . Доведемо, що 0-лупами четвертого порядку є такі:

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

$\oplus$	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

(5)

$\bullet$	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	1	0
3	3	2	0	1

$\diamond$	0	1	2	3
0	0	1	2	3
1	1	3	0	2
2	2	0	3	1
3	3	2	1	0

(6)

Точніше, істинна така теорема.

Теорема 3. Кожна 0-лупа четвертого порядку $(Z_4; \circ, 0)$ є однією із таких луп:

- група Кляйна $(Z_4; \oplus, 0)$ з (5), якщо $1 \circ 1 = 0$ і $2 \circ 2 = 0$;
- група $(Z_4; \bullet, 0)$ з (6) і $s = (12)$ є ізоморфізмом циклічній групі, якщо $1 \circ 1 = 0$ і $2 \circ 2 = 1$;
- циклічна група $(Z_4; +, 0)$ з (5), якщо $1 \circ 1 = 2$;

- група $(Z_4; \diamond, 0)$ з (6) і $r = (23)$ є ізоморфізмом циклічній групі, якщо $1 \diamond 1 = 3$.

Доведення. Нехай $(Z_4; \circ, 0)$ є 0-лупою, тоді її таблиця Келі має вигляд

$\circ$	0	1	2	3
0	0	1	2	3
1	1			
2	2			
3	3			

Якщо $1 \circ 1 = 0$, то її таблиця Келі перша із таблиць

$\circ$	0	1	2	3
0	0	1	2	3
1	1	0		
2	2			
3	3			

$\circ$	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3		
3	3	2		

(7)

Оскільки і в рядках, і в стовпцях елементи різні, то однозначно заповнюються такі комірки: $1 \circ 2 = 3$, $1 \circ 3 = 2$, $2 \circ 1 = 3$, $3 \circ 1 = 2$. У результаті отримуємо другу таблицю з (7). Маємо дві можливості: $2 \circ 2 = 0$ або $2 \circ 2 = 1$. Надалі кожна з двох отриманих таблиць заповнюється однозначно.

Якщо $2 \circ 2 = 0$, то отримуємо другу таблицю із (5). В результаті одержали групу Кляйна $(Z_4; \oplus, 0)$.

Якщо $2 \circ 2 = 1$, то маємо першу таблицю із (6). Лупа $(Z_4; \bullet, 0)$ ізоморфна циклічній групі $(Z_4; +, 0)$ і $s = (12)$ є відповідним ізоморфізмом. Зокрема,

$$x + y = s(s(x) \bullet s(y)). \quad (8)$$

Оскільки обидві лупи комутативні і мають один і той самий нейтральний елемент, то достатньо перевірити рівність (8) для пар $(1, 2)$, $(1, 3)$, $(2, 3)$:

$$1 + 2 = s(s(1) \bullet s(2)) = s(2 \bullet 1) = s(3) = 3,$$

$$1 + 3 = s(s(1) \bullet s(3)) = s(2 \bullet 3) = s(0) = 0,$$

$$2 + 3 = s(s(2) \bullet s(3)) = s(1 \bullet 3) = s(2) = 1.$$

Отже, лупи $(Z_4; +, 0)$ та $(Z_4; \bullet, 0)$ ізоморфні, тому $(Z_4; \bullet, 0)$ також є групою.

Повернемось до початкової таблиці і розглянемо випадок, коли $1 \circ 1 = 2$. Існує шлях однозначного заповнення таблиці $1 \circ 3 = 0$, $1 \circ 2 = 3$, $2 \circ 3 = 1$, $2 \circ 2 = 0$, $2 \circ 1 = 3$ і так далі. В результаті отримаємо таблицю Келі для циклічної групи.

І, нарешті, нехай $1 \circ 1 = 3$. Тоді також існує шлях однозначного заповнення таблиці: $1 \circ 2 = 0$, $1 \circ 3 = 2$, $2 \circ 1 = 0$, $2 \circ 3 = 1$, $2 \circ 2 = 3$ і так далі. У результаті отримуємо другу таблицю Келі із (6). Лупа $(Z_4; \diamond, 0)$ також ізоморфна групі $(Z_4; +, 0)$, а ізоморфізмом є перестановка носія $r = (23)$. $\diamond$

З теореми (3) випливає таке твердження.

Наслідок 5. Нуль-лупа четвертого порядку є групою Кляйна або ізоморфна циклічній 0-групі.

Теорема 4. Кількість квазігруп четвертого порядку дорівнює 576. Кожна з них, нехай $(Z_4; f)$, має єдине подання у вигляді

$$f(x, y) = \alpha(x) \nabla \beta(y),$$

де ∇ – одна із операцій (5), (6); α, β – підстановки носія $Z_4 := \{0, 1, 2, 3\}$, причому $\alpha(0) = 0$.

Доведення. З наслідку 4 випливає, що кількість квазігруп четвертого порядку дорівнює $3! \cdot 4! \cdot 4 = 576$. З теореми 1 кожна квазігрупа має єдиний 0-канонічний розклад, а всі 0-лупи описані в теоремі 3. $\diamond$

3.3. Квазігрупи четвертого порядку на носіїв Z_2^2 . У теоремі 4 встановлено канонічний розклад кожної оборотної операції на носіїв $Z_4 := \{0, 1, 2, 3\}$. Нижче подамо кожну квазігрупу в зручному для обчислення вигляді. Для цього розглянемо квазігрупи на носіїв $Z_2^2 := \{00; 01; 10; 11\}$. До того ж у запропонованому канонічному розкладі будуть лише дві групи – циклічна та Кляйна.

Відмітимо, що на чотириелементній множині існує $3! = 6$ унітарні підстановки (ті, які не рухають нуль, тобто залишають на місці). Нехай A – квадратна матриця другого порядку, тоді рівність

$$\lambda(\bar{x}) := \bar{x} \cdot A$$

визначає перетворення множини Z_2^2 . При цьому $\bar{x}$ розглядаємо як матрицю розмірності 1×2 . Це перетворення оборотне, якщо матриця оборотна, тобто її визначник дорівнює 1. А це можливо лише тоді, коли обидва елементи однієї з діагоналей точно дорівнюють 1, тому таких матриць шість:

$$U := \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \right\}. \quad (9)$$

Отже, всі унітарні перетворення визначають матриці. Оскільки множення матриць дистрибутивне, то λ є автоморфізмом адитивної групи кільця $Z_2 \times Z_2$, тобто групи Кляйна $(Z_2^2; \oplus)$. Це означає, що автоморфізмами групи Кляйна є всі унітарні перетворення множини Z_2^2 . Таблиці Келі, які визначають циклічну групу і групу Кляйна, є таблицями (4).

Лема. Нехай $(Z_2^2; \circ, \bar{0})$ – група, де $\bar{0} := 00$. Для довільної підстановки γ множини Z_2^2 існує оборотна матриця $A \in \mathbb{U}$ з (9) та елемент $\bar{a} \in Z_2^2$ такі, що

$$\gamma(\bar{x}) = \bar{x}A \circ \bar{a}.$$

Доведення. Перетворення α , яке визначає рівність $\alpha(\bar{x}) := \gamma(\bar{x}) - \gamma(\bar{0})$, є унітарною підстановкою групи $(Z_2^2; \circ, \bar{0})$, тому існує така оборотна матриця $A \in \mathbb{U}$ з (9), що $\alpha(\bar{x}) = \bar{x}A$. Отже,

$$\gamma(\bar{x}) = \alpha(\bar{x}) + \gamma(\bar{0}) = \bar{x}A + \bar{a}, \text{ де } \bar{a} := \gamma(\bar{0}). \quad \diamond$$

Теорема 5. Кожну квазігрупову операцію f на носіїв $Z_2^2 := \{00; 01; 10; 11\}$ визначає точно одна із формул

$$f(\bar{x}, \bar{y}) = \bar{x}A \oplus \bar{y}B \oplus \bar{a}, \quad (10)$$

$$f(\bar{x}, \bar{y}) = (\bar{x}A + \bar{y}B + \bar{a})C, \quad (11)$$

де операції $(\oplus)$, $(+)$ – адитивні групи кілець $Z_2 \times Z_2$ та Z_4 з (4), $\bar{a} \in Z_2^2$, $A, B \in U$ – з (9), $C \in V$, де

$$V := \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\}.$$

Доведення. Оскільки канонічний розклад довільної оборотної операції завжди існує і єдиний, згідно з теоремою 1, то множину всіх квазігруп четвертого порядку розбиваємо на чотири підмножини залежно від 0-групи, якій вона канонічно ізотопна. Розглянемо квазігрупи над кожною із них.

Група Кляйна $(Z_4; \oplus, \bar{0})$ з (4). За означенням 2, згідно з теоремою 1, канонічний розклад має вигляд $f(\bar{x}, \bar{y}) = \alpha\bar{x} \oplus \beta\bar{y}$. Згідно з лемою 1, існують такі матриці A, B та елемент $\bar{a}$, що $\alpha(\bar{x}) = \bar{x}A$ і $\beta(\bar{y}) = \bar{y}B \oplus \bar{a}$. Врахувавши ці рівності, отримуємо (10).

Циклічна група $(Z_4; +, \bar{0})$ з (4). Виразимо компоненти канонічної ізотопії через матриці циклічної групи: $\alpha(\bar{x}) = \bar{x}A$ і $\beta(\bar{y}) = \bar{y}B + \bar{a}$. Підставивши в канонічний розклад $f(\bar{x}, \bar{y}) = \alpha\bar{x} + \beta\bar{y}$, отримаємо рівність (11), якщо матриця C єдинична.

Група $(Z_4; \bullet, \bar{0})$ з (6). З теореми 3 випливає, що підстановка $s = (01.10)$ є ізоморфізмом між операціями $(\bullet)$ та $(+)$, тобто виконується рівність

$$\bar{x} \bullet \bar{y} = s(s(\bar{x}) + s(\bar{y})).$$

Підставимо в канонічний розклад

$$f(\bar{x}, \bar{y}) = \alpha\bar{x} \bullet \beta\bar{y} = s(s\alpha(\bar{x}) + s\beta(\bar{y})).$$

Згідно з лемою, існують такі матриці A, B та елемент $\bar{a}$, що виконуються рівності $s\alpha(\bar{x}) = \bar{x}A$ і $s\beta(\bar{y}) = \bar{y}B + \bar{a}$. У результаті отримаємо (11) за умови, якщо матриця C має вигляд

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

що відповідає підстановці s .

Доведення для групи $(Z_4; \diamond, 0)$ з (6) аналогічне. $\diamond$

Означення 3. Формули (10) і (11) назовемо *матричним канонічним розкладом* квазігрупи.

3.4. Приклад для застосування. Такі приклади для IP-квазігруп та ортогональності через канонічні розклади у вигляді матричного та векторного подань наведені у працях [7, 8]. Тут подамо критерій виконання деякої тотожності серед ізоотопів групи Кляйна, який для криптографії описано в працях [1–3].

Твердження 3. Квазігрупа $(Z_2^2; \circ)$ задовольняє тотожність

$$(\bar{x} \circ \bar{y}) \circ (\bar{x} \circ \bar{x}) = \bar{y} \tag{12}$$

над групою Кляйна $(Z_2^2; \oplus, \bar{0})$ тоді і тільки тоді, коли вона має один із таких розкладів:

$$\bar{x} \circ \bar{y} = \bar{x}A \oplus \bar{y}A^2 \oplus \bar{a}, \quad \bar{x} \circ \bar{y} = \bar{x}A^2 \oplus \bar{y}A \oplus \bar{a},$$

$$\text{де } A = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \text{ і } \bar{a} \in \{00, 01, 10, 11\}.$$

Доведення. Нехай у квазігрупі $(Q; \circ)$ виконується тотожність (12). Враховуючи теорему 1 та формулу (10) з теореми 5, тотожність запишемо у вигляді

$$(\bar{x}A \oplus \bar{y}B \oplus \bar{a})A \oplus (\bar{x}A \oplus \bar{x}B \oplus \bar{a})B \oplus \bar{a} = y.$$

Оскільки операція $(\oplus)$ асоціативна і комутативна, а множення матриць дистрибутивне, то отримуємо рівносильну тотожність:

$$\bar{x}(A^2 \oplus AB \oplus B^2) \oplus \bar{y}BA \oplus \bar{a}(A \oplus B \oplus I) = \bar{y}.$$

Поклавши по черзі $\bar{x} = \bar{y} = \bar{0}$, $\bar{x} = \bar{0}$, $\bar{y} = \bar{0}$, одержимо, що цій тотожності рівносильна система рівностей

$$\begin{cases} A^2 \oplus AB \oplus B^2 = O, \\ BA = I, \\ \bar{a}(A \oplus B \oplus I) = \bar{0}, \end{cases}$$

де I – одинична матриця, а O – нульова. З другої рівності цієї системи випливає, що матриці A і B взаємно обернені, тобто $B = A^{-1}$.

Якщо матриця $A^2 = I$, то $B^2 = I$, тоді перша рівність системи має вигляд $I \oplus I \oplus I = O$. Але матриці булеві, тоді $I \oplus I = O$, а тому одинична матриця та матриці другого порядку із $\mathbb{U}$ в (9) не задовольняють систему.

Залишилось розглянути матриці третього порядку $A^3 = I$, тобто $B = A^{-1} = A^2$. Тоді перша рівність системи має вигляд

$$A^2 \oplus A \oplus I = O \quad \text{або} \quad A \oplus A^2 \oplus I = O.$$

Звідси, зокрема, випливає, що третя рівність системи завжди виконується незалежно від елемента $\bar{a}$. Множина матриць U з (9) має лише дві матриці третього порядку:

$$A := \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \quad A^2 := \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}.$$

Отримуємо $A^2 \oplus A \oplus I = I \oplus I = \bar{0}$. □

Отже, для застосування у малоресурсній криптографії в програмний код пристрою достатньо записувати лише саму формулу канонічного розкладу відповідної квазігрупи з необхідними властивостями. А для апаратної реалізації достатньо використовувати лише комірки пар елементів, які працюють в операційному блоці криптографічної системи.

Приклад. Побудуємо таблицю Келі на носіїв $Z_4 := \{0, 1, 2, 3\}$ однієї з восьми квазігруп, що відповідають критеріям твердження 3.

Для цього достатньо сформулювати порожню таблицю Келі та заповнити її, використавши канонічний розклад, наприклад,

$$\bar{x} \circ \bar{y} = \bar{x}A \oplus \bar{y}A^2 \oplus 01,$$

тобто парі елементів $x = 2 = 10_2$, $y = 3 = 11_2$ відповідає елемент

$$2 \circ 3 = 10_2 \circ 11_2 = 10 \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \oplus 11 \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^2 \oplus 01 = 01_2 = 1.$$

Обчисливши всі значення, отримуємо таку таблицю Келі:

◦	0	1	2	3
0	0	3	1	2
1	2	1	3	0
2	3	0	2	1
3	1	2	0	3

Висновки. Розв'язано пряму задачу для квазігруп четвертого порядку, коли важливо побудувати квазігрупу для застосування. Для подальших досліджень варто розглянути і зворотню задачу, коли відомий латинський квадрат, а невідомий його канонічний розклад серед всіх квазігруп четвертого порядку.

1. Крайнічук Г., Пилявець І., Радченко Є. СІР-квазігрупи 4-го порядку з оборотним елементом x^2 серед ізотопів групи Клейна // Міжнар. наук. конф. «Сучасні проблеми механіки та математики – 2023», присвячена 95-річчю від дня народження академіка НАН України Я. С. Підстригача. Львів: ІППММ ім. Я.С. Підстригача, 2023. – С. 285–286.
2. Крайнічук Г., Радченко Є., Пилявець І. Концепція шифру на основі СІР-квазігруп // Theoretical and Applied Cybersecurity. Матеріали Першої Всеукр. наук.-практ. конф., присвяченої 100-річчю ювілею акад. В. М. Глушкова. – Київ: КПІ ім. Ігоря Сікорського, 2023. – С. 199–202.
3. Лужецький В., Баришев Ю., Дереч В. Псевдонедедетерміністичний підхід до криптографічного захисту систем керування // Інформаційні технології в окремих сферах управління (наук. ред. Л. Петришин). – Краків: Вид-во АГХ, 2018. – С. 25–38.
4. Sokhatsky F. Invertible binary functions and quasigroups of the order four // Book of abstracts of the 13th International Algebraic Conference in Ukraine (July 6–9, 2021, Kyiv, Ukraine). – Київ: КНУ ім. Т. Шевченка, 2021. – С. 77.
5. Сохацький Ф. М. Про ізотопи груп. I // Укр. мат. журн. – 1995. – 47, № 10. – С. 1387–1398.
6. Сохацький Ф. М. Про ізотопи груп. II // Укр. мат. журн. – 1995. – 47, № 12. – С. 1692–1703.
7. Сохацький Ф. М., Луценко А. В. Матричні ІР-квазігрупи 4-го порядку // 36. матеріалів I Міжнар. наук.-практ. конф. «Прикладні аспекти сучасних міждисциплінарних досліджень». – Вінниця: ДонНУ ім. В. Стуса, 2022. – С. 288–290.
8. Сохацький Ф. М., Луценко А. В., Фриз І. В. Побудова квазігруп із властивістю оборотності // Мат. методи та фіз.-мех. поля. – 2021. – 64, № 4. – С. 5–17. – <https://doi.org/10.15407/mmpmf2021.64.4.5-17>.
9. Artamonov V. A., Chakrabarti S., Gangopadhyay S., Pal S. K. On Latin squares of polynomially complete quasigroups and quasigroups generated by shifts // Quasigroups and Related Systems. – 2013. – 21. – P. 117–130.
10. Gligorski D., Dimitrova V., Markovski S. Quasigroups as boolean functions, their equation systems and Gröbner bases // In: M. Sala et al. (eds.), Gröbner Bases, Coding, and Cryptography. – Berlin–Heidelberg: Springer, 2009. – P. 415–420. – https://doi.org/10.1007/978-3-540-93806-4_31
11. Dimitrova V., Bakeva V., Popovska-Mitrovikj A., Krapež A. Cryptographic properties of parastrophic quasigroup transformation // ICT Innovations 2012: Conf. Proc. – Ser. Advances in Intelligent Systems and Computing. – Vol. 207. – Berlin–Heidelberg, Springer, 2012. – P. 235–243. – https://doi.org/10.1007/978-3-642-37169-1_23
12. Dimitrova V., Markovski S., Gligorski D. Classification of quasigroups as Boolean functions, their algebraic complexity and application of Gröbner bases in solving systems of quasigroup equations // In: Gröbner Bases, Coding and Cryptography. – Springer, 2007.

13. Keedwell A. D., Denes J. Latin Squares and their Applications. – Amsterdam–Boston: North-Holland, 2015. – 438 p.
14. Krainichuk H. Classification of group isotopes according to their symmetry groups // Folia Math. – 2017. – 19, No. 1. – P. 84–98.
15. Siljanoska M., Mihova M., Markovski S. Matrix presentation of quasigroups of order 4 // Proc. of the 10th Conference for Informatics and Information Technology (CIIT 2013). – P. 192–196.
16. Sokhatskyj F., Syvakivskyj P. On linear isotopes of cyclic groups // Quasigroups and Related Systems. – 1994. – 1, No. 1(1). – P. 66–76.

CANONICAL AND MATRIX FIGURATION OF QUASIGROUPS OF THE FOURTH ORDER

A quasigroup is called a loop if it has a neutral element. When it is denoted by 0, it is called a 0-loop. There are 4 0-loops of the fourth order, one of which is a Klein group, the other three are isomorphic to a cyclic group. The obtained results are: 1) every quasigroup of the fourth order has a unique canonical decomposition over exactly one of these four 0-loops; 2) every quasigroup of the fourth order has a unique matrix canonical decomposition over either a cyclic group or a Klein group; 3) the corresponding formulas and examples for their use are given.

Keywords: quasigroup, loop, canonical decomposition, matrix, isotopism, isomorphism, Klein group, cyclic group.

¹ Інститут прикладних проблем механіки і математики
ім. Я.С. Підстригача НАН України, Львів

² Вінницький нац. техн. ун-т, Вінниця