Ортогональність операцій та умови оборотності операції

І. В. Фриз, Ф. М. Сохацький

В даній роботі дається алгебричне (на мові багатомісних операцій) та комбінаторне (на мові гіперкубів) означення ортогональності двох операцій різної арності, яке відрізняється від загальновідомих означень, встановлено зв'язок між композицією і ортогональністю, а також знайдено критерій ортогональності лінійних квазігруп.

Вступ

Функція, що визначена на скінченній чи нескінченній множині називається квазігруповою або оборотною, якщо вона оборотна по кожній своїй змінній. Вивчення оборотних функцій спричинено різноманітними їх застосуваннями в комбінаториці [2], алгебрі [2], криптології [3], геометрії [2] тощо.

Одне з питань, яке виникає при вивченні оборотних функцій — це подання багатомісної оборотної функції у вигляді композиції оборотних функцій від меншої кількості змінних. При цьому основними є такі питання:

1) можливість розкладу оборотних функцій;
2) описання всіх розкладів оборотних функцій;
3) умови, за яких композиція оборотних функцій є оборотною.

На перше питання для оборотних функцій, що визначені на скінченній множині, дає відповідь результат М.М.Глухова [4] про те, що кожна багатомісна оборотна функція є композицією бінарних оборотних функцій, які визначені на тій самій множині.

Третє питання вивчалось багатьма авторами. Композиція оборотних операцій завжди є оборотною, якщо композиція безповторна, тобто предметні змінні не повторюються. Якщо ж принаймні дві предметні змінні повторюються, то композиція навіть двох квазігруп не завжди є квазігрупою. Наприклад, операція f, яка визначена рівністю $f(x;y) = g(h^{\ell}(x;y);y)$, є оборотною тоді і тільки тоді, коли g є лівооборотною і ортогональною до h ($g \perp h$) [5]. Критерій через правооборотну функцію g аналогічний.

В даній роботі знайдено критерій оборотності композиції двох операцій не обов'язково однієї арності. Цим самим, як випливає із вище сказаного, узагальнюється поняття ортогональності двох операцій на багатомісний випадок, причому дане поняття не співпадає із введеним раніше (див. [1]).

Нагадаємо, що дві бінарні операції g і h, що визначені на Q, називаються ортогональними, якщо система $\{g(x;y) = a,\ \ h(x;y) = b\}$ має єдиний розв'язок для всіх $a, b \in Q$. Кожній бінарній операції відповідає деякий квадрат (тобто таблиця Келі без обмежень), а оборотній — відповідає латинський квадрат. Ортогональність операцій означає ортогональність відповідних квадратів, тобто їх накладання дає квадрат, в клітинках якого всі пари різні.

Ортогональність операцій різної арності

Нехай υ — довільне монотонно зростаюче відображення множини $\overline{0,k} := \{0,1,\ldots,k\}$ в $\overline{0,n}$, де $k \le n$.

Нехай операції g і h мають арності $n+1$ і $k+1$ відповідно, тоді пара бінарних операцій $(\circ;\bullet)$, які визначені рівностями

$$x \circ y := g(a_0, ..., a_{\upsilon p-1}, x, a_{\upsilon p+1}, ..., a_{\upsilon m-1}, y, a_{\upsilon m+1}, ..., a_n);$$

$$x \bullet y := h(a_{\upsilon 0}, ..., a_{\upsilon(p-1)}, x, a_{\upsilon(p+1)}, ..., a_{\upsilon(m-1)}, y, a_{\upsilon(m+1)}, ..., a_{\upsilon k}),$$

якщо $m > p$, і рівностями

$$x \circ y := g(a_0, ..., a_{\upsilon m-1}, y, a_{\upsilon m+1}, ..., a_{\upsilon p-1}, x, a_{\upsilon p+1}, ..., a_n);$$

$$x \bullet y := h(a_{\upsilon 0}, ..., a_{\upsilon(m-1)}, y, a_{\upsilon(m+1)}, ..., a_{\upsilon(p-1)}, x, a_{\upsilon(p+1)}, ..., a_{\upsilon k}),$$

якщо $m < p$, називається *υ-відповідними $\{m; p\}$-ретрактами.*

Означення 1. Дві операції g і h арностей $n+1$ і $k+1$ відповідно, називаються *ортогональними типу* (m, υ), якщо для всіх $p \in \overline{0,k}$ кожна пара υ-відповідних $\{m; p\}$-ретрактів є ортогональною.

Означення 2. Назвемо *$\{m, p\}$-зрізом* гіперкуба H латинський квадрат, який отримується з H фіксацією усіх координат крім m і p.

Приклад. Нехай маємо тернарну операцію $f(x_0, x_1, x_2) = x_0 + x_1 + x_2$, яка задана на множині Z_5. Розглянемо $\{0, 2\}$-зріз куба, який відповідає операції f. Зафіксуємо $x_1 = 1$, тоді $\{0, 2\}$-зрізом даного куба є такий латинський квадрат:

1	2	3	4	0
2	3	4	0	1
3	4	0	1	2
4	0	1	2	3
0	1	2	3	4

Комбінаторним еквівалентом означення ортогональності операцій є таке:

Означення 3. Два гіперкуби H_1 і H_2, розмірностей $n+1$ і $k+1$ відповідно, називаються *ортогональними типу* (m, υ), якщо $\{m, p\}$-зріз гіперкуба H_1 і $\{\upsilon m, \upsilon p\}$-зріз гіперкуба H_2 є ортогональними для всіх $p \in \overline{0,k}$.

Критерій оборотності операції

Теорема 1. Нехай υ — довільне монотонно зростаюче відображення множини $\overline{0,k}$ в $\overline{0,n}$, де $k \leq n$, операції g і h мають арності $n+1$ і $k+1$ відповідно, а операція f визначається рівністю

$$f(x_0, ..., x_n) := g(x_0, ..., x_{\upsilon m-1}, h(x_{\upsilon 0}, ..., x_{\upsilon k}), x_{\upsilon m+1}, ..., x_n), \tag{1}$$

до того ж операція h є m-оборотною. Тоді i-оборотність операції f еквівалентна:

- i-оборотності g, якщо $i \notin \mathrm{Im}\upsilon$ або $i = \upsilon m$;[1]
- ортогональності типу (m, υ) операцій f і $h^{(m)}$, якщо $i \in \mathrm{Im}\upsilon$ і $i \neq \upsilon m$,

де $h^{(m)}$ є m-те ділення операції h.

Ортогональність лінійних квазігруп

Композиція трансляцій і автоморфізмів групи називається *лінійним перетворенням* групи. Якщо багатоарна квазігрупа (Q, g) є ізотопом бінарної групи $(Q; +)$, тобто $(Q; g)$ є ізотопною до $(Q; d)$, де $d(x_0, \ldots, x_n) = x_0 + \cdots + x_n$, і всі компоненти ізотопії є лінійними перетвореннями, тоді кажуть що $(Q; g)$ *лінійна*. Відомо, що кожна $(n+1)$-арна квазігрупа g, будучи лінійною над групою $(Q; +)$, має єдиний розклад:

$$g(x_0, \ldots, x_n) = \alpha_0 x_0 + \cdots + \alpha_n x_n + a, \tag{2}$$

[1] $\mathrm{Im}\upsilon$ позначає множину всіх значень відображення υ.

де $a \in Q$. Він називається *канонічним розкладом*, а перетворення $\alpha_0, \ldots, \alpha_n$ — автоморфізмами розкладу $(Q;+)$ [6]. Лінійний ізотоп абелевої групи називається *T-квазігрупою.*

Теорема 2. Нехай $(Q;+)$ — група, (1), (2) і

$$h(x_{\upsilon 0}, \ldots, x_{\upsilon k}) := \beta_0 x_{\upsilon 0} + \cdots + \beta_k x_{\upsilon k} + c \tag{3}$$

є канонічними розкладами операцій f, g, h. Операція f є квазігрупою тоді і тільки тоді коли існує $b \in Q$ такий що $\alpha_m \beta_p + I_b \alpha_p$ є підстановкою множини Q для всіх $p \in \overline{0,k} \backslash \{m\}$.

Наслідок 1. Нехай виконуються умови теореми 2 та g, h є T-квазігрупами. Операція f є квазігрупою тоді і тільки тоді коли $\alpha_m \beta_p + \alpha_p$ є автоморфізмом групи $(Q;+)$ для всіх $p \in \overline{0,k} \backslash \{m\}$.

Теорема 3. Нехай виконуються умови теореми 2 та g, h є T-квазігрупами. Операція f є ортогональною типу (m, υ) до g тоді і тільки тоді коли відображення

- $\beta_m^{-1}\beta_p + (\alpha_{\upsilon m}\beta_m)^{-1}\alpha_{\upsilon p} - \alpha_m^{-1}\alpha_p$, якщо $m < p$;
- $\alpha_{\upsilon m}\beta_m - \alpha_{\upsilon m}\beta_p\alpha_p^{-1}\alpha_m - \gamma_{\upsilon p}\alpha_{\upsilon p}\alpha_p^{-1}\alpha_m$, якщо $m > p$

є автоморфізмом групи $(Q;+)$ для всіх $p \in \overline{0,k} \backslash \{m\}$.

Наслідок 2. Нехай $(Q;g)$ і $(Q;h)$ — бінарні T-квазігрупи, $\alpha, \beta, \gamma, \delta, \varepsilon$ — автоморфізми $(Q;+)$ та f визначається (1), тоді операція f ортогональна типу $(0, \varepsilon)$ до операції g тоді і тільки тоді коли $\delta\beta^{-1}\alpha + \varepsilon - \gamma$ є автоморфізмом групи $(Q;+)$.

Аналогічний результат отримуємо для ортогональності типу $(1, \varepsilon)$.

Висновки

Знайдено критерій оборотності композиції двох операцій не обов'язково однакової арності. Цим самим знайдено інше узагальнення ортогональності двох операцій, а саме: дві операції ортогональні типу (m, υ), якщо ортогональні υ-відповідні бінарні ретракти. Побудовані приклади ортогональних квазігруп, які лінійні над деякою абелевою групою. Отже, встановлено існування ортогональних операцій довільної арності та гіперкубів довільної розмірності та будь-якого порядку, крім 2 і 6.

Список літератури

[1] Belyavskaya G., Mullen G.L. Orthogonal hypercubes and n-ary operations.// Quasigroups and Related Systems, 2005. — No 13. — 73-86.

[2] Chein O., Pflugfelder H.O., Smith J.D.H. Quasigroups and Loops: Theory and Applications.// Sigma Series in Pure Mathematics, 1990. — V.8. — 567 p.

[3] Shcherbacov V.A. Quasigroup in cryptology.//Computer Science Journal of Moldova, 2009. — V.17, no.2(50). — 193-228.

[4] Глухов М.М. Об α-замкнутых классах и α-полных системах функций k-значной логики. // Дискретная математика, 1989. — Т.1, №1. — С.16-21.

[5] Белоусов В.Д. Скрещенные изотопии квазигрупп.// Квазигруппы и их системы. Кишинев: Штиинца, 1990. — С. 14-20.

[6] Sokhatskyj Fedir, Syvakivskyj Petro. On linear isotopes of cyclic groups.// Quasigroups and Related Systems,1994. — v. 1, no. 1(1). — P.66-76.

Автори

Ірина Василівна Фриз — науковий співробітник, відділ науки і міжнародних зв'язків, Вінницький соціально-економічний інститут ВМУРоЛ "Україна Вінниця, Україна; E-mail: *friz_irina@ukr.net*

Федір Миколайович Сохацький — доктор фізико-математичних наук, проректор з науки і міжнародних зв'язків, Вінницький соціально-економічний інститут ВМУРоЛ "Україна Вінниця, Україна; E-mail: *fmsokha@ukr.net*