Хмельницький національний університет
Міністерство освіти і науки України

ДВНЗ "Прикарпатський національний університет
імені Василя Стефаника"
Міністерство освіти і науки України

Кваліфікаційна наукова
праця на правах рукопису

Фриз Ірина Василівна

УДК 512.548

ДИСЕРТАЦІЯ

ОРТОГОНАЛЬНІСТЬ БАГАТОМІСНИХ ОПЕРАЦІЙ ТА АЛГОРИТМИ ЇХ ПОБУДОВИ

01.01.06 – алгебра та теорія чисел

Подається на здобуття наукового ступеня
кандидата фізико-математичних наук

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело. _____ І.В. Фриз

Науковий керівник
Сохацький Федір Миколайович
доктор фізико-математичних наук,
доцент

Хмельницький – 2019

АНОТАЦІЯ

Фриз І.В. Ортогональність багатомісних операцій та алгоритми їх побудови. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня кандидата фізико-математичних наук за спеціальністю 01.01.06 – алгебра і теорія чисел. – Хмельницький національний університет. – ДВНЗ "Прикарпатський національний університет імені Василя Стефаника", Івано-Франківськ, 2019.

У дисертаційній роботі досліджуються n-арні операції і квазігрупи, вибірки операцій і їхні комбінаторні властивості: ортогональність та її види. Основними завданнями роботи є: дослідити оборотність довільної композиції двох багатомісних операцій; узагальнити рекурсивний алгоритм побудови ортогональних операцій; дослідити залежність між ортогональністю вибірки операцій і ортогональністю ретрактів цих операцій; знайти і дослідити методи доповнення ортогональних операцій і гіперкубів, дослідити кількість можливих доповнень за цими алгоритмами.

Перший розділ дисертаційної роботи присвячений огляду літератури з теми дослідження і систематизації основних понять і твердження, які використовуються у дисертації, зокрема наведено різні формулювання означення ортогональності операцій і показано зв'язки між ними.

У другому розділі досліджуються умови, за яких композиція оборотних операцій також є оборотною. Відомо, що безповторна композиція оборотних операцій завжди оборотна. Критерій оборотності повторної композиції двох оборотних бінарних операцій встановлений В.Д. Білоусовим. В цьому розділі знайдено критерій оборотності довільної композиції двох оборотних операцій довільних арностей. З цією метою вводиться поняття перпендикулярності двох операцій, яке визначається через ортогональність бінарних ретрактів певного виду. Як наслідок отримуємо критерій В.Д. Білоусова для повторної композиції двох бінарних операцій. Доведено, що максимальний тип перпендикулярності, тобто коли опера-

ції мають однакову арність, спричинює ортогональність у класичному розумінні, проте обернене твердження хибне. Також описано еквівалентні поняття мовою гіперкубів.

У третьому розділі описано і доведено блочний рекурсивний алгоритм побудови ортогональних n-арних операцій. А саме, для довільного розбиття множини $\{1, \ldots, n\}$ на блоки, рекурсивно будується n-вибірка n-арних операцій, причому на кожному наступному кроці будуються операції, що індексуються числами із одного із блоків розбиття, а при побудові використовуються всі операції, які побудовані на попередніх кроках. Доводиться, що побудовані операції ортогональні, якщо вхідні операції, які індексовані числами із одного блоку, є ретрактно ортогональними. Якщо зазначене розбиття тривіальне, тобто блоки розбиття одноелементні, то ретрактна ортогональність означає оборотність вхідних операцій на певних місцях і деякі з таких блочних рекурсивних алгоритмів збігаються з алгоритмом побудови ортогональних n-арних операцій, який запропоновано Г.Б. Білявською і Г.Л. Мулленом у 2005 р. Також отримано блочний композиційний алгоритм побудови ортогональних n-арних операцій із блоків ортогональних операцій меншої арності.

У четвертому розділі досліджується залежність ортогональності і ретрактної ортогональності, а також проблема доповнення ортогональних n-арних операцій.

Доведено, що ретрактна ортогональність спричинює ортогональність, але обернене твердження хибне. Показано, що за певних умов поняття ортогональності і ретрактної ортогональності еквівалентні, наприклад, для центральних квазігруп (лінійних ізотопів абелевих груп) над полем простого порядку. Доведено, що кожна вибірка ортогональних k-арних операцій є продовжувальною за допомогою безповторної композиції до вибірки ортогональних n-арних операцій, де $k < n$.

Описано залежність між різними узагальненнями ортогональності бінарних операцій: ретрактною ортогональністю, сильною ортогональністю

і перпендикулярністю максимального типу.

Обчислено: 1) кількість i-оборотних n-арних операцій порядку m; 2) кількість різних продовжень s-вибірки ортогональних k-арних операцій порядку m до s-вибірки ортогональних n-арних операцій, де $s \leqslant k$; 3) кількість k-вибірок δ-ретрактно ортогональних операцій, які можна побудувати, за допомогою композиційного алгоритму.

Г.Б. Білявська і Г.Л. Муллен у 2005 році довели, що кожна k-вибірка ортогональних n-арних операцій $(k < n)$ вбудовна у деяку n-вибірку ортогональних n-арних операцій, тобто доведено існування ортогонального доповнення, але не запропоновано спосіб доповнення. В цьому розділі доведено, що ортогональне доповнення можна побудувати за допомогою блочного рекурсивного алгоритму, зокрема, за допомогою тривіального доповнення, тобто такого що на кожному кроці алгоритму додається точно одна операція. Для тривіальних доповнень знайдено нижню та верхню оцінки їх кількості, а також знайдено нижню оцінку кількості всіх можливих доповнень.

Описано алгоритм побудови ортогональних доповнень довільної k-вибірки ортогональних k-арних операцій до n-вибірки ортогональних n-арних операцій для довільного n, такого що $n > k$, і знайдено нижню оцінку кількості таких доповнень.

У п'ятому розділі знайдено методи побудови n-арної квазігрупи з допустимими бінарними ретрактами, а також описано метод побудови пари перпендикулярних квазігруп.

Описано та класифіковано блочні рекурсивні алгоритми побудови і доповнення ортогональних тернарних операцій і показано, що їх можна розподілити на три класи відносно парастрофії визначаючих розбиттів. Для двох із отриманих класів знайдено умови, коли побудовані ортогональні операції є квазігрупами. Проілюстровано побудову і доповнення ортогональних кубів.

Ключові слова: n-арна операція, гіперкуб, ортогональність,

перпендикулярність, квазігрупа, оборотна операція, ретрактна ортогональність, ортогональне доповнення, лінійна операція, центральна квазігрупа.

Fryz I.V. Orthogonality of multuary operations and algorithms of their construction. – Qualifying scientific work on rights of manuscript.

The thesis for obtaining the Candidate of Physical and Mathematical Sciences degree on the speciality 01.01.06 — algebra and number theory. — Khmelnytskyi National University. – Vasyl Stefanyk Precarpathian National University, Ivano-Frankivsk, 2019.

In the thesis, n-ary operations and quasigroups, tuples of operations and their combinatorial properties such as orthogonality and its kinds are studied. The main directions of this work are to study invertibility of an arbitrary composition of two multiary operations; to generalize the recursive algorithm for construction of orthogonal operations; to investigate the dependence between orthogonality of operations and orthogonality of retracts of these operations; to find and investigate methods for constructing an orthogonal complement of operations and hypercubes and to estimate the number of complements by the obtained algorithms.

Chapter 1 of the thesis is devoted to the literature review on the topic of research and systematization of the main concepts and statements, in particular different formulations of the orthogonality definition are given and the relations among them are shown.

In chapter 2, conditions under which a composition of invertible operations is invertible are studied. It is well known that a repetition-free composition of invertible operations is invertible. A criterion of invertibility of a repetition composition of two invertible binary operations is proved by V.D. Belousov. In the chapter, an invertibility criterion of an arbitrary composition of two invertible operations of arbitrary arities is found. For this purpose, the notion of perpendicularity of two operations is introduced, it is defined by orthogonality of binary retracts of a certain kind. As a result, we have the criterion

of V.D. Belousov for a repetition composition of two binary operations. It is proved that perpendicularity of a maximal type, i.e., when the operations have the same arity, implies orthogonality in its classical meaning, however the inverse statement is not true. Equivalent concepts for hypercubes are described.

In chapter 3, a block-wise recursive algorithm for constructing a tuple of orthogonal operations is described and proved. Namely, for an arbitrary partition of the set $\{1, \ldots, n\}$ into blocks, an n-tuple of n-ary operations is constructed recursively. Besides for every step, the constructed operations are indexed by the numbers taken from one of the partition blocks, and all operations that are constructed by the previous steps are used for this construction. It is proved that the constructed operations are orthogonal if input operations that are indexed by the numbers from the same block are retractly orthogonal. If the partition is trivial, i.e., the partition blocks are singletons, then retract orthogonality means invertibility of input operations in some places and some of such block-wise recursive algorithms coincide with the algorithm for the construction of orthogonal n-ary operations by G.B. Belyavskaya and G.L. Mullen (2005). Also, a block composition algorithm for the construction of orthogonal n-ary operations using blocks of orthogonal operations of a less arity is obtained.

In chapter 4, the problem of dependence of orthogonality and retract orthogonality and the problem of complementing orthogonal operations are researched.

It is shown that a retract orthogonality implies orthogonality, but the inverse statement is not true. It is proved that under some conditions, notions of orthogonality and retract orthogonality are equivalent, for example, for central quasigroups (linear isotopes of an abelian group) over a prime order field. It is proved that every tuple of orthogonal k-ary operations is prolongable by a repetition-free composition to a tuple of orthogonal n-ary operations, where $k < n$.

The dependence among different generalizations of orthogonality of binary operations (retract orthogonality, strong orthogonality, perpendicularity of a

maximal type) is described.

The number of 1) i-invertible n-ary operations of order m; 2) different prolongations of an s-tuple of orthogonal k-ary operations of order m into an s-tuple of orthogonal n-ary operations, where $s \leqslant k$; 3) k-tuples of δ-retractly orthogonal operations that are constructible by the composition algorithm are calculated.

G.B. Belyavskaya and G.L. Mullen in 2005 proved that every k-tuple of orthogonal n-ary operations ($k < n$) is embedded into an n-tuple of orthogonal n-ary operations, i.e., the existence of an orthogonal complement is proved, however a method for the complementing is not proposed. In this chapter it is proved that using a block-wise recursive algorithm, an orthogonal complement for a tuple of orthogonal operations can be constructed, in particular using trivial complementing, i.e., when exactly one operation is added at every step. A lower bound and an upper bound of the number of different trivial complements and a lower bound of the number of all possible complements are found.

An algorithm for construction of orthogonal complements of an arbitrary k-tuple of orthogonal k-ary operations to an n-tuple of orthogonal n-ary operations for an arbitrary n such that $n > k$ is suggested, also a lower bound of the number of such complements is found.

In chapter 5, a method for constructing an n-ary quasigroup having admissible binary retracts is found and a method for the construction of a pair of perpendicular quasigroups is described.

The algorithms for the constructing and complementing a tuple of orthogonal ternary operations are described and classified into three classes up to parastrophy of defining partitions. For two obtained classes, the conditions, under which the constructed orthogonal operations are quasigroups, are found. The constructing and complementing of orthogonal cubes are illustrated.

Key words: n-ary operation, hypercube, orthogonality, perpendicularity, quasigroup, invertible operation, retract orthogonality, orthogonal complement, linear operation, central quasigroup.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА, В ЯКИХ ОПУБЛІКОВАНІ ОСНОВНІ НАУКОВІ РЕЗУЛЬТАТИ ДИСЕРТАЦІЇ

1. Sokhatsky F.M., Fryz I.V. *Invertibility criterion of composition of two multiary quasigroups* // Comment. Math. Univ. Carolin. – 2012. – Vol. 53, №3. – P. 429-445.

2. Фриз І.В. *Про побудову n-арних квазігруп* // Вісник Донецького національного університету. Сер. А: Природничі науки. – 2015. – №1/2. – С. 89-96.

3. Fryz I.V., Sokhatsky F.M. *Block composition algorithm for constructing orthogonal n-ary operations* // Discrete Math. – 2017. – Vol.340, Iss. 8. – P. 1957-1966.

4. Фриз І.В. *Ортогональні доповнення тернарних операцій* // Вісник Донецького національного університету. Сер. А: Природничі науки. – 2017. – №1/2. – С. 119-127.

5. Fryz I.V.*Orthogonality and retract orthogonality of operations* // Bul. Acad. Ştiinţe Repub. Mold. Mat. – 2018. – №1(86). – P. 24-33.

6. Fryz I.V. *Algorithm for the complement of orthogonal operations* // Comment. Math. Univ. Carolin. – 2018. – Vol.59, №2. – P. 135-151.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА, ЯКІ ЗАСВІДЧУЮТЬ АПРОБАЦІЮ МАТЕРІАЛІВ ДИСЕРТАЦІЇ

1. Sokhatsky F.M., Fryz I.V. *Invertibility of repetition compositions and its connection with orthogonality* // International Mathematical Conference on Quasigroups and Loops “Loops’11” (Trest, Czech Republic, 21-27 July, 2011): Booklet of Abstracts. – Електрон. текст. дані. – URL: http://www.karlin.mff.cuni.cz/∼loops11/ (дата звернення: 20.01.2019).

2. Fryz I.V. *Some construction method of orthogonal n-ary operations and hypercubes* // International Conference dedicated to the 120-th anniversary of Stefan Banach, 17-21 September 2012, Lviv: Abstracts of Reports. – Lviv, 2012. – P. 253.

3. Fryz I.V. *Block composition algorithm for constructing orthogonal multi-ary operations* // International Mathematical Conference on Quasigroups and Loops "Loops'15", 28 June - 04 July 2015, Ohrid: Book of Extended Abstracts. – Skopje, 2015. – P. 53-53.

4. Fryz I.V. *On construction of n-ary quasigroups* // 7 European Congress of Mathematics, 18-22 July 2016, Berlin: Book of Abstracts. – Berlin, 2016. – P. 524.

5. Fryz I.V. *Retract orthogonality and orthogonality of operations and hypercubes* // Fourth Mile High Conference on Nonassociative Mathematics, 29 July - 5 August 2017, Denver: Abstracts of Talks. – Denver, 2017. – P. 9.

6. Fryz I.V. *Orthogonal complements of n-ary operations* // International Conference on Mathematics, Informatics and Information Technologies dedicated to the illustrious scientist Valentin Belousov, 19-21 April 2018, Balti: Communications. – Balti, 2018. – P. 43-44.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

$:=$ – рівність за означенням.

$:\Leftrightarrow$ – рівносильність за означенням.

$\overline{1,n} := \{1,\dots,n\}$.

$\mathbb{Z}_m$ – кільце лишків за модулем m.

S_A – множина всіх перестановок множини A.

S_n – множина всіх перестановок множини $\overline{1,n}$, де n – натуральне число.

$\mathrm{S}'_{n+1} := \{\sigma \in \mathrm{S}_{n+1} \mid (n+1)\sigma = n+1\}$.

$\mathrm{S}^A_{n+1} := \left\{\tau \in \mathrm{S}'_{n+1} \mid (A)\tau = \{1,\dots,|A|\}\right\} \subseteq \mathrm{S}_{n+1}$.

$J_\tau(i) := |\{1\tau,\dots,i\tau\}|$.

$x_i^j := \{x_i, x_{i+1},\dots,x_{j-1},x_j\}$, якщо $i \leqslant j$, і позначає порожню послідовність у іншому випадку.

$\mathrm{Im}\,\tau$ – множина значень відображення τ.

${}^{(i)}f$ – i-те ділення операції f.

${}^{\sigma}f$ – σ-парастроф операції f.

$f_{(\bar{a};\delta)}$ – δ-ретракт n-арної операції f, що визначений послідовністю $\bar{a}$.

f_δ – δ-ретракт n-арної операції f.

$f_{\{i,j\}}$ – бінарний $\{i,j\}$-ретракт n-арної операції f.

$f \underset{m}{\oplus} g$ – m-суперпозиція Мана n-арних операцій g і h.

ВСТУП

Актуальність теми. У комбінаториці, аналогом n-арної операції, що визначена на множині Q, є n-вимірний гіперкуб (n-куб), заповнений елементами множини Q. Оборотній (квазігруповій) n-арній операції відповідає латинський n-куб, тобто такий що кожний його рядок є перестановкою елементів носія. Інакше кажучи, n-арна операція називається оборотною, якщо для всіх $i \in \{1, \ldots, n\}$ кожна її i-та трансляція є підстановкою носія.

Кожне відображення f множини Q^n в множину Q^k однозначно визначає і визначається координатизуючою вибіркою n-арних операцій $(f_1, \ldots, f_k)$. k-вибірка n-арних операцій називається ортогональною, якщо вона координатизує повне відображення Q^n в Q^k, тобто відображення, в якому множини прообразів усіх елементів із Q^k рівнопотужні.

Звідси, зокрема, випливає взаємнооднозначна відповідність між вибірками ортогональних операцій та вибірками ортогональних гіперкубів, тобто гіперкубів, накладання яких визначає гіперкуб, у якому кожна вибірка із Q^k має m^{n-k} поява, де $m := |Q|$. Тому усі твердження сформульовані для операцій можна переформулювати для гіперкубів і навпаки.

Ортогональні n-арні операції вивчалися у працях [19, 20, 22, 32, 93] та інших, ортогональні n-вимірні гіперкуби – у [29, 50, 66, 80, 87] та інших, зокрема великий внесок у розвиток теорії ортогональних n-арних операцій зроблений П. Сирбу [38, 39, 43, 44]. Проте найбільш систематизовано теорія ортогональних операцій і гіперкубів подана в роботах Г.Б. Білявської [63, 69, 70, 83], Г.Б. Білявської і Г.Л. Муллена [64, 67] та Т. Етьєра і Г.Л. Муллена [80].

Теорія квазігруп і ортогональних операцій добре розвинена для бінарних квазігруп і їхнього комбінаторного аналога – латинських квадратів, що систематизовано та описано в [86], [94] і [95]. Однак більшість резуль-

татів складно, а то й неможливо перенести з теорії бінарних на теорію багатомісних операцій. Для прикладу, будь-яка пара бінарних ортогональних квазігруп завжди є сильно ортогональною, але ортогональність n-арних квазігруп не спричинює їхню сильну ортогональність. Навіть саме поняття ортогональності узагальнюється по-різному, і всі ці узагальнення є актуальними, оскільки застосовуються для дослідження різних проблем. Окрім того, у теорії багатомісних функцій існують проблеми, аналогів яким немає в бінарному випадку: роздільність квазігруп, побудова квазігруп з допомогою квазігруп меншої арності, ортогональність ретрактів операцій тощо.

Поняття ортогональності сильно пов'язане із іншими алгебричними об'єктами. Для прикладу, кожна

- n-вибірка ортогональних n-арних операцій на скінченній множині Q еквівалентна підстановці множини Q^n [14, 20];
- k-вибірка ортогональних n-арних лінійних операцій над полем простого порядку еквівалентна тому, що ранг матриці побудованої із коефіцієнтів цих операцій становить k, відповідно n-вибірка ортогональних n-арних лінійних операцій над полем простого порядку еквівалентна оборотності відповідної матриці [80];
- n-вибірка ортогональних n-арних лінійних операцій над полем еквівалентна лінійній незалежності векторів n-вимірного векторного простору над цим полем [80].

Вивчення функційних рівнянь, багатомісних функцій, багатомісних квазігруп потребує розв'язування деяких проблем. Одна із них – це дослідження умов, за яких композиція операцій є оборотною. Відомо, що безповторна композиція квазігруп є квазігрупою, проте повторна композиція навіть двох квазігруп не завжди є оборотною. Для повторної композиції двох бінарних квазігруп цю проблему розв'язав В.Д. Білоусов [14], оборотність повторної композиції двох n-арних операцій досліджувала О.В. Юревич [61], проте проблема, коли довільна повторна композиція операцій є оборотною, залишається відкритою.

У роботі [53] доведено, що будь-яка вибірка сильно ортогональних операцій є еквівалентною максимально дистанційно роздільному (МДР) коду, звідки випливає, що довільна квазігрупа є еквівалентною МДР коду відстані 2. В роботі [80] описаний взаємозв'язок між сильно ортогональними гіперкубами і МДР кодами детальніше, до того ж доведено еквівалентність $(n+s)$-вибірок ортогональних n-арних операцій, де s є цілим числом, і МДР кодів відстані $s+1$. Звідси випливає, що побудова МДР кодів сильно пов'язана із побудовою ортогональних операцій.

Одним із важливих питань, що з'являється під час дослідження ортогональних n-арних операцій, є знаходження доповнень k-вибірки ортогональних n-арних операцій до n-вибірки ортогональних n-арних операцій $(k < n)$. У бінарному випадку цю проблему розв'язано і показано, що операція має ортогональне доповнення тоді і тільки тоді, коли вона є повною, тому кожний метод побудови ортогональної пари для операції є методом доповнення. До того ж, якщо операція є оборотною (квазігруповою), то вона має ортогональне квазігрупове доповнення тоді і тільки тоді, коли вона є допустимою [13, 86].

Для багатомісних операцій Г.Б. Білявська і Г.Л. Муллен [64] довели, що кожна k-вибірка ортогональних n-арних операцій є вбудовною у деяку n-вибірку ортогональних n-арних операцій, звідки випливає, що кожна повна n-арна операція може бути вкладена у деяку n-вибірку ортогональних n-арних операцій. Таким чином, доведено існування ортогонального доповнення для кожної k-вибірки ортогональних n-арних операцій до n-вибірки ортогональних n-арних операцій. Проте методи побудови ортогональних доповнень невідомі, лише у випадку $k = 1$ можна скористатися методом побудови ортогональних операцій, який вони запропонували.

Мета і задачі дослідження. *Метою дослідження* є розвиток теорії ортогональних багатомісних операцій і гіперкубів, зокрема вивчення методів побудови і доповнення ортогональних операцій і гіперкубів, описання залежностей між різними узагальненнями ортогональності бі-

нарних операцій, а також вивчення розкладів оборотних операцій, які пов'язані із ортогональністю.

Задачі дослідження:

- дослідити оборотність довільної композиції двох багатомісних операцій;
- узагальнити рекурсивний алгоритм побудови ортогональних операцій;
- дослідити залежність між ортогональністю вибірки операцій і ортогональністю ретрактів цих операцій;
- знайти і дослідити методи доповнення ортогональних операцій і гіперкубів, дослідити кількість можливих доповнень за цими алгоритмами.

Об'єктом дослідження є скінченні n-арні операції і квазігрупи (оборотні операції), вибірки операцій і їхні комбінаторні властивості: ортогональність та її види. У дисертації розглядаються повні операції, тобто такі, що у відповідному гіперкубі кожний із елементів носія має однакову кількість появ.

Предметом дослідження є методи побудови і доповнення ортогональних операцій, розклади n-арних операцій і квазігруп.

Методи дослідження. У роботі використовуються методи дослідження багатомісних операцій за допомогою суперпозицій, методи теорії квазігруп і комбінаторні методи.

Наукова новизна отриманих результатів. Усі результати дисертаційної роботи є новими і полягають у такому:

- знайдено критерій оборотності довільної композиції двох багатомісних операцій;
- визначено поняття перпендикулярності і показано зв'язок між тривіальною перпендикулярністю та ортогональністю;
- запропоновано інший підхід до визначення ретракту операції та ортогональності ретрактів, описано і доведено алгоритм побудови ретрактно ортогональних операцій;

– описано і доведено блочний рекурсивний алгоритм побудови ортогональних операцій;
– описано і доведено блочний композиційний алгоритм побудови ортогональних операцій із блоків ортогональних операцій меншої арності;
– доведено, що ретрактна ортогональність є необхідною, але не достатньою умовою ортогональності;
– доведено, що для центральних квазігруп над полем простого порядку ретрактна ортогональність є необхідною і достатньою умовою ортогональності;
– описано та доведено алгоритм побудови ортогональних доповнень k-вибірки ортогональних n-арних операцій (гіперкубів) до n-вибірки ортогональних n-арних операцій (гіперкубів);
– отримано деякі оцінки кількості ортогональних доповнень ортогональних операцій, побудовних знайденими алгоритмами, зокрема, нижню і верхню оцінки кількості тривіальних доповнень та нижню оцінку кількості всіх можливих доповнень;
– описано і доведено алгоритм побудови доповнень довільної k-вибірки ортогональних k-арних операцій до n-вибірки ортогональних n-арних операцій, де $n > k$;
– описано методи побудови квазігруп, що мають перпендикулярну пару, і метод побудови пари перпендикулярних квазігруп;
– уточнено отримані результати для тернарних операцій, зокрема описано та класифіковано алгоритми побудови і доповнення ортогональних тернарних операцій.

Практичне значення отриманих результатів. Робота має теоретичний характер. Отримані результати є внеском у теорію неасоціативних структур, скінченних багатомісних дискретних функцій, теорію функційних рівнянь, а також можуть бути застосованими в загальній теорії n-арних операцій і квазігруп, комбінаториці, теорії кодування і шифрування інформації та в інших суміжних галузях математики.

Особистий внесок здобувача. Основні результати, висвітлені в дисертації, отримано здобувачем самостійно. У спільних із науковим керівником працях Ф. М. Сохацькому належать теорема 7, теорема 9, наслідок 10 із [82] та теорема 3 із [90].

Апробація результатів дисертації. Результати дисертаційної роботи доповідалися і обговорювалися на таких конференціях і семінарах:

1. Міжнародна математична конференція з квазігруп та луп "Loops'11" (м. Трешт, Чехія, 21-27 липня 2011 р.).
2. Міжнародна конференція, присвячена 120-річчю з дня народження Стефана Банаха (м. Львів, Україна, 17-21 вересня 2012 р.).
3. Міжнародна математична конференція з квазігруп та луп "Loops'15" (м. Охрід, Македонія, 28 червня - 4 липня 2015 р.).
4. 7 Європейський конгрес математиків (м. Берлін, Німеччина, 18-22 липня 2016 р.).
5. Четверта конференція з неасоціативної математики (м. Денвер, США, 29 липня - 5 серпня 2017 р.).
6. Міжнародна конференція з математики, інформатики та інформаційних технологій, присвячена відомому вченому Валентину Білоусову (м. Бєльці, Молдова, 19-21 квітня 2018 р.).
7. Алгебраїчний семінар Інституту математики НАН України (м. Київ, 30 жовтня 2018 р., керівник – доктор фізико-математичних наук, член-кореспондент НАН України Ю.А. Дрозд).
8. Алгебраїчний семінар Київського національного університету імені Тараса Шевченка (м. Київ, 27 вересня 2018 р., керівники – доктор фізико-математичних наук, член-кореспондент НАН України Ю.А. Дрозд, доктор фізико-математичних наук А.П. Петравчук).

Публікації. Результати дисертаційного дослідження опубліковано у 12 працях, з них 6 – у фахових виданнях із фізико-математичних наук [82, 84, 90, 91, 97, 98], 6 – у матеріалах міжнародних наукових конференцій [78,

81, 85, 89, 92, 96], 4 – у виданнях, включених до міжнародної наукометричної бази “Scopus” [82, 90, 97, 98].

Структура дисертації Дисертація складається з переліку умовних позначень, вступу, п’яти розділів, висновків, списку використаних джерел, що містить 98 найменувань, і додатків. Повний обсяг роботи – 144 сторінки.

РОЗДІЛ 1

n-АРНІ КВАЗІГРУПИ ТА ОРТОГОНАЛЬНІ ОПЕРАЦІЇ

Цей розділ має вступний характер та присвячений ключовим поняттям дослідження: розклади та композиції операцій, ортогональні операції, їхні властивості і побудова.

n-арною функцією (операцією) [18, с. 6], яка визначена на множині Q, є відображення Q^n в Q. Функція, що визначена на скінченій чи нескінченній множині називається квазігруповою або оборотною, якщо вона оборотна по кожній своїй змінній. Вивченню алгебричної теорії n-арних квазігруп поклали початок роботи В.Д. Білоусова та М.Д. Сандіка [12] і В.Д. Білоусова [18].

1.1. Огляд літератури

Одне з питань, яке виникає під час вивчення оборотних функцій – це представлення багатомісної оборотної функції композицією оборотних функцій від меншої кількості змінних. Найбільш вивченими є роздільні квазігрупи, тобто такі, що розкладаються в безповторну композицію квазігруп меншої арності. Зокрема, В.Д. Білоусов [5] вивів критерій розкладу квазігрупової операції на дві квазігрупи, іншими словами, розв'язане рівняння загальної асоціативності, що пізніше було опубліковано з повним доведенням у [9]. Відомо, що безповторна композиція двох квазігруп є квазігрупою, але у скінченному випадку істинним також є обернене твердження. Ф.М. Сохацький [52] описав всі безповторні розклади квазігруп, чим показав, що різні представлення сильно залежних функцій k-значної логіки у вигляді безповторної композиції формул, які відповідають нероздільним функціям, майже однакові. Цим узагальнено відповідний результат А.В. Кузнєцова [6] для двозначної логіки та Л.М. Сосинського [11] для тризначної логіки. А.В. Черьомушкін [56]

показав, що для кожної сильно залежної функції можна визначити однозначно із точністю до визначеного відношення еквівалентності канонічний розклад.

Повторні розклади квазігруп є менш вивченими, проте відомі такі результати: М.М. Глухов [40] показав, що будь-яку багатомісну квазігрупу можна подати як композицію (як повторну так і безповторну) бінарних квазігруп, які ізотопні одній і тій самій квазігрупі, і підстановок. Крім того, Ф.М. Сохацький [45] встановив, що за допомогою безповторної композиції можна побудувати лише тривіальні лупи із властивістю оборотності. Із іншої роботи Ф.М. Сохацького [60] випливає, що між цілком роздільними та нероздільними операціями існує лише схрещена ізотопія максимального типу, тобто ізотопія одна із компонент якої замінена деякою операцією. До того ж, Д.С. Кротов, В.Н. Потапов та П.В. Соколова [74] довели, що для будь-яких $n \geqslant 3$ і $k \geqslant 4$ існує нероздільна n-арна квазігрупа порядку k. Зокрема, Д.С. Кротов та В.Н. Потапов [76] показали, що кожна n-арна квазігрупа порядку 4 є роздільною або напівлінійною, тобто такою, яку можна отримати за допомогою прямого добутку двох n-арних квазігруп порядку 2.

Одним із методів побудови n-арних квазігруп є застосування безповторної композиції, оскільки безповторна композиція n-арної та k-арної квазігруп є $(n + k - 1)$-арною квазігрупою. В.Д. Білоусов [14] і Ф.М. Сохацький [52] показали, що повторна композиція двох квазігруп не завжди є квазігрупою. Для бінарних операцій В.Д. Білоусов [14] знайшов критерій оборотності повторної композиції двох квазігруп. Аналогічні умови для композиції Мана n-арних квазігруп описала О.В. Юревич [61]. Оборотність композиції двох багатомісних квазігруп, які мають не обов'язково однакову арність, вивчається у другому розділі дисертації.

Серед інших методів побудови багатомісних квазігруп відомі такі: використовуючи часткові булеві функції Д.С. Кротов [73] побудував нероздільні багатомісні квазігрупи порядку $4r$ такі, що всі їхні ретракти

отримані фіксуванням однієї змінної є роздільними; за допомогою G-луп Д.С. Кротов, В.Н. Потапов [88] побудували тополінійні латинські гіперкуби порядку $n \geqslant 4$ і за допомогою квадратичних функцій гіперкуби із тією ж властивістю для порядків подільних на квадрат. Крім того існують приклади побудови окремих квазігруп, наприклад, В.І. Оной [42] за допомогою асоціативно-комутативного кільця із одиницею побудував тернарну лупу із властивістю оборотності, яка є нероздільною згідно наслідку 2 теореми 1 із [45].

В теорії бінарних і n-арних операцій цікавими для вивчення є не лише квазігрупи, а й вибірки операцій і квазігруп, зокрема, їхні комбінаторні властивості, такі як ортогональність. Виникнення поняття ортогональності пов'язують з ім'ям Л. Ейлера. Перша задача щодо ортогональності була сформульована ним в 1779 році, яка еквівалентна побудові пари ортогональних латинських квадратів порядку 6 і має назву "задача про 36 офіцерів". Оскільки ця задача не піддавалася розв'язку, Л. Ейлер [1] опублікував у 1782 році гіпотезу про те, що не існує взаємно ортогональних латинських квадратів порядку m для кожного $m = 4k+2$. Для $m = 6$ правильність гіпотези Ейлера доведена Г. Таррі [2] в 1900 році. Проте для інших значень m гіпотезу Ейлера спростували у 1959 році Р. Боуз та С. Шрикхенд [7] і Е. Паркер [8].

Ортогональність n-арних операцій більш вивчена для випадку $n = 2$. Нині глибоко розроблена теорія ортогональних квазігруп і латинських квадратів. Детальний огляд цієї теорії, а також її застосування викладені у книзі [23] і її другому перевиданні [86], у книгах [94] та [95].

Як було зазначено вище В.Д. Білоусов вивчав оборотність повторної композиції двох бінарних квазігруп і показав її зв'язок із ортогональністю квазігруп, а також вивчав ортогональність і сітки [14], парастрофно ортогональні квазігрупи та тотожності, які їх визначають [62]. Дещо раніше опублікована робота К.Т. Фелпса [31] присвячена вивченню парастрофно ортогональних квазігруп. В.О. Щербаков і Г.Л. Муллен [65]

вивчали ортогональні групоїди і квадрати, а також квазігрупи і латинські квадрати, ортогональність квазігрупи до своїх парастрофів. Одне із узагальнень ортогональності бінарних операцій – r-ортогональність або часткова ортогональність вивчали Г.Б. Білявська в [26], [27] (результати ввійшли до книги [46]), С. Колборн і Л. Зу [49], Л. Зу і Г. Занг [54, 55] та інші. Допустимі бінарні квазігрупи (відповідно латинські квадрати, які мають трансверсалі), тобто ті які мають ортогональне квазігрупове доповнення (наявність максимальної кількості трансверсалей гарантує наявність ортогональної пари) вивчала Г.Б. Білявська [36], розгорнутий список робіт присвячених трансверсалям та повним підстановкам міститься в огляді Є. Ванлеса [71], один із методів побудови ортогональних доповнень використовуючи трансверсалі описав Л.Дж. Пейдж [4].

Часто в теорії багатомісних операцій термін "ортогональність" відноситься до декількох понять, які є узагальненнями ортогональності бінарних операцій. В дисертаційній роботі будемо дотримуватися означення ортогональності n-арних операцій із [64], яке є найзагальнішим із них. З іншими підходами до визначення ортогональних багатомісних операцій можна ознайомитися, наприклад, у [53] або [72] та інших.

В теорії ортогональних n-арних операцій у випадку $n > 2$ багато питань залишаються поза увагою, особливо ті, що не мають аналогів у бінарному випадку. До того ж, багато фактів, які виконуються в бінарному випадку не виконуються для операцій більшої арності. Наприклад, відомо, що кожна підстановка на Q^n координатизується ортогональними операціями. Для бінарних операцій ортогональні квазігрупи і сильно ортогональні квазігрупи – це те ж саме. Якщо ж підстановка множини Q^2 координатизується квазігрупами, то обернена до неї підстановка також координатизується квазігрупами. Проте, навіть коли $n = 3$, ортогональні квазігрупи та сильно ортогональні квазігрупи – це нетотожні поняття. Якщо підстановка множини Q^n, $n > 2$, координатизується квазігрупами, то обернена до неї підстановка не обов'язково координатизується квазігру-

пами, а якщо ж підстановка координатизується сильно ортогональними квазігрупами, то обернена до неї підстановка координатизується ортогональними квазігрупами, що не означає сильну ортогональність.

Суттєвий вклад у розвиток загальної теорії ортогональних n-арних операцій та гіперкубів зробили В.Д. Білоусов [32], В.Д. Білоусов і Т. Якубов [22], А.С. Бектєнов [19], А.С. Бектєнов і Т. Якубов [20], П.Н. Сирбу [38, 39, 43], Г.Б. Білявська [63, 69, 70, 83], Г.Б. Білявська і Г.Л. Муллен [64,67] та Т. Етьєр і Г.Л. Муллен [80], а також досліджувалися такі напрямки:

– допустимі n-арні квазігрупи, тобто які можуть бути вкладеними в деяку вибірку ортогональних квазігруп (Г.Б. Білявська і А. Руссу [25] та Г.Б. Білявська і С. Муратхуджаєв [28,30,33], С. Муратхуджаєв [37] та інші);

– сильно ортогональні операції і гіперкуби (Г.Б. Білявська і Г.Л. Муллен [67], Дж.Т. Етьєр і Г.Л. Муллен [80]), і пов'язані із ними структури – мультиквазігрупи (Ж. Чупона, Й. Ужан, З. Стоякович [34, 35] та інші);

– ортогональні гіперкуби (Дж. Аркін, І.Г. Страус [24], Г.Б. Білявська і Г.Л. Муллен [64], Дж.Т. Етьєр і Г.Л. Муллен [80], С.Т. Догерті і Т.А. Щерпанскі [72]);

– методи побудови ортогональних операцій і гіперкубів (Т. Іванс [29], Ф. Лейвін, Г.Л. Муллен, Г. Уітл [50], М. Тренклер [66], Г.Б. Білявська і Г.Л. Муллен [64]);

– зв'язок ортогональних операцій, квазігруп, гіперкубів із кодами (Е. Косусело та інші [53], Г.Л. Муллен і В. Щербаков [58], С.Т. Догерті і Т.А. Щерпанскі [72], Е. Соедармаджі [68], Дж.Т. Етьєр і Г.Л. Муллен [80], В. Ізбаш і П. Сирбу [57] та інші) і розподіляючими секрет схемами (Г.Б. Білявська [75]);

– зв'язок ортогональних операцій, квазігруп, гіперкубів із (t, n, m)-сітками (В.Д. Білоусов [17], А.С. Бектєнов [19], В.Д. Білоусов і А.С. Бектєнов [32], Ф. Лейвін, Г.Л. Муллен, Г. Уітл [50], Г.Л. Муллен і

В.Ч. Шмід [51] та інші).

Одним із найпростіших для дослідження класів операцій є лінійні операції. Кожна лінійна квазігрупа над абелевою групою, тобто T-квазігрупа, є роздільною. А дослідження ортогональності лінійних квазігруп над абелевими групами з попарно комутуючими коефіцієнтами, тобто медіальних квазігруп, зводиться до дослідження оборотності або рангу відповідної матриці. Варто зазначити, що поняття T-квазігрупи введено та вивчено у роботах [15] і [16], їх ще називають центральними квазігрупами, оскільки центральні алгебри в класі квазігруп і є лінійними ізотопами абелевих груп [47].

1.2. Необхідні означення

У цій роботі усі операції розглядатимемо над довільною множиною Q, яку називатимемо базовою або носієм. У більшості випадків розглядатимемо скінченну множину, при цьому будемо зазначати її порядок.

Символом x_i^j будемо позначати послідовність $x_i, x_{i+1}, \dots, x_j$ елементів із Q, якщо $i \leqslant j$, і порожню послідовність у іншому випадку. Вважатимемо, що якщо $i = 1$, то послідовність $x_1, \dots, x_{i-1}$ є порожньою, а у випадку $n = i$ послідовність $x_{i+1}, \dots, x_n$ є порожньою.

Для полегшення запису відповідних термів унарних операцій будемо опускати дужки, тобто $\alpha x := \alpha(x)$.

Нижче нагадаємо необхідні означення із [12] та [18].

n-арна операція f, яка визначена на множині Q, називається i-оборотною, якщо для довільних елементів $a_1, \dots, a_{i-1}$, b, $a_{i+1}, \dots, a_n$ із Q існує єдиний елемент $x \in Q$ такий, що

$$f(a_1, \dots, a_{i-1}, x, a_{i+1}, \dots, a_n) = b. \tag{1.1}$$

Операція f називається оборотною або квазігруповою, якщо вона є i-оборотною для всіх $i \in \overline{1,n} := \{1, \dots, n\}$. При цьому групоїд $(Q; f)$ називається n-арною квазігрупою.

Нехай σ є підстановкою множини $\overline{1,n}$, тоді функція ${}^{\sigma}f$, яка визначена співвідношенням

$${}^{\sigma}f(x_{1\sigma},\dots,x_{n\sigma}) = x_{(n+1)\sigma} :\Longleftrightarrow f(x_1,\dots,x_n) = x_{n+1},$$

називається σ-парастрофом операції f, зокрема σ-парастроф називається

1) i-діленням, якщо $\sigma = (i, n+1)$;

2) головним (комутуванням), якщо $(n+1)\sigma = n+1$.

i-ділення операції f позначатимемо ${}^{(i)}f$.

Відповідно до означення, головний σ-парастроф можна визначити за допомогою однією з рівностей:

$${}^{\sigma}f(x_{1\sigma},\dots,x_{n\sigma}) = f(x_1,\dots,x_n) \tag{1.2}$$

або

$${}^{\sigma}f(x_1,\dots,x_n) = f(x_{1\sigma^{-1}},\dots,x_{n\sigma^{-1}}). \tag{1.3}$$

У бінарному випадку σ є перестановкою множини $\{1,2,3\}$, тобто $\mathrm{S}_3 = \{\iota, s, \ell, r, s\ell, sr\}$, де ι позначає тотожню перестановку, $s := (12)$, $\ell := (13)$, $r := (23)$, $s\ell := (12)(13)$, $sr := (12)(23)$. До того ж, виконуються рівності

$$\ell s = r\ell, \qquad rs = \ell r, \qquad \ell r\ell = r\ell r = s.$$

Таким чином, s-парастроф або комутування операції f визначається співвідношенням:

$${}^{s}f(x_2,x_1) = x_3 :\Longleftrightarrow f(x_1,x_2) = x_3;$$

ліве ділення операції f визначається співвідношенням:

$${}^{\ell}f(x_3,x_2) = x_1 :\Longleftrightarrow f(x_1,x_2) = x_3;$$

праве ділення операції f визначається співвідношенням:

$${}^{r}f(x_1,x_3) = x_2 :\Longleftrightarrow f(x_1,x_2) = x_3;$$

комутування лівого ділення операції f визначається співвідношенням:

$${}^{s\ell}f(x_2,x_3) = x_1 :\Longleftrightarrow f(x_1,x_2) = x_3;$$

комутування правого ділення операції f визначається співвідношенням:

$$^{sr}f(x_3, x_1) = x_2 :\Longleftrightarrow f(x_1, x_2) = x_3.$$

Якщо f є квазігрупою, то ^{s}f, $^{\ell}f$, ^{r}f, $^{s\ell}f$ і ^{sr}f є також квазігрупами.

Усі перестановки множини індексів $\overline{1, n+1}$ n-арної операції утворюють симетричну групу S_{n+1}. Нехай

$$\mathrm{S}'_{n+1} := \{\sigma \in \mathrm{S}_{n+1} \mid (n+1)\sigma = n+1\} \simeq \mathrm{S}_n.$$

Очевидно, що S'_{n+1} є підгрупою симетричної групи S_{n+1}.

Вибірка операцій $^{\sigma}f_1, \ldots, {}^{\sigma}f_n$ називається σ-парастрофною до вибірки $f_1, \ldots, f_n$, якщо $\sigma \in \mathrm{S}_{n+1}$.

Нехай f є n-арною операцією на множині Q. Для довільних $a_1, \ldots, a_{i-1}$, $a_{i+1}, \ldots, a_n \in Q$ відображення α_i, яке визначається рівністю

$$\alpha_i x_i := f(a_1, \ldots, a_{i-1}, x_i, a_{i+1}, \ldots, a_n),$$

називається i-тою трансляцією операції f. Якщо f є i-оборотною, то кожна i-та трансляція є підстановкою множини Q. Таким чином, можна сформулювати ще одне означення оборотної (квазігрупової) операції: n-арна операція f називається i-оборотною, якщо кожна її i-та трансляція є підстановкою множини Q; n-арна операція f називається оборотною, якщо всі її трансляції є підстановками.

n-арна операція g називається ізотопом n-арної операції f, якщо існує вибірка підстановок $(\alpha_1, \ldots, \alpha_n, \alpha)$ множини Q, така, що виконується рівність

$$g(x_1, \ldots, x_n) = \alpha^{-1} f(\alpha_1 x_1, \ldots, \alpha_n x_n).$$

Вибірка $(\alpha_1, \ldots, \alpha_n, \alpha)$ називається ізотопізмом, і якщо $f = g$, то ця вибірка називається автотопізмом. Ізотоп, який утворений вибіркою

– $(\underbrace{\iota, \ldots, \iota}_{i-1}, \alpha_i, \underbrace{\iota, \ldots, \iota}_{n-i}, \iota)$, називається i-тим крученням операції g;

– $(\underbrace{\iota, \ldots, \iota}_{n}, \alpha)$, називається середнім крученням операції g.

У бінарному випадку ізотопи, які визначаються трійками (α, ι, ι), (ι, β, ι) і (ι, ι, γ), називаються відповідно лівим, правим і середнім крученнями, де α, β, γ – підстановки базової множини.

Операція $g \underset{i}{\oplus} h$ називається i-им множенням (суперпозиція Мана) двох n-арних операцій g і h та визначається рівністю

$$(g \underset{i}{\oplus} h)(x_1, \ldots, x_n) := g(x_1, \ldots, x_{i-1}, h(x_1, \ldots, x_n), x_{i+1}, \ldots, x_n).$$

Для бінарних операцій 1-множення, яке називатимемо лівим множенням, і 2-множення, яке називатимемо правим множенням, позначатимемо $\underset{\ell}{\oplus}$ і $\underset{r}{\oplus}$ відповідно.

Операція $g[h_1, \ldots, h_n]$, яка визначається рівністю

$$g[h_1, \ldots, h_n](x_1, \ldots, x_n) := g(h_1(x_1, \ldots, x_n), \ldots, h_n(x_1, \ldots, x_n)),$$

називається суперпозицією Менгера операцій g і $h_1, \ldots, h_n$ (див. наприклад [59]). Алгебричні властивості суперпозицій Менгера описані у книзі В.С. Трохименка і В. Дудека [79].

Нехай $\{i_1, \ldots, i_k\}$, $\{j_1, \ldots, j_s\} \subseteq \overline{1, n}$. Композиція операцій g і h, яка визначається рівністю

$$f(x_1, \ldots, x_n) := g(x_{i_1}, \ldots, x_{i_{m-1}}, h(x_{j_1}, \ldots, x_{j_s}), x_{i_{m+1}}, \ldots, x_{i_n}), \qquad (1.4)$$

де g і h – принамні бінарні, називається

- безповторною [18, с. 95], якщо $\{i_1, \ldots, i_k\} \cap \{j_1, \ldots, j_s\} = \varnothing$;
- повторною, якщо $\{i_1, \ldots, i_k\} \cap \{j_1, \ldots, j_s\} \neq \varnothing$.

n-арна квазігрупа f називається роздільною [6], якщо вона має безповторний розклад. В іншому випадку квазігрупа називається нероздільною.

Щоб нагадати означення центральної квазігрупи наведемо деякі означення із [47, 48].

Багатомісна квазігрупа (Q, f) називається ізотопом бінарної групи $(Q; +)$, якщо $(Q; f)$ є ізотопною до $(Q; d)$, де $d(x_1, \ldots, x_n) := x_1 + \cdots + x_n$.

До того ж, якщо всі компоненти ізотопізму є лінійними над $(Q;+)$, то $(Q;f)$ називається лінійною на $(Q;+)$. Лінійне перетворення групи визначається як композиція її трансляцій та автоморфізмів.

Операція, яка визначається рівністю

$$g(x_1,\dots,x_n)=\alpha_1x_1+\dots+\alpha_nx_n+a, \tag{1.5}$$

де $a\in Q$ і $\alpha_1,\dots,\alpha_n$ – лінійні перетворення групи $(Q;+)$, називається лінійною.

Лінійна n-арна квазігрупа (Q,g) над абелевою групою $(Q;+)$ із розкладом (1.5), де $\alpha_1,\dots,\alpha_n$ – автоморфізми групи $(Q;+)$, $a\in Q$, називається T-квазігрупою або центральною квазігрупою. Цей факт для бінарних квазігруп був встановлений у [58]. Якщо автоморфізми розкладу попарно комутують, то квазігрупа називається медіальною [18, с. 47].

$\underbrace{m\times m\times\dots\times m}_{n}$-вимірна таблиця елементів множини Q, де $|Q|=m$, називається n-вимірним гіперкубом або n-кубом (див. [50]) порядку m. 1-куб називається лінією, 2-куб називається квадратом.

Як було зазначено у [72] гіперкуб можна розглядати як множину його підгіперкубів, зокрема, його i-ліній. i-лінією називається підгіперкуб, який отриманий із заданого n-куба фіксуванням усіх координат, окрім i. Для кожного $i\in\overline{1,n}$ існує точно m^{n-1} i-ліній, тобто всього існує nm^{n-1}, які розподіляються в n множин по m^{n-1} ліній. Наприклад, у квадраті стовпці є 1-лініями, а рядки є 2-лініями. Квадрат порядку m має m рядків і m стовпців. У кубі 1-лінії отримуються, коли друга і третя координати є зафіксованими, 2-лінії – коли перша і третя координати є зафіксованими, і 3-лінії – коли перша і друга координати є зафіксованими. Для кожного $i\in\{1,2,3\}$ є m^2 i-ліній.

Якщо i-лінія є перестановкою множини $\overline{1,n}$, то ця i-лінія називається латинською. Якщо для деякого $i\in\overline{1,n}$ кожна з i-ліній гіперкуба є латинською, то відповідна до нього операція є i-оборотною. n-куб називається латинським, якщо для всіх $i\in\overline{1,n}$ кожна його i-лінія є латинською, тобто кожен із його рядків є перестановкою множини Q.

Кожній n-арній операції відповідає n-вимірний гіперкуб, а кожній бінарній операції відповідає квадрат. Кожній n-арній квазігрупі відповідає n-вимірний латинський гіперкуб, кожній бінарній операції відповідає латинський квадрат (див. наприклад [64]).

n-куб називатимемо σ-транспонованим до заданого n-куба, якщо його напрямки (координати) переставлені відповідно до перестановки $\sigma \in \mathrm{S}_n$.

Зазначимо, що головно парастрофним операціям відповідають транспоновані гіперкуби за відповідними напрямками. У бінарному випадку є лише один головний парастроф – комутування, тому квадрат і транспонований до нього є s-парастрофними.

Ізотопним операціям відповідають гіперкуби, які відрізняються перестановкою рядків у межах кожної координати та перестановкою елементів. Наприклад, для бінарних операцій перша компонента ізотопізму переставляє рядки, друга – стовпці, а третя – елементи квадрата.

1.3. Ортогональні бінарні операції і квадрати

Дві бінарні операції g і h, які визначені на Q, називаються ортогональними (див. наприклад [13, с. 117]), якщо для довільних $a, b \in Q$ система $\{g(x;y) = a,\ \ h(x;y) = b\}$ має єдиний розв'язок. Цей факт позначається символом $g \perp h$.

Твердження 1.1 (Р.С. Боуз, С.С. Шрікхенд, Е.Т. Паркер [10]). *Існують пари ортогональних квазігруп довільного порядку m, крім $m = 2, 6$.*

Теорема 1.1 (Г.Б. Білявська [63]). *Нехай g і h є бінарними квазігрупами. Тоді*

$$g \underset{r}{\oplus} h \text{ є оборотною} \Leftrightarrow g \perp^r h.$$

З цієї теореми випливає як наслідок критерій В.Д. Білоусова [14, лема 2] для скінченних бінарних квазігруп. Аналогічне твердження виконується і для лівої суперпозиції Мана.

Теорема 1.2. *Нехай g і h є бінарними квазігрупами. Тоді*

$$g \underset{\ell}{\oplus} h \text{ є оборотною} \Leftrightarrow g \perp^{\ell} h.$$

Кажуть, що дві підстановки α і β множини Q є неперехресними, якщо для всіх $a \in Q$ виконується нерівність $\alpha a \neq \beta a$. Дві підстановки α і β множини Q називатимемо майже неперехресними, якщо існує точно один елемент $a \in Q$, для якого виконується умова $\alpha a = \beta a$.

Підстановка φ множини Q називається повною [3] для квазігрупи h, якщо відображення φ', яке визначається рівністю

$$\varphi' x := h(x, \varphi x),$$

також є підстановкою множини Q.

Термін "допустимість" був введений Л.Дж. Пейджом у [4] для груп, які мають повну підстановку. Аналогічно, бінарна квазігрупа називається допустимою [13, с. 115], якщо вона має принаймні одну повну підстановку.

Тут ми будемо розрізняти "допустимість" і "цілковита допустимість" для зручності викладу результатів підрозділу 5.1. Говоритимемо, що квазігрупа порядку m є цілком допустимою, якщо вона має m повних попарно неперехресних підстановок, інакше кажучи, має повний набір повних попарно неперехресних підстановок.

Твердження 1.2 (В.Д. Білоусов [13, с. 117])**.** *Бінарна квазігрупа $(Q; \cdot)$, яка ізотопна допустимій квазігрупі $(Q; \circ)$, є допустимою.*

Теорема 1.3 (В.Д. Білоусов [13, с. 117])**.** *Квазігрупа має ортогональне квазігрупове доповнення тоді і тільки тоді, коли вона є цілком допустимою.*

Нижче наведемо комбінаторні означення деяких термінів, які систематизовано та викладено в [86].

Квадрат заповнений елементами множини Q називається латинським, якщо кожен рядок і кожен стовпець цього квадрата є перестановкою множини Q. Кожній бінарній операції на множині Q відповідає квадрат, який

є внутрішньою частиною її таблиці Келі, а квазігрупі – латинський квадрат. Ортогональним операціям відповідають ортогональні квадрати, тобто квадрати, відносно накладання яких всі утворені пари різні.

Діагоналлю латинського квадрата називається сукупність комірок $(x, \varphi x)$, узятих по одній із кожного рядка і кожного стовпця, яка містить елементи $f(x, \varphi x)$, тобто φ є деякою підстановкою множини Q. Трансверсаллю латинського квадрата називається діагональ, всі елементи якої є різними, тобто φ є повною для f. Відомо, що кожній повній підстановці квазігрупи відповідає трансверсаль відповідного латинського квадрата. Таким чином, квазігрупа порядку m є цілком допустимою, якщо відповідний латинський квадрат має m попарно неперехресних трансверсалей.

Теорема 1.4 (А.Д. Кідвел, Дж. Денеш [86, с. 160]). *Латинський квадрат порядку m має ортогональне доповнення тоді і тільки тоді коли він має m попарно неперехресних трансверсалей.*

Л.Дж. Пейдж запропонував метод побудови квазігрупи, яка ортогональна заданій, використовуючи повні підстановки.

Теорема 1.5 (Л.Дж. Пейдж [4]). *Нехай f є цілком допустимою квазігрупою, яка визначена на множині Q порядку m, та φ_1, φ_2, ..., φ_m є відповідним повним набором повних попарно неперехресних підстановок. Побудуємо латинський квадрат методом розміщення елемента $a_j \in Q$ в комірки $\big(k, \varphi_j(k)\big)$ для всіх $j \in \overline{1,m}$ і всіх $k \in Q$. Тоді отриманий латинський квадрат є ортогональним до латинського квадрата відповідного квазігрупі f. Цим методом можна побудувати всі квазігрупи, які є ортогональними до f.*

1.4. Ортогональні багатомісні операції і гіперкуби

На противагу бінарним операціям для більшої арності існує декілька нееквівалентних узагальнень ортогональності, два з яких наведено у цьому

розділі (ортогональність і сильна ортогональність) і ще одне введено у підрозділі 2.1 (перпендикулярність).

Означення 1.1 (Г.Б. Білявська, Г.Л. Муллен [64]). *Якщо $k \leqslant n$, то k-вибірка n-арних операцій $f_1, \ldots, f_k$, які визначені на множині Q порядку m, називається ортогональною, якщо для будь-яких $b_1, \ldots, b_k \in Q$ система*

$$\begin{cases} f_1(x_1, \ldots, x_n) = b_1, \\ \ldots\ldots\ldots\ldots\ldots \\ f_k(x_1, \ldots, x_n) = b_k \end{cases}$$

має точно m^{n-k} розв'язків, зокрема має єдиний розв'язок, якщо $k = n$.

Означення ортогональності для випадку $k = n$ вивчали А.С. Бектєнов і Т. Якубов у [20]. Автори показали, що кожному перетворенню θ множини Q^n ставиться у відповідність єдина n-ка операцій $f_1, \ldots, f_n$, тобто виконується співвідношення:

$$\overline{\theta}(x_1, \ldots, x_n) = (f_1(x_1, \ldots, x_n), \ldots, f_n(x_1, \ldots, x_n)).$$

До того ж, операції $f_1, \ldots, f_n$ є ортогональними тоді і тільки тоді, коли перетворення $\overline{\theta} = (f_1, \ldots, f_n)$ є підстановкою множини Q^n. Іншими словами, наведене співвідношення визначає взаємнооднозначну відповідність між множиною всіх вибірок ортогональних операцій визначених на Q і множиною всіх перестановок множини Q^n. Отже, вибірка ортогональних операцій $\{f_1, \ldots, f_n\}$ визначає $n!$ підстановок множини Q^n. Таким чином, $f_1, \ldots, f_k$ координатизують підстановку.

Звідси випливає таке означення:

Означення 1.2 (А.С. Бектєнов, Т. Якубов [20]). *n-вибірка n-арних операцій $f_1, \ldots, f_n$, які визначені на множині Q, називається ортогональною, якщо вона координатизує підстановку Q^n.*

Г.Б. Білявська і Г.Л. Муллен [64] описали зв'язок між відображеннями $\alpha : Q^n \to Q^k$, де $k \leqslant n$, та ортогональними операціями. Нехай $m := |Q|$. При відображенні α кожній n-вибірці елементів із множини Q ставиться у

відповідність k-вибірка елементів із множини Q, тобто

$$\alpha(a_1, \ldots, a_n) = (b_1, \ldots, b_k).$$

Це означає, що існують операції $f_1, \ldots, f_k$ такі, що

$$\alpha(a_1, \ldots, a_n) = \alpha\left(f_1(a_1, \ldots, a_n), \ldots, f_k(a_1, \ldots, a_n)\right),$$

про які будемо говорити, що вони координатизують α. Із наведених у [64] міркувань випливає, що якщо кожна вибірка $(b_1, \ldots, b_k) \in Q^n$ має m^{n-k} прообразів відносно α, де прообразом є послідовність виду $(x_1, \ldots, x_n)$, то операції $f_1, \ldots, f_k$ є ортогональними. Якщо $k = n$, то отримуємо означення 1.2.

Якщо $k = 1$, то поняття ортогональності збігається із поняттям повноти операції. Нижче наведемо означення повної операції і селектора із [21].

Скінченна операція f_1 порядку m називається повною, якщо для будь-якого $a \in Q$ рівняння

$$f_1(x_1, \ldots, x_n) = a$$

має точно m^{n-1} розв'язків.

Операцію e_i називають i-тим селектором або i-тою тотожньою операцією, якщо вона визначається рівністю

$$e_i(x_1, \ldots, x_n) := x_i.$$

Існує інше означення повної операції: n-арна операція f, яка визначена на множині Q, називається повною , якщо існує підстановка $\overline{\varphi}$ на Q^n, така що $f = e_1\overline{\varphi}$.

Нехай $\overline{\theta} := (f_1, \ldots, f_n)$ є підстановкою множини Q^n і нехай $(g_1, \ldots, g_n) := \overline{\theta}^{-1}$, тоді рівність $\overline{\theta}^{-1}\overline{\theta} = \iota$ означає, що

$$\begin{cases} g_1(f_1(x_1, \ldots, x_n), \ldots, f_n(x_1, \ldots, x_n)) = x_1, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ g_n(f_1(x_1, \ldots, x_n), \ldots, f_n(x_1, \ldots, x_n)) = x_n. \end{cases} \tag{1.6}$$

Теорема 1.6 (П.Н. Сирбу [38]). *n-арні операції $f_1, \ldots, f_n$ є ортогональними тоді і тільки тоді, коли існують n-арні операції $g_1, \ldots, g_n$ такі, що виконуються рівності* (1.6).

Отже, тотожності (1.6) гарантують ортогональність операцій $f_1, \ldots, f_n$.

Означення 1.3 (А.С. Бектєнов, Т. Якубов [20]). *Якщо $t > n$, то t-вибірка n-арних операцій $f_1, \ldots, f_t$ називається ортогональною, якщо кожна її n-підвибірка є ортогональною.*

У кожній вибірці ортогональних операцій усі операції є попарно різними і кожні два набори, які відрізняються лише порядком операцій, є ортогональними одночасно. Саме тому довільну вибірку ортогональних операцій із множини $\{(f_{1\sigma}, \ldots, f_{n\sigma}) \mid \sigma \in S_n\}$ будемо позначати $\{f_1, \ldots, f_n\}$.

Означення 1.4 (Г.Б. Білявська, Г.Л. Муллен [64]). *k-вибірка n-вимірних гіперкубів ($k < n$), які визначені на множині Q порядку m, називається ортогональною, якщо відносно їхнього накладання в результуючому гіперкубі кожна вибірка із Q^k має m^{n-k} появ.*

Зауважимо, що при $k = n$ в результуючому кубі кожна n-вибірка має точно одну появу, а при $k = 1$ результуючий гіперкуб збігається з даним і в ньому кожний елемент має m^{n-1} появ, тобто цей гіперкуб відповідає повній операції і також називається повним.

Означення 1.5 (Г.Б. Білявська, Г.Л.Муллен [64]). *s-вибірка n-арних операцій $f_1, \ldots, f_s$ ($s > n$) називається k-кратно ортогональною, якщо кожна її k-підвибірка $f_{i_1}, \ldots, f_{i_k}$ різних операцій є ортогональною.*

Теорема 1.7 (Г.Б. Білявська, Г.Л. Муллен [64]). *Якщо n-арні операції $f_1, \ldots, f_k$ ($k > n$) є k-кратно ортогональними, то $f_1, \ldots, f_k$ є ℓ-кратно ортогональними для всіх ℓ, таких, що $1 \leqslant \ell \leqslant k$.*

Отже, будь-яка підвибірка вибірки ортогональних операцій є також ортогональною.

Теорема 1.8 (П.Н. Сирбу [64, с. 32]). *Нехай $f_1, \ldots, f_k$ є n-арними операціями визначеними на множині Q ($k \leqslant n$) і $T = (\alpha_1, \ldots, \alpha_n, \alpha)$, де $\alpha_1, \ldots, \alpha_n, \alpha$ є підстановками множини Q. Вибірка $f_1, \ldots, f_k$ є ортогональною тоді і тільки тоді, коли вибірка $Tf_1, \ldots, Tf_k$ є ортогональною.*

Теорема 1.9 (П.Н. Сирбу [38, с. 33]). *Нехай $f_1, \ldots, f_k$ є n-арними операціями визначеними на множині Q ($k \leqslant n$) і $\sigma \in \mathrm{S}_n$. Вибірка $f_1, \ldots, f_k$ є ортогональною тоді і тільки тоді, коли вибірка ${}^{\sigma}f_1, \ldots, {}^{\sigma}f_k$ є ортогональною.*

Теорема 1.10 (Г.Б. Білявська, Г.Л. Муллен [64]). *Будь-яка k-вибірка ортогональних n-арних операцій ($k < n$) є вбудовною у деяку n-вибірку ортогональних n-арних операцій.*

Це означає, що для будь-якої k-вибірки ортогональних n-арних операцій існує доповнення до n-вибірки ортогональних n-арних операцій. Будь-яка повна n-арна операція є вбудовною в деяку n-вибірку ортогональних n-арних операцій. У бінарному випадку задача знаходження ортогонального доповнення зводиться до побудови ортогональної пари.

Теорема 1.11 (Г.Б. Білявська, Г.Л. Муллен [64]). *n-арна операція може бути вбудовною в ортогональну n-вибірку операцій тоді і тільки тоді, коли вона є повною.*

Для довільного $i \in \overline{1,n}$ операція e_i є повною. До того ж, n-арна операція f є i-оборотною тоді і тільки тоді, коли $e_1, \ldots, e_{i-1}, f, e_{i+1}, \ldots, e_n$ є ортогональними та є оборотною (квазігруповою) тоді і тільки тоді коли цей набір операцій є ортогональним для довільного $i \in \overline{1,n}$ [20].

Означення 1.6 (А.С. Бектєнов, Т. Якубов [20]). *Вибірка n-арних операцій $f_1, \ldots, f_k$ ($k \geqslant 1$) називається сильно ортогональною, якщо вибірка $f_1, \ldots, f_k, e_1, \ldots, e_n$ є ортогональною.*

Це означає, що кожна із операцій сильно ортогональної вибірки є квазігрупою. У бінарному випадку ортогональність квазігруп та сильна ортогональність квазігруп збігаються.

Означення 1.7 (Дж.Т. Етьєр, Г.Л. Муллен [80]). *r-вибірка n-кубів порядку m називається сильно ортогональною, якщо відносно накладання відповідних j-підкубів будь-яких j гіперкубів із цієї вибірки, де $1 \leqslant j \leqslant \min(n, r)$, кожна впорядкована j-вибірка зустрічається точно один раз.*

У роботах В.Д. Білоусова [14] для бінарного випадку та А.С. Бектєнова і Т. Якубова [20] для арності n доведено, що n-вибірка n-арних операцій $g_1, \ldots, g_n$ є ортогональною, якщо

$$(g_1, \ldots, g_n) = \bar{\varphi}(f_1, \ldots, f_n),$$

де $f_1, \ldots, f_n$ є ортогональними n-арними операціями і $\bar{\varphi}$ є підстановкою множини Q^n. Таким чином, ще одну n-вибірку ортогональних n-арних операцій можна отримати за допомогою суперпозиції Менгера двох n-вибірок ортогональних n-арних операцій, оскільки координатизуючі операції підстановки $\bar{\varphi}$ є ортогональними (див. означення 1.2).

Т. Іванс [29] запропонував метод побудови ортогональних латинських гіперкубів за допомогою двох вибірок ортогональних латинських гіперкубів меншої розмірності, що на мові операцій означає:

Теорема 1.12. *Нехай $h_1, \ldots, h_\ell$ і $g_1, \ldots, g_k$ є вибірками ортогональних ℓ-арних і k-арних квазігруп на множині $\{1, 2, \ldots, n\}$ і нехай $n = \ell + k - 1$. Вибірка n-арних операцій f_{ij}, $i = 1, \ldots, \ell$, $j = 1, \ldots, k$, де*

$$f_{ij}(x_1, \ldots, x_n) := h_i(x_1, \ldots, x_{\ell-1}, g_j(x_\ell, \ldots, x_n)),$$

містить $k\ell^{k-1}$ n-вибірок ортогональних n-арних квазігруп.

М. Тренклер [66], для доведення існування ортогональних латинських гіперкубів порядку n, $n \neq 2, 6$, використав метод побудови ортогональних латинських гіперкубів за допомогою двох ортогональних латинських квадратів. Сформулюємо тут його мовою операцій.

Теорема 1.13 (М. Тренклер [66])**.** *Нехай f і h є ортогональними бінарними квазігрупами. n-арні операції g_i, $i = 1, \ldots, n$, які визначаються рівностями*

$$g_i(x_1^n) = f(x_1, f(x_2, \ldots, f(x_{i-1}, h(x_i, \ldots, h(x_{n-2}, h(x_{n-1}, x_n)) \ldots)) \ldots)),$$

є ортогональними квазігрупами.

Г.Б. Білявська і Г.Л.Муллен [64] запропонували інший підхід до побудови ортогональних операцій, який не передбачає заданої вибірки орто-

гональних операцій. Згідно з їхнім алгоритмом, кожна наступна операція будується рекурсивно за допомогою нової операції та всіх попередньо визначених операцій.

Теорема 1.14 (Г.Б. Білявська, Г.Л. Муллен [64]). *Нехай f_i є $(n-i+1)$-оборотною n-арною операцією для всіх $i \in \overline{1,n}$. Рекурсивно визначена вибірка операцій $g_1, \ldots, g_n$ за допомогою*

$$\begin{cases} g_1(x_1^n) = f_1(x_1^n), \\ g_2(x_1^n) = f_2(x_1^{n-1}, g_1(x_1^n)), \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ g_i(x_1^n) = f_{i-1}(x_1^{n-i+1}, g_1(x_1^n), \ldots, g_{i-1}(x_1^n)), \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ g_n(x_1^n) = f_n(x_n, g_1(x_1^n), \ldots, g_{n-1}(x_1^n)). \end{cases} \tag{1.7}$$

є ортогональною.

У роботі [93] описані інші можливі модифікації цього алгоритму, які випливають із блочного рекурсивного алгоритму, описаного в розділі 3. А також авторами запропонований метод побудови $(n+1)$-вибірки ортогональних n-арних операцій.

РОЗДІЛ 2

ОБОРОТНІСТЬ КОМПОЗИЦІЇ ДВОХ БАГАТОМІСНИХ ОПЕРАЦІЙ

Для бінарних операцій умови оборотності повторної композиції двох операцій знайдені В.Д. Білоусовим [14], для n-арних операцій, які є композицією двох n-арних операцій, аналогічні умови знайдені О.В. Юревич у [61]. Для знаходження аналогічних умов для багатомісних операцій, які розкладаються в повторну композицію двох операцій не обов'язково однакової арності, у цьому розділі вводиться поняття перпендикулярності, яке є узагальненням поняття ортогональності для бінарних операцій і є спеціальним видом ортогональності багатомісних операцій.

2.1. Перпендикулярність операцій

2.1.1. Оборотність композиції двох багатомісних операцій

У бінарному випадку теореми 1.1 і 1.2 спричинюють твердження:

$$g \underset{r}{\oplus} {}^s h \text{ є оборотною} \Leftrightarrow g \perp^{rs} h, \qquad g \underset{\ell}{\oplus} {}^s h \text{ є оборотною} \Leftrightarrow g \perp^{\ell s} h.$$

Нехай τ є частковим ін'єктивним перетворенням множини $\overline{1,n}$ і нехай $\operatorname{Im}\tau$ позначає множину значень перетворення τ. Якщо τ є повним перетворенням, то τ є перестановкою множини $\overline{1,n}$. Зазначимо, що a_u позначає порожній символ, якщо u є порожнім, тобто якщо для деякого $k \in \overline{1,n}$ $k\tau$ не існує, то $a_{k\tau}$ є порожнім символом.

Нехай n-арна операція f є композицією операцій g і h. Тоді існують часткові ін'єктивні перетворення τ і υ множини $\overline{1,n}$ такі, що (1.4) можна подати у вигляді

$$f(x_1,\dots,x_n) = g(x_{1\tau},\dots,x_{(m\tau^{-1}-1)\tau}, h(x_{1\upsilon},\dots,x_{n\upsilon}), x_{(m\tau^{-1}+1)\tau},\dots,x_{n\tau}), \tag{2.1}$$

де $m \in \operatorname{Im}\tau$.

Введемо позначення

$$J_\tau(i) := |\{1\tau, \ldots, i\tau\}|, \quad i = 1, \ldots, n.$$

Визначимо поняття перпендикулярності, яке є одним із узагальнень ортогональності бінарних операцій, і узагальнює поняття i-ортогональності із [61]. Для цього введемо допоміжне означення:

Означення 2.1. *Нехай τ і υ є довільними частковими ін'єктивними перетвореннями множини $\overline{1,n}$ і $\operatorname{Im}\tau \cup \operatorname{Im}\upsilon = \overline{1,n}$. Тоді пару бінарних операцій називатимемо (τ,υ)-відповідними $\{m;p\}$-ретрактами операцій g і h, якщо вони визначаються термами, отриманими із*

$$g(x_{1\tau}, \ldots, x_{n\tau}), \qquad h(x_{1\upsilon}, \ldots, x_{n\upsilon})$$

таким чином: усі змінні термів замінюються деякими елементами із Q, окрім x_m і x_p, де $p \neq m$; зокрема, якщо змінна зустрічається в обох термах, то вона замінюється тим самим елементом.

Означення 2.2. *Нехай τ і υ є довільними частковими ін'єктивними перетвореннями множини $\overline{1,n}$, $\operatorname{Im}\tau \cup \operatorname{Im}\upsilon = \overline{1,n}$ і $m \in (\operatorname{Im}\tau \cap \operatorname{Im}\upsilon)$. Операції g і h називатимемо перпендикулярними типу $(\tau,\upsilon;m)$, якщо для всіх $p \in (\operatorname{Im}\tau \cap \operatorname{Im}\upsilon)\backslash\{m\}$ кожна пара (τ,υ)-відповідних $\{m;p\}$-ретрактів є ортогональною.*

Тип перпендикулярності називається максимальним, якщо τ і υ є повними перетвореннями, тобто обидві операції мають однакову арність. Частинний випадок даного поняття, а саме коли $\tau = \upsilon = \iota$, розглянутий О.В. Юревич у [61].

Нехай (2.1) є істинною. Якщо $i \notin \operatorname{Im}\tau \cup \operatorname{Im}\upsilon$, тоді $x_{i\tau}$ і $x_{i\upsilon}$ є порожніми символами, то операція f не може бути i-оборотною. Отже, для знаходження критерію i-оборотності операції f достатньо розглянути три різні випадки:

$$i \in \operatorname{Im}\tau \backslash \operatorname{Im}\upsilon, \quad i \in \operatorname{Im}\upsilon \backslash \operatorname{Im}\tau, \quad i \in (\operatorname{Im}\upsilon \cap \operatorname{Im}\tau)\backslash\{m\}.$$

Теорема 2.1. *Нехай τ і υ є довільними частковими ін'єктивними перетвореннями множини $\overline{1,n}$ і нехай* (2.1) *виконується. Нижче наведені твердження є істинними:*

1) якщо h є $J_\upsilon(m)$-оборотною та $i \in \operatorname{Im}\tau \setminus \operatorname{Im}\upsilon$, то i-оборотність операції f еквівалентна $J_\tau(i)$-оборотності операції g;

2) якщо g є $J_\tau(m)$-оборотною та $i \in \operatorname{Im}\upsilon \setminus \operatorname{Im}\tau$, то i-оборотність операції f еквівалентна $J_\upsilon(i)$-оборотності операції h;

3) якщо h є $J_\upsilon(m)$-оборотною та $i \in (\operatorname{Im}\tau \cap \operatorname{Im}\upsilon)\setminus\{m\}$, то i-оборотність операції f еквівалентна ортогональності (τ,υ)-відповідних $\{m,i\}$-ретрактів операцій g і ${}^{(J_\upsilon(m))}h$, де ${}^{(J_\upsilon(m))}h$ позначає $J_\upsilon(m)$-ділення операції h.

Доведення. Нехай припущення п. 1) істинні. Оскільки виконується (2.1), то рівняння (1.1) є еквівалентним рівнянню

$$g(a_{1\tau},\dots,a_{(i\tau^{-1}-1)\tau},x,a_{(i\tau^{-1}+1)\tau},\dots,a_{(m\tau^{-1}-1)\tau}, h(a_{1\upsilon},\dots,a_{n\upsilon}),a_{(m\tau^{-1}+1)\tau},\dots,a_{n\tau}) = b \tag{2.2}$$

для $i < m$ і рівнянню

$$g(a_{1\tau},\dots,a_{(m\tau^{-1}-1)\tau},h(a_{1\upsilon},\dots,a_{n\upsilon}), a_{(m\tau^{-1}+1)\tau},\dots,a_{(i\tau^{-1}-1)\tau},x,a_{(i\tau^{-1}+1)\tau},\dots,a_{n\tau}) = b \tag{2.3}$$

для $i > m$. i-оборотність операції f означає, що рівняння (1.1) має єдиний розв'язок. Операція h є сюр'єктивною, оскільки h є $J_\upsilon(m)$-оборотною. Тому g є $J_\tau(i)$-оборотною.

Навпаки, нехай g є $J_\tau(i)$-оборотною для деякого $i \in \operatorname{Im}\tau\setminus\operatorname{Im}\upsilon$. Покажемо, що (1.1) має єдиний розв'язок для всіх $a_1,\dots,a_{i-1}$, $a_{i+1},\dots,a_n,b \in Q$. Нехай $i < m$. Якщо скомбінувати $i \in \operatorname{Im}\tau$, $i \notin \operatorname{Im}\upsilon$, (2.1), (1.1), то отримаємо рівняння (2.2). Якщо ж $i > m$, то, враховуючи $i \in \operatorname{Im}\tau$, $i \notin \operatorname{Im}\upsilon$, (2.1), (1.1), отримаємо рівняння (2.3). Рівняння (2.2) і (2.3) мають єдиний розв'язок для всіх $a_1,\dots, a_{(i\tau^{-1}-1)\tau}$, $a_{(i\tau^{-1}+1)\tau},\dots, a_n$,

$b \in Q$, тому що g є $J_\tau(i)$-оборотною. Це означає, що (1.1) має єдиний розв'язок для всіх $a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n, b \in Q$, тому f є i-оборотною.

Нехай припущення п. 2) є істинними. Беручи до уваги (2.1), рівняння (1.1) є еквівалентним рівнянню

$$g(a_{1\tau}, \ldots, a_{(m\tau^{-1}-1)\tau}, h(a_{1\upsilon}, \ldots, a_{(i\upsilon^{-1}-1)\upsilon}, x,$$

$$a_{(i\upsilon^{-1}+1)\upsilon}, \ldots, a_{n\upsilon}), a_{(m\tau^{-1}+1)\tau}, \ldots, a_{n\tau}) = b. \qquad (2.4)$$

Позначимо

$$\beta_i(x) := f(a_1, \ldots, a_{i-1}, x, a_{i+1}, \ldots, a_n), \quad i = 1, \ldots, n,$$
$$\gamma_m(x) := g(a_{1\tau}, \ldots, a_{(m\tau^{-1}-1)\tau}, x, a_{(m\tau^{-1}+1)\tau}, \ldots, a_{n\tau}), \quad m = 1, \ldots, n,$$
$$\delta_i(x) := h(a_{1\upsilon}, \ldots, a_{(i\upsilon^{-1}-1)\upsilon}, x, a_{(i\upsilon^{-1}+1)\upsilon}, \ldots, a_{n\upsilon}), \quad i = 1, \ldots, n.$$

Тоді (2.4) має вигляд: $\beta_i = \gamma_m \delta_i$. Оскільки γ_m є підстановкою, то перетворення β_i і δ_i є підстановками одночасно, тобто β_i є підстановкою тоді і тільки тоді, коли δ_i є підстановкою. Це означає, що i-оборотність операції f є еквівалентною $J_\upsilon(i)$-оборотності операції h.

Нехай припущення п. 3) є істинними. Розглянемо випадок $i < m$. Тоді рівняння (1.1) є еквівалентним рівнянню

$$g(a_{1\tau}, \ldots, a_{(i\tau^{-1}-1)\tau}, x, a_{(i\tau^{-1}+1)\tau}, \ldots, a_{(m\tau^{-1}-1)\tau}, h(a_{1\upsilon}, \ldots, a_{(i\upsilon^{-1}-1)\upsilon},$$

$$x, a_{(i\upsilon^{-1}+1)\upsilon}, \ldots, a_{n\upsilon}), a_{(m\tau^{-1}+1)\tau}, \ldots, a_{n\tau}) = b. \qquad (2.5)$$

Введемо позначення:

$$h(a_{1\upsilon}, \ldots, a_{(i\upsilon^{-1}-1)\upsilon}, x, a_{(i\upsilon^{-1}+1)\upsilon}, \ldots, a_{n\upsilon}) =: y. \qquad (2.6)$$

Оскільки h є $J_\upsilon(m)$-оборотною, тоді ${}^{(J_\upsilon(m))}h$ існує, тому (2.6) і

$${}^{J_\upsilon(m)}h(a_{1\upsilon}, \ldots, a_{(i\upsilon^{-1}-1)\upsilon}, x, a_{(i\upsilon^{-1}+1)\upsilon}, \ldots,$$

$$a_{(m\upsilon^{-1}-1)\upsilon}, y, a_{(m\upsilon^{-1}+1)\upsilon}, \ldots, a_{n\upsilon}) = a_m$$

є еквівалентними. Таким чином, однозначність розв'язку рівняння (2.5)

еквівалентне однозначності розв'язку системи

$$\begin{cases} {}^{(J_\upsilon(m))}h(a_{1\upsilon},\dots,a_{(i\upsilon^{-1}-1)\upsilon},x,a_{(i\upsilon^{-1}+1)\upsilon},\dots, \\ \qquad\qquad a_{(m\upsilon^{-1}-1)\upsilon},y,a_{(m\upsilon^{-1}+1)\upsilon},\dots,a_{n\upsilon})=a_m, \\ g(a_{1\tau},\dots,a_{(i\tau^{-1}-1)\tau},x,a_{(i\tau^{-1}+1)\tau},\dots, \\ \qquad\qquad a_{(m\tau^{-1}-1)\tau},y,a_{(m\tau^{-1}+1)\tau},\dots,a_{n\tau})=b, \end{cases}$$

яка означає ортогональність (τ,υ)-відповідних $\{m,i\}$-ретрактів операцій g і ${}^{(J_\upsilon(m))}h$.

Розглянемо випадок $i>m$. Тоді рівняння (1.1) є еквівалентним рівнянню

$$\begin{aligned} g(a_{1\tau},\dots,a_{(m\tau^{-1}-1)\tau},h(a_{1\upsilon},\dots,a_{(i\upsilon^{-1}-1)\upsilon},x,a_{(i\upsilon^{-1}+1)\upsilon},\dots,a_{n\upsilon}), \\ a_{(m\tau^{-1}+1)\tau},\dots,a_{(i\tau^{-1}-1)\tau},x,a_{(i\tau^{-1}+1)\tau},\dots,a_{n\tau})=b. \end{aligned} \tag{2.7}$$

Враховуючи $J_\upsilon(m)$-оборотність операції h і позначення (2.6), випишемо ${}^{(J_\upsilon(m))}h$:

$${}^{(J_\upsilon(m))}h(a_{1\upsilon},\dots,a_{(m\upsilon^{-1}-1)\upsilon},y,a_{(m\upsilon^{-1}+1)\upsilon},\dots, \\ a_{(i\upsilon^{-1}-1)\upsilon},x,a_{(i\upsilon^{-1}+1)\upsilon},\dots,a_{n\upsilon})=a_m.$$

Таким чином, однозначність розв'язку рівняння (2.7) є еквівалентним однозначності розв'язку системи

$$\begin{cases} {}^{(J_\upsilon(m))}h(a_{1\upsilon},\dots,a_{(m\upsilon^{-1}-1)\upsilon},y,a_{(m\upsilon^{-1}+1)\upsilon},\dots, \\ \qquad\qquad a_{(i\upsilon^{-1}-1)\upsilon},x,a_{(i\upsilon^{-1}+1)\upsilon},\dots,a_{n\upsilon})=a_m, \\ g(a_{1\tau},\dots,a_{(m\tau^{-1}-1)\tau},y,a_{(m\tau^{-1}+1)\tau},\dots, \\ \qquad\qquad a_{(i\tau^{-1}-1)\tau},x,a_{(i\tau^{-1}+1)\tau},\dots,a_{n\tau})=b, \end{cases}$$

яка означає ортогональність (τ,υ)-відповідних $\{m,i\}$-ретрактів операцій g і ${}^{(J_\upsilon(m))}h$. □

Наслідок 2.1. *Нехай τ і υ є частковими ін'єктивними перетвореннями множини $\overline{1,n}$, g і h є оборотними операціями і (2.1) виконується. Тоді оборотність операції f рівносильна перпендикулярності типу $(\tau,\upsilon;m)$ операцій g і ${}^{(J_\upsilon(m))}h$.*

Доведення. Оскільки g і h є оборотними операціями, то згідно із п. 1) і п. 2) теореми 2.1 операція f є i-оборотною для всіх $i \in (\operatorname{Im}\tau \setminus \operatorname{Im}\upsilon) \cup (\operatorname{Im}\upsilon \setminus \operatorname{Im}\tau)$. Таким чином, оборотність операції f є еквівалентною перпендикулярності типу $(\tau, \upsilon; m)$ операцій g і ${}^{(J_\upsilon(m))}h$. □

Поняття ортогональності та перпендикулярності типів $(\iota, \iota; 1)$ і $(\iota, \iota; 2)$ збігаються у бінарному випадку. Отже, теорема 2.1 спричинює теорему 1.1, теорему 1.2, теорему 2 із [41] і наслідок 1 із [63].

2.1.2. Перпендикулярність центральних квазігруп

У цьому підрозділі розглянемо деякі питання щодо перпендикулярності лінійних операцій над абелевою групою. З цією метою наведемо теорему 2.2, теорему 2.3 і наслідок 2.3, які належать Ф.М. Сохацькому [82].

Нехай τ є довільним частковим перетворенням множини $\overline{1,n}$. Якщо $|\{1\tau, \ldots, n\tau\}|$-арна квазігрупа f є лінійною на групі $(Q;+)$, то відповідно до (1.5) вона має розклад:

$$g(x_{1\tau}, \ldots, x_{n\tau}) = \alpha_{1\tau}x_{1\tau} + \cdots + \alpha_{n\tau}x_{n\tau} + a, \tag{2.8}$$

де $a \in Q$ і $\alpha_{1\tau}, \ldots, \alpha_{n\tau}$ є автоморфізмами групи $(Q;+)$, але якщо $i\tau$ не існує, тоді $\alpha_{i\tau}x_{i\tau}$ позначає порожній символ.

Теорема 2.2 (Ф.М. Сохацький, І.В. Фриз [82]). *Нехай $(Q;+)$ є групою і $\alpha, \beta, \gamma, \delta$ є її автоморфізмами. Система*

$$\begin{cases} \alpha x + \beta y = a, \\ \gamma x + \delta y = b \end{cases} \tag{2.9}$$

має єдиний розв'язок для всіх $a, b \in Q$ тоді і тільки тоді, коли $-\gamma^{-1}\delta + \alpha^{-1}\beta$ (або $\beta^{-1}\alpha - \delta^{-1}\gamma$) є підстановкою множини Q.

Наслідок 2.2 (Г.Л. Муллен, В.О. Щербаков [65]). *Нехай $(Q;+)$ є абелевою групою і $\alpha, \beta, \gamma, \delta$ є її автоморфізмами. Тоді система* (2.9) *має*

єдиний розв'язок тоді і тільки тоді, коли $\alpha^{-1}\beta - \gamma^{-1}\delta$ *є автоморфізмом групи* $(Q;+)$.

Теорема 2.3 (Ф.М. Сохацький, І.В. Фриз [82]). *Нехай* f, g, h *є лінійними квазігрупами над абелевою групою* $(Q;+)$, *які визначаються рівностями* (2.1), (2.8), *і*

$$h(x_{1\upsilon},\dots,x_{n\upsilon}) := \beta_{1\upsilon}x_{1\upsilon} + \cdots + \beta_{n\upsilon}x_{n\upsilon} + c. \tag{2.10}$$

Операція f *є оборотною тоді і тільки тоді, коли для кожного* $p \in (\operatorname{Im}\upsilon \cap \operatorname{Im}\tau)\backslash\{m\}$ *перетворення* $\alpha_p + \alpha_m\beta_p$ *є автоморфізмом групи* $(Q;+)$.

Наслідок 2.3 (Ф.М. Сохацький, І.В. Фриз [82]). *Нехай в умовах теореми* 2.3 $(Q;+)$ *є адитивною групою лишків за модулем* s. *Операція* f *оборотна тоді і тільки тоді, коли число* $\alpha_p + \alpha_m\beta_p$ *є взаємно простим із* s *для всіх* $p \in (\operatorname{Im}\upsilon \cap \operatorname{Im}\tau)\backslash\{m\}$.

Доведемо теорему, яка дає відповідь на питання: коли центральна квазігрупа є перпендикулярною до одного із компонентів свого розкладу?

Теорема 2.4. *Нехай* $(Q;+)$ *є абелевою групою, квазігрупова операція* f *і лінійні квазігрупи* g *і* h *визначаються рівностями* (2.1), (2.8) *і* (2.10) *відповідно. Операція* f *є перпендикулярною типу* $(\iota,\tau;m)$ *до операції* g *тоді і тільки тоді, коли нижче наведені умови є істинними:*

1) *відображення* $\alpha_p+\alpha_m(\iota-\beta_m)^{-1}\beta_p$ *і* $\alpha_p+\alpha_m\beta_p$ *є автоморфізмами групи* $(Q;+)$ *для всіх* $p \in (\operatorname{Im}\upsilon \cap \operatorname{Im}\tau)\backslash\{m\}$;

2) *відображення* $\iota - \beta_m$ *є автоморфізмом групи* $(Q;+)$ *для всіх* $p \in \operatorname{Im}\tau\backslash\operatorname{Im}\upsilon$.

Доведення. Операція f є лінійною над абелевою групою $(Q;+)$. Щоб записати вигляд операції f підставимо у рівність (2.1) рівності (2.8) і (2.10):

$$f(x_1,\dots,x_n) = \alpha_{1\tau}x_{1\tau} + \cdots + \alpha_{(m\tau^{-1}-1)\tau}x_{(m\tau^{-1}-1)\tau} +$$

$$+\alpha_m(\beta_{1\upsilon}x_{1\upsilon} + \cdots + \beta_{n\upsilon}x_{n\upsilon} + c) +$$

$$+\alpha_{(m\tau^{-1}+1)\tau}x_{(m\tau^{-1}+1)\tau} + \cdots + \alpha_{n\tau}x_{n\tau} + a.$$

За теоремою 2.3 оборотність операції f означає, що перетворення $\alpha_p+\alpha_m\beta_p$ є автоморфізмом групи $(Q;+)$ для всіх $p\in(\operatorname{Im}\upsilon\cap\operatorname{Im}\tau)\backslash\{m\}$.

Розглянемо перпендикулярність операцій f і g типу $(\iota,\tau;m)$, де ι є перетворенням, що відповідає операції g, оскільки множиною індексів операції f є множина $\operatorname{Im}\tau\cap\operatorname{Im}\upsilon=\overline{1,n}$. Однією з умов перпендикулярності операцій f і g є однозначність розв'язку системи

$$\begin{cases}\alpha_m\beta_m y+(\alpha_m\beta_p+\alpha_p)x=c_0,\\ \\ \alpha_m y+\alpha_p x=d_0\end{cases}\tag{2.11}$$

для всіх $p\in(\operatorname{Im}\tau\cap\operatorname{Im}\upsilon)\backslash\{m\}$ та довільних елементів c_0 і d_0 із Q. Згідно з наслідком 2.2, ця система має єдиний розв'язок тоді і тільки тоді, коли перетворення $-\alpha_m^{-1}\alpha_p+(\alpha_m\beta_m)^{-1}(\alpha_m\beta_p+\alpha_p)$ є автоморфізмом $(Q;+)$. Перетворення $\alpha_p+\alpha_m(\iota-\beta_m)^{-1}\beta_p$ є автоморфізмом групи $(Q;+)$ для всіх $p\in(\operatorname{Im}\tau\cap\operatorname{Im}\upsilon)\backslash\{m\}$, оскільки

$$-\alpha_m^{-1}\alpha_p+(\alpha_m\beta_m)^{-1}(\alpha_m\beta_p+\alpha_p)=$$

$$=-\alpha_m^{-1}\alpha_p+\beta_m^{-1}\alpha_m^{-1}\alpha_m\beta_p+\beta_m^{-1}\alpha_m^{-1}\alpha_p=$$

$$=-\alpha_m^{-1}\alpha_p+\beta_m^{-1}\beta_p+\beta_m^{-1}\alpha_m^{-1}\alpha_p=(\beta_m^{-1}-\iota)\alpha_m^{-1}\alpha_p+\beta_m^{-1}\beta_p=$$

$$=\beta_m^{-1}\beta_m\big((\beta_m^{-1}-\iota)\alpha_m^{-1}\alpha_p+\beta_m^{-1}\beta_p\big)=\beta_m^{-1}\big((\iota-\beta_m)\alpha_m^{-1}\alpha_p+\beta_p\big)$$

і

$$(\iota-\beta_m)\alpha_m^{-1}\alpha_p+\beta_p=(\iota-\beta_m)\alpha_m^{-1}\big(\alpha_p+\alpha_m(\iota-\beta_m)^{-1}\beta_p\big).$$

Таким чином, операція f перпендикулярна типу $(\iota,\tau;m)$ до g тоді і тільки тоді, коли перетворення $\alpha_p+\alpha_m(\iota-\beta_m)^{-1}\beta_p$ і $\alpha_p+\alpha_m\beta_p$ є автоморфізмами групи $(Q;+)$ одночасно для всіх $p\in(\operatorname{Im}\tau\cap\operatorname{Im}\upsilon)\backslash\{m\}$.

Іншою умовою перпендикулярності операцій f і g типу $(\iota,\tau;m)$ є однозначність розв'язку системи

$$\begin{cases}\alpha_m\beta_m y+\alpha_p x=c_0,\\ \\ \alpha_m y+\alpha_p x=d_0\end{cases}$$

для всіх $p\in\operatorname{Im}\tau\backslash\operatorname{Im}\upsilon$. Ця система має єдиний розв'язок тоді і тільки тоді, коли перетворення $-\alpha_m^{-1}\alpha_p+(\alpha_m\beta_m)^{-1}\alpha_p$ є автоморфізмом групи $(Q;+)$.

Перетворення $\iota - \beta_m$ є автоморфізмом $(Q;+)$ також для всіх $p \in \operatorname{Im}\tau \setminus \operatorname{Im}\upsilon$, оскільки

$$-\alpha_m^{-1}\alpha_p + (\alpha_m\beta_m)^{-1}\alpha_p = -\alpha_m^{-1}\alpha_p + \beta_m^{-1}\alpha_m^{-1}\alpha_p = \beta_m^{-1}(\iota - \beta_m)\alpha_m^{-1}\alpha_p.$$

Якщо $p \in \operatorname{Im}\upsilon \setminus \operatorname{Im}\tau$, тоді система (2.11) має вигляд

$$\begin{cases} \alpha_m\beta_m y + \alpha_p x = c_0, \\ \\ \alpha_m y = d_0. \end{cases}$$

Ця система має єдиний розв'язок, але оскільки операція g не має $\{m;p\}$-ретракту, то f і g не є перпендикулярними типу $(\iota, \tau; m)$. □

2.1.3. Перпендикулярність гіперкубів

Нехай ρ є довільним частковим ін'єктивним перетворенням множини $\overline{1,n}$. Якщо $i\rho$ є порожнім символом, то у відповідному гіперкубі у напрямку $i\rho$ усі зрізи порожні.

Означення 2.3. *Квадрат називатимемо $\{m,p\}$-зрізом гіперкуба H, якщо він отриманий із H фіксуванням усіх координат, крім m і p.*

Кожній парі перпендикулярних операцій є відповідною пара перпендикулярних гіперкубів того ж самого типу. Переформулюємо означення 2.2 мовою гіперкубів.

Означення 2.4. *Два гіперкуби H_1 і H_2 називатимемо перпендикулярними типу $(\tau, \upsilon; m)$, якщо для всіх $p \in \big(\operatorname{Im}\upsilon \cap \operatorname{Im}\tau\big)\setminus\{m\}$ кожна пара $\{m,p\}$-зрізів гіперкубів H_1 і H_2 є ортогональною.*

Зауважмо, що один і той же куб можна представити трьома способами: за допомогою $\{1,2\}$-зрізів, $\{1,3\}$-зрізів або $\{2,3\}$-зрізів.

Приклад 2.1. *Операції f_1 і f_2, які визначені на Z_5 рівностями*

$$f_1(x_1,x_2,x_3) := x_1 + x_2 + x_3 \;\; i \;\; f_2(x_1,x_2,x_3) := 2x_1 + 3x_2 + x_3,$$

є перпендикулярними типу $(\iota, \iota; 1)$.

Дійсно, відповідно до наслідку 2.3, оскільки числа $1+3=4$, $1+1\cdot 1=2$ є взаємнопростими із 5, то f_1 і f_2 перпендикулярні типу $(\iota,\iota;1)$.

Оскільки перпендикулярність має тип $(\iota,\iota;1)$, то щоб проілюструвати перпендикулярність відповідних кубів обираємо ті типи зрізів, які містять номер змінної із типу заданої перпендикулярності, тобто $\{1,2\}$-зрізи і $\{1,3\}$-зрізи.

Зобразимо куб H_1 за допомогою $\{1,2\}$-зрізів:

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

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

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

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

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

Зобразимо куб H_2 за допомогою $\{1,2\}$-зрізів:

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

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

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

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

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

Накладемо відповідні $\{1,2\}$-зрізи кубів H_1 і H_2:

00	13	21	34	42
12	20	33	41	04
24	32	40	03	11
31	44	02	10	23
43	01	14	22	30

11	24	32	40	03
23	31	44	02	10
30	43	01	14	22
42	00	13	21	34
04	12	20	33	41

22	30	43	01	14
34	42	00	13	21
41	04	12	20	33
03	11	24	32	40
10	23	31	44	02

33	41	04	12	20
40	03	11	24	32
02	10	23	31	44
14	22	30	43	01
21	34	42	00	13

44	02	10	23	31
01	14	22	30	43
13	21	34	42	00
20	33	41	04	12
32	40	03	11	24

Оскільки у кожному з утворених відносно накладання квадратів кожна пара має точно одну появу, то це означає ортогональність відповідних $\{1,2\}$-зрізів кубів H_1 і H_2.

Зобразимо куб H_1 за допомогою $\{1,3\}$-зрізів:

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

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

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

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

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

Зобразимо куб H_2 за допомогою $\{1,3\}$-зрізів:

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

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

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

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

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

Накладемо відповідні $\{1,3\}$-зріз кубів H_1 і H_2:

00	11	22	33	44
12	23	34	40	01
24	30	41	02	13
31	42	03	14	20
43	04	10	21	32

13	24	30	41	02
20	31	42	03	14
32	43	04	10	21
40	00	11	22	33
01	12	23	34	40

21	32	43	04	10
33	44	00	11	22
40	01	12	23	34
02	13	24	30	41
14	20	31	42	03

34	40	01	12	23
41	02	13	24	30
03	14	20	31	42
10	21	32	43	04
22	33	44	00	11

42	03	14	20	31
04	10	21	32	43
11	22	33	44	00
23	34	40	01	12
30	41	02	13	24

Отже, відповідні $\{1,3\}$-зрізи кубів H_1 і H_2 є також ортогональними.

Таким чином, за означенням 2.4 куби H_1 і H_2 є перпендикулярними типу $(\iota;\iota;1)$.

Приклад 2.2. *Операції f_1 і f_2, які визначені на Z_5 рівностями*

$$f_1(x_1,x_2,x_3) := x_1+x_2+x_3, \qquad f_2(x_1,x_3) := 2x_1+x_3,$$

є перпендикулярними типу $(\iota,\upsilon;1)$, де 2υ є порожнім символом.

З термів, що відповідають операціям f_1 і f_2, очевидно, що $\tau=\iota$ і $1\upsilon=1$, $3\upsilon=3$. Оскільки $1+1\cdot 1=2$ є взаємно простим із 5, то відповідно до наслідку 2.3 операції f_1 та f_2 є перпендикулярними типу $(\iota,\upsilon;1)$.

Щоб проілюструвати перпендикулярність відповідних гіперкубів, представимо їх $\{1,3\}$-зрізами, оскільки тип перпендикулярності є $(\iota,\upsilon;1)$. Інших відповідних зрізів не існує. Квадрат H_2, що є відповідним операції f_2 має вигляд:

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

Куб H_1, який відповідає операції f_1, подамо за допомогою $\{1,3\}$-зрізів:

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

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

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

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

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

Зазначимо, що кожного разу, фіксуючи x_2 у операції f_1, ми отримуємо той самий квадрат H_2, тому розглянемо накладання цього квадрата на кожен із $\{1,3\}$-зрізів куба H_1.

00	11	22	33	44
12	23	34	40	01
24	30	41	02	13
31	42	03	14	20
43	04	10	21	32

10	21	32	43	04
22	33	44	00	11
34	40	01	12	23
41	02	13	24	30
03	14	20	31	42

20	31	42	03	14
32	43	04	10	21
44	00	11	22	33
01	12	23	34	40
13	24	30	41	02

30	41	02	13	24
42	03	14	20	31
04	10	21	32	43
11	22	33	44	00
23	34	40	01	12

40	01	12	23	34
02	13	24	30	41
14	20	31	42	03
21	32	43	04	10
33	44	00	11	22

Таким чином, відповідні $\{1,3\}$-зрізи куба H_1 і квадрата H_2 є ортогональними, тому f_1 і f_2 є перпендикулярними типу $(\iota, \upsilon; 1)$. До того ж f_1 і f_2

є перпендикулярними також типу $(\iota, \upsilon; 3)$, оскільки відповідних ретрактів є лише одна пара.

2.2. Зв'язок між ортогональністю і перпендикулярністю

У цьому підрозділі розглянемо взаємозв'язок між поняттями ортогональності і перпендикулярності. З цією метою припустимо, що τ і υ є повними ін'єктивними перетвореннями множини $\overline{1,n}$, тобто є її перестановками. Нехай g і h є перпендикулярними типу $(\tau, \upsilon; m)$. Оскільки кожна змінна у термі характеризується місцем, на якому вона знаходиться, то перепозначивши індекси змінних, відповідно до порядку їхнього знаходження у термі $g(x_{1\tau}, \ldots, x_{n\tau})$ (тобто діємо на індекси перестановкою τ^{-1}), отримуємо перетворення ι і $\tau^{-1}\upsilon$. Це означає, що тип перпендикулярності має вигляд $(\iota, \sigma; m)$, де σ є деякою перестановкою множини $\overline{1,n}$, ι – її тотожне перетворення.

Якщо g є перпендикулярною до h типу $(\iota, \sigma; m)$, то g є перпендикулярною до ${}^{\sigma^{-1}}h$ типу $(\iota, \iota; m)$, до того ж σ у своєму розкладі не містить циклу $(m\ i)$, $i \in \overline{1,n}/\{m\}$. Справді, за означенням 2.2 з перпендикулярності g і h тиму $(\iota, \sigma; m)$ випливає, що для будь-яких $a, b \in Q$ і $i \in \overline{1,n}/\{m\}$ система

$$\begin{cases} f(a_1, \ldots, a_{m-1}, x_m, a_{m+1}, \ldots, a_{i-1}, y_i, a_{i+1}, \ldots, a_n) = a, \\ \\ g(a_{1\sigma}, \ldots, a_{(m-1)\sigma}, x_{m\sigma}, a_{(m+1)\sigma}, \ldots, a_{(i-1)\sigma}, y_{i\sigma}, a_{(i+1)\sigma}, \ldots, a_{n\sigma}) = b \end{cases}$$

має єдиний розв'язок. Використовуючи (1.3), отримуємо рівносильну систему

$$\begin{cases} f(a_1, \ldots, a_{m-1}, x_m, a_{m+1}, \ldots, a_{i-1}, y_i, a_{i+1}, \ldots, a_n) = a, \\ \\ {}^{\sigma^{-1}}g(a_1, \ldots, a_{m-1}, x_m, a_{m+1}, \ldots, a_{i-1}, y_i, a_{i+1}, \ldots, a_n) = b. \end{cases}$$

Отже, достатньо розглянути випадок $\tau = \upsilon = \iota$.

Твердження 2.1. *Якщо дві скінченні операції є перпендикулярними типу $(\iota, \iota; m)$, то вони є ортогональними.*

Доведення. Нехай n-арні операції f і g є визначеними на скінченній множині Q, $k := |Q|$ і припустимо f і g є перпендикулярними типу $(\iota, \iota; m)$, тобто система

$$\begin{cases} f(a_1, \ldots, a_{m-1}, x, a_{m+1}, \ldots, a_{p-1}, y, a_{p+1}, \ldots, a_n) = a, \\ \\ g(a_1, \ldots, a_{m-1}, x, a_{m+1}, \ldots, a_{p-1}, y, a_{p+1}, \ldots, a_n) = b \end{cases}$$

має єдиний розв'язок для кожної пари $(a; b) \in Q^2$ і довільної послідовності $(a_1, \ldots, a_{m-1}, a_{m+1}, \ldots, a_{p-1}, a_{p+1}, \ldots, a_n) \in Q^{n-1}$. Система

$$\begin{cases} f(x_1, \ldots, x_n) = a, \\ \\ g(x_1, \ldots, x_n) = b \end{cases}$$

має k^{n-1} розв'язків, оскільки для кожної пари $(a; b)$ існує точно $|Q^{n-1}| = k^{n-1}$ різних послідовностей. Це означає, що операції f і g є ортогональними згідно означення 1.1. □

Обернене твердження є неправильним. Щоб підтвердити це наведемо такий приклад.

Приклад 2.3. *Операції f і g, які визначені рівностями*

$$f(x_1, x_2, x_3) = 3x_1 + x_2 + 2x_3, \quad g(x_1, x_2, x_3) = x_1 + x_2 + x_3$$

на Z_6, є ортогональними, але не є перпендикулярними типу $(\iota, \iota; 1)$.

Доведення. Операція g є оборотною, але f не є 2- і 3-оборотною, оскільки 2 і 3 не є взаємнопростими із 6. Розглянемо відповідні куби H_f і H_g.

Зобразимо куб H_f за допомогою $\{1, 2\}$-зрізів:

0	1	2	3	4	5
3	4	5	0	1	2
0	1	2	3	4	5
3	4	5	0	1	2
0	1	2	3	4	5
3	4	5	0	1	2

2	3	4	5	0	1
5	0	1	2	3	4
2	3	4	5	0	1
5	0	1	2	3	4
2	3	4	5	0	1
5	0	1	2	3	4

4	5	0	1	2	3
1	2	3	4	5	0
4	5	0	1	2	3
1	2	3	4	5	0
4	5	0	1	2	3
1	2	3	4	5	0

0	1	2	3	4	5
3	4	5	0	1	2
0	1	2	3	4	5
3	4	5	0	1	2
0	1	2	3	4	5
3	4	5	0	1	2

2	3	4	5	0	1
5	0	1	2	3	4
2	3	4	5	0	1
5	0	1	2	3	4
2	3	4	5	0	1
5	0	1	2	3	4

4	5	0	1	2	3
1	2	3	4	5	0
4	5	0	1	2	3
1	2	3	4	5	0
4	5	0	1	2	3
1	2	3	4	5	0

Зобразимо куб H_g за допомогою $\{1,2\}$-зрізів:

0	1	2	3	4	5
1	2	3	4	5	0
2	3	4	5	0	1
3	4	5	0	1	2
4	5	0	1	2	3
5	0	1	2	3	4

1	2	3	4	5	0
2	3	4	5	0	1
3	4	5	0	1	2
4	5	0	1	2	3
5	0	1	2	3	4
0	1	2	3	4	5

2	3	4	5	0	1
3	4	5	0	1	2
4	5	0	1	2	3
5	0	1	2	3	4
0	1	2	3	4	5
1	2	3	4	5	0

3	4	5	0	1	2
4	5	0	1	2	3
5	0	1	2	3	4
0	1	2	3	4	5
1	2	3	4	5	0
2	3	4	5	0	1

4	5	0	1	2	3
5	0	1	2	3	4
0	1	2	3	4	5
1	2	3	4	5	0
2	3	4	5	0	1
3	4	5	0	1	2

5	0	1	2	3	4
0	1	2	3	4	5
1	2	3	4	5	0
2	3	4	5	0	1
3	4	5	0	1	2
4	5	0	1	2	3

Накладемо відповідні $\{1,2\}$-зрізи кубів H_f і H_g:

00	11	22	33	44	55
31	42	53	04	15	20
02	13	24	35	40	51
33	44	55	00	11	22
04	15	20	31	42	53
35	40	51	02	13	24

21	32	43	54	05	10
52	03	14	25	30	41
23	34	45	50	01	12
54	05	10	21	32	43
25	30	41	52	03	14
50	01	12	23	34	45

42	53	04	15	20	31
13	24	35	40	51	02
44	55	00	11	22	33
15	20	31	42	53	04
40	51	02	13	24	35
11	22	33	44	55	00

03	14	25	30	41	52
34	45	50	01	12	23
05	10	21	32	43	54
30	41	52	03	14	25
01	12	23	34	45	50
32	43	54	05	10	21

24	35	40	51	02	13
55	00	11	22	33	44
20	31	42	53	04	15
51	02	13	24	35	40
22	33	44	55	00	11
53	04	15	20	31	42

45	50	01	12	23	34
10	21	32	43	54	05
41	52	03	14	25	30
12	23	34	45	50	01
43	54	05	10	21	32
14	25	30	41	52	03

Оскільки в результаті накладання $\{1,2\}$-зрізів кубів H_f і H_g, кожен з утворених квадратів містить однакові пари, то ці куби не є перпендикулярними типу $(\iota,\iota;1)$. Однак, вони ортогональні згідно з означенням 1.4, оскільки кожна пара зустрічається шість разів. □

Висновки до розділу 2

У цьому розділі введено нове поняття перпендикулярність як одне із узагальнень ортогональності бінарних операцій і описано взаємозв'язки між оборотністю повторної композиції двох квазігруп різних арностей і перпендикулярністю компонентів цієї композиції.

Основні результати розділу:

1) знайдено критерій оборотності композиції двох багатомісних операцій, які мають різну арність;
2) знайдено умови, коли центральна квазігрупа є перпендикулярною до одного із компонентів свого розкладу;
3) описано поняття перпендикулярності мовою гіперкубів;
4) доведено, що для максимального типу перпендикулярність спричинює ортогональність і показано, що обернене твердження не є істинним.

Результати цього розділу опубліковані у [78] і [82].

РОЗДІЛ 3

АЛГОРИТМИ ПОБУДОВИ ОРТОГОНАЛЬНИХ ОПЕРАЦІЙ

У цьому розділі розглянемо один із методів побудови ортогональних операцій, а саме – узагальнення методу визначення рекурсивних похідних функцій, які пов'язані з рекурсивними МДР-кодами, як показано в [53]. Пізніше ця ідея була розвинута Г.Б. Білявською та Г.Л. Мулленом у [64]. Запропонований ними алгоритм побудови ортогональних операцій є одним із тривіальних рекурсивних алгоритмів, інші тривіальні рекурсивні алгоритми описали С. Марковський та А. Мілева в [93]. Відповідно до тривіальної рекурсії, кожна наступна операція будується із нової операції і всіх попередньо побудованих операцій.

У цьому розділі розглядаємо та доводимо блочний рекурсивний алгоритм побудови ортогональних операцій, який є узагальненням тривіального рекурсивного алгоритму, одним із параметрів якого є розбиття множини індексів у блоки. Відповідно до блочної рекурсії, кожний наступний блок операцій будується із блоку нових операцій і всіх блоків операцій побудованих до цього. Як інструмент для побудови ортогональних операцій вводиться нове поняття ретрактної ортогональності.

3.1. Ретрактна ортогональність

Деякі проблеми щодо ортогональності n-арних операцій не мають аналогів у бінарному випадку, зокрема серед них є важливою проблема ортогональності ретрактів вибірки операцій. Саме цьому питанню і присвячений цей підрозділ.

Зазначимо, що В.Д. Білоусов у роботі [18, с. 9] описав метод отримання одних квазігруп із інших фіксуванням деяких змінних елементами із носія і назвав цю дію ретракцією. Г.Б. Білявська і Г.Л. Муллен у [67]

конкретизували поняття ретракту операції таким чином: нехай

$$\bar{a} = (i_1, \ldots, i_j; a_{i_1}, \ldots, a_{i_j}) \in \mathrm{I}_j,$$

де

$$\mathrm{I}_j = \left\{(i_1, \ldots, i_j; a_{i_1}, \ldots, a_{i_j}) | \{i_1, \ldots, i_j\} \subseteq \overline{1,n}, (a_{i_1}, \ldots, a_{i_j}) \in Q^j\right\}.$$

$(n-j)$-арна операція $f_{\bar{a}}$ називається $(n-j)$-ретрактом n-арної операції f, якщо у відповідному термі змінні з індексами із множини $\{i_1, \ldots, i_j\}$ фіксуються елементами із послідовності $(a_{i_1}, \ldots, a_{i_j})$, тобто визначається вибіркою $\bar{a} \in \mathrm{I}_j$.

Означуючи таким чином поняття ретракту його параметром є множина індексів зафіксованих змінних, тобто $\{i_1, \ldots, i_j\}$.

У цій роботі використовуємо інший підхід до визначення ретракту, а саме параметром є множина індексів незафіксованих змінних.

Нехай f є n-арною операцією, яка визначена на множині Q, і нехай

$$\delta := \{i_1, \ldots, i_k\} \subseteq \overline{1,n}, \quad \{j_1, \ldots, j_{n-k}\} := \overline{1,n} \setminus \delta, \tag{3.1}$$

$$\bar{a} := (a_{j_1}, \ldots, a_{j_{n-k}}) \in Q^{n-k}.$$

Операція $f_{(\bar{a},\delta)}$, яка визначається рівністю

$$f_{(\bar{a},\delta)}(x_{i_1}, \ldots, x_{i_k}) := f(y_1, \ldots, y_n),$$

де $y_i := \begin{cases} x_i, & \text{якщо } i \in \delta, \\ a_i, & \text{якщо } i \notin \delta \end{cases}$, називається $(\bar{a}, \delta)$-ретрактом або δ-ретрактом операції f.

Множина всіх індексів змінних x у цій системі є множиною δ.

Розбиття множини індексів змінних лежить в основі блочного рекурсивного алгоритму побудови ортогональних операцій, який викладено в підрозділі 3.2, а кожен із блоків розбиття означає, що відповідні ретракти деякого набору операцій є ортогональними. Взагалі кажучи, множина доповнень блоків розбиття множини не є розбиттям, а лише покриттям цієї множини. Тому підхід до визначення ретракту, що викладений у дисертації, дав можливість сформулювати та довести блочний рекурсивний алгоритм.

Означення 3.1. *Операції* $f_{1;(\bar{a}_1,\delta)}$, $f_{2;(\bar{a}_2,\delta)}$, ..., $f_{k;(\bar{a}_k,\delta)}$ *називатимемо подібними* δ*-ретрактами* n*-арних операцій* f_1, f_2, ..., f_k, *якщо виконується умова* $\bar{a}_1 = \bar{a}_2 = \cdots = \bar{a}_k$.

Означення 3.2. *Операції* f_1, f_2, ..., f_k *називатимемо* δ*-ретрактно ортогональними, якщо всі їхні подібні* δ*-ретракти є ортогональними.*

У роботі [67] введено поняття j-рівномірної ортогональності, яке є частковим випадком означення δ-ретрактної ортогональності, що введено тут.

Якщо $\delta = \overline{1,n}$, то δ-ретрактна ортогональність є ортогональністю за класичним означенням (див. означення 1.1). Якщо $\delta := \{i\} \subset \overline{1,n}$, то унарні $\{1\}$-,..., $\{n\}$-ретракти n-арної операції f є її 1-шою, ..., n-ою трансляціями відповідно. Оскільки кожний ретракт квазігрупи є квазігрупою, то унарний ретракт квазігрупи є підстановкою множини Q. Це означає, що δ-ретрактна ортогональність вироджується в i-оборотність операції f_i, тобто ретрактну ортогональність можна розглядати як деяке узагальнення оборотності.

Бінарні операції не цікаві для розгляду ретрактів, оскільки вони мають лише тривіальні ретракти: унарні і бінарні. Ортогональність унарних ретрактів є відповідною оборотності операції, ортогональність бінарних ретрактів є ортогональністю за класичним означенням.

Нехай f_1, ..., f_k є δ-ретрактно ортогональними операціями. З огляду на означення ортогональності, це означає, що для кожної послідовності $\bar{a} \in Q^{n-k}$ їхні $(\bar{a},\delta)$-ретракти $f_{1;(\bar{a},\delta)}$, ..., $f_{k;(\bar{a},\delta)}$ є ортогональними. Іншими словами, перетворення

$$\overline{\theta} := (f_{1;(\bar{a},\delta)}, \ldots, f_{k;(\bar{a},\delta)})$$

множини Q^k є її підстановкою.

Відповідно до теореми 1.9 δ-ретрактна ортогональність n-арних операцій f_1, ..., f_k означає, що для кожної послідовності $\bar{a} \in Q^{n-k}$ існують

k-арні операції $g_1, \ldots, g_k$, такі, що виконується система тотожностей

$$\begin{cases} g_1(f_1(y_1,\ldots,y_n),\ldots,f_k(y_1,\ldots,y_n)) = x_{i_1}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ g_k(f_1(y_1,\ldots,y_n),\ldots,f_k(y_1,\ldots,y_n)) = x_{i_k}, \end{cases} \tag{3.2}$$

де $y_i := \begin{cases} x_i, & \text{якщо } i \in \delta, \\ a_i, & \text{якщо } i \notin \delta. \end{cases}$

Ретрактно ортогональні операції можна будувати за допомогою безповторної композиції. Для того щоб сформулювати алгоритм побудови ретрактно ортогональних операцій наведемо теорему 3.1, яка належить Ф.М. Сохацькому [90].

Теорема 3.1 (І.В. Фриз, Ф.М. Сохацький [90]). *Нехай $p_1, \ldots, p_k$ є довільними 1-оборотними $(n-k+1)$-арними операціями, $h_1, \ldots, h_k$ є довільними k-арними операціями, і нехай операції $f_1, \ldots, f_k$ визначаються рівностями*

$$\begin{cases} f_1(x_1,\ldots,x_n) := p_1(h_1(x_1,\ldots,x_k),x_{k+1},\ldots,x_n), \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ f_k(x_1,\ldots,x_n) := p_k(h_k(x_1,\ldots,x_k),x_{k+1},\ldots,x_n). \end{cases} \tag{3.3}$$

Тоді n-арні операції $f_1,\ldots,f_k$ є $\overline{1,k}$-ретрактно ортогональними тоді і тільки тоді, коли k-арні операції $h_1, \ldots, h_k$ є ортогональними.

Нехай $\delta := \{i_1,\ldots,i_k\}$ і $\sigma \in \mathrm{S}'_{n+1}$, тоді

$$^{\sigma}\delta := \{(i_1)\sigma^{-1},\ldots,(i_k)\sigma^{-1}\}. \tag{3.4}$$

Залежність між різними ретрактними ортогональностями показує така лема:

Лема 3.1. *Нехай $f_1, \ldots, f_k$ є n-арними операціями і $\sigma \in \mathrm{S}'_{n+1}$. Вибірка $\{f_1, \ldots, f_k\}$ є δ-ретрактно ортогональною тоді і тільки тоді, коли вибірка $\{^{\sigma}f_1, \ldots, {}^{\sigma}f_k\}$ є ${}^{\sigma}\delta$-ретрактно ортогональною.*

Доведення. Нехай $\delta := \{i_1, \ldots, i_k\}$. Відповідно до рівності (1.2) систему (3.2) можна переписати таким чином:

$$\begin{cases} g_1({}^{\sigma}f_1(y_{1\sigma}, \ldots, y_{n\sigma}), \ldots, {}^{\sigma}f_k(y_{1\sigma}, \ldots, y_{n\sigma})) = x_{i_1}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ g_k({}^{\sigma}f_1(y_{1\sigma}, \ldots, y_{n\sigma}), \ldots, {}^{\sigma}f_k(y_{1\sigma}, \ldots, y_{n\sigma})) = x_{i_k}. \end{cases}$$

У цій системі змінна x_{i_1} знаходиться на місці $i_1\sigma^{-1}$, …, змінна x_{i_k} – на місці $i_k\sigma^{-1}$. З огляду на (3.4) вибірка $\{{}^{\sigma}f_1, \ldots, {}^{\sigma}f_k\}$ має ортогональні ${}^{\sigma}\delta$-ретракти. Таким чином, $\{{}^{\sigma}f_1, \ldots, {}^{\sigma}f_k\}$ є ${}^{\sigma}\delta$-ретрактно ортогональною. □

Отже, достатньо розглядати випадок, коли $\delta = \{1, \ldots, k\}$. З цієї леми випливає теорема 1.9, коли $\delta = \{1, \ldots, n\}$.

Для довільного δ, вибірку n-арних δ-ретрактно ортогональних операцій можна побудувати за допомогою нижче наведеного алгоритму.

Алгоритм 3.1 (Композиційний алгоритм)**.** *Нехай $\delta \subseteq \overline{1,n}$, $n \geqslant k$ і нехай $h_1, \ldots, h_k$ є k-арними операціями, $p_1, \ldots, p_k$ є $(n-k+1)$-арними операціями, $\sigma \in \mathrm{S}'_{n+1}$.*

Операції ${}^{\sigma}f_1$, …, ${}^{\sigma}f_k$ будуються за допомогою таких кроків:

1) *операції f_1, …, f_k будуються за допомогою (3.3);*
2) *операції ${}^{\sigma}f_1$, …, ${}^{\sigma}f_k$ отримуються з f_1, …, f_k, використовуючи рівність (1.3).*

Для $\tau \in \mathrm{S}_{n+1}$ символ $(X)\tau$ позначатиме образ множини X відносно перетворення τ, тобто $(X)\tau := \{x\tau \mid x \in X\}$. Визначимо підмножину S^A_{n+1} множини S_{n+1}:

$$\mathrm{S}^A_{n+1} := \left\{\tau \in \mathrm{S}'_{n+1} \mid (A)\tau = \{1, \ldots, |A|\}\right\}.$$

Теорема 3.2. *Нехай p_1, …, p_k є 1-оборотними $(n-k+1)$-арними операціями, h_1, …, h_k є k-арними ортогональними операціями і $\sigma^{-1} \in \mathrm{S}^{\delta}_{n+1}$. Тоді операції ${}^{\sigma}f_1$, …, ${}^{\sigma}f_k$, які побудовні за композиційним алгоритмом, є δ-ретрактно ортогональними.*

Доведення. Відповідно до теореми 3.1, операції $f_1, \ldots, f_k$ є $\overline{1,k}$-ретрактно ортогональними. З огляду на лему 3.1 операції ${}^{\sigma}f_1, \ldots, {}^{\sigma}f_k$ є ${}^{\sigma}\overline{1,k}$-ретрактно ортогональними. Але $\sigma^{-1} \in \mathrm{S}_{n+1}^{\delta}$, тобто ${}^{\sigma^{-1}}\delta = \overline{1,k}$, звідки ${}^{\sigma}\overline{1,k} = \delta$. Таким чином, операції які побудовані за алгоритмом 3.1 є δ-ретрактно ортогональними. □

Теорема 3.3. *Нехай h є довільною 1-оборотною $(n-k+1)$-арною операцією, $p_1, \ldots, p_k$ є довільними k-арними операціями, і нехай операції $f_1, \ldots, f_k$ визначаються рівностями*

$$\begin{cases} f_1(x_1, \ldots, x_n) := p_1(x_1, \ldots, x_{k-1}, h(x_k, \ldots, x_n)), \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ f_k(x_1, \ldots, x_n) := p_k(x_1, \ldots, x_{k-1}, h(x_k, \ldots, x_n)). \end{cases} \tag{3.5}$$

Тоді n-арні операції $f_1, \ldots, f_k$ є $\overline{1,k}$-ретрактно ортогональними тоді і тільки тоді, коли операції $p_1, \ldots, p_k$ є ортогональними.

Доведення. $\overline{1,k}$-ретрактна ортогональність операцій $f_1, \ldots, f_k$ еквівалентна однозначності розв'язку системи

$$\begin{cases} f_1(x_1, \ldots, x_k, a_{k+1} \ldots, a_n) = b_1, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ f_k(x_1, \ldots, x_k, a_{k+1} \ldots, a_n) = b_k \end{cases}$$

для довільних елементів носія $a_{k+1}, \ldots, a_n, b_1, \ldots, b_k$. Відповідно до (3.5) це рівносильно однозначності розв'язку такої системи

$$\begin{cases} p_1(x_1, \ldots, x_{k-1}, h(x_k, a_{k+1} \ldots, a_n)) = b_1, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ p_k(x_1, \ldots, x_{k-1}, h(x_k, a_{k+1} \ldots, a_n)) = b_k, \end{cases}$$

тобто ортогональності операцій $Tp_1, \ldots, Tp_k$, де $T := (\iota, \ldots, \alpha_k, \iota)$, $\alpha_k x_k := h(x_k, a_{k+1} \ldots, a_n)$. Зазначимо, що α_k є підстановкою носія, оскільки h є 1-оборотною. За теоремою 1.8, це рівносильно ортогональності операцій $p_1, \ldots, p_k$. □

3.2. Блочний рекурсивний алгоритм

Метою цього підрозділу є описання алгоритму побудови вибірки n-арних операцій із блоків ретрактно ортогональних n-арних операцій. "Рекурсивний" означає, що кожний наступний блок операцій будується зі всіх операцій, які були побудовані до цього.

Нехай n є довільним натуральним числом, де $n \geqslant 2$, π є розбиттям множини $\overline{1,n}$:

$$\pi := \{\pi_1, \pi_2 \ldots, \pi_k\}.$$

Нехай $f_1, \ldots, f_n$ є n-арними операціями на Q. Розподілимо ці операції у блоки відповідно до розбиття π їхніх індексів:

$$\{f_j \mid j \in \pi_i\}, \quad i = 1, 2, \ldots, k.$$

S_A позначатиме множину всіх перестановок множини A.

Алгоритм 3.2 (π-блочний рекурсивний алгоритм)**.** *Нехай* $\pi = \{\pi_1, \ldots, \pi_k\}$ *є розбиттям множини* $\overline{1,n}$ *і* $f_1, \ldots, f_n$ *є* n*-арними операціями,* $\tau_1 \in \mathrm{S}_{\pi_1}$, $\tau_2 \in \mathrm{S}_{\pi_1 \cup \pi_2}$, $\ldots$, $\tau_{k-1} \in \mathrm{S}_{\pi_1 \cup \cdots \cup \pi_{k-1}}$.

Операції $g_1, \ldots, g_n$ *будуються за допомогою таких кроків:*

1) першим блоком операцій є

$$g_j(x_1, \ldots, x_n) := f_j(x_1, \ldots, x_n), \quad j \in \pi_1;$$

2) для кожного $i = 2, \ldots, k$ *і-им блоком операцій є*

$$g_j(x_1, \ldots, x_n) := f_j(t_1, \ldots, t_n), \quad j \in \pi_i,$$

де

$$t_s := \begin{cases} g_{s\tau_{i-1}}(x_1, \ldots, x_n), & \text{якщо } s \in \pi_1 \cup \cdots \cup \pi_{i-1}, \\ x_s & \text{в інших випадках.} \end{cases}$$

Означення 3.3. *Вибірку операцій* $f_1, \ldots, f_n$ *називатимемо* π*-блочно ретрактно ортогональною, якщо для всіх* $i \in \overline{1,k}$ *вибірка* $\{f_j \mid j \in \pi_i\}$ *є* π_i*-ретрактно ортогональною.*

Теорема 3.4. *Нехай операції $f_1, \ldots, f_n$ є π-блочно ретрактно ортогональними. Тоді операції $g_1, \ldots, g_n$, побудовні за π-блочним рекурсивним алгоритмом, є ортогональними.*

Доведення. Доведемо твердження теореми методом математичної індукції по кількості блоків розбиття π, яку ми позначатимемо символом k.

База індукції. Якщо $k = 1$, то $\pi = \{\pi_1\} = \{\overline{1,n}\}$. Таким чином, операції $f_1, \ldots, f_n$ містяться в одному блоці, і вони є ортогональними відповідно до умови теореми. Отже, для $k = 1$ твердження є істинним.

Індуктивне припущення. Припустимо, що твердження теореми є істинним для $k = m$. Це означає, що розбиття має m блоків, і вибірка операцій, будучи побудованою за блочним рекурсивним алгоритмом, є ортогональною.

Індуктивний крок. Розглянемо твердження для $k = m + 1$, тобто розбиття π має $m + 1$ блоків. Ми маємо довести, що кожна довільна вибірка n-арних операцій $g_1, \ldots, g_n$, будучи побудованою за деяким π-блочним рекурсивним алгоритмом, є ортогональною. Іншими словами, нам потрібно довести, що для всіх $b_1, \ldots, b_n \in Q$ система

$$\big\{g_j(x_1, \ldots, x_n) = b_j, \quad j \in \overline{1,n} \tag{3.6}$$

має єдиний розв'язок.

Щоб записати π-блочний рекурсивний алгоритм для $g_1, \ldots, g_n$, введемо позначення:

- $\pi = \{\pi_1, \ \ldots, \pi_m, \pi_{m+1}\}$;
- $f_1, \ldots, f_n$ є π-блочно ретрактно ортогональними операціями, тобто для кожного $i \in \overline{1, m+1}$ вибірка $\{f_j \mid j \in \pi_i\}$ є π_i-ретрактно ортогональною;
- $\tau_1 \in \mathrm{S}_{\pi_1}$, $\tau_2 \in \mathrm{S}_{\pi_1 \cup \pi_2}$, $\ldots$, $\tau_m \in \mathrm{S}_{\pi_1 \cup \cdots \cup \pi_m}$.

Отже, блочний рекурсивний алгоритм має бути записаний у такий спосіб:

1) перший блок операцій визначається рівностями:

$$g_j(x_1, \ldots, x_n) := f_j(x_1, \ldots, x_n), \quad j \in \pi_1;$$

2) для кожного $i = 2, \ldots, m+1$ i-ий блок операцій:

$$g_j(x_1, \ldots, x_n) := f_j(t_1, \ldots, t_n), \quad j \in \pi_i,$$

де

$$t_s := \begin{cases} g_{s\tau_{i-1}}(x_1, \ldots, x_n), & \text{якщо } s \in \pi_1 \cup \cdots \cup \pi_{i-1}, \\ x_s & \text{в інших випадках.} \end{cases}$$

Для зручності введемо позначення

$$\pi' := \{\pi_1, \ldots, \pi_m\} = \pi \backslash \{\pi_{m+1}\},$$

$$\pi_0 := \pi_1 \cup \cdots \cup \pi_m = \overline{1,n} \backslash \pi_{m+1}.$$

Розглянемо підсистему системи (3.6):

$$\{g_j(x_1, \ldots, x_n) = b_j, \quad j \in \pi_{m+1}. \tag{3.7}$$

Використовуючи щойно наведений алгоритм, отримуємо

$$\begin{cases} f_j(t_1, \ldots, t_n) = b_j, \quad j \in \pi_{m+1}, \\ t_s := \begin{cases} g_{s\tau_m}(x_1, \ldots, x_n), & \text{якщо } s \in \pi_0, \\ x_s & \text{в інших випадках.} \end{cases} \end{cases}$$

У цій системі замінимо всі підтерми $g_{s\tau}(x_1, \ldots, x_n)$, де $s \in \pi_0$, їхніми значеннями, отриманими із (3.6):

$$\{f_j(t_1, \ldots, t_n) = b_j, \quad j \in \pi_{m+1}, \tag{3.8}$$

де

$$t_s := \begin{cases} b_{s\tau_m}, & \text{якщо } s \in \pi_0, \\ x_s & \text{в інших випадках.} \end{cases}$$

Оскільки π є розбиттям множини $\overline{1,n}$ і τ_m є підстановкою π_0, то із (3.8) випливає, що множина π_{m+1} збігається із множиною усіх індексів при змінних x:

$$\overline{1,n} \backslash \pi_0 = \pi_{m+1}.$$

Тоді всі ліві частини рівнянь із (3.8) є π_{m+1}-ретрактами операцій f_j, $j \in \pi_{m+1}$. За умовою теореми операції $f_1, \ldots, f_n$ є π-блочно ретрактно ортогональними, тому операції π_{m+1}-блоку є π_{m+1}-ретрактно ортогональними. Таким чином, система (3.8) має єдиний розв'язок:

$$x_s := a_s, \qquad s \in \pi_{m+1}. \tag{3.9}$$

Підставимо (3.9) в інші рівняння системи (3.6), тобто у всі рівняння системи (3.6), за винятком рівнянь системи (3.7):

$$\{g_j(y_1, \ldots, y_n) = b_j, \quad j \in \pi_0, \tag{3.10}$$

де

$$y_s := \begin{cases} x_s, & \text{якщо } s \in \pi_0, \\ a_s & \text{в інших випадках.} \end{cases}$$

У лівій частині отримали π_0-ретракти операцій g_j, $j \in \pi_0$, і далі в доведенні будемо дотримуватися позначень: $\{r_1, \ldots, r_\ell\} := \pi_0$,

$$\begin{aligned} f'_j(x_{r_1}, \ldots, x_{r_\ell}) &:= f_j(y_1, \ldots, y_n), \\ g'_j(x_{r_1}, \ldots, x_{r_\ell}) &:= g_j(y_1, \ldots, y_n) \end{aligned} \tag{3.11}$$

для всіх $j \in \pi_0$, де

$$y_s := \begin{cases} x_s, & \text{якщо } s \in \pi_0, \\ a_s & \text{в інших випадках.} \end{cases}$$

З індуктивного припущення випливає, що система (3.10) має єдиний розв'язок. Щоб цим скористатися, потрібно довести такі твердження:

1) операції f'_j, де $j \in \pi_0$, є π'-блочно ретрактно ортогональними;

2) операції g'_j, де $j \in \pi_0$, є побудовними за π'-блочним рекурсивним алгоритмом.

Доведемо твердження 1). Припущення теореми спричинює, що для довільного $i = 1, \ldots, m$ блок операцій $\{f_j, j \in \pi_i\}$ є π_i-ретрактно ортогональним. Це означає, що всі подібні π_i-ретракти цих операцій є ортогональними. Оскільки операції f'_j, де $j \in \pi_i$, є π_0-ретрактами операцій

f_j, де $j \in \pi_i$, то множина всіх вибірок подібних π_i-ретрактів операцій f'_j є підмножиною множини всіх вибірок подібних π_i-ретрактів операцій f_j. Але якщо кожна вибірка останньої множини є ортогональною, то кожна попередня множина є також ортогональною. Отже, операції f'_j, де $j \in \pi_i$, є π_i-ретрактно ортогональними. Оскільки i є довільним, то операції f'_j, де $j \in \pi_0$, є π'-блочно ретрактно ортогональними, тобто твердження 1) доведено.

Доведемо твердження 2). Застосовуючи (3.9) і (3.11) до перших m блоків алгоритму 1, отримуємо перший блок операцій:

$$g'_j(x_{s_1}, \ldots, x_{s_\ell}) = f'_j(x_{s_1}, \ldots, x_{s_\ell}), \quad j \in \pi_1;$$

та для кожного $i = 2, \ldots, m$ i-ий блок операцій:

$$g'_j(x_{s_1}, \ldots, x_{s_\ell}) = f'_j(t_{s_1}, \ldots, t_{s_\ell}), \quad j \in \pi_i,$$

де

$$t_s := \begin{cases} g'_{s\tau_{i-1}}(x_{s_1}, \ldots, x_{s_\ell}), & \text{якщо } s \in \pi_1 \cup \cdots \cup \pi_{i-1}, \\ x_s & \text{в інших випадках.} \end{cases}$$

Відповідно до означення блочного рекурсивного алгоритму, цей алгоритм будує $\{g'_j,\ j \in \pi_0\}$ із f'_j, де $j \in \pi_0$, тобто виконується твнрдження 2).

Відповідно до індуктивного припущення, система (3.10) має єдиний розв'язок:

$$x_s := a_s, \qquad s \in \pi_0. \tag{3.12}$$

Комбінуючи (3.9) і (3.12) з'ясовуємо, що $(a_1, \ldots, a_n)$ є розв'язком (3.6). Це означає ортогональність операцій $g_1, \ldots, g_n$.

Таким чином, відповідно до індуктивного припущення твердження теореми істинне для всіх натуральних k, тобто для довільного числа блоків розбиття π. □

В умові теореми 3.4 покладемо $\pi = \{\delta, \overline{1,n}\backslash\delta\}$, де мають місце позначення (3.1), тоді

$$g_1 = f_1,\ g_2 = f_2, \ldots, g_k = f_k,\ g_{k+1} = e_{j_1}, \ldots, g_n = e_{j_{n-k}},$$

тобто отримали необхідність леми 1 із [67]. Переформулюємо відповідно до нашої системи означень:

Твердження 3.1. *Якщо k-вибірка n-арних операцій $f_1,\ldots,f_k$ є δ-ретрактно ортогональною, то n-вибірка $f_1,\ldots,f_k,e_{j_1},\ldots,e_{j_{n-k}}$ є ортогональною.*

π-блочний рекурсивний алгоритм називатимемо тривіальним рекурсивним алгоритмом, якщо π є тривіальним, тобто кожен блок розбиття π є одноелементною множиною.

Розглянемо загальний вигляд тривіального рекурсивного алгоритму. Оскільки блоки операцій є одноелементними множинами, то кожен блок містить лише одну операцію. Ретрактна ортогональність операції є її i-оборотністю.

Алгоритм 3.3 (Тривіальний рекурсивний алгоритм)**.** *Нехай $\pi := \{\{i_1\},\ldots,\{i_n\}\}$ є розбиттям множини $\overline{1,n}$ і $f_1,\ldots,f_n$ є n-арними операціями, $\tau_1\in \mathrm{S}_{\{i_1\}}$, $\tau_2\in \mathrm{S}_{\{i_1,i_2\}}$, $\ldots$, $\tau_{n-1}\in \mathrm{S}_{\{i_1,\ldots,i_{n-1}\}}$.*

Операції $g_1,\ldots,g_n$ будуються за допомогою таких кроків:

1) першою операцією є

$$g_{i_1}(x_1,\ldots,x_n) := f_{i_1}(x_1,\ldots,x_n);$$

2) для кожного $j\in\{i_2,\ldots,i_n\}$, j-ю операцією є

$$g_j(x_1,\ldots,x_n) := f_j(t_1,\ldots,t_n),$$

де

$$t_s := \begin{cases} g_{s\tau_{j-1}}(x_1,\ldots,x_n), & \text{якщо } s\in\{i_1,\ldots,i_{s-1}\},\\ x_s & \text{в інших випадках.}\end{cases}$$

Наслідок 3.1. *Нехай операції $f_1,\ldots,f_n$ є i_1-, $\ldots$, i_n-оборотними. Тоді операції $g_1,\ldots,g_n$, які побудовані за тривіальним рекурсивним алгоритмом, є ортогональними.*

Це твердження є прямим наслідком теореми 3.4.

Якщо $i_1 = n$, $i_2 = n-1$, $\ldots$, $i_n = 1$ і τ_1, τ_2, $\ldots$, τ_{n-1} є тривіальними перетвореннями, то отримуємо алгоритм (1.7) (див. теорема 1.14), що запропонували Г.Б. Білявська і Г.Л. Муллен у [64].

Алгоритм 3.3 при умові, що τ_1, τ_2, $\ldots$, τ_{n-1} є тривіальними перетвореннями, також отримали С. Марковські та А. Мілева у роботі [93] використовуючи підхід Г.Б. Білявської і Г.Л. Муллена.

Зазначимо, що одна із вхідних операцій тривіального рекурсивного алгоритму входить до вибірки побудованих ортогональних операцій, отже, вона залишається незмінною. Тому з того, що ця операція є i-оборотною для деякого $i \in \overline{1,n}$ випливає, що принаймні одна із операцій побудованої за цим алгоритмом вибірки є i-оборотною для деякого $i \in \overline{1,n}$.

Твердження 3.2. *Якщо вибірка ортогональних n-арних операцій є побудовною за тривіальним рекурсивним алгоритмом, то існує $i \in \overline{1,n}$ таке, що принаймні одна із побудованих операцій є i-оборотною.*

Якщо вибірка ортогональних n-арних операцій є побудовною за тривіальним рекурсивним алгоритмом з визначаючим розбиттям виду $\{\{i\}, \pi_2, \ldots, \pi_k\}$, то одна із побудованих операцій є i-оборотною.

Нижче наводимо один із найпростіших прикладів існування вибірок ортогональних операцій, які є побудовними за блочним рекурсивним алгоритмом, але є непобудовними за тривіальним рекурсивним алгоритмом.

Приклад 3.1. *Розглянемо четвірку операцій*

$$\begin{aligned} f_1(x,y,z,t) &= 3x + 2y + 3z + 4t, \\ f_2(x,y,z,t) &= 2x + 3y + 3z + 2t, \\ f_3(x,y,z,t) &= 4x + 2y + 3z + 2t, \\ f_4(x,y,z,t) &= 2x + 2y + 2z + 3t \end{aligned}$$

на $\mathbb{Z}_6$. Оскільки f_1, f_2 є $\{1,2\}$-ретрактно ортогональними, f_3, f_4 є $\{3,4\}$-ретрактно ортогональними, тоді $\pi = \big\{\{1,2\},\{3,4\}\big\}$. Існує два варіанти вибору τ_1, оскільки τ_1 є перестановкою множини $\{1,2\}$: $\tau_1 = \iota$ і $\tau_1 = (12)$, де ι є тотожньою перестановкою. Для кожного із цих варіантів будуємо

четвірку ортогональних операцій за блочним рекурсивним алгоритмом.

Нехай $\tau_1 = \iota$, *тоді за* π*-блочним рекурсивним алгоритмом*

$$g_1(x,y,z,t) = 3x + 2y + 3z + 4t,$$
$$g_2(x,y,z,t) = 2x + 3y + 3z + 2t,$$
$$g_3(x,y,z,t) = 4(3x + 2y + 3z + 4t) + 2(2x + 3y + 3z + 2t) + 3z + 2t,$$
$$g_4(x,y,z,t) = 2(3x + 2y + 3z + 4t) + 2(2x + 3y + 3z + 2t) + 2z + 3t,$$

тобто

$$g_1(x,y,z,t) = 3x + 2y + 3z + 4t,$$
$$g_2(x,y,z,t) = 2x + 3y + 3z + 2t,$$
$$g_3(x,y,z,t) = 4x + 2y + 3z + 4t,$$
$$g_4(x,y,z,t) = 4x + 4y + 2z + 3t.$$

І нехай $\tau_1 = (12)$, *тоді за* π*-блочним рекурсивним алгоритмом*

$$g'_1(x,y,z,t) = 3x + 2y + 3z + 4t,$$
$$g'_2(x,y,z,t) = 2x + 3y + 3z + 2t,$$
$$g'_3(x,y,z,t) = 4(2x + 3y + 3z + 2t) + 2(3x + 2y + 3z + 4t) + 3z + 2t,$$
$$g'_4(x,y,z,t) = 2(2x + 3y + 3z + 2t) + 2(3x + 2y + 3z + 4t) + 2z + 3t,$$

тобто

$$g'_1(x,y,z,t) = 3x + 2y + 3z + 4t,$$
$$g'_2(x,y,z,t) = 2x + 3y + 3z + 2t,$$
$$g'_3(x,y,z,t) = 2x + 4y + 3z + 0t,$$
$$g'_4(x,y,z,t) = 4x + 4y + 2z + 3t.$$

Тривіальний рекурсивний алгоритм вимагає, щоб принаймні одна із побудованих операцій була i*-оборотною для деякого* $i \in \{1,2,3,4\}$. *Кожна із побудованих четвірок не є побудовною за тривіальним рекурсивним алгоритмом, оскільки усі операції* g_1, g_2, g_3, g_4 *і* g'_1, g'_2, g'_3, g'_4 *не є* i*-оборотними для всіх* $i \in \{1,2,3,4\}$.

Цей приклад доводить таке твердження:

Твердження 3.3. *Існують вибірки ортогональних операцій, які є*

побудовними за блочним рекурсивним алгоритмом, але є непобудовними за тривіальним рекурсивним алгоритмом.

3.3. Блочний композиційний алгоритм

У цьому параграфі подається алгоритм побудови ортогональних n-арних операцій з вибірок ортогональних операцій меншої арності. Цей алгоритм є композицією наведених вище алгоритмів, а саме, композиційного алгоритму та блочного рекурсивного алгоритму, і складається із k блоків. Для кожного $i \in \overline{1,k}$ кожний i-ий блок містить n_i-вибірку n_i-арних ортогональних операцій і $n_1+n_2+\cdots+n_k = n$, тобто на вході маємо блоки ортогональних операцій такі, що сума кількостей цих операцій становить n.

Опишемо цей алгоритм детальніше.

Алгоритм 3.4 (π-блочний композиційний алгоритм)**.** *Нехай* $\pi = \{\pi_1, \ldots, \pi_k\}$ *є розбиттям множини* $\overline{1,n}$ *і нехай для всіх* $i = 1, \ldots, k$ *виконуються умови*

– h_j, *де* $j \in \pi_i$, *є* $|\pi_i|$*-арними операціями,*

– p_j, *де* $j \in \pi_i$, *є* $(n - |\pi_i| + 1)$*-арними операціями,*

– $\sigma_i \in \mathrm{S}_{n+1}^{\pi_i}$,

– $\tau_{i-1} \in \mathrm{S}_{\pi_1 \cup \cdots \cup \pi_{i-1}}$, $i > 1$.

Операції $g_1, \ldots, g_n$ *будуються за допомогою нижче наведених кроків:*

1) для всіх $j \in \pi_i$, $i = 1, \ldots, k$, *операції* f_j *будуються таким чином:*

$$f_j(x_1, \ldots, x_n) := p_j\big(h_j(x_1, \ldots, x_{|\pi_i|}), x_{|\pi_i|+1}, \ldots, x_n\big);$$

2) парастрофи ${}^{\sigma_i}f_j$, *де* $j \in \pi_i$, *утворюються із операцій* f_j, $i = 1, \ldots, k$;

3) операції $g_1, \ldots, g_n$ *будуються за допомогою блочного рекурсивного алгоритму:*

3.1) першим блоком операцій є

$$g_j(x_1, \ldots, x_n) := {}^{\sigma_1}f_j(x_1, \ldots, x_n), \quad j \in \pi_1,$$

3.2) для кожного $i = 2, \ldots, k$, *і-им блоком операцій є*

$$g_j(x_1, \ldots, x_n) := {}^{\sigma_i}f_j(t_1, \ldots, t_n), \quad j \in \pi_i,$$

де

$$t_s := \begin{cases} g_{s\tau_{i-1}}(x_1, \ldots, x_n), & \text{якщо } s \in \pi_1 \cup \cdots \cup \pi_{i-1}, \\ x_s & \text{в інших випадках.} \end{cases}$$

Теорема 3.5. *Нехай* $\pi = \{\pi_1, \ldots, \pi_k\}$ *є розбиттям множини* $\overline{1,n}$ *і для всіх* $i = 1, \ldots, k$ *виконуються умови:*

– h_j, *де* $j \in \pi_i$, *є* $|\pi_i|$*-арними ортогональними операціями,*

– p_j, *де* $j \in \pi_i$, *є* 1*-оборотними* $(n - |\pi_i| + 1)$*-арними операціями.*

Тоді n*-арні операції* g_1, ..., g_n, *які є побудовними за* π*-блочним композиційним алгоритмом, є ортогональними.*

Доведення. Припустимо, що умови теореми виконуються. Розглянемо доведення відповідно до кроків блочного композиційного алгоритму для довільного $j \in \pi_i$, де $i \in \overline{1,k}$.

1. За теоремою 3.1, операції f_j є $\{1, \ldots, |\pi_i|\}$-ретрактно ортогональними для всіх $i \in \overline{1,k}$.

2. Оскільки $\{1, \ldots, |\pi_i|\}\sigma_i^{-1} = \pi_i$, то для всіх $i \in \overline{1,k}$ операції ${}^{\sigma_i}f_j$ є π_i-ретрактно ортогональними відповідно до леми 3.1.

3. Оскільки для всіх $i \in \overline{1,k}$ операції ${}^{\sigma_i}f_j$ є π_i-ретрактно ортогональними, до них можна застосувати блочний рекурсивний алгоритм. Відповідно до теореми 3.4 операції g_1, ..., g_n є ортогональними. □

Зауваження 3.1. *Якщо* π_i *є одноелементною множиною, то вона містить лише* j, *тобто* $\pi_i = \{j\}$. *Звідси* p_j *є* 1*-оборотною* n*-арною операцією і* h_j *є унарною квазігрупою, тобто підстановкою носія. Таким чином, операція* f_j, *що визначається рівністю*

$$f_j(x_1, \ldots, x_n) := p_j(h_j(x_1), x_2, \ldots, x_n),$$

є ізотопною до p_j. Параметр σ_i є циклом $(1\,j)$.

Кожен із цих алгоритмів описує серію алгоритмів. Загалом, навіть для тривіальних класів операцій кожний вибір параметрів алгоритму дає можливість отримати різні вибірки операцій, які не обов'язково є парастрофними. Розглянемо цей факт у нижче наведеному прикладі.

Приклад 3.2. *Нехай $\mathbb{Z}_6$ є носієм і пари операцій h_1, h_2 та h_3, h_4, які визначаються рівностями*

$$h_1(x_1, x_2) = 3x_1 + 2x_2, \qquad h_3(x_1, x_2) = 3x_1 + 2x_2,$$
$$h_2(x_1, x_2) = 2x_1 + 3x_2, \qquad h_4(x_1, x_2) = 2x_1 + 3x_2,$$

є ортогональними, операції p_1, p_2, p_3, p_4, які визначаються рівностями

$$p_1(u, x_3, x_4) = u + 2x_3 + 2x_4,$$
$$p_2(u, x_3, x_4) = u + 3x_3 + 4x_4,$$
$$p_3(u, x_3, x_4) = u + 4x_3 + 2x_4,$$
$$p_4(u, x_3, x_4) = u + 2x_3 + 2x_4,$$

є 1-оборотними, $\sigma_1 \in \mathrm{S}_5^{\{1,2\}}$, $\sigma_2 \in \mathrm{S}_5^{\{3,4\}}$, де

$$\mathrm{S}_5^{\{1,2\}} = \{\iota,\ (12),\ (34),\ (12)(34)\},$$

$$\mathrm{S}_5^{\{3,4\}} = \{(13)(24),\ (14)(23),\ (1324),\ (1423)\},$$

і $\tau_1 \in \mathrm{S}_{\{1,2\}}$, де $\mathrm{S}_{\{1,2\}} = \big\{\iota,\ (12)\big\}$.

Використовуючи ці дані, побудуємо ортогональні операції за блочним композиційним алгоритмом.

За кроком 1 алгоритму 3.4 із заданих операцій будуємо ретрактно ортогональні операції:

$$B_1 : \begin{cases} f_1(x_1, x_2, x_3, x_4) := p_1(h_1(x_1, x_2), x_3, x_4) = 3x_1 + 2x_2 + 2x_3 + 2x_4, \\ f_2(x_1, x_2, x_3, x_4) := p_2(h_2(x_1, x_2), x_3, x_4) = 2x_1 + 3x_2 + 3x_3 + 4x_4, \end{cases}$$
$$B_2 : \begin{cases} f_3(x_1, x_2, x_3, x_4) := p_2(h_2(x_1, x_2), x_3, x_4) = 3x_1 + 2x_2 + 4x_3 + 2x_4, \\ f_4(x_1, x_2, x_3, x_4) := p_3(h_3(x_1, x_2), x_3, x_4) = 2x_1 + 3x_2 + 2x_3 + 2x_4. \end{cases}$$

За кроком 2 застосовуємо перестановки σ_1, σ_2 до відповідних блоків операцій. Існує 16 різних випадків. Щоб показати залежність між різними вибірками розглянемо дві із них. Наприклад, якщо $\sigma_1 = \iota$, $\sigma_2 = (13)(24)$ і якщо $\sigma_1 = (12)$, $\sigma_2 = (23)(14)$.

Якщо $\sigma_1 = \iota$, $\sigma_2 = (13)(24)$, то

$$B_1 : \begin{cases} {}^{\sigma_1}f_1(x_1, x_2, x_3, x_4) = 3x_1 + 2x_2 + 2x_3 + 2x_4, \\ {}^{\sigma_1}f_2(x_1, x_2, x_3, x_4) = 2x_1 + 3x_2 + 3x_3 + 4x_4, \end{cases}$$

$$B_2 : \begin{cases} {}^{\sigma_2}f_3(x_1, x_2, x_3, x_4) = 4x_1 + 2x_2 + 3x_3 + 2x_4, \\ {}^{\sigma_2}f_4(x_1, x_2, x_3, x_4) = 2x_1 + 2x_2 + 2x_3 + 3x_4. \end{cases}$$

Якщо $\sigma_1 = (12)$, $\sigma_2 = (23)(14)$, то

$$B_1 : \begin{cases} {}^{\sigma_1}f_1(x_1, x_2, x_3, x_4) = 2x_1 + 3x_2 + 2x_3 + 2x_4, \\ {}^{\sigma_1}f_2(x_1, x_2, x_3, x_4) = 3x_1 + 2x_2 + 3x_3 + 4x_4, \end{cases}$$

$$B_2 : \begin{cases} {}^{\sigma_2}f_3(x_1, x_2, x_3, x_4) = 2x_1 + 4x_2 + 2x_3 + 3x_4, \\ {}^{\sigma_2}f_4(x_1, x_2, x_3, x_4) = 2x_1 + 2x_2 + 3x_3 + 2x_4. \end{cases}$$

За кроком 3 застосовуємо блочний рекурсивний алгоритм до побудованих операцій, для прикладу розглянемо коли $\tau_1 = \iota$.

Якщо $\sigma_1 = \iota$, $\sigma_2 = (13)(24)$, $\tau_1 = \iota$, то

$$B_1 : \begin{cases} g_1(x_1, x_2, x_3, x_4) = 3x_1 + 2x_2 + 2x_3 + 2x_4, \\ g_2(x_1, x_2, x_3, x_4) = 2x_1 + 3x_2 + 3x_3 + 4x_4, \end{cases}$$

$$B_2 : \begin{cases} g_3(x_1, x_2, x_3, x_4) = 4x_1 + 2x_2 + 5x_3 + 0x_4, \\ g_4(x_1, x_2, x_3, x_4) = 4x_1 + 4x_2 + 0x_3 + 3x_4. \end{cases}$$

Якщо $\sigma_1 = (12)$, $\sigma_2 = (23)(14)$, $\tau_1 = \iota$, то

$$B_1 : \begin{cases} g_1(x_1, x_2, x_3, x_4) = 2x_1 + 3x_2 + 2x_3 + 2x_4, \\ g_2(x_1, x_2, x_3, x_4) = 3x_1 + 2x_2 + 3x_3 + 4x_4, \end{cases}$$

$$B_2 : \begin{cases} g_3(x_1, x_2, x_3, x_4) = 4x_1 + 2x_2 + x_3 + 2x_4, \\ g_4(x_1, x_2, x_3, x_4) = 0x_1 + x_2 + 2x_3 + 5x_4. \end{cases}$$

Побудовані вибірки ортогональних операцій є різними і відповідно до означення парастрофних вибірок вони не є парастрофними. Існує 32 можливі побудови із заданих операцій. Справді, оскільки їхня кількість залежить від кількості можливих перестановок σ_1, σ_2 і τ_1, то

$$|\mathrm{S}_5^{\{1,2\}}| \cdot |\mathrm{S}_5^{\{3,4\}}| \cdot |\mathrm{S}_{\{1,2\}}| = 4 \cdot 4 \cdot 2 = 32.$$

Зауваження 3.2. *За допомогою тих самих операцій для різних наборів параметрів можна побудувати різні вибірки ортогональних операцій. Але проблема, коли ці вибірки збігаються або частково збігаються, потребує додаткового дослідження.*

Наведений нижче приклад ілюструє побудову за блочним композиційним алгоритмом.

Приклад 3.3. *Нехай $\pi = \{\{2\}, \{1,3,4\}\}$, $\mathbb{Z}_{15}$ є носієм і операції*

$$\begin{aligned} p_1(x_1, x_2, x_3, x_4) &= x_1 + 4x_2 + 2x_3 + x_4, \\ p_2(x_3, x_4) &= x_3 + 5x_4, \\ p_3(x_3, x_4) &= 4x_3 + x_4, \\ p_4(x_3, x_4) &= x_3 + 11x_4 \end{aligned}$$

є 1-оборотними, операція h_1, яка визначається рівністю $h_1(x_1) = 5x_1$, є підстановкою ($\{1\}$-ретрактно ортогональною), операції

$$\begin{aligned} h_2(x_1, x_2, x_3) &= 3x_1 + 2x_2 + 6x_3, \\ h_3(x_1, x_2, x_3) &= 2x_1 + 3x_2 + 3x_3, \\ h_4(x_1, x_2, x_3) &= 2x_1 + x_2 + 2x_3 \end{aligned}$$

є ортогональними, $\sigma_1 = (12)$, $\sigma_2 = (234)$, $\tau_1 = \iota$.

Побудуємо ортогональні операції із заданих операцій для розбиття π за блочним композиційним алгоритмом.

За кроком 1 алгоритму 3.4 відповідно до (3.3), будуємо операції f_1, f_2,

f_3, f_4:

$$B_1 : \begin{cases} f_1(x_1, x_2, x_3, x_4) := p_1(h_1(x_1), x_2, x_3, x_4) = 7x_1 + 4x_2 + 2x_3 + x_4, \end{cases}$$

$$B_2 : \begin{cases} f_2(x_1, x_2, x_3, x_4) := p_2(h_2(x_1, x_2, x_3), x_4) = 3x_1 + 2x_2 + 6x_3 + 5x_4, \\ f_3(x_1, x_2, x_3, x_4) := p_3(h_3(x_1, x_2, x_3), x_4) = 8x_1 + 12x_2 + 12x_3 + x_4, \\ f_4(x_1, x_2, x_3, x_4) := p_4(h_4(x_1, x_2, x_3), x_4) = 2x_1 + x_2 + 2x_3 + 11x_4. \end{cases}$$

За кроком 2 застосовуємо перестановку σ_1 до першого блоку:

$$^{\sigma_1}f_1(x_1, x_2, x_3, x_4) = 4x_1 + 7x_2 + 2x_3 + x_4$$

і σ_2 до другого блоку:

$$\begin{aligned} ^{\sigma_2}f_2(x_1, x_2, x_3, x_4) &= 3x_1 + 5x_2 + 6x_3 + 2x_4, \\ ^{\sigma_2}f_3(x_1, x_2, x_3, x_4) &= 8x_1 + x_2 + 12x_3 + 12x_4, \\ ^{\sigma_2}f_4(x_1, x_2, x_3, x_4) &= 2x_1 + 11x_2 + 2x_3 + x_4. \end{aligned}$$

За лемою 3.1, операція $^{\sigma_1}f_2$ є 2-оборотною і $^{\sigma_2}f_2$, $^{\sigma_2}f_3$, $^{\sigma_2}f_4$ є $\{1, 3, 4\}$-ретрактно ортогональними.

За кроком 3 записуємо ортогональні операції g_1, g_2, g_3, g_4 для заданого розбиття π:

$$\begin{aligned} g_1(x_1, x_2, x_3, x_4) &= 7x_1 + 4x_2 + 2x_3 + x_4, \\ g_2(x_1, x_2, x_3, x_4) &= 3x_1 + 5(7x_1 + 4x_2 + 2x_3 + x_4) + 6x_3 + 2x_4, \\ g_3(x_1, x_2, x_3, x_4) &= 8x_1 + (7x_1 + 4x_2 + 2x_3 + x_4) + 12x_3 + 12x_4, \\ g_4(x_1, x_2, x_3, x_4) &= 2x_1 + 11(7x_1 + 4x_2 + 2x_3 + x_4) + 2x_3 + x_4, \end{aligned}$$

тобто

$$\begin{aligned} g_1(x_1, x_2, x_3, x_4) &= 7x_1 + 4x_2 + 2x_3 + x_4, \\ g_2(x_1, x_2, x_3, x_4) &= 8x_1 + 5x_2 + x_3 + 7x_4, \\ g_3(x_1, x_2, x_3, x_4) &= 0x_1 + 4x_2 + 14x_3 + 13x_4, \\ g_4(x_1, x_2, x_3, x_4) &= 4x_1 + 14x_2 + 9x_3 + 12x_4. \end{aligned}$$

Відповідно до блочного композиційного алгоритму, операції g_1, g_2, g_3, g_4 є ортогональними.

Зауваження 3.3. *Теорема 1.7 спричинює, що будь-яка підвибірка операцій із вибірки ортогональних операцій є ортогональною. Відповідно до теореми 1.10 будь-яку k-вибірку ортогональних n-арних операцій, де $k < n$, можна занурити в деяку n-вибірку ортогональних n-арних операцій. Таким чином, блочний рекурсивний алгоритм і блочний композиційний алгоритм дають можливість будувати ℓ-вибірки ортогональних n-арних операцій, де $\ell \leqslant n$.*

Висновки до розділу 3

У цьому розділі запропоновано новий метод побудови ортогональних операцій "блочний рекурсивний алгоритм", який є узагальненням алгоритмів із [64] і [93]. У зв'язку з цим використано інший підхід до означення операцій, які мають ортогональні ретракти, так що одним із параметрів алгоритму побудови є розбиття множини індексів змінних, а кожен із блоків розбиття визначає ретрактну ортогональність відповідної заданої вибірки операцій.

Основні результати розділу:

1) запропоновано алгоритм побудови ретрактно ортогональних операцій (композиційний алгоритм);
2) запропоновано блочний рекурсивний алгоритм побудови ортогональних операцій та доведено існування вибірок ортогональних операцій, які є побудовними за блочним рекурсивним алгоритмом, але є непобудовними за тривіальними випадками цього алгоритму;
3) запропоновано алгоритм побудови ортогональних операцій із блоків ортогональних операцій меншої арності (блочний композиційний алгоритм).

Результати цього розділу опубліковано в [85] і [90].

РОЗДІЛ 4

ДОПОВНЕННЯ ОРТОГОНАЛЬНИХ ОПЕРАЦІЙ

Цей розділ присвячений вивченню методів побудови ортогональних доповнень ортогональних багатомісних операцій. Для цього вивчаються зв'язки між ретрактною ортогональністю і ортогональністю. А також зроблено певні наслідки для лінійних операцій і центральних квазігруп.

Ортогональність ретрактів також вивчали Г.Б. Білявська і Г.Л. Муллен у [67] для описання зв'язку між сильною ортогональністю вибірки операцій і ортогональністю ретрактів операцій цієї вибірки, зокрема вони довели критерій ретрактної ортогональності операцій.

4.1. Ретрактна ортогональність та ортогональність

4.1.1. Відношення між поняттями ортогональності та ретрактної ортогональності

У цьому підрозділі ми вивчаємо зв'язки між ортогональністю та ретрактною ортогональністю.

У розділі 3 наведено означення δ-ретрактної ортогональності лише для випадку, коли $|\delta|$ збігається із кількістю операцій у вибірці. Нижче наводимо означення для інших випадків відповідно до підходу викладеного у підрозділі 3.1.

Означення 4.1. *Нехай $\delta \subset \overline{1,n}$, $|\delta| = k$ і $t \in \overline{1,n}$ таке що $t < k < n$. t-вибірку n-арних операцій $f_1, \dots, f_t$ визначених на множині Q називатимемо δ-ретрактно ортогональною, якщо всі подібні δ-ретракти цих операцій є ортогональними, тобто для довільної послідовності $\bar{a} \in Q^{n-k}$ і довільних елементів $b_1, \dots, b_t \in Q$, система*

$$\begin{cases} f_{1;(\bar{a},\delta)}(x_{i_1}, \dots, x_{i_k}) = b_1, \\ \dots\dots\dots\dots\dots\dots\dots \\ f_{t;(\bar{a},\delta)}(x_{i_1}, \dots, x_{i_k}) = b_t \end{cases}$$

має m^{k-t} *розв'язків, де* $m = |Q|$.

Означення 4.2. *Нехай* $\delta \subset \overline{1,n}$, $|\delta| = k$ *і* s *таке, що* $s > k$. s*-вибірку* n*-арних операцій називатимемо* δ*-ретрактно ортогональною, якщо кожна її* k*-підвибірка є* δ*-ретрактно ортогональною.*

Означення 4.3. *Нехай* $\delta \subset \overline{1,n}$, $|\delta| = k$ *і* $\ell \in \overline{1,n}$ *таке, що* $\ell \leqslant k$. k*-вибірку* n*-арних операцій називатимемо* ℓ*-кратно* δ*-ретрактно ортогональною, якщо кожна її* ℓ*-підвибірка є* δ*-ретрактно ортогональною.*

Очевидно, що кожний ретракт квазігрупи є також квазігрупою. Але існують повні операції такі, що для деякого δ їхні ретракти не є повними.

Приклад 4.1. n*-арний селектор* e_i *є повною операцією.* δ*-ретракт операції* e_i *є повним* ($|\delta| = k$)*, якщо* $i \in \delta$*, до того ж, цей ретракт є селектором також. Якщо ж* $i \notin \delta$*, то* δ*-ретракт не є повним, оскільки для кожної послідовності* $\bar{a} := (a_{j_1}, \ldots, a_{j_{n-k}}) \in Q^{n-k}$ *відповідний гіперкуб для* $e_{i;(\bar{a},\delta)}$ *містить лише один елемент, яким зафіксовано* x_i.

Теорема 4.1. *Якщо для деякого* $\delta \subset \overline{1,n}$ *вибірка* n*-арних операцій є* δ*-ретрактно ортогональною, то вона є ортогональною.*

Доведення. Припустимо, що n-арні операції $f_1, \ldots, f_k$ є δ-ретрактно ортогональними і $|\delta| = k$, де $k < n$. Розглянемо розбиття $\pi = \{\delta, \pi_2, \ldots, \pi_r\}$ множини $\overline{1,n}$, де $\pi_2, \ldots, \pi_r$ є довільними попарно неперехресними підмножинами множини $\overline{1,n}\backslash\delta$. Операції $f_1, \ldots, f_k$ завжди можуть бути вибрані першим блоком вхідних операцій π-блочного рекурсивного алгоритму, тоді вибіркою вихідних операцій є $f_1, \ldots, f_k, g_{k+1}, \ldots, g_n$, де $g_{k+1}, \ldots, g_n$ є n-арними операціями, які отримані за кроками 2) – r) цього алгоритму із блоків довільних π_2-,$\ldots$, π_r-ретрактно ортогональних операцій. За теоремою 3.4, операції $f_1, \ldots, f_k, g_{k+1}, \ldots, g_n$ є ортогональними, тобто вони є n-кратно ортогональними. За теоремою 1.7, вони є також ℓ-кратно ортогональними для всіх $\ell < n$, отже, для $\ell = k$ також. Звідси вибірка операцій $f_1, \ldots, f_k, g_{k+1}, \ldots, g_n$ є k-кратно ортогональною, тобто кожна її

k-підвибірка операцій є ортогональною, тобто $f_1, \ldots, f_k$ є також ортогональними.

Якщо $|\delta| =: t$, де $k < t < n$, тоді, за теоремою 1.10, кожна k-вибірка δ-ретрактно ортогональних n-арних операцій може бути вбудована у t-вибірку δ-ретрактно ортогональних n-арних операцій. Тому існує $(t-k)$-вибірка n-арних операцій $f_{k+1}, \ldots, f_t$ таких, що t-вибірка $f_1, \ldots, f_k$, $f_{k+1}, \ldots, f_t$ є δ-ретрактно ортогональною. Як показано вище, ця вибірка є ортогональною. Отже, відповідно до теореми 1.7, кожна її k-підвибірка є ортогональною. □

Твердження теореми 4.1 можна також отримати як наслідок леми 1 із [67] використовуючи теорему 1.7. Проте побудова і доведення основного алгоритму потребує підходу викладеного в доведенні теореми 4.1.

Нехай $|\delta| = k$ і $\ell < k < n$. За теоремою 4.1 ретрактна ортогональність спричинює ортогональність, звідси

– ℓ-кратна δ-ретрактна ортогональність k-вибірки n-арних операцій спричинює ℓ-кратну ортогональність цієї вибірки відповідно до означення 4.3;

– δ-ретрактна ортогональність n-вибірки n-арних операцій спричинює її k-кратну ортогональність відповідно до означення 4.2.

Переформулюємо достатність леми 1 із [67] відповідно до нашої системи означень та позначень:

Твердження 4.1. *Якщо* $f_1,\ldots, f_k, e_{j_1},\ldots, e_{j_{n-k}}$, *де мають місце позначення* (3.1), *є ортогональними, то* $f_1,\ldots, f_k$ *є* δ*-ретрактно ортогональними.*

Доведемо, що обернене твердження до теореми 4.1 не є істинним.

Приклад 4.2. *Нехай g, h, t і p є 4-арні операції:*

$$g(x_1, x_2, x_3, x_4) = 2x_1 - 4x_2 + 2x_3 + 5x_4,$$
$$h(x_1, x_2, x_3, x_4) = 4x_1 + 6x_2 + x_3 + 5x_4,$$
$$t(x_1, x_2, x_3, x_4) = x_1 - x_2 + x_3 + x_4,$$
$$p(x_1, x_2, x_3, x_4) = -x_1 + 2x_2 - 7x_3 + x_4$$

на $\mathbb{Z}_{20}$. Вони є ортогональними, оскільки їхній визначник -171 є взаємнопростим із 20. За теоремою 1.7 операції g і h є ортогональними також. Перевіримо ортогональність їхніх відповідних бінарних ретрактів. Розглянемо $\{1,2\}$-ретракти операцій g і h:

$$g(x_1, x_2, a, b) = 2x_1 - 4x_2 + 2a + 5b,$$
$$h(x_1, x_2, a, b) = 4x_1 + 6x_2 + a + 5b$$

Операції g і h є $\{1,2\}$-ретрактно ортогональними тоді і тільки тоді, коли всі їхні подібні $\{1,2\}$-ретракти є ортогональними. Оскільки операції визначені над кільцем лишків, то розв'язність відповідної системи не залежить від фіксації змінних x_3 та x_4. Для будь-яких $a, b, c, d \in \mathbb{Z}_{20}$ система

$$2x_1 - 4x_2 + 2a + 5b = c,$$
$$4x_1 + 6x_2 + a + 5b = d$$

не має розв'язків, тому що

$$\begin{vmatrix} 2 & -4 \\ 4 & 6 \end{vmatrix} = 28$$

і не є взаємнопростим із модулем. Отже, g і h не є $\{1,2\}$-ретрактно ортогональними.

Аналогічно можна переконатися, що g і h не є δ-ретрактно ортогональними для кожного $|\delta| = 2$. До того ж, всі подібні тернарні ретракти операцій g і h також не є ортогональними, оскільки частина коефіцієнтів цих операцій не є взаємнопростими із модулем. Таким чином, множини розв'язків відповідних систем рівнянь не є максимальними.

Ортогональні операції h і t не є $\{1,2\}$-, $\{3,4\}$-ретрактно ортогональними, але є ретрактно ортогональними для інших можливих випадків $|\delta| = 2$.

Твердження 4.2. *Нехай $k < n$. Тоді існує k-вибірка ортогональних n-арних операцій таких, що для деякого $\delta \subset \overline{1,n}$, де $|\delta| = k$, вона не є δ-ретрактно ортогональною.*

Доведення. Припустимо, що ортогональність k-вибірки n-арних операцій спричинює, що для всіх $|\delta| = k$ ця вибірка є δ-ретрактно ортогональною. Якщо $k = 1$, то ортогональність операції означає її повноту. З іншого боку, відповідно до нашого припущення, для всіх $i \in \overline{1,n}$ ця операція є $\{i\}$-ретрактно ортогональною, тобто для всіх $i \in \overline{1,n}$ вона є i-оборотною. Звідси повна операція є квазігруповою. Отримана суперечність свідчить про хибність нашого припущення.

Переформулювавши твердження 4.1 за законом контрапозиції маємо: якщо $f_1,\ldots,f_k$ не є δ-ретрактно ортогональними, то $f_1,\ldots,f_k, e_{j_1},\ldots,e_{j_{n-k}}$ не є ортогональними. Але це не означає, що $f_1,\ldots,f_k$ не є ортогональними. Наприклад, існує $\delta_1 \in \overline{1,n}$ таке, що $|\delta_1| = k$ і $\delta_1 \neq \delta$, тоді за теоремою 4.1 операції $f_1,\ldots,f_k$ є ортогональними. Зокрема для нетривіального випадку контрприкладом є приклад 4.2.

Більше того доведено існування k-вибірки ортогональних n-арних операцій такої, що для всіх $\delta \subset \overline{1,n}$ ця вибірка не є δ-ретрактно ортогональною. □

k-вибірка n-арних операцій $f_1,\ldots,f_k$ $(k < n)$, яка побудована за допомогою (3.3), називатимемо продовженням k-вибірки ортогональних k-арних операцій $h_1,\ldots,h_k$ до k-вибірки n-арних операцій, де $p_1,\ldots,p_k$ є довільними 1-оборотними $(n-k+1)$-арними операціями.

Лема 4.1. *Кожна k-вибірка ортогональних k-арних операцій є продовжувальною до k-вибірки ортогональних n-арних операцій.*

Доведення. Відповідно до теореми 3.2, кожне продовження k-вибірки

ортогональних k-арних операцій є вибіркою $\overline{1,k}$-ретрактно ортогональних операцій і, отже, за теоремою 4.1 ці операції є ортогональними. Оскільки завжди існує k-вибірка 1-оборотних $(n-k+1)$-арних операцій, то кожна k-вибірка ортогональних k-арних операцій може бути продовжена до k-вибірки ортогональних n-арних операцій. □

Зауваження 4.1. *Нехай $p_1,\dots,p_k$ є довільними 1-оборотними $(n-k+1)$-арними операціями, $h_1,\dots,h_k$ є довільними k-арними операціями. Відповідно до теореми 3.2 і теореми 4.1 виконуються такі твердження:*

1) операції $f_1,\dots,f_k$, побудовні за формулами (3.3), є ортогональними і до того ж $\overline{1,k}$-ретрактно ортогональними тоді і тільки тоді, коли $h_1,\dots,h_k$ є ортогональними;

2) операції $f_1,\dots,f_k$, побудовні за формулами (3.5), є ортогональними і до того ж $\overline{1,k}$-ретрактно ортогональними тоді і тільки тоді, коли $p_1,\dots,p_k$ є ортогональними;

3) операції ${}^{\sigma}f_1,\dots,{}^{\sigma}f_k$, побудовні за композиційним алгоритмом, є δ-ретрактно ортогональними і є ортогональними.

Зауваження 4.2. *Якщо покласти підстановки носія $\alpha_1,\dots,\alpha_k$ замість $p_1,\dots,p_k$ у (3.3) відповідно, випливає відоме твердження: операції $\alpha_1 h_1,\dots,\alpha_k h_k$ є ортогональними тоді і тільки тоді, коли $h_1,\dots,h_k$ є ортогональними.*

Зауваження 4.3. *Вибірки ортогональних n-арних квазігруп $f_{i1},\dots,f_{ik}$, які побудовані за методом Т. Іванса (див. теорема 1.12) є $\{\ell,\dots,n\}$-ретрактно ортогональними відповідно до теореми 3.2, де ${}^{\sigma}\overline{1,k}=\{\ell,\dots,n\}$.*

4.1.2. Ретрактна ортогональність, перпендикулярність і сильна ортогональність

Опишемо залежність між різними узагальненнями ортогональності бінарних операцій. Зазначимо, що згідно означень 2.1 і 3.1, (ι, ι)-відповідні $\{m, i\}$-ретракти є тим же, що подібні $\{m, i\}$-ретракти.

Твердження 4.3. *Нехай g і h є n-арними операціями. Такі твердження є еквівалентними:*

1) g і h є перпендикулярними типу $(\iota, \iota; m)$, $m \in \overline{1,n}$;

2) g і h є δ-ретрактно ортогональними для всіх $\delta \subset \overline{1,n}$ таких, що $m \in \delta$ і $|\delta| = 2$.

Доведення. Припустимо, g і h є перпендикулярними типу $(\iota, \iota; m)$, $m \in \overline{1,n}$. Тоді, відповідно до означення 2.2, для всіх $i \in \overline{1,n} \backslash \{m\}$ кожна пара подібних $\{m, i\}$-ретрактів є ортогональною, тобто вони є $\{m, i\}$-ретрактно ортогональними для всіх $i \in \overline{1,n} \backslash \{m\}$. □

Наслідок 4.1. *Якщо n-арні операції g і h є перпендикулярними типу $(\iota, \iota; m)$, $m \in \overline{1,n}$, то вони є δ-ретрактно ортогональними для всіх $\delta \subset \overline{1,n}$, де $|\delta| > 1$ і $m \in \delta$.*

Доведення. За теоремою 4.1, $\{m, i\}$-ретрактна ортогональність операцій g і h спричинює їхню δ-ретрактну ортогональність для всіх $\delta \subset \overline{1,n}$, де $|\delta| > 2$, таких, що $m \in \delta$. □

Відповідно до твердження 4.3, перпендикулярність максимального типу є ретрактною ортогональністю, але обернене твердження не є правильним. Отже, часткове твердження теореми 4.1 доведено у розділі 2, а саме твердження 2.1, яке доводить, що максимальна перпендикулярність є ортогональністю.

Із твердження 4.3 випливає інше означення перпендикулярності максимального типу.

Означення 4.4. *n-арні операції g і h називаються перпендикулярними типу $(\iota, \iota; m)$, якщо вони є δ-ретрактно ортогональними для всіх δ таких, що $|\delta| = 2$ і $m \in \delta$.*

Зв'язок між ретрактною ортогональністю і сильною ортогональністю описаний Г.Б. Білявською і Г.Л. Мулленом у наслідку 8 із [67], звідки випливає ще одне означення сильної ортогональності. Сформулюємо його відповідно до означення 1.7 і означення 3.2.

Означення 4.5. *Вибірка n-арних операцій є сильно ортогональною, якщо вона є ℓ-кратно δ-ретрактно ортогональною для кожного ℓ і k таких що $1 \leqslant \ell \leqslant n$, $1 \leqslant k \leqslant n$.*

Наслідок 4.2. *Нехай g і h є n-арними квазігрупами. Такі твердження є еквівалентними:*

1) g і h є сильно ортогональними;

2) g і h є перпендикулярними типу $(\iota, \iota; m)$ для всіх $m \in \overline{1,n}$;

3) g і h є δ-ретрактно ортогональними для всіх $\delta \subset \overline{1,n}$;

4) для довільного $m \in \overline{1,n}$ операція $g \underset{m}{\oplus} h$ є оборотною.

Доведення. Відповідно до означення 4.5, сильна ортогональність операцій g і h спричинює їхню δ-ретрактну ортогональність для всіх $\delta \subset \overline{1,n}$, тобто 1) і 3) є еквівалентними. А згідно твердження 4.3, 2) і 3) є еквівалентними. Наслідок 2.1 спричинює еквівалентність 2) і 4). □

4.1.3. Кількість ретрактно ортогональних операцій

Нагадаємо, що відповідно до означення 1.2 k-арні операції $f_1, \ldots, f_k$, які визначені на множині Q є ортогональними тоді і тільки тоді, коли ці операції координатизують підстановку Q^k, тобто коли відображення $\theta := (f_1, \ldots, f_k)$ є підстановкою Q^k.

Лема 4.2. *Кількість k-вибірок ортогональних k-арних операцій, які визначені на множині Q порядку m, є* $\dfrac{(m^k)!}{k!}$.

Доведення. Оскільки кожна k-вибірка ортогональних k-арних операцій порядку m координатизує деяку перестановку Q^k, то існує $(m^k)!$ різних k-послідовностей ортогональних k-арних операцій. Зазначимо, що якщо $f_1,\ldots,\ f_k$ є ортогональними, то для всіх $\sigma \in \mathrm{S}_k$ послідовності виду $(f_{1\sigma},\ldots,f_{k\sigma})$ визначають різні підстановки, тобто кожна k-вибірка ортогональних операцій визначає $k!$ різних підстановок множини Q^k. Оскільки є точно $(m^k)!$ підстановок Q^k, тоді кількість k-наборів ортогональних k-арних операцій є $\dfrac{(m^k)!}{k!}$. □

Лема 4.3. *Для кожного $i \in \overline{1,n}$ існує точно $(m!)^{m^{n-1}}$ i-оборотних n-арних операцій на множині Q порядку m.*

Доведення. Нехай Q є довільною множиною, $m := |Q| < \infty$ і S_Q є групою всіх підстановок множини Q, тому $|S_Q| = m!$. Якщо f є i-оборотною n-арною операцією на множині Q, то перетворення α_i таке, що

$$\alpha_i(x) := f(a_1,\ldots,a_{i-1},x,a_{i+1},\ldots,a_n),$$

є підстановкою множини Q, тобто кожне відображення із S_Q має цю форму.

Визначимо відображення $\lambda_i : Q^{n-1} \to S_Q$:

$$\lambda_i(x_1,\ldots,x_{i-1},x_{i+1},\ldots,x_n)(x) := f(x_1,\ldots,x_{i-1},x,x_{i+1},\ldots,x_n).$$

Це співвідношення встановлює взаємнооднозначну відповідність між i-оборотними n-арними операціями і відображеннями λ_i. Очевидно, що $|Q^{n-1}| = m^{n-1}$. Тому $|\Lambda_i| = (m!)^{m^{n-1}}$, де

$$\Lambda_i = \{\lambda_i |\, \lambda_i : Q^{n-1} \to S_Q\}.$$

Отже, доведено, що кількість всіх бієктивних відображень $Q^{n-1} \to S_Q$ і кількість i-оборотних n-арних операцій на Q є однаковою і становить $(m!)^{m^{n-1}}$. □

Зазначимо, що для деяких випадків істинність цього твердження є очевидною. У випадку довільного m і $n = 1$, кожна оборотна унарна операція є підстановкою множини Q, отже, їхньою кількістю є $m!$. У випадку $m = 2$ і $n = 2$, існує точно 6 повних бінарних булевих операцій (повних квадратів порядку 2). Серед них 4 ліво (право) оборотних операцій, враховуючи 2 квазігрупи. У випадку $m = 2$ і $n = 3$, кожний зріз куба порядку 2 є квадратом порядку 2, тому можна знайти всі тернарні 1-оборотні булеві операції, використовуючи бінарні 1-оборотні операції. Оскільки їхньою кількістю є 4, то кількістю всіх 1-оборотних тернарних булевих операцій є $4^2 = 16$.

Зауважмо, що перетин усіх множин 1-, 2-, ..., n-оборотних n-арних операцій на Q є клас всіх n-арних квазігруп на Q.

Лема 4.4. *Для кожної s-вибірки ортогональних k-арних операцій ($s \leqslant k$) на множині Q порядку m існує точно $(m!)^{s\,m^{n-k}}$ різних продовжень у s-вибірку ортогональних n-арних операцій.*

Доведення. Для того, щоб продовжити s-вибірку ортогональних k-арних операцій на Q порядку m за формулами (3.3), маємо взяти s-вибірку 1-оборотних $(n-k+1)$-арних операцій, до того ж деякі операції в цій вибірці можуть збігатися. За лемою 4.3, кількістю 1-оборотних $(n-k+1)$-арних операцій є $(m!)^{m^{n-k}}$, тому кількістю s-вибірок 1-оборотних $(n-k+1)$-арних операцій є $(m!)^{s\,m^{n-k}}$. □

Зазначимо, що у випадку $k = n$, маємо знову вибірку ортогональних k-арних операцій.

Якщо ж $s = k$, то є точно $(m!)^{k\,m^{n-k}}$ різних продовжень k-вибірки ортогональних k-арних операцій до k-вибірки ортогональних n-арних операцій.

Теорема 4.2. *Нехай $|\delta| = k$, $n - k \geqslant 1$. Тоді кількість усіх різних k-вибірок δ-ретрактно ортогональних n-арних операцій на множині Q порядку m, які є побудовними за композиційним алгоритмом, становить*

$$\frac{(m^k)!}{k!}(m!)^{km^{n-k}}.$$

Доведення. Вхідними даними композиційного алгоритму є k-вибірка ортогональних k-арних операцій, k-послідовність $(n-k+1)$-арних операцій і $\sigma \in \mathrm{S}_n$ таке, що ${}^{\sigma}\overline{1,k} = \delta$. За першим кроком алгоритму будуємо $\overline{1,k}$-ретрактно ортогональні n-арні операції. За лемою 4.2 кількість k-вибірок ортогональних k-арних операцій є $\dfrac{(m^k)!}{k!}$ і за лемою 4.4 кількість k-послідовностей $(n-k+1)$-арних 1-оборотних операцій є $(m!)^{km^{n-k}}$. Тому кількість побудованих k-вибірок операцій є $\dfrac{(m^k)!}{k!}(m!)^{km^{n-k}}$.

Для того, щоб отримати δ-ретрактно ортогональні операції із $\overline{1,k}$-ретрактно ортогональних операцій, ми маємо застосувати $\sigma \in \mathrm{S}_n$ таке, що ${}^{\sigma}\overline{1,k} = \delta$. Припустимо, що $f_1,\ldots,\ f_k$ є $\overline{1,k}$-ретрактно ортогональними n-арними операціями і $g_1,\ldots,\ g_k$ є δ-ретрактно ортогональними n-арними операціями. Рівність

$$\{f_1,\ldots,f_k\} = \{{}^{\sigma}g_1,\ldots,{}^{\sigma}g_k\}$$

установлює взаємнооднозначну відповідність між класами $\overline{1,k}$-ретрактно ортогональних n-арних операцій і δ-ретрактно ортогональних n-арних операцій. Отже, їхні кількості однакові. □

4.2. Ретрактна ортогональність деяких класів операцій

4.2.1. Ретрактна ортогональність роздільних операцій

n-арну операцію f називатимемо δ-роздільною, де $\delta = \{i_1,\ldots,i_k\} \subset \overline{1,n}$, якщо існує s-оборотна $(n-k)$-арна операція g і k-арна операція h такі, що операцію f можна подати у вигляді

$$f(x_1,\ldots,x_n) = g(x_{j_1},\ldots,x_{j_{s-1}},h(x_{i_1},\ldots,x_{i_k}),x_{j_{s+1}},\ldots,x_{j_{n-k+1}}).$$

Лема 4.5. *Нехай $\delta \subset \overline{1,n}$, $|\delta| = k$ і кожна операція деякої k-вибірки n-арних операцій є δ-роздільною. Якщо існує вибірка ортогональних подібних δ-ретрактів операцій цієї вибірки, то ця k-вибірка є δ-ретрактно ортогональною.*

Доведення. Нехай

$$\delta := \{i_1, \ldots, i_k\} \subseteq \overline{1,n}, \qquad \overline{1,n} \setminus \delta := \{j_1, \ldots, j_{s-1}, j_{s+1}, \ldots, j_{n-k+1}\}$$

і для всіх $i \in \overline{1,k}$ n-арна операція f_i є δ-роздільною, тобто існують s-оборотна $(n-k)$-арна операція g_i та k-арна операція h_i такі, що f_i можна подати у вигляді

$$f_i(x_1, \ldots, x_n) = g_i(x_{j_1}, \ldots, x_{j_{s-1}}, h_i(x_{i_1}, \ldots, x_{i_k}), x_{j_{s+1}}, \ldots, x_{j_{n-k+1}}).$$

Припустимо, існує вибірка ортогональних δ-ретрактів операцій $f_1, \ldots, f_k$, тобто існує послідовність $\bar{a} = (a_{j_1}, \ldots, a_{j_{s-1}}, a_{j_{s+1}}, \ldots, a_{j_{n-k+1}}) \in Q^{n-k}$ така, що для всіх $b_1, \ldots, b_k$ система

$$\begin{cases} g_1(a_{j_1}, \ldots, a_{j_{s-1}}, h_1(x_{i_1}, \ldots, x_{i_k}), a_{j_{s+1}}, \ldots, a_{j_{n-k+1}}) = b_1, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ g_k(a_{j_1}, \ldots, a_{j_{s-1}}, h_k(x_{i_1}, \ldots, x_{i_k}), a_{j_{s+1}}, \ldots, a_{j_{n-k+1}}) = b_k \end{cases} \tag{4.1}$$

має єдиний розв'язок. Оскільки $g_1, \ldots, g_k$ є s-оборотними, то відповідні s-трансляції є підстановками множини Q, тобто для всіх $i \in \overline{1,k}$ перетворення α_i, яке визначене рівністю

$$\alpha_i u := g_i(a_{j_1}, \ldots, a_{j_{s-1}}, u, a_{j_{s+1}}, \ldots, a_{j_{n-k+1}}),$$

є підстановкою множини Q. Звідси, систему (4.1) можна переписати у вигляді

$$\begin{cases} h_1(x_{i_1}, \ldots, x_{i_k}) = \alpha_1^{-1} b_1, \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ h_k(x_{i_1}, \ldots, x_{i_k}) = \alpha_k^{-1} b_k. \end{cases}$$

Зазначимо, що $\alpha_1^{-1} b_1, \ldots, \alpha_k^{-1} b_k$ набувають всіх значень множини Q одночасно із $b_1, \ldots, b_k$. Це означає, що однозначність розв'язку системи (4.1) не залежить від $\bar{a}$. Тому ця система має єдиний розв'язок для всіх $\bar{a} \in Q^{n-k}$. Таким чином, операції $f_1, \ldots, f_k$ є δ-ретрактно ортогональними. □

Поєднуючи лему 4.5 і теорему 4.1, отримуємо твердження:

Наслідок 4.3. *Нехай $\delta \subset \overline{1,n}$, $|\delta| = k$ і кожна операція k-вибірки n-арних операцій є δ-роздільною. Тоді, якщо існує k-вибірка ортогональних подібних δ-ретрактів цих операцій, то задана k-вибірка є ортогональною.*

4.2.2. Ретрактна ортогональність лінійних операцій

Очевидно, що кожна лінійна операція над абелевою групою є розділльною, тобто вона має безповторний розклад за допомогою двох лінійних операцій над цією групою. До того ж, кожні дві змінні можна відокремити. Таким чином, лема 4.5 і наслідок 4.3 виконуються також для лінійних операцій над абелевою групою.

Твердження 4.4. *Нехай*

$$\delta := \{i_1, \dots, i_k\} \subset \overline{1,n}, \quad \overline{1,n} \setminus \delta := \{j_1, \dots, j_{n-k}\}.$$

Тоді n-арні лінійні операції $f_1, \dots, f_k$ над абелевою групою $(Q;+)$ є δ-ретрактно ортогональними тоді і тільки тоді, коли для всіх $q \in \overline{1,k}$ кожну з цих операцій можна подати у вигляді

$$f_q(x_1, \dots, x_n) = p_q(h_q(x_{i_1}, \dots, x_{i_k}), x_{j_1}, \dots, x_{j_{n-k}}), \tag{4.2}$$

де $h_1, \dots, h_k$ є ортогональними і $p_1, \dots, p_k$ є 1-оборотними.

Доведення. Нехай для всіх $q \in \overline{1,k}$,

$$f_q(x_1, \dots, x_n) := \alpha_{q1}x_1 + \dots + \alpha_{qn}x_n + a_q, \tag{4.3}$$

де $\alpha_{q1}, \dots, \alpha_{qn}$ є лінійними перетвореннями групи $(Q;+)$ і $a_q \in Q$. Припустимо, що $f_1, \dots, f_k$ є δ-ретрактно ортогональними.

Оскільки $(Q;+)$ є абелевою групою, то рівність (4.3) можна записати інакше:

$$f_q(x_1, \dots, x_n) = \alpha_{qi_1}x_{i_1} + \dots + \alpha_{qi_k}x_{i_k} + \\ + \alpha_{qj_1}x_{j_1} + \dots + \alpha_{qj_{n-k}}x_{j_{n-k}} + a_q,$$

де $\{i_1, \dots, i_k\} \cup \{j_1, \dots, j_{n-k}\} = \overline{1,n}$, тоді

$$f_q(x_1, \dots, x_n) = \beta(\beta^{-1}\alpha_{qi_1}x_{i_1} + \dots + \beta^{-1}\alpha_{qi_k}x_{i_k}) + \\ + \alpha_{qj_1}x_{j_1} + \dots + \alpha_{qj_{n-k}}x_{j_{n-k}} + a_q,$$

де β є довільним автоморфізмом групи $(Q;+)$. Звідси, для всіх $q \in \overline{1,k}$ операція f_q має вигляд (4.2), де

$$h_q(x_{i_1},\dots,x_{i_k}) := \beta^{-1}\alpha_{qi_1}x_{i_1} + \dots + \beta^{-1}\alpha_{qi_k}x_{i_k},$$

$$p_q(u,x_{j_1},\dots,x_{j_{n-k}}) := \beta u + \alpha_{qj_1}x_{j_1} + \dots + \alpha_{qj_{n-k}}x_{j_{n-k}} + a_q.$$

Ортогональність операцій $h_1,\dots, h_k$ випливає із δ-ретрактної ортогональності операцій $f_1,\dots, f_k$ і зауваження 4.2.

Зауваження 4.1 спричинює достатність цієї теореми. □

Наслідок 4.4. *Нехай $k \leqslant n$ і $f_1, \dots, f_k$ є n-арними лінійними операціями над $(\mathbb{Z}_m;+)$. Мінор порядку k відповідної матриці для операцій $f_1, \dots, f_k$, який є взаємнопростим із m, існує тоді і тільки тоді, коли ці операції є ортогональними.*

Доведення. Припустимо, що існує мінор порядку k відповідної матриці для операцій $f_1, \dots, f_k$, який є взаємнопростим із m. Цей мінор є відповідним визначником для деяких k-арних ретрактів операцій $f_1, \dots, f_k$, тобто $f_1, \dots, f_k$ є ретрактно ортогональними. Тоді, за теоремою 4.1, операції $f_1, \dots, f_k$ є ортогональними.

Припустимо $f_1, \dots, f_k$ є ортогональними, тоді ранг відповідної матриці дорівнює k. З означення рангу матриці, існує мінор порядку k цієї матриці, який є взаємнопростим із m. □

Для лінійних операцій визначених над полем простого порядку подібне твердження наведено у [80, лема 4.1]

Ретрактна ортогональність спричинює ортогональність, але обернене твердження не є істинним, зокрема існують ортогональні лінійні операції над абелевою групою, які не є ретрактно ортогональними (див. приклад 4.2). Проте для певного класу лінійних операцій ретрактна ортогональність є необхідною і достатньою умовою ортогональності.

Наслідок 4.5. *Нехай $k \leqslant n$ і p є простим числом. n-арні центральні квазігрупи $f_1, \dots, f_k$ над полем $(\mathbb{Z}_p;+,\cdot)$ є ортогональними тоді і*

тільки тоді, коли існує δ таке, що $|\delta| = k$ і $f_1, \ldots, f_k$ є δ-ретрактно ортогональними.

Доведення. Для всіх $i \in \overline{1,k}$, центральна квазігрупа f_i арності n має вигляд

$$f_i(x_1, \ldots, x_n) = a_{i1}x_1 + a_{i2}x_2 + \cdots + a_{in}x_n + a_i,$$

де $a_{i1}, a_{i2}, \ldots, a_{in}$ є довільними оборотними елементами із $(\mathbb{Z}_p; +, \cdot)$ і $a_i \in \mathbb{Z}_p$.

Припустимо, що $f_1, \ldots, f_k$ є ортогональними. Це означає, що для всіх $b_1, \ldots, b_k \in \mathbb{Z}_p$ система

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n + a_1 = b_1, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{k1}x_1 + a_{k2}x_2 + \cdots + a_{kn}x_n + a_k = b_k \end{cases}$$

має p^{n-k} розв'язків, тобто $rank(A) = k$, де

$$A = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{k1} & a_{k2} & \ldots & a_{kn} \end{pmatrix}.$$

Оскільки $f_1, \ldots, f_k$ є ортогональними, то за наслідком 4.4 існує оборотна підматриця M порядку k матриці A, тобто її визначник є ненульовим. Матриця M відповідає деякій k-вибірці k-арних δ-ретрактів операцій $f_1, \ldots, f_k$, де $|\delta| = k$. Отже, за наслідком 4.3 квазігрупи $f_1, \ldots, f_k$ є δ-ретрактно ортогональними.

Достатність випливає із теореми 4.1. □

Приклад 4.3. *Нехай відповідна матриця для k-арних центральних квазігруп $f_1, \ldots, f_k$ над полем $(\mathbb{Z}_p; +, \cdot)$ є матрицею Вандермонда:*

$$V = \begin{pmatrix} 1 & a_1 & a_1^2 & \ldots & a_1^{k-1} \\ 1 & a_2 & a_2^2 & \ldots & a_2^{k-1} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 1 & a_k & a_k^2 & \ldots & a_k^{k-1} \end{pmatrix}.$$

Відомо, що її визначник можна обчислити за формулою

$$\Delta = \prod_{1 \leqslant j < i \leqslant k} (a_i - a_j).$$

Він відмінний від нуля тоді і тільки тоді коли для всіх $i, j \in \overline{1,k}$, *де* $i \neq j$, *виконується нерівність* $a_i \neq a_j$. *Як зазначено у [67] операції* $f_1, \ldots, f_k$ *є ортогональними. Більше того за допомогою матриці Вандермонда можна будувати* t*-вибірки* k*-арних центральних квазігруп, де* $t > k$.

Кожна s*-вибірка операцій із* $f_1, \ldots, f_k$, *де* $s \leqslant k$, *є* $\overline{1,s}$*-ретрактно ортогональною тоді і тільки тоді, коли* $a_i \neq a_j$. *Справді, кожен мінор відповідної матриці розмірності* $s \times k$, *що отриманий викреслюванням стовпців із номерами* $s{+}1, s{+}2, \ldots, n$, *є також матрицею Вандермонда.*

4.3. Доповнення ортогональних операцій і гіперкубів

Відповідно до теореми 4.1, якщо k-вибірка є ретрактно ортогональною, то для доповнення цієї вибірки можна використати блочний рекурсивний алгоритм, який описаний у розділі 3.

$(n-k)$-вибірку n-арних операцій $f_{k+1},\ldots, f_n$ називатимемо ортогональним доповненням k-вибірки ортогональних n-арних операцій $f_1,\ldots, f_k$ до n-вибірки ортогональних n-арних операцій, якщо n-вибірка $f_1,\ldots, f_n$ є ортогональною. До того ж, вибірка $f_{k+1},\ldots, f_n$ є ортогональною за теоремою 1.7.

4.3.1. Алгоритм побудови доповнень ортогональних операцій

Довільну k-вибірку δ-ретрактно ортогональних n-арних операцій, де $|\delta| = k$, можна доповнити до n-вибірки ортогональних n-арних операцій використовуючи блочний рекурсивний алгоритм.

Алгоритм 4.1. *Нехай* $\delta = \{i_1, \ldots, i_k\} \subset \overline{1,n}$, $|\delta| = k$ *і* $g_{i_1},\ldots, g_{i_k}$ *є* δ*-ретрактно ортогональними* n*-арними операціями.*

Операції $g_{i_{k+1}}, \ldots, g_{i_n}$ *будуються за такими кроками:*

1) вибираємо довільні n-арні операції $f_{i_{k+1}},\dots,f_{i_n}$ такі, що для кожного $r\in\overline{2,q}$ вибірка $\{f_j|j\in\pi_r\}$ є довільною π_r-ретрактно ортогональною, тобто відповідним розбиттям множини $\overline{1,n}$ є $\pi:=\{\delta,\pi_2,\dots,\pi_q\}$, і перестановки $\tau_1\in \mathrm{S}_\delta$, $\tau_2\in \mathrm{S}_{\delta\cup\pi_2}$, $\dots$, $\tau_{q-1}\in \mathrm{S}_{\delta\cup\pi_2\cup\dots\cup\pi_{q-1}}$;

2) для кожного $j\in\pi_2$, операція g_j визначається за допомогою рівності

$$g_j(x_1,\dots,x_n):=f_j(t_1,\dots,t_n), \tag{4.4}$$

де

$$t_s:=\begin{cases} g_{s\tau_1}(x_1,\dots,x_n), & \text{якщо } s\in\delta,\\ x_s & \text{в інших випадках;}\end{cases}$$

r) для кожного $j\in\pi_r$, $r=3,\dots,q$, операція g_j визначається за допомогою рівності (4.4), де

$$t_s:=\begin{cases} g_{s\tau_{r-1}}(x_1,\dots,x_n), & \text{якщо } s\in\delta\cup\pi_2\cup\dots\cup\pi_{r-1},\\ x_s & \text{в інших випадках.}\end{cases}$$

Теорема 4.3. *$(n-k)$-вибірка n-арних операцій $g_{i_{k+1}},\dots,g_{i_n}$, яка побудована за алгоритмом 4.1, є доповненням k-вибірки δ-ретрактно ортогональних n-арних операцій $g_{i_1},\dots,g_{i_k}$ до n-вибірки ортогональних n-арних операцій.*

Доведення. Доведення випливає із теореми 3.4, якщо використати π-блочний рекурсивний алгоритм, а δ взяти першим блоком визначаючого розбиття π множини $\overline{1,n}$. □

Нехай $\delta\subset\overline{1,n}$ і $|\delta|=k$. δ-підгіперкубом називатимемо k-вимірний гіперкуб H_δ n-куба H, якщо він отримується з H фіксуванням $n-k$ координат з індексами із множини $\overline{1,n}\backslash\delta$. Зазначимо, що це означення є більш загальним ніж означення До кожного k-арного ретракту n-арної операції є відповідним k-вимірний підгіперкуб відповідного n-куба. Якщо $\delta=\{i,j\}$, то H_δ є $\{i,j\}$-зрізом гіперкуба H. Якщо $\delta=\{i\}$, то δ-підгіперкуб є *i-лінією*.

Підгіперкуби $H_{1,\delta},\ldots,\ H_{k,\delta}$ порядку m гіперкубів $H_1,\ldots,\ H_k$ називатимемо подібними, якщо кожен із них визначається фіксацією всіх координат з множини $\overline{1,n}\backslash\delta$ тими самими елементами базової множини.

Означення 3.2 можна переформулювати для гіперкубів: гіперкуби $H_1,\ldots,\ H_k$ називатимемо δ-ретрактно ортогональними, якщо всі їхні подібні підгіперкуби $H_{1,\delta},\ldots,\ H_{k,\delta}$ є ортогональними.

Зауваження 4.4. *Всі подані твердження можна переформулювати для гіперкубів. Таким чином, алгоритм 1 є застосовним для побудови доповнень ортогональних гіперкубів.*

Зазначимо, що алгоритм 4.1 дає можливість побудувати доповнення k-вибірки δ-ретрактно ортогональних n-арних операцій до $(k+s)$-вибірки ортогональних n-арних операцій для всіх $s \in \overline{1,n-k}$ так само як блочний рекурсивний алгоритм дає можливість будувати $(k+s)$-вибірки ортогональних n-арних операцій, що спричинено теоремою 1.7. В обох випадках потрібно закінчити алгоритм на відповідному кроці. Для цього маємо розглянути два випадки:

- якщо $|\pi_1|+\cdots+|\pi_r| = s$, тоді алгоритм маємо завершити кроком r);
- якщо $|\pi_1|+\cdots+|\pi_r| < s < |\pi_{r+1}|$, тоді алгоритм маємо завершити на відповідному кроці $(r+1)$-го кроку алгоритму.

Припустимо, що t-вибірка n-арних операцій, де $t > n$, є ортогональною. Візьмемо з неї довільну ℓ-вибірку операцій, де $\ell < n$. За теоремою 1.7 ця вибірка є ортогональною, тому за теоремою 1.10 вона є вбудовною в деяку n-вибірку ортогональних n-арних операцій. Однак існує доповнення, яке не належить заданій t-вибірці.

4.3.2. Тривіальні доповнення

Найбільш простими і найбільш вивченими доповненнями ортогональних операцій є тривіальні доповнення, тобто ті у яких додається точно

одна операція на кожному кроці алгоритму. Для побудови тривіальних доповнень достатньо мати лише операції, які є односторонньо оборотними на всіх різних місцях, що не належать δ. Якщо в алгоритмі 4.1 розбиття має вигляд $\pi = (\{n\}, \{n-1\}, \ldots, \{1\})$, то маємо алгоритм доповнення n-арної n-оборотної операції до n-вибірки ортогональних n-арних операцій, який тривіально спричинюється алгоритмом Г. Білявської і Г. Мулена [64].

Поєднуючи алгоритм 4.1 і тривіальний рекурсивний алгоритм, сформулюємо алгоритм для тривіального доповнення.

Алгоритм 4.2. *Нехай $g_{i_1}, \ldots, g_{i_k}$ є δ-ретрактно ортогональними n-арними операціями, де $\delta = \{i_1, \ldots, i_k\} \subset \overline{1,n}$.*

Операції $g_{i_{k+1}}, \ldots, g_{i_n}$ будуються за такими кроками:

r_0) вибираємо довільні n-арні операції $f_{i_{k+1}}, \ldots, f_{i_n}$, такі, що для всіх $r \in \overline{1,n-k}$ операції $f_{i_{k+r}}$ є i_{k+r}-оборотними і перестановки $\tau_1 \in \mathrm{S}_\delta$, $\tau_2 \in \mathrm{S}_{\delta\cup\{i_{k+1}\}}$, $\ldots$, $\tau_{n-k} \in \mathrm{S}_{\delta\cup\{i_{k+1}\}\cup\cdots\cup\{i_{n-k}\}}$;

1) операція $g_{i_{k+1}}$ визначається рівністю

$$g_{i_{k+1}}(x_1, \ldots, x_n) := f_{i_{k+1}}(t_1, \ldots, t_n),$$

де

$$t_s := \begin{cases} g_{s\tau_1}(x_1, \ldots, x_n), & \text{якщо } s \in \delta, \\ x_s & \text{в інших випадках;} \end{cases}$$

r) для кожного $r = \overline{2,n-k}$, операція $g_{i_{k+r}}$ визначається рівністю

$$g_{i_{k+r}}(x_1, \ldots, x_n) := f_{i_{k+r}}(t_1, \ldots, t_n),$$

де

$$t_s := \begin{cases} g_{s\tau_{r-1}}(x_1, \ldots, x_n), & \text{якщо } s \in \delta \cup \{i_{k+1}\} \cup \{i_{k+r-1}\}, \\ x_s & \text{в інших випадках.} \end{cases}$$

Наслідок 4.6. *Кожна k-вибірка δ-ретрактно ортогональних n-арних операцій ($|\delta| = k$) є тривіально доповнювальною, тобто за алгоритмом 4.2, до n-вибірки ортогональних n-арних операцій.*

Доведення. Припустимо, що в алгоритмі 4.1 блоки $\pi_2,\dots\pi_q$ є одноелементними множинами. Введемо позначення

$$\pi_2 := \{i_{k+1}\}, \quad \dots \quad \pi_q := \{i_{k+q}\},$$

де $k+q=n$, тому визначаючим є розбиття $\pi' = \{\delta, \{i_{k+1}\}, \dots, \{i_{k+q}\}\}$ множини $\overline{1,n}$. Алгоритм 4.2 отримуємо, переформулювавши алгоритм 4.1 для π', тобто він є частковим випадком алгоритму 4.1. Відповідно до теореми 4.3, операції, які є побудованими за алгоритмом 4.2, утворюють доповнення цієї k-вибірки δ-ретрактно ортогональних n-арних операцій до n-вибірки ортогональних n-арних операцій. Оскільки для довільного цілого числа n і для кожного $k \in \overline{1,n}$ завжди існує $(n-k)$-вибірка i_{k+1}-, …, i_n-оборотних операцій, то кожна вибірка δ-ретрактно ортогональних n-арних операцій є доповнювальною за алгоритмом 4.2 до n-вибірки ортогональних n-арних операцій. □

4.4. Оцінки кількості доповнень δ-ретрактно ортогональних операцій

Кількість доповнень довільної даної вибірки ортогональних n-арних операцій до n-вибірки ортогональних n-арних операцій невідома, але ми можемо знайти деякі оцінки доповнень.

Два доповнення тієї ж вибірки ортогональних операцій будемо називати різними, якщо вони відрізняються принаймні однією операцією. Для довільного $\sigma \in \mathrm{S}_n$ припускається, що k-вибірки n-арних операцій $f_1, \dots, f_k$ і $f_{1\sigma}, \dots, f_{k\sigma}$ є однаковими.

Визначимо функцію p на множині пар додатніх цілих чисел:

$$p(1,s) := 1! \cdot 2! \cdot 3! \cdot \ldots \cdot s!.$$

Перепишемо цю рівність:

$$p(1,s) = 2^{s-1} \cdot 3^{s-2} \cdot \ldots \cdot (s-1)^2 \cdot s. \tag{4.5}$$

Таким чином,

$$1! \cdot 2! \cdot 3! \cdot \ldots \cdot s! = \prod_{j=1}^{s} j^{s-j+1},$$

тоді

$$p(k,s) := k! \cdot (k+1)! \cdot \ldots \cdot s! =$$

$$= 2^{s-k+1} \cdot \ldots \cdot k^{s-k+1} \cdot (k+1)^{s-k} \cdot \ldots \cdot (s-1)^2 \cdot s.$$

Отже,

$$k! \cdot (k+1)! \cdot \ldots \cdot s! = \prod_{j=1}^{k} j^{s-k+1} \prod_{j=k+1}^{s} j^{s-j+1}. \tag{4.6}$$

Формула (4.5) є частковим випадком формули (4.6). Якщо $k = 1$ у (4.6), то

$$\prod_{j=1}^{1} j^{s-1+1} = 1.$$

Нехай $\mathfrak{C}_n(k,s;m)$ позначає кількість усіх різних доповнень побудованих за алгоритмом 4.1 k-вибірки δ-ретрактно ортогональних n-арних операцій визначених на Q порядку m до s-вибірки ортогональних n-арних операцій і $\mathfrak{c}_n(k,s;m)$ позначає кількість усіх різних тривіальних доповнень k-вибірки δ-ретрактно ортогональних n-арних операцій на множині Q порядку m до s-вибірки ортогональних n-арних операцій $(k < s \leqslant n)$.

Теорема 4.4. *Нехай $m = |Q|$, $k = |\delta|$, $r \leqslant n-k$. Тоді*

$$\frac{(m!)^{rm^{n-1}}}{r!} < \mathfrak{c}_n(k,k+r;m) < \frac{(n-k)!(m!)^{rm^{n-1}}}{(n-k-r)!} \prod_{j=1}^{k} j^r \prod_{j=k+1}^{k+r} j^{k+r-j}.$$

Доведення. Припустимо $\delta = \{i_1, \ldots, i_k\}$ і послідовність $(g_{i_1}, \ldots, g_{i_k})$ є довільною фіксованою впорядкованою k-вибіркою δ-ретрактно ортогональних n-арних операцій на множині Q. За теоремою 4.1, ця вибірка є ортогональною.

Знаходимо нижню оцінку кількості доповнень $\mathfrak{c}_n(k,k+r;m)$. Припустимо, що для кожного $q \in \overline{1,r}$

$$\Delta := \delta \cup \{i_{k+1}\} \cdots \cup \{i_{k+q-1}\}.$$

Зазначимо, якщо $q = 1$, то $i_{k+q-1} = i_k$. Оскільки $i_k \in \delta$, то $\Delta = \delta \cup \{i_k\} = \delta$.

Для довільної i_{k+q}-оборотної n-арної операції $f_{i_{k+q}}$ побудуємо n-арну операцію $g_{i_{k+q}}$ за допомогою рівності

$$g_{i_{k+q}}(x_1, \ldots, x_n) := f_{i_{k+q}}(t_1, \ldots, t_n), \qquad q = 1, \ldots, r, \tag{4.7}$$

де $i_{k+q} \in \overline{1,n} \setminus \delta \cup \{i_{k+1}\} \cdots \cup \{i_{k+q-1}\}$ і

$$t_i := \begin{cases} g_i, & \text{якщо } \ i \in \Delta, \\ x_i, & \text{якщо } \ i \notin \Delta. \end{cases}$$

За алгоритмом 4.2 і наслідком 4.6, вибірка $(g_{i_1}, \ldots, g_{i_k}, g_{i_{k+1}}, \ldots, g_{i_{k+q}})$ є ортогональною. Зазначимо, що на кожному кроці $q \in \overline{1,r}$, додаємо лише одну операцію за допомогою i_{k+q}-оборотної n-арної операції.

Припустимо, що $(g_{i_1}, \ldots, g_{i_k}, g_{i_{k+1}}, \ldots, g_{i_{k+q-1}}, g'_{i_{k+q}})$ є іншою вибіркою ортогональних операцій, де $g'_{i_{k+q}}$ є побудовною за (4.7) з іншої i_{k+q}-оборотної операції $f'_{i_{k+q}}$:

$$g'_{i_{k+q}}(x_1, \ldots, x_n) := f'_{i_{k+q}}(t_1, \ldots, t_n).$$

До того ж

$$(g_{i_1}, \ldots, g_{i_k}, g_{i_{k+1}}, \ldots, g_{i_{k+q-1}}, g_{i_{k+q}}) \neq (g_{i_1}, \ldots, g_{i_k}, g_{i_{k+1}}, \ldots, g_{i_{k+q-1}}, g'_{i_{k+q}})$$

тоді і тільки тоді, коли $f_{i_{k+q}} \neq f'_{i_{k+q}}$.

Справді, нехай

$$(g_{i_1}, \ldots, g_{i_k}, g_{i_{k+1}}, \ldots, g_{i_{k+q-1}}, g_{i_{k+q}}) = (g_{i_1}, \ldots, g_{i_k}, g_{i_{k+1}}, \ldots, g_{i_{k+q-1}}, g'_{i_{k+q}}),$$

отже, $g_{i_{k+q}} = g'_{i_{k+q}}$, тобто

$$f_{i_{k+q}}(t_1, \ldots, t_n) = f'_{i_{k+q}}(t_1, \ldots, t_n).$$

Оскільки за теоремою 1.7 для кожного $q \in \overline{1, n-k}$ вибірка $(g_{i_1}, \ldots, g_{i_k}, g_{i_{k+1}}, \ldots, g_{i_{k+q}})$ є ортогональною, то вона набуває всіх значень із множини Q^{k+q}. Це означає, що вибірка $(t_1, \ldots, t_n)$ набуває всіх значень із Q^n. Тому, $f_{i_{k+q}} = f'_{i_{k+q}}$. Обернене твердження є очевидним.

Таким чином, для будь-якого $q \in \overline{1,r}$ кількість усіх різних доповнень $(k+q-1)$-вибірки ортогональних операцій, побудованих за допомогою

(4.7) за допомогою i_{k+q}-оборотної операції, дорівнює кількості всіх i_{k+q}-оборотних n-арних операцій на множині Q порядку m, і це число становить $(m!)^{m^{n-1}}$ відповідно до леми 4.3. Отже, існує принаймні $(m!)^{m^{n-1}}$ різних доповнень $(k+q-1)$-вибірки ортогональних n-арних операцій до $(k+q)$-вибірки ортогональних n-арних операцій.

Повторюємо ці кроки r разів, доки отримаємо $(k+r)$-вибірку ортогональних n-арних операцій. Кількість вибірок виду

$$(f_{i_1}, \ldots, f_{i_k}, g_{i_{k+1}}, \ldots, g_{i_{k+r}})$$

становить $(m!)^{rm^{n-1}}$. Вибірка $g_{i_{k+1}}$, $\ldots$, $g_{i_{k+r}}$ є невпорядкованою. Припустимо, що серед побудованих вибірок існують вибірки $(g_{i_{k+1}}, \ldots, g_{i_{k+r}})$ і $(g'_{i_{k+1}}, \ldots, g'_{i_{k+r}})$, такі, що

$$(g'_{i_{k+1}}, \ldots, g'_{i_{k+r}}) = (g_{i_{(k+1)\sigma}}, \ldots, g_{i_{(k+r)\sigma}}),$$

де $\sigma \in \mathrm{S}_r$, тобто те ж саме доповнення отримуємо двічі. Максимальна кількість усіх можливих повторень є $r!$. Отже,

$$\mathfrak{c}_n(k, k+r; m) > \frac{(m!)^{rm^{n-1}}}{r!}.$$

Розглянемо верхню оцінку числа $\mathfrak{c}_n(k, k+r; m)$. За блочним рекурсивним алгоритмом, використовуючи перестановки із множин S_δ, $\mathrm{S}_{\delta\cup\{i_1\}}$,$\ldots$, $\mathrm{S}_{\delta\cup\{i_1\}\cup\cdots\cup\{i_{r-1}\}}$, отримуємо також ортогональні операції. Оскільки

$$|\mathrm{S}_\delta| = k!, \qquad |\mathrm{S}_{\delta\cup\{i_1\}}| = (k+1)!, \quad \ldots \quad |\mathrm{S}_{\delta\cup\{i_1\}\cup\cdots\cup\{i_{r-1}\}}| = (k+r-1)!,$$

маємо ще відповідно до рівності (4.6)

$$k! \cdot (k+1)! \cdot \ldots \cdot (k+r-1) = \prod_{j=1}^{k} j^r \prod_{j=k+1}^{k+r} j^{k+r-j}$$

способів для побудови ортогональних доповнень.

Для кожного $q \in \overline{1,r}$ виконується належність $i_{k+q} \in \overline{1,n} \setminus \Delta$, тому існує $n-k-q+1$ способів вибору i_{k+q}, тобто

$$(n-k) \cdot \ldots \cdot (n-k-r+1) = \frac{(n-k)!}{(n-k-r)!}$$

способів для вибору послідовності $(i_{k+1}, \ldots, i_{k+r})$ без повторень. Оскільки для всіх $i, j \in \overline{1,n}$, де $i \neq j$, класи i-оборотних і j-оборотних n-арних операцій мають непорожній перетин, то маємо нерівність

$$\mathfrak{c}_n(k, k+r; m) < \frac{(n-k)!(m!)^{rm^{n-1}}}{(n-k-r)!} \prod_{j=1}^{k} j^r \prod_{j=k+1}^{k+r} j^{k+r-j}.$$

□

В наступному твердженні подані оцінки кількості ортогональних доповнень k-вибірки δ-ретрактно ортогональних операцій до $(k+1)$-вибірки ортогональних n-арних операцій, де $k+1 \neq n$

Наслідок 4.7. *Нехай $m = |Q|$, $k = |\delta|$ і $k+1 \neq n$, тоді*

$$(m!)^{m^{n-1}} < \mathfrak{c}_n(k, k+1; m) < (n-k)k!(m!)^{m^{n-1}}.$$

Доведення. Якщо $r = 1$, то, за теоремою 4.4,

$$\frac{(m!)^{rm^{n-1}}}{r!} = (m!)^{m^{n-1}}$$

і

$$\prod_{j=1}^{k} j^r \prod_{j=k+1}^{k+r} j^{k+r-j} = \prod_{j=1}^{k} j \prod_{j=k+1}^{k+1} (k+1)^{k+1-(k+1)} = k!.$$

Тому

$$\frac{(n-k)!(m!)^{rm^{n-1}}}{(n-k-r)!} \prod_{j=1}^{k} j^r \prod_{j=k+1}^{k+r} j^{k+r-j} = \frac{(n-k)!k!(m!)^{m^{n-1}}}{(n-k-1)!} = (n-k)k!(m!)^{m^{n-1}}.$$

□

Для доповнення $(n-1)$-вибірки δ-ретрактно ортогональних n-арних операцій ($|\delta| = n-1$) до n-вибірки ортогональних n-арних операцій можна знайти точніші оцінки.

Наслідок 4.8. *Нехай $m = |Q|$ і $|\delta| = n-1$. Тоді*

$$(m!)^{m^{n-1}} \leqslant \mathfrak{C}_n(n-1, n; m) \leqslant (n-1)!(m!)^{m^{n-1}}. \tag{4.8}$$

Доведення. В умові теореми 4.4, рівність $k = n-1$ спричинює $r = n-(n-1) = 1$. У цьому випадку будь-яке можливе доповнення є тривіальним.

Ось чому $\mathfrak{c}_n(n-1,n;m) = \mathfrak{C}_n(n-1,n;m)$. За наслідком 4.7, його нижня оцінка становить $(m!)^{m^{n-1}}$, а верхня – $(n-1)!(m!)^{m^{n-1}}$.

З доведення теореми 4.4 випливає, що n-арна операція g_{i_n} є однозначно побудовною за допомогою i_n-оборотної операції f_{i_n}. Отже, впорядкована вибірка $(g_{i_1},\dots,g_{i_k})$ є однозначно доповнювальною за допомогою (4.7). Тому маємо нестрогі нерівності для $\mathfrak{C}_n(n-1,n;m)$. □

Приклад 4.4. *Розглянемо доповнення бінарних булевих операцій. Підставивши $n=2$ і $m=2$ у (4.8), маємо*

$$4 \leqslant \mathfrak{C}_2(1,2;2) \leqslant 4,$$

отже, $\mathfrak{C}_2(1,2;2) = 4$.

Це також можна перевірити накладанням відповідних квадратів: кожна ліво (право) оборотна бінарна булева операція має 4 доповнення. Оскільки існує 4 ліво (право) оборотних бінарних булевих операцій, то всі ці доповнення є побудовними за алгоритмом 4.2.

Також наведемо уточнення теореми 4.4 для оцінок кількості доповнень k-вибірки δ-ретрактно ортогональних n-арних операцій до n-вибірки ортогональних операцій.

Наслідок 4.9. *Нехай $m=|Q|$, $k=|\delta|$ і $k<n$. Тоді*

$$\frac{(m!)^{(n-k)m^{n-1}}}{(n-k)!} < \mathfrak{c}_n(k,n;m) < (n-k)!(m!)^{(n-k)m^{n-1}} \prod_{j=1}^{k} j^{n-k} \prod_{j=k+1}^{n} j^{n-j}.$$

Доведення. Якщо $k+r=n$, то, за теоремою 4.4,

$$\frac{(n-k)!(m!)^{rm^{n-1}}}{(n-k-r)!} \prod_{j=1}^{k} j^{r} \prod_{j=k+1}^{k+r} j^{k+r-j} =$$

$$\frac{(n-k)!(m!)^{(n-k)m^{n-1}}}{(n-n)!} \prod_{j=1}^{k} j^{n-k} \prod_{j=k+1}^{n} j^{n-j} =$$

$$(n-k)!(m!)^{(n-k)m^{n-1}} \prod_{j=1}^{k} j^{n-k} \prod_{j=k+1}^{n} j^{n-j}$$

і

$$\frac{(m!)^{rm^{n-1}}}{r!} = \frac{(m!)^{(n-k)m^{n-1}}}{(n-k)!}.$$

□

Для того, щоб знайти кількість усіх доповнень k-вибірки δ-ретрактно ортогональних n-арних операцій на множині Q порядку m до n-вибірки ортогональних n-арних операцій, ми маємо знайти доповнення для всіх можливих визначаючих розбиттів, де першим блоком є δ, і тоді відкинути всі повторення доповнень. Кількість різних алгоритмів для такого доповнення є кількістю всіх послідовностей параметрів алгоритму 4.1. Припустимо, що кожне з доповнень збігається з одним із тривіальних доповнень, тоді теорема 4.4 дає нижню оцінку кількості всіх доповнень.

Оскільки алгоритм 4.2 є частковим випадком алгоритму 4.1, то теорема 4.4 та її наслідки дають також нижню оцінку кількості $\mathfrak{C}_n(k, r; m)$ всіх доповнень.

Наслідок 4.10. *Нехай $m = |Q|$, $k = |\delta|$ і $k + r \leqslant n$. Якщо*

1) $r = 1$, то

$$\mathfrak{C}(k, k+1; m) \geqslant (m!)^{m^{n-1}};$$

2) $1 < r < n - k$, то

$$\mathfrak{C}(k, k+r; m) > \frac{(m!)^{rm^{n-1}}}{r!};$$

3) $r = n - k$, то

$$\mathfrak{C}(k, n; m) > \frac{(m!)^{(n-k)m^{n-1}}}{(n-k)!}.$$

Як зазначено в теоремі 4.4, ми не можемо порахувати навіть кількість тривіальних доповнень безпосередньо. Якщо припустити, що для різних параметрів деякі доповнення тієї ж вибірки операцій збігаються, то це призводить до серії функційних рівнянь.

4.5. Доповнення ортогональних операцій до іншої арності та їхня оцінка

З огляду на композиційний алгоритм можна сформулювати алгоритм доповнення k-вибірки ортогональних k-арних операцій до n-вибірки ортогональних n-арних операцій. Зазначимо, що додаткові обмеження на задану k-вибірку не накладаються.

Алгоритм 4.3. *Нехай $\delta \subseteq \overline{1,n}$ і $h_1, \dots, h_k$ є k-арними ортогональними операціями.*

Операції $g_{i_{k+1}}, \dots, g_{i_n}$ будуються таким чином:

1) *вибираємо 1-оборотні $(n-k+1)$-арні операції $p_1, \dots, p_k$ і перестановку $\sigma \in \mathrm{S}_n$ таку, що ${}^{\sigma^{-1}}\delta = \overline{1,k}$;*

2) *операції $f_1, \dots, f_k$ будуються за формулою (3.3);*

3) *операції $g_{i_1}, \dots, g_{i_k}$ отримуємо із $f_1, \dots, f_k$ таким чином:*

$$g_{i_1} := {}^{\sigma}f_1, \quad \dots, \quad g_{i_k} := {}^{\sigma}f_k;$$

4) *виконання алгоритму 4.1.*

Теорема 4.5. *Алгоритм 4.3 будує ортогональні доповнення k-вибірки ортогональних k-арних операцій до n-вибірки ортогональних n-арних операцій. До того ж, кожна k-вибірка ортогональних k-арних операцій є доповнювальною за алгоритмом 4.3 до n-вибірки ортогональних n-арних операцій.*

Доведення. Відповідно до теореми кроки 1)-3) алгоритму 4.3 будують вибірку δ-ретрактно ортогональних операцій. За алгоритмом 4.1 і теоремою 4.3, можна знайти доповнення цієї вибірки до n-вибірки ортогональних n-арних операцій.

Істинність другої частини теореми випливає з існування k-вибірки $(n-k+1)$-арних 1-оборотних операцій і теореми 4.6. □

Лема 4.4 і наслідок 4.9 теореми 4.4 спричинюють нижченаведене твердження.

Теорема 4.6. *Кількість усіх доповнень побудовних за алгоритмом 3 заданої k-вибірки ортогональних k-арних операцій до n-вибірки ортогональних n-арних операцій є більшою, ніж*

$$\frac{(m!)^{(n-k)m^{n-1}+km^{n-k}}}{(n-k)!}.$$

Доведення. З огляду на крок 3) алгоритму 4.3, для того, щоб отримати δ-ретрактно ортогональні операції з $\overline{1,k}$-ретрактно ортогональних операцій, маємо застосувати перестановку $\sigma \in \mathrm{S}_n$ таку, що ${}^{\sigma}\overline{1,k} = \delta$. Припустимо, що $f_1,\ldots,\ f_k$ є $\overline{1,k}$-ретрактно ортогональними n-арними операціями і $g_1,\ldots,\ g_k$ є δ-ретрактно ортогональними n-арними операціями. Рівність

$$\{f_1,\ldots,f_k\} = \{{}^{\sigma}g_1,\ldots,{}^{\sigma}g_k\}$$

встановлює взаємнооднозначну відповідність між класом $\overline{1,k}$-ретрактно ортогональних n-арних операцій і класом δ-ретрактно ортогональних n-арних операцій. Отже, їхні кількості є однаковими.

За лемою 4.4, кількість різних k-вибірок n-арних операцій побудовних за кроком 2) алгоритму 4.3 є $(m!)^{km^{n-k}}$. Відповідно до наслідку 4.9, нижня межа кількості доповнень ретрактно ортогональних операцій є $\dfrac{(m!)^{(n-k)m^{n-1}}}{(n-k)!}$. □

Висновки до розділу 4

У цьому розділі описані методи побудови ортогональних доповнень ортогональних n-арних операцій, а саме доведено, що довільна k-вибірка δ-ретрактно ортогональних n-арних операцій ($|\delta| = k,\ k < n$) є доповнювальною до n-вибірки ортогональних n-арних операцій за блочним рекурсивним алгоритмом.

Основні результати розділу:

1) доведено, що ретрактна ортогональність спричинює ортогональність, але обернене твердження не є істинним, більше того доведено існування ортогональних операцій, які не мають ортогональних ретрактів;

2) доведено, що для центральних квазігруп над полем простого порядку, ретрактна ортогональність є необхідною і достатньою умовою ортогональності;

3) описано і доведено алгоритм побудови ортогональних доповнень k-вибірки δ-ретрактно ортогональних n-арних операцій ($k < n$) до n-вибірки ортогональних n-арних операцій;

4) описано тривіальний випадок алгоритму побудови ортогональних доповнень;

5) знайдено верхню та нижню оцінки кількості тривіальних ортогональних доповнень, а також нижню оцінку кількості всіх можливих ортогональних доповнень k-вибірки δ-ретрактно ортогональних n-арних операцій;

6) описано і доведено алгоритм доповнення k-вибірки ортогональних k-арних операцій до n-вибірки ортогональних n-арних операцій ($k < n$), а також знайдено нижню оцінку кількості ортогональних доповнень, які є побудовними за цим алгоритмом.

Результати цього розділу опубліковано у [92, 96–98].

РОЗДІЛ 5

ДЕЯКІ ЗАСТОСУВАННЯ ОТРИМАНИХ РЕЗУЛЬТАТІВ

У цьому розділі ілюструємо застосування отриманих результатів для тернарних операцій враховуючи їх специфіку, а також деякі наслідки щодо перпендикулярності операцій.

5.1. Ортогональні доповнення бінарних квазігруп та деякі наслідки для n-арних операцій

5.1.1. Рекурсивний алгоритм для бінарних операцій

У цьому підрозділі наведемо наслідки із блочного рекурсивного алгоритму для бінарних операцій. Очевидно, що блочний рекурсивний алгоритм є тривіальним рекурсивним алгоритмом у бінарному випадку. Існує лише два розбиття:

$$\wp_1 := \big\{\{1\},\{2\}\big\}, \qquad \wp_2 := \{1,2\}.$$

До розбиття $\wp_1$ відповідними є два впорядкованих розбиття:

1) $\big(\{1\},\{2\}\big)$, алгоритм має вигляд

$$\begin{cases} g_1(x,y) = f_1(x,y), \\ g_2(x,y) = f_2(f_1(x,y),y) \end{cases} \tag{5.1}$$

і назвемо його лівим рекурсивним алгоритмом;

2) $\big(\{2\},\{1\}\big)$, алгоритм має вигляд

$$\begin{cases} g_1(x,y) = f_1(x,y), \\ g_2(x,y) = f_2(x,f_1(x,y)) \end{cases} \tag{5.2}$$

і назвемо його правим рекурсивним алгоритмом.

Зазначимо, що перший блок розбиття визначає оборотність першої вхідної операції і місце на яке має бути підставлена ця операція до другої вхідної операції, другий блок визначає оборотність другої вхідної операції.

Наведені алгоритми побудови ортогональних операцій відомі із [77]. Вони є також наслідками із тривіального рекурсивного алгоритму. Беручи до уваги теорему 1.1 і теорему 1.2 маємо:

Твердження 5.1. *Нехай f_1 і f_2 є бінарними операціями на Q. Тоді істинними є такі імплікації:*

1) якщо f_1 є лівооборотною і f_2 є правооборотною, то операції g_1 і g_2, які є побудовними за (5.1), є ортогональними;

2) якщо f_1 є правооборотною і f_2 є лівооборотною, то операції g_1 і g_2, які є побудовними за (5.2), є ортогональними;

3) якщо f_1 і f_2 є оборотними, то операції g_1 і g_2, які є побудовними за (5.1), є ортогональними квазігрупами тоді і тільки тоді, коли f_2 і ${}^{\ell}f_1$ є ортогональними;

4) якщо f_1 і f_2 є оборотними, то операції g_1 і g_2, які є побудовними за (5.2), є ортогональними квазігрупами тоді і тільки тоді, коли f_2 і ${}^{r}f_1$ є ортогональними.

Нехай (g_1, g_2) і (g_1', g_2') є впорядкованими парами ортогональних операцій, які є побудовними за лівим рекурсивним алгоритмом. Це означає, що g_1 і g_1' є лівооборотними, і існують правооборотні операції f_2 і f_2' такі, що

$$g_2(x, y) := f_2(g_1(x, y), y), \qquad g_2' := f_2'(g_1'(x, y), y).$$

Припустимо $(g_1, g_2) = (g_1', g_2')$, тоді $g_1 = g_1'$ і

$$f_2(g_1(x, y), y) = f_2'(g_1'(x, y), y).$$

Звідси, $f_2 = f_2'$. Отже, дві впорядковані пари ортогональних операцій, які є побудовними за лівим рекурсивним алгоритмом, збігаються тоді і тільки тоді, коли впорядковані пари вхідних операцій збігаються.

Аналогічне твердження виконується для операцій побудовних за правим рекурсивним алгоритмом: дві впорядковані пари ортогональних операцій, які є побудовними за правим рекурсивним алгоритмом збігаються тоді і тільки тоді, коли пари вхідних операцій збігаються.

Приклад 5.1. *Нехай h_1 і h_2 є бінарними операціями, які визначені на множині $Q = \{0, 1, 2\}$ квадратами H_1 і H_2. Квадрат M є результатом накладання квадратів H_1 і H_2:*

H_1

0	0	1
1	1	2
2	0	2

H_2

0	2	2
0	1	1
0	1	2

M

00	02	12
10	11	21
20	01	22

Операції h_1 і h_2 є повними і вони є ортогональними, але не є оборотними. Отже, ці операції не є побудовними за рекурсивним алгоритмом.

Таким чином, існують пари ортогональних бінарних операцій такі, що кожна із операцій не є i-оборотною ($i = 1$ або 2). Такі операції не побудовні за рекурсивним алгоритмом відповідно до твердження 3.2.

Однак існують множини, на яких усі пари ортогональних операцій є побудовними за рекурсивним алгоритмом.

Приклад 5.2. *Розглянемо булеві операції f_1, f_2, f_3, f_4, f_5 і f_6, які визначаються квадратами L_1, L_2, L_3, L_4, L_5 і L_6:*

L_1

0	0
1	1

L_2

1	1
0	0

L_3

0	1
1	0

L_4

1	0
0	1

L_5

0	1
0	1

L_6

1	0
1	0

Інших повних бінарних булевих операцій не існує.

L_1, L_2, L_3, L_4 визначають ℓ-оборотні операції, а квадрати L_3, L_4, L_5, L_6 визначають r-оборотні операції, отже, L_3, L_4 визначають квазігрупові операції. Очевидно пари квадратів L_1 і L_5, L_2 і L_6 є транспонованими, а L_3 і L_4 є симетричними відносно головної діагоналі, тоді

$$f_1 = {}^s f_5, \qquad f_2 = {}^s f_6, \qquad f_3 = {}^s f_3, \qquad f_4 = {}^s f_4.$$

Ортогональне доповнення для f_1 може бути побудованим за лівим рекурсивним алгоритмом. За твердженням 5.1 у такий спосіб можна отримати 4 ортогональні доповнення і не існує інших ортогональних доповнень. Операція f_2 має 4 ортогональні доповнення, які будуються за лівим рекурсивним алгоритмом. Операції f_5 і f_6 також мають по 4 ортогональні доповнення, які можна побудувати за правим рекурсивним алгоритмом.

Ортогональне доповнення для f_3 може бути побудованим як за лівим, так і за правим рекурсивним алгоритмом. За твердженням 1.1 квазігрупа f_3 не має ортогонального квазігрупового доповнення. Таким чином, f_1, f_2, f_5 і f_6 є ортогональними доповненнями для f_3. Аналогічно f_1, f_2, f_5 і f_6 є ортогональними доповненнями для f_4.

Таким чином, кожна пара бінарних булевих операцій є побудовною за лівим або правим рекурсивним алгоритмом. Кількість ортогональних доповнень бінарних булевих операцій є також обчисленою у прикладі 4.4 використовуючи формулу оцінок кількості ортогональних доповнень.

Розбиття $\wp_2$ не є цікавим для вивчення, оскільки припущення збігається з висновком.

5.1.2. Ортогональність ізотопів квазігрупи

Для того, щоб дати побудову пари перпендикулярних квазігруп максимального типу розглянемо деякі допоміжні факти, а саме розглянемо найпростіші ізотопії, тобто коли дві компоненти ізотопізму є тотожніми перетвореннями носія. Нагадаємо, що ізотопізм виду (α, ι, ι) називається лівим крученням, (ι, β, ι) називається правим крученням, (ι, ι, γ) називається середнім крученням. Підстановки α, β, γ називатимемо визначаючими для відповідного ізотопізму.

Очевидно, що середні ізотопи однієї і тієї ж квазігрупи не є ортогональними, що випливає із дослідження розв'язків відповідної системи рівнянь.

Тут ми розглянемо умови, коли ліві кручення квазігрупи є ортогональними. Аналогічні умови є істинними і для правих кручень.

Зазначимо, що М.М. Глухов у роботі [77] вивчав методи побудови систем ортогональних бінарних операцій за допомогою груп, зокрема ним запропоновано метод побудови попарно ортогональних квазігруп (латинських квадратів) за допомогою груп Фробеніуса і доведено, що отримані ортогональні квазігрупи головно ізотопні одній і тій же групі і до того ж компоненти ізотопії є автоморфізмами цієї групи, зокрема усі ці квазігрупи лінійні.

Казатимемо, що підстановка α має одну нерухому точку, якщо вона майже неперехресна із тотожньою підстановкою ι, тобто існує єдиний елемент $a \in Q$, для якого виконується рівність $\alpha a = a$.

Лема 5.1. *Цілком допустима квазігрупа на Q і її лівий ізотоп є ортогональними тоді і тільки тоді, коли визначаюче відображення лівого ізотопізму має одну нерухому точку.*

Доведення. Припустимо h є бінарною цілком допустимою квазігрупою на Q, α є нетотожною підстановкою множини Q. Ортогональність квазігруп Th і h для будь-яких $a, b \in Q$, де $T := (\alpha, \iota, \iota)$, є еквівалентною однозначності розв'язку системи

$$\begin{cases} h(x, y) = a, \\ h(\alpha x, y) = b, \end{cases}$$

яка є еквівалентною однозначності розв'язку рівняння

$${}^{r}h(x, b) = {}^{r}h(\alpha x, a).$$

Для $a \neq b$ виконується нерівність $\alpha x \neq x$, тобто α є нетотожною підстановкою множини Q. Якщо ж $a = b$, то виконується рівність $\alpha x = x$, тобто існує єдиний елемент a_1, такий, що $\alpha a_1 = a_1$. Це означає, що підстановка α має одну нерухому точку. □

Метод побудови ортогональних операцій, який описаний в лемі 5.1, є частковим випадком методу описаного в теоремі 1.5. Справді, нехай маємо

латинський квадрат L на множині Q, який має повний набір попарно неперехресних трансверсалей, і нехай θ – одна із його трансверсалей з координатами $(x, \varphi x)$ для довільного $x \in Q$, де φ – відповідна повна підстановка. Застосуємо до квадрата L перестановку рядків за підстановкою α, тоді для будь-якого $x \in Q$ множина комірок виду $(\alpha x, \varphi x)$ також утворює трансверсаль θ' квадрата L^T, який є $T = (\alpha, \iota, \iota)$-ізотопний до L. Оскільки α має одну нерухому точку, то комірка цієї трансверсалі, яка знаходиться в першому рядку квадрата L, збігається з коміркою трансверсалі θ' квадрата L^T. Таким чином, існує повний набір попарно неперехресних трансверсалей квадрата L такий, що квадрат L^T можна отримати заміною елементів кожної із трансверсалей з цього набору за допомогою елемента, який знаходиться на перетині цієї трансверсалі і першого рядка латинського квадрата.

Теорема 5.1. *Дві ліво ізотопні цілком допустимі квазігрупи на Q є ортогональними тоді і тільки тоді, коли визначаючі підстановки відповідних ізотопізмів є майже неперехресними.*

Доведення. Припустимо h є цілком допустимою квазігрупою на Q, α і β є підстановками множини Q, $\alpha \neq \beta$, $T_1 := (\alpha, \iota, \iota)$, $T_2 := (\beta, \iota, \iota)$.

Відповідно до теореми 1.8, ортогональність квазігруп $T_1 h$ і $T_2 h$ є еквівалентною ортогональності h і $T_1^{-1} T_2 h$. Згідно з лемою 5.1, це означає, що перетворення $\alpha^{-1}\beta$ має одну нерухому точку на Q, тобто існує елемент $a \in Q$, такий, що $\alpha^{-1}\beta a = a$, звідки $\beta a = \alpha a$. Це означає, що α і β є майже неперехресними підстановками. □

Наслідок 5.1. *k-вибірка ліво ізотопних цілком допустимих квазігруп на Q є ортогональною тоді і тільки тоді, коли визначаючі відображення відповідних ізотопізмів є майже неперехресними.*

Метод побудови попарно ортогональних квазігруп за наслідком 5.1 зводиться до знаходження попарно майже неперехресних підстановок носія. Зазначимо, що при цій побудові не накладається умова лінійності на квазігрупи.

Приклад 5.3. *Нехай маємо квазігрупу f на $\mathbb{Z}_7$, яка визначається рівністю*

$$f(x, y) := 4x + 6y,$$

та дві майже неперехресні підстановки α і β множини $\mathbb{Z}_7$, які визначаються рівностями $\alpha x := 2x$, $\beta x := 3x$. Очевидно, що вони перетинаються в одній точці 0. Справді, $2 \cdot 0 = 3 \cdot 0$. Нехай існує елемент $a \in \mathbb{Z}_7 \backslash \{0\}$ такий, що $2 \cdot a = 3 \cdot a$, звідси $2 = 3$. Отримана суперечність вказує, згідно з наслідком 5.1, на ортогональність квазігруп g та h, які визначаються рівностями

$$g(x, y) = x + 6y, \qquad h(x, y) = 5x + 6y$$

і є (α, ι, ι)- та (β, ι, ι)-ізотопами операції f відповідно. Ортогональність цих квазігруп можна перевірити іншим чином: оскільки $\mathbb{Z}_7$ є полем, то визначник відповідної системи дорівнює 4, тобто взаємно простий із модулем, а тому система має єдиний розв'язок. До того ж, неважко перевірити, що квазігрупи f, g, h є взаємноортогональними, оскільки ι, α і β є попарно майже неперехресними.

Приклад 5.4. *Розглянемо таблицю Келі квазігрупи f на $\mathbb{Z}_7$:*

f	0	1	2	3	4	5	6
0	0	6	5	4	3	2	1
1	4	3	2	1	0	6	5
2	1	0	6	5	4	3	2
3	5	4	3	2	1	0	6
4	2	1	0	6	5	4	3
5	6	5	4	3	2	1	0
6	3	2	1	0	6	5	4

Як зазначено у прикладі 5.3, підстановки α і β є майже неперехресними. Запишемо таблиці Келі для $T_1 f$ і $T_2 f$, застосувавши до рядків перестановки α і β:

T_1f	0	1	2	3	4	5	6
$\alpha 0$	0	6	5	4	3	2	1
$\alpha 1$	4	3	2	1	0	6	5
$\alpha 2$	1	0	6	5	4	3	2
$\alpha 3$	5	4	3	2	1	0	6
$\alpha 4$	2	1	0	6	5	4	3
$\alpha 5$	6	5	4	3	2	1	0
$\alpha 6$	3	2	1	0	6	5	4

T_2f	0	1	2	3	4	5	6
$\beta 0$	0	6	5	4	3	2	1
$\beta 1$	4	3	2	1	0	6	5
$\beta 2$	1	0	6	5	4	3	2
$\beta 3$	5	4	3	2	1	0	6
$\beta 4$	2	1	0	6	5	4	3
$\beta 5$	6	5	4	3	2	1	0
$\beta 6$	3	2	1	0	6	5	4

Переставивши рядки в таблицях Келі відповідно до натурального порядку значень підстановок α і β, маємо відповідні для T_1f та T_2f латинські квадрати:

0	6	5	4	3	2	1
1	0	6	5	4	3	2
2	1	0	6	5	4	3
3	2	1	0	6	5	4
4	3	2	1	0	6	5
5	4	3	2	1	0	6
6	5	4	3	2	1	0

0	6	5	4	3	2	1
5	4	3	2	1	0	6
3	2	1	0	6	5	4
1	0	6	5	4	3	2
6	5	4	3	2	1	0
4	3	2	1	0	6	5
2	1	0	6	5	4	3

Отримані латинські квадрати є ортогональними, що можна перевірити їхнім накладанням.

5.1.3. Побудова багатомісних квазігруп з допустимими бінарними ретрактами

Відповідно до теореми 2.1 і наслідку 2.1, побудова квазігруп за допомогою повторної суперпозиції двох квазігруп зводиться до побудови пар перпендикулярних квазігруп. Нагадаємо, що основною вимогою перпендикулярності квазігруп є ортогональність певних їхніх бінарних ретрактів (означення 2.2). Тут запропоновані методи побудови квазігруп, які мають перпендикулярну пару, та пар перпендикулярних квазігруп.

У підрозділі 2.4 доведено, що серед перпендикулярностей максимальних типів достатньо розглядати перпендикулярність типу $(\iota, \iota; m)$.

Твердження 5.2. *n-арна квазігрупа має перпендикулярне квазігрупове доповнення типу $(\iota, \iota; m)$ тоді і тільки тоді, коли всі її $\{m, i\}$-ретракти є цілком допустимими, де $i \in \overline{1,n} \setminus \{m\}$.*

Доведення. За означенням 2.2, перпендикулярність визначається через ортогональність бінарних ретрактів. Для будь-якого $i \in \overline{1,n} \setminus \{m\}$ всі $\{m, i\}$-ретракти квазігрупи є квазігрупами, а за теоремою 1.4 до бінарних квазігруп існують ортогональні квазігрупові доповнення тоді і тільки тоді, коли вони є цілком допустимими. Звідси випливає істинність даного твердження. □

Наслідок 5.2. *Існують квазігрупи, які не мають перпендикулярного квазігрупового доповнення. Іншими словами, існує квазігрупа, композиція якої із довільною іншою квазігрупою, ні за яких умов не є квазігрупою.*

Приклад 5.5. *Довільні n-арні квазігрупи порядків 2 і 6 не мають перпендикулярної квазігрупової пари, тому що не існує цілком допустимих бінарних квазігруп цих порядків.*

Наступна теорема дає можливість будувати n-арні квазігрупи, які мають перпендикулярне квазігрупове доповнення.

Теорема 5.2. *Нехай f_1 є довільною бінарною квазігрупою і f_2 є довільною $(n-1)$-арною квазігрупою. n-арна квазігрупа f, яка визначається рівністю*

$$f(x_1, \ldots, x_n) := f_1(x_1, f_2(x_2, \ldots, x_n)),$$

для всіх $j \in \overline{2,n}$ має (цілком) допустимі $\{1, j\}$-ретракти тоді і тільки тоді, коли f_1 є (цілком) допустимою.

Доведення. Нехай $\bar{a} := (a_1, \ldots, a_n) \in Q^n$. Для довільного $j \in \overline{2,n}$

розглянемо $\{1,j\}$-ретракт квазігрупи f визначений вибіркою $\bar{a}$:

$$f_{\{1,j\}}(x_1,x_j) := f(x_1,a_2,\dots,a_{j-1},x_j,a_{j+1},\dots,a_n) =$$

$$= f_1(x_1,f_2(a_2,\dots,a_{j-1},x_j,a_{j+1},\dots,a_n)) = f_1(x_1,\beta_j x_j),$$

де $\beta_j x_j := f_2(a_2,\dots,a_{j-1},x_j,a_{j+1},\dots,a_n)$.

Відображення β_j є підстановкою множини Q, оскільки f_2 є квазігрупою. Отже, квазігрупи $f_{\{1,j\}}$ та f_1 є ізотопними. Відповідно до твердження 1.2, квазігрупа $f_{\{1,j\}}$ є (цілком) допустимою тоді і тільки тоді, коли квазігрупа f_1 є (цілком) допустимою. З довільності $j \in \overline{2,n}$, випливає, що квазігрупа f має (цілком) допустимі $\{1,j\}$-ретракти тоді і тільки тоді, коли f_1 є (цілком) допустимою. □

Таким чином, для того, щоб побудувати n-арну квазігрупу, яка має перпендикулярне квазігрупове доповнення типу $(\iota,\iota;1)$, достатньо мати одну цілком допустиму бінарну квазігрупу та іншу довільну $(n-1)$-арну квазігрупу.

Наслідок 5.3. *Нехай f_1, …, f_{n-1} є бінарними квазігрупами. n-арна квазігрупа f, яка визначається рівністю*

$$f(x_1,\dots,x_n) := f_1(x_1,f_2(x_2,\dots,f_{n-1}(x_{n-1},x_n)\dots)),$$

для всіх $i,j \in \overline{1,n}$, $i \neq j$, має (цілком) допустимі $\{i,j\}$-ретракти тоді і тільки тоді, коли f_1, …, f_{n-1} є (цілком) допустимими.

Доведення. Істинність цього твердження для $\{1,j\}$-ретрактів випливає із теореми 5.2. Аналогічно для довільних $i,j \in \overline{1,n}$, де $i \neq j$, доводиться ізотопність квазігруп $f_{\{i,j\}}$ та f_i. За твердженням 1.2, квазігрупа $f_{\{i,j\}}$ є (цілком) допустимою тоді і тільки тоді, коли f_i є (цілком) допустимою. З довільності i,j, $i \neq j$, випливає, що будь-який $\{i,j\}$-ретракт квазігрупи f є (цілком) допустимим тоді і тільки тоді, коли f_1, …, f_{n-1} є (цілком) допустимими бінарними квазігрупами. □

Отже, щоб побудувати n-арну квазігрупу, яка для будь-якого $i \in \overline{1,n}$ має перпендикулярне квазігрупове доповнення типу $(\iota,\iota;i)$, потрібно мати $(n-1)$-вибірку цілком допустимих бінарних квазігруп.

Наступне твердження описує один із методів побудови перпендикулярних квазігруп максимального типу.

Наслідок 5.4. *Нехай f є n-арною квазігрупою з цілком допустимими $\{1,j\}$-ретрактами, $j \in \overline{2,n}$. Квазігрупи f і Tf, де $T = (\alpha, \underbrace{\iota, \ldots, \iota}_{n})$, є перпендикулярними типу $(\iota, \iota; 1)$ тоді і тільки тоді, коли α має одну нерухому точку.*

Доведення. Перпендикулярність типу $(\iota, \iota; 1)$ квазігруп f і Tf є еквівалентною ортогональності їхніх однотипних $\{1,j\}$-ретрактів. Очевидно, що ці однотипні ретракти є ізотопними, причому ізотопізм має вигляд $T = (\alpha, \iota, \iota)$. За теоремою 5.1 ортогональність цих ретрактів рівносильна тому, що α має одну нерухому точку. □

Зазначимо, що для інших видів кручень, крім середнього, істинними є аналогічні твердження.

5.2. Побудова і доповнення ортогональних тернарних операцій і кубів

Тернарну операцію f на Q називатимемо лівооборотною (ℓ-оборотною), якщо вона є 1-оборотною, середньооборотною (m-оборотною), якщо вона є 2-оборотною і правооборотною (r-оборотною), якщо вона є 3-оборотною. Тобто (14)-парастроф тернарної операції f є лівим діленням, її (24)-парастроф є середнім діленням, а (34)-парастроф є правим діленням і позначатимемо ${}^{\ell}f$, ${}^{m}f$ і ${}^{r}f$ відповідно.

Пояснимо детальніше деякі із введених у розділі 3 понять для тернарних операцій. Операції $f_{(c,\{1,2\})}$, $f_{(b,\{1,3\})}$, $f_{(a,\{2,3\})}$, які визначаються рівностями

$$f_{(c,\{1,2\})}(x,y) := f(x,y,c),$$
$$f_{(b,\{1,3\})}(x,z) := f(x,b,z),$$
$$f_{(a,\{2,3\})}(y,z) := f(a,y,z),$$

називаються $\{1,2\}$-, $\{1,3\}$-, $\{2,3\}$-ретрактами операції f за допомогою елементів a, b, c відповідно, де $a,b,c \in Q$. $\{i,j\}$-ретракт та $\{j,i\}$-ретракт однієї операції є тотожними поняттями.

Нехай $\delta := \{i_1,i_2\} \subset \{1,2,3\}$, f і g є тернарними операціями на Q і $a,b \in Q$. Бінарні операції $f_{(a,\delta)}$ і $g_{(b,\delta)}$ називаються подібними δ-ретрактами операцій f і g, якщо $a = b$.

5.2.1. Побудова ортогональних тернарних операцій

У цьому підрозділі розглядатимемо блочні рекурсивні алгоритми (див. алгоритм 3.2) побудови ортогональних тернарних операцій. Нагадаємо, що одним із параметрів блочного рекурсивного алгоритму є розбиття множини індексів змінних. Зазначимо, що для тернарних операцій існують як тривіальні, так і нетривіальні розбиття множини індексів змінних.

Існує 5 розбиттів множини $\{1,2,3\}$:

$$\begin{aligned}
\pi_1 &:= \big\{\{1\},\{2\},\{3\}\big\},\\
\pi_2 &:= \big\{\{1\},\{2,3\}\big\},\\
\pi_3 &:= \big\{\{1,2\},\{3\}\big\},\\
\pi_4 &:= \big\{\{1,3\},\{2\}\big\},\\
\pi_5 &:= \{1,2,3\}.
\end{aligned}$$

Кожне з цих розбиттів визначає серію алгоритмів.

Розглянемо класифікацію блочних рекурсивних алгоритмів побудови ортогональних тернарних операцій за визначаючими розбиттями.

Алгоритм 5.1 (Тривіальний рекурсивний алгоритм з визначаючим розбиття $\big(\{1\},\{2\},\{3\}\big)$).

$$\begin{aligned}
g_1(x,y,z) &:= f_1(x,y,z),\\
g_2(x,y,z) &:= f_2(f_1(x,y,z),y,z),\\
g_3(x,y,z) &:= f_3(f_1(x,y,z),f_2(f_1(x,y,z),y,z),z),
\end{aligned} \tag{5.3}$$

або

$$g_1(x,y,z) := f_1(x,y,z),$$

$$g_2(x,y,z) := f_2(f_1(x,y,z),y,z), \tag{5.4}$$

$$g_3(x,y,z) := f_3(f_2(f_1(x,y,z),y,z), f_1(x,y,z),z).$$

Нижче наведена теорема є прямим наслідком теореми 3.4 для визначаючого розбиття $\big(\{1\},\{2\},\{3\}\big)$.

Теорема 5.3. *Нехай f_1 є ℓ-оборотною, f_2 є m-оборотною і f_3 є r-оборотною операціями на множині Q. Тоді операції g_1, g_2 і g_3, які побудовані за (5.3) або (5.4), є ортогональними.*

Для тернарних операцій існує 6 тривіальних рекурсивних алгоритмів (як кількість різних перестановок множини $\{1,2,3\}$) із такими вхідними даними:

1) f_1 – ℓ-оборотна, f_2 – m-оборотна і f_3 – r-оборотна операції;

2) f_1 – ℓ-оборотна, f_2 – r-оборотна і f_3 – m-оборотна операції;

3) f_1 – m-оборотна, f_2 – ℓ-оборотна і f_3 – r-оборотна операції;

4) f_1 – m-оборотна, f_2 – r-оборотна і f_3 – ℓ-оборотна операції;

5) f_1 – r-оборотна, f_2 – m-оборотна і f_3 – ℓ-оборотна операції;

6) f_1 – r-оборотна, f_2 – ℓ-оборотна і f_3 – m-оборотна операції.

Для кожного з цих випадків можна переформулювати теорему 5.3. Для прикладу, у випадку 5), операція f_1 є r-оборотною, тобто 3-оборотною, тому g_2 будуємо, поклавши f_1 на третє місце в операцію f_2 (f_2 є m-оборотною, тобто 2-оборотною), а операцію g_3 будуємо, поклавши f_1 і g_2 на третє і друге місця операції f_3 (f_3 є ℓ-оборотною, тобто 1-оборотною). Таким чином, відповідним впорядкованим розбиттям є $\big(\{3\},\{2\},\{1\}\big)$.

Нехай $\sigma \in \{s_1, s_2, s_3, s_4, s_5, s_6\}$, де $s_1 := (12)$, $s_2 := (13)$, $s_3 := (23)$, $s_4 := (12)(13)$, $s_5 := (13)(23)$, $s_6 := (12)(23) = \iota$. Щоб від визначаючого

розбиття $\big(\{3\},\{2\},\{1\}\big)$ перейти до визначаючого розбиття $\big(\{1\},\{2\},\{3\}\big)$ застосуємо до кожного елемента кожного із блоків розбиття парастроф s_2:

$$^{s_2}\big(\{3\},\{2\},\{1\}\big) = \big(\{3s_2\},\{2s_2\},\{1s_2\}\big) = \big(\{1\},\{2\},\{3\}\big).$$

Відповідно якщо f_1 є r-оборотною, то $^{s_2}f_1$ є ℓ-оборотною, якщо f_2 є m-оборотною, то $^{s_2}f_2$ є m-оборотною, якщо f_3 є ℓ-оборотною, то $^{s_2}f_3$ є r-оборотною.

Алгоритм 5.2 (Блочний рекурсивний алгоритм з визначаючим розбиттям $\big(\{1\},\{2,3\}\big)$).

$$\begin{aligned} g_1(x,y,z) &:= f_1(x,y,z), \\ g_2(x,y,z) &:= f_2(f_1(x,y,z),y,z), \\ g_3(x,y,z) &:= f_3(f_1(x,y,z),y,z). \end{aligned} \tag{5.5}$$

Нижче наведена теорема є прямим наслідком теореми 3.4 для визначаючого розбиття $\big(\{1\},\{2,3\}\big)$.

Теорема 5.4. *Нехай f_1 є ℓ-оборотною тернарною операцією і f_2, f_3 є $\{2,3\}$-ретрактно ортогональними операціями на Q. Тоді операції g_1, g_2 і g_3, які є побудовними за (5.5), є ортогональними.*

Існує 3 алгоритми цього виду (як кількість різних видів бінарних ретрактів тернарних операцій) з такими вхідними даними:

1) f_1 – ℓ-оборотна операція і f_2, f_3 – $\{2,3\}$-ретрактно ортогональні;

2) f_1 – m-оборотна операція і f_2, f_3 – $\{1,3\}$-ретрактно ортогональні;

3) f_1 – r-оборотна операція і f_2, f_3 – $\{1,2\}$-ретрактно ортогональні.

Для кожного із цих випадків можна переформулювати теорему 5.4. Для прикладу, у випадку 3) операція f_1 є r-оборотною (3-оборотною), тому операції g_2 і g_3 будуються шляхом заміни змінної z на $f_1(x,y,z)$ у термах $f_2(x,y,z)$ і $f_3(x,y,z)$. Отже, відповідним упорядкованим розбиттям є $\big(\{3\},\{1,2\}\big)$.

Щоб від визначаючого розбиття $\big(\{3\},\{1,2\}\big)$ перейти до визначаючого розбиття $\big(\{1\},\{2,3\}\big)$ застосуємо до кожного елемента кожного із блоків розбиття парастроф s_5:

$$^{s_5}\big(\{3\},\{1,2\}\big)=\big(\{3s_5\},\{1s_5,2s_5\}\big)=\big(\{1\},\{2,3\}\big).$$

Відповідно якщо f_1 є r-оборотною, то $^{s_5}f_1$ є ℓ-оборотною, якщо f_2, f_3 є $\{2,3\}$-ретрактно ортогональними, то за лемою 3.1 операції $^{s_5}f_2$, $^{s_5}f_3$ є $\{1,2\}$-ретрактно ортогональними.

Алгоритм 5.3 (Блочний рекурсивний алгоритм з визначаючим розбиттям $\big(\{1,2\},\{3\}\big)$).

$$\begin{aligned} g_1(x,y,z)&:=f_1(x,y,z),\\ g_2(x,y,z)&:=f_2(x,y,z),\\ g_3(x,y,z)&:=f_3(f_1(x,y,z),f_2(x,y,z),z) \end{aligned} \tag{5.6}$$

або

$$\begin{aligned} g_1(x,y,z)&:=f_1(x,y,z),\\ g_2(x,y,z)&:=f_2(x,y,z),\\ g_3(x,y,z)&:=f_3(f_2(x,y,z),f_1(x,y,z),z). \end{aligned} \tag{5.7}$$

Нижче наведена теорема є прямим наслідком теореми 3.4 для визначаючого розбиття $\big(\{1,2\},\{3\}\big)$.

Теорема 5.5. *Нехай f_1 і f_2 є $\{1,2\}$-ретрактно ортогональними операціями і f_3 є r-оборотною тернарною операцією, які визначені на множині Q. Тоді операції g_1, g_2 і g_3, які побудовні за (5.6) або (5.7), є ортогональними.*

Існує 3 алгоритми цього виду з такими вхідними даними:

1) f_1, f_2 – $\{1,2\}$-ретрактно ортогональні і f_3 – r-оборотна;

2) f_1, f_2 – $\{1,3\}$-ретрактно ортогональні і f_3 – m-оборотна;

3) f_1, f_2 – $\{2,3\}$-ретрактно ортогональні і f_3 – ℓ-оборотна.

Для кожного із цих випадків можна переформулювати теорему 5.5. Розглянемо випадок 2). Операції f_1, f_2 є $\{1,3\}$-ретрактно ортогональними, тому операція g_3 будується шляхом заміни змінних x і z у термі $f_3(x,y,z)$ термами $f_1(x,y,z)$ і $f_2(x,y,z)$. Отже, визначаючим розбиттям є $\big\{\{1,3\},\{2\}\big\}$. Щоб від визначаючого розбиття $\big\{\{1,3\},\{2\}\big\}$ перейти до визначаючого розбиття $\big\{\{1,2\},\{3\}\big\}$ застосуємо до кожного елемента кожного із блоків розбиття парастроф s_3:

$$^{s_3}\big(\{1,3\},\{2\}\big) = \big(\{1s_3,3s_3\},\{2s_3\}\big) = \big(\{1,2\},\{3\}\big).$$

Відповідно якщо f_1, f_2 є $\{1,3\}$-ретрактно ортогональними, то за лемою 3.1 операції $^{s_3}f_1$, $^{s_3}f_2$ є $\{1,3\}$-ретрактно ортогональними, якщо f_3 є m-оборотною, то $^{s_3}f_3$ є ℓ-оборотною.

Отже, блочні рекурсивні алгоритми побудови ортогональних тернарних операцій розподіляються на три класи із представниками (5.3), (5.5) і (5.6) відносно парастрофії визначаючих розбиттів.

З означення 4.4 випливає, що дві тернарні операції є перпендикулярними типу

- $(\iota,\iota;1)$, якщо всі пари подібних $\{1,2\}$- і $\{1,3\}$-ретрактів є ортогональними;
- $(\iota,\iota;2)$, якщо всі пари подібних $\{1,2\}$- і $\{2,3\}$-ретрактів є ортогональними;
- $(\iota,\iota;3)$, якщо всі пари подібних $\{1,3\}$- і $\{2,3\}$-ретрактів є ортогональними,

де ι позначає тотожну перестановку множини $\overline{1,3}$.

Наступне твердження є прямим наслідком теореми 2.1 і наслідку 2.1 для тернарних операцій.

Наслідок 5.5. *Нехай g і h є тернарними квазігрупами. Тоді*

1) операція f, яка визначена рівністю

$$f(x,y,x) = g(h(x,y,z),y,z),$$

є квазігрупою тоді і тільки тоді, коли g *і* ${}^{\ell}h$ *є перпендикулярними типу* $(\iota, \iota; 1)$*;*

2) операція f*, яка визначена рівністю*

$$f(x, y, x) = g(x, h(x, y, z), z),$$

є квазігрупою тоді і тільки тоді, коли g *і* ${}^{m}h$ *є перпендикулярними типу* $(\iota, \iota; 2)$*;*

3) операція f*, яка визначена рівністю*

$$f(x, y, x) = g(x, y, h(x, y, z)),$$

є квазігрупою тоді і тільки тоді, коли g *і* ${}^{r}h$ *є перпендикулярними типу* $(\iota, \iota; 3)$*.*

Теорема 5.6. *Нехай* f_1*,* f_2*,* f_3 *є квазігрупами. Трійка ортогональних операцій* (g_1, g_2, g_3)*, побудованих за* (5.3)*, є квазігруповою тоді і тільки тоді, коли*

1) f_2 *і* ${}^{\ell}f_1$ *є перпендикулярними типу* $(\iota, \iota; 1)$*;*

2) $f_3 \underset{2}{\oplus} f_2$ *і* ${}^{\ell}f_1$ *є перпендикулярними типу* $(\iota, \iota; 1)$*;*

3) f_3 *і* ${}^{m}f_2$ *є перпендикулярними типу* $(\iota, \iota; 2)$*.*

Доведення. Відповідно до 1) наслідку 5.5, операція g_2 є квазігрупою тоді і тільки тоді, коли f_2 і ${}^{\ell}f_1$ є перпендикулярними типу $(\iota, \iota; 1)$. Останню рівність із (5.3) переписуємо таким чином:

$$g_3(x, y, z) = \big(f_3 \underset{2}{\oplus} f_2\big)(f_1(x, y, z), y, z),$$

де $\big(f_3 \underset{2}{\oplus} f_2\big)(x, y, z) := f_3(x, f_2(x, y, z), z)$.

Відповідно до 1) наслідку 5.5, операція g_3 є квазігрупою тоді і тільки тоді, коли $f_3 \underset{2}{\oplus} f_2$ і ${}^{\ell}f_1$ є перпендикулярними типу $(\iota, \iota; 1)$, до того ж операція $f_3 \underset{2}{\oplus} f_2$ мусить бути квазігрупою також. Відповідно до 2) наслідку 5.5, вона є квазігрупою тоді і тільки тоді, коли f_3 і ${}^{m}f_2$ є перпендикулярними типу $(\iota, \iota; 2)$. □

Теорема 5.7. *Нехай f_1, f_2, f_3 є квазігрупами. Трійка ортогональних операцій (g_1, g_2, g_3), побудованих за (5.5), є квазігруповою тоді і тільки тоді, коли*

1) f_2 і ${}^{\ell}f_1$ є перпендикулярними типу $(\iota, \iota; 1)$;

2) f_3 і ${}^{\ell}f_1$ є перпендикулярними типу $(\iota, \iota; 1)$.

Доведення цього твердження випливає з 1) наслідку 5.5.

Проблема, коли операція g_3, побудована за допомогою останньої рівності із (5.6) або (5.7), є квазігрупою, залишається відкритою.

5.2.2. Ортогональні доповнення тернарних операцій

Використовуючи запропоновані алгоритми опишемо алгоритми доповнення ортогональних тернарних операцій.

Алгоритм 5.1 дає можливість доповнити ℓ-оборотну тернарну операцію до трійки ортогональних тернарних операцій, використовуючи лише оборотні на одному місці операції, тобто до ℓ-оборотної операції додаємо дві операції, які будуються рекурсивно за допомогою m-оборотної та r-оборотної операцій.

Теорема 5.8. *Нехай f_1 є ℓ-оборотною тернарною операцією на множині Q. Операції g_2 і g_3, які визначені рівностями (5.3) і (5.4) через довільні m-оборотну операцію f_2 і r-оборотну операцію f_3, є ортогональним доповненням операції f_1 до трійки ортогональних тернарних операцій f_1, g_2, g_3.*

Доведення цієї теореми випливає з теореми 5.3.

Алгоритм 5.2 дає можливість доповнювати ℓ-оборотну тернарну операцію до трійки ортогональних тернарних операцій. Для цього потрібно додати дві операції, які є побудовними за допомогою пари $\{2, 3\}$-ретрактно ортогональних тернарних операцій.

Теорема 5.9. *Нехай f_1 є ℓ-оборотною тернарною операцією на множині Q. Операції g_2 і g_3, які визначені рівностями (5.5) через до-*

вільні тернарні $\{2,3\}$-ретрактно ортогональні операції, є доповненням операції f_1 до трійки ортогональних тернарних операцій f_1, g_2, g_3.

Доведення цієї теореми випливає з теореми 5.4.

Очевидно, що за допомогою алгоритму 5.2 отримуємо ту ж саму трійку ортогональних операцій тоді і тільки тоді, коли взяти ту ж саму пару $\{2,3\}$-ретрактно ортогональних операцій.

Зауваження 5.1. *Довільна ℓ-оборотна тернарна операція є доповнювальною до трійки ортогональних операцій за алгоритмом 5.1 і алгоритмом 5.2.*

Нехай f_1 є ℓ-оборотною тернарною операцією. Припустимо (g_2, g_3) є доповненням операції f_1 до трійки ортогональних операцій за алгоритмом 5.1 з допомогою операцій f_2, f_3 і (g_2', g_3') є доповненням операції f_1 до трійки ортогональних операцій за алгоритмом 5.2 з допомогою операцій f_2', f_3'. У першому випадку маємо два варіанти: 1) f_2 є m-оборотною і f_3 є r-оборотною; 2) f_2 є r-оборотною і f_3 є m-оборотною. У другому випадку f_2', f_3' є $\{2,3\}$-ретрактно ортогональними.

Розглянемо випадок 1). Якщо $g_2 = g_2'$, то

$$f_2(f_1(x,y,z),y,z) = f_2'(f_1(x,y,z),y,z),$$

отже, $f_2 = f_2'$.

Якщо $g_3 = g_3'$, то

$$f_3(f_1(x,y,z), f_2'(f_1(x,y,z),y,z),z) = f_3'(f_1(x,y,z),y,z).$$

Покладемо в останню рівність довільний елемент $a \in Q$ замість терму $f_1(x,y,z)$:

$$f_3(a, f_2'(a,y,z),z) = f_3'(a,y,z).$$

Визначимо бінарні операції h_2, h_3 і m_3 таким чином:

$$h_2(y,z) := f_2'(a,y,z), \quad h_3(y,z) := f_3'(a,y,z), \quad m_3(v,z) := f_3(a,v,z),$$

тобто h_2, h_3 і m_3 є $\{2,3\}$-ретрактами операцій f_2', f_3' і f_3 відповідно. Ретрактна ортогональність операцій f_2' і f_3' спричинює ортогональність бінарних

операцій h_2 і h_3 та r-оборотність операції f_3 спричинює r-оборотність операції m_3. Відповідно до цих позначень маємо рівність

$$h_3(y,z) = m_3(h_2(y,z),z).$$

Це означає, що операції h_2 і h_3 є побудовними за (5.1). Отже, ортогональні доповнення за алгоритмами 5.1 і 5.2 збігаються тоді і тільки тоді, коли кожна пара $\{2,3\}$-ретрактів вхідних $\{2,3\}$-ретрактно ортогональних операцій є побудовною за лівим рекурсивним алгоритмом.

Аналогічно розглядаючи випадок 2), доводимо, що доповнення за алгоритмами 5.1 і 5.2 збігаються тоді і тільки тоді, коли кожна пара $\{2,3\}$-ретрактів вхідних $\{2,3\}$-ретрактно ортогональних операцій побудовна за правим рекурсивним алгоритмом.

Таким чином, множина доповнень ℓ-оборотної тернарної операції до трійки ортогональних операцій, які є побудовними за тривіальним рекурсивним алгоритмом, і множина доповнень, які є побудовними за алгоритмом 5.2, мають непорожній перетин і не збігаються. Це випливає із підрозділу 3.2: існують ортогональні операції, такі що жодна її операція не є навіть односторонньооборотною, в той час, як принаймні одна з ортогональних операцій, побудовних за тривіальним рекурсивним алгоритмом, мусить бути оборотною хоча б на одному місці. До того ж очевидно, що трійка тернарних лінійних операцій над абелевою групою є ортогональною тоді і тільки тоді, коли відповідна матриця є оборотною, однак існують оборотні матриці, елементи яких не є автоморфізмами.

Використовуючи алгоритм 5.3, можна доповнити пару $\{1,2\}$-ретрактно ортогональних тернарних операцій до трійки ортогональних операцій. Для цього необхідно додати одну операцію, яка є побудовною рекурсивно за допомогою довільної r-оборотної операції.

Теорема 5.10. *Нехай f_1, f_2 є $\{1,2\}$-ретрактно ортогональними тернарними операціями на Q. Операція g_3, яка визначається останньою рівністю із* (5.6) *і* (5.7) *за допомогою довільної правооборотної операції, є доповненням операцій f_1, f_2 до трійки ортогональних операцій f_1, f_2, g_3.*

Справді, за наслідком 4.1, $\{1,2\}$-ретрактно ортогональні операції є ортогональними, тому їх можна доповнити до трійки ортогональних операцій, а відповідно до теореми 5.5, операція g_3 є ортогональним доповненням ортогональних операцій f_1, f_2.

Зауважимо, що два ортогональних доповнення g_3 і g_3' пари $\{1,2\}$-ретрактно ортогональних операцій f_1, f_2 до трійки ортогональних тернарних операцій за допомогою r-оборотних операцій f_3 і f_3' відповідно збігаються тоді і тільки тоді, коли $f_3 = f_3'$.

Теореми 5.8, 5.9 і 5.10 можна переформулювати для інших блочних рекурсивних алгоритмів, які описані у підрозділі 5.2.

5.2.3. Побудова і доповнення ортогональних кубів

Кожен куб на Q можна подати за допомогою його $\{i,j\}$-зрізів для фіксованих $i,j \in \{1,2,3\}$. Нехай $G_{(\{1,2\},a)}$ позначає $\{1,2\}$-зріз куба G коли третя координата є зафіксованою елементом $a \in Q$.

Приклад 5.6. *Нехай куби G і H є визначеними на множині $\{1,2,3\}$. Нижче подамо їх за допомогою $\{1,2\}$-зрізів:*

G :

$G_{(\{1,2\},0)}$		
0	0	1
1	1	2
2	0	2

$G_{(\{1,2\},1)}$		
0	2	1
2	2	0
1	0	1

$G_{(\{1,2\},2)}$		
0	0	2
1	2	0
1	2	1

H :

$H_{(\{1,2\},0)}$		
0	2	2
0	1	1
0	1	2

$H_{(\{1,2\},1)}$		
0	0	0
1	2	1
2	2	1

$H_{(\{1,2\},2)}$		
1	0	1
2	0	2
0	2	1

Куби G і H є $\{1,2\}$-ретрактно ортогональними. Справді, накладемо

подібні $\{1,2\}$*-ретракти цих кубів:*

00	02	12
10	11	21
20	01	22

00	20	10
21	22	01
12	02	11

01	00	21
12	20	02
10	22	11

Кожна пара кожного із квадратів зустрічається точно один раз, тобто їхні подібні $\{1,2\}$*-зрізи є ортогональними, тому, за означенням 3.2, куби* G *і* H *є* $\{1,2\}$*-ретрактно ортогональними. Їхня ортогональність випливає із теореми 4.1.*

У наступному прикладі проілюструємо побудову та доповнення ортогональних кубів за алгоритмом 5.2.

Приклад 5.7. *Нехай* G *і* H *є* $\{1,2\}$*-ретрактно ортогональними кубами. Для того, щоб доповнити пару* $\{1,2\}$*-ретрактно ортогональних кубів* G *і* H *з прикладу 5.6 до трійки ортогональних кубів, скористаємося алгоритмом 5.2 і теоремою 5.10. Відповідно до кроку 1) алгоритму 5.2, потрібно обрати деякий куб, кожна із* 3*-ліній якого є латинською, наприклад, куб* L*, який подамо за допомогою його* $\{1,2\}$*-зрізів:*

L :

0	0	2
1	2	0
2	1	1

1	2	1
0	1	1
0	2	2

2	1	0
2	0	2
1	0	0

Оскільки G *і* H *є* $\{1,2\}$*-ретрактно ортогональними, то першим блоком визначаючого розбиття алгоритму є* $\{1,2\}$*, а другим –* $\{2\}$*, тобто визначаюче розбиття має вигляд* $\pi = \{\{1,2\},\{3\}\}$*.*

Тоді за кроком 2) алгоритму 5 будуємо куб K *за допомогою куба* L*, використовуючи формулу*

$$K(x,y,z) := L\big(G(x,y,z), H(x,y,z), z\big).$$

Знайдемо $\{1,2\}$*-зріз куба* K*, який визначений елементом* 0*:*

$$K(0,0,0) = L\big(G(0,0,0), H(0,0,0), 0\big) = L\big(0,0,0\big) = 0,$$

$$K(0,1,0) = L\big(G(0,1,0), H(0,1,0), 0\big) = L\big(0,2,0\big) = 2,$$

$$K(0,2,0) = L\big(G(0,2,0), H(0,2,0), 0\big) = L\big(1,2,0\big) = 0,$$

$$K(1,0,0) = L\big(G(1,0,0), H(1,0,0), 0\big) = L\big(1,0,0\big) = 1,$$

$$K(1,1,0) = L\big(G(1,1,0), H(1,1,0), 0\big) = L\big(1,1,0\big) = 2,$$

$$K(1,2,0) = L\big(G(1,2,0), H(1,2,0), 0\big) = L\big(2,1,0\big) = 1,$$

$$K(2,0,0) = L\big(G(2,0,0), H(2,0,0), 0\big) = L\big(2,0,0\big) = 2,$$

$$K(2,1,0) = L\big(G(2,1,0), H(2,1,0), 0\big) = L\big(0,1,0\big) = 0,$$

$$K(2,2,0) = L\big(G(2,2,0), H(2,2,0), 0\big) = L\big(2,2,0\big) = 1.$$

Знайдемо $\{1,2\}$*-зріз куба* K*, який визначений елементом* 1*:*

$$K(0,0,1) = L\big(G(0,0,1), H(0,0,1), 1\big) = L\big(0,0,1\big) = 1,$$

$$K(0,1,1) = L\big(G(0,1,1), H(0,1,1), 1\big) = L\big(2,0,1\big) = 0,$$

$$K(0,2,1) = L\big(G(0,2,1), H(0,2,1), 1\big) = L\big(1,0,1\big) = 0,$$

$$K(1,0,1) = L\big(G(1,0,1), H(1,0,1), 1\big) = L\big(2,1,1\big) = 2,$$

$$K(1,1,1) = L\big(G(1,1,1), H(1,1,1), 1\big) = L\big(2,2,1\big) = 2,$$

$$K(1,2,1) = L\big(G(1,2,1), H(1,2,1), 1\big) = L\big(0,1,1\big) = 2,$$

$$K(2,0,1) = L\big(G(2,0,1), H(2,0,1), 1\big) = L\big(1,2,1\big) = 1,$$

$$K(2,1,1) = L\big(G(2,1,1), H(2,1,1), 1\big) = L\big(0,2,1\big) = 1,$$

$$K(2,2,1) = L\big(G(2,2,1), H(2,2,1), 1\big) = L\big(1,1,1\big) = 1.$$

Знайдемо $\{1,2\}$*-зріз куба* K*, який визначений елементом* 2*:*

$$K(0,0,2) = L\big(G(0,0,2), H(0,0,2), 2\big) = L\big(0,1,2\big) = 1,$$

$$K(0,1,2) = L\big(G(0,1,2), H(0,1,2), 2\big) = L\big(0,0,2\big) = 2,$$

$$K(0,2,2) = L\big(G(0,2,2), H(0,2,2), 2\big) = L\big(2,1,2\big) = 0,$$

$$K(1,0,2) = L\big(G(1,0,2), H(1,0,2), 2\big) = L\big(1,2,2\big) = 2,$$

$$K(1,1,2) = L\big(G(1,1,2), H(1,1,2), 2\big) = L\big(2,0,2\big) = 1,$$

$$K(1,2,2) = L\big(G(1,2,2), H(1,2,2), 2\big) = L\big(0,2,2\big) = 0,$$
$$K(2,0,2) = L\big(G(2,0,2), H(2,0,2), 2\big) = L\big(1,0,2\big) = 2,$$
$$K(2,1,2) = L\big(G(2,1,2), H(2,1,2), 2\big) = L\big(2,2,2\big) = 0,$$
$$K(2,2,2) = L\big(G(2,2,2), H(2,2,2), 2\big) = L\big(1,1,2\big) = 0.$$

Отже, куб L представлений $\{1,2\}$-зрізами має такий вигляд:

$K:$

0	2	0
1	2	1
2	0	1

1	0	0
2	2	2
1	1	1

1	2	0
2	1	0
2	0	0

За теоремою 5.10, куб K є ортогональним доповненням кубів G і H. Це можна перевірити їхнім накладанням:

000	022	120
101	112	211
202	010	221

001	200	100
212	222	012
121	021	111

011	002	210
122	201	020
102	220	110

Кожна впорядкована трійка в отриманих квадратах зустрічається точно один раз, що означає ортогональність G, H, K.

Відповідно до теореми 5.5, з кубів G, H і L можна побудувати ортогональну трійку кубів G, H, K.

Висновки до розділу 5

Цей розділ містить деякі уточнення для бінарних операцій, наслідки результатів із попередніх розділів для тернарних і n-арних операцій.

Основними результатами цього розділу є такі:

1) знайдено методи побудови n-арних квазігруп, які мають перпендикулярну пару і пари перпендикулярних квазігруп;

2) наведено класифікацію блочних рекурсивних алгоритмів побудови та доповнення ортогональних тернарних операцій і гіперкубів відносно парастрофії визначаючих розбиттів.

Основні результати цього розділу викладені у [84, 89, 91].

ВИСНОВКИ

Дисертаційна робота присвячена дослідженню ортогональності вибірок багатомісних операцій і гіперкубів та інших узагальнень ортогональності бінарних операцій, вивченню методів побудови та доповнення багатомісних операцій, дослідженню умов оборотності композиції двох багатомісних операцій та інших суміжних проблем.

Знайдено необхідні і достатні умови оборотності довільної повторної композиції двох багатомісних операцій і доведено, що ця оборотність пов'язана із перпендикулярністю операцій, яка є одним із узагальнень ортогональності бінарних операцій. Описано відповідні поняття мовою гіперкубів.

Узагальнено алгоритм побудови ортогональних n-арних операцій, який описали і довели Г.Б. Білявська і Г.Л. Муллен (2005 р.), а потім узагальнили С. Марковскі та А. Мілева (2017 р.). Для цього уточнено поняття ретракту операції та ортогональності ретрактів і запропоновано алгоритм побудови ретрактно ортогональних операцій. Одним із параметрів узагальнення, що названо блочним рекурсивним алгоритмом, є розбиття множини індексів змінних, а зазначеним алгоритмам відповідають лише тривіальні розбиття. Доведено існування вибірок ортогональних операцій, які побудовні за блочним рекурсивним алгоритмом і непобудовні за його тривіальними випадками. Як наслідок описано та доведено алгоритм побудови ортогональних операцій із блоків операцій меншої арності.

Уточнено деякі результати Г.Б. Білявської та Г.Л. Муллена (2006 р.), що стосуються ортогональності ретрактів, а саме доведено, що ретрактна ортогональність є необхідною, але не достатньою умовою ортогональності. Більше того доведено, що існують ортогональні операції, які не мають ортогональних ретрактів. Звідси випливає, що, збільшуючи арність ортогональних операцій за допомогою безповторної композиції, властивість ортогональності зберігається. Крім цього, описано залежність між різними

видами ортогональності (класичне означення, перпендикулярність, ретрактна ортогональність, сильна ортогональність). Встановлені зв'язки між ортогональністю і ретрактною ортогональністю дали можливість описати алгоритм доповнення ортогональних n-арних операцій за допомогою блочного рекурсивного алгоритму. Доведено, що довільна вибірка ретрактно ортогональних n-арних операцій є доповнювальною до n-вибірки ортогональних n-арних операцій за цим алгоритмом. Крім того описано і доведено алгоритм побудови доповнень довільної k-вибірки ортогональних k-арних операцій до n-вибірки ортогональних n-арних операцій, де $n > k$.

Описано метод побудови n-арних квазігруп, які мають перпендикулярну пару, і пари перпендикулярних квазігруп. Зроблено деякі наслідки із отриманих результатів для тернарних операцій, зокрема класифіковано блочні рекурсивні алгоритми побудови і доповнення ортогональних тернарних операцій відносно парастрофії визначаючих розбиттів і показано, що їх є три класи.

Задачі, які потребують подальшого дослідження – це знаходження умов оборотності композиції Менгера n-арних квазігруп та її узагальнень; дослідження блочного рекурсивного алгоритму; побудова $(n+k)$-вибірок ортогональних n-арних операцій; знаходження методів доповнення n-вибірки ортогональних n-арних операцій до $(n+s)$-вибірки ортогональних n-арних операцій та інші.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Euler L. *Recherces sur une nouvelle especе de quarres magiques* // Verh. Zeeuwsch. Wetensch. Genootsch. Vlissingen. – 1782. – №9. – P. 85-239.
2. Tarry G. *Le Probleme de 36 Officers* // Comptes Rendu de l'Association Française pour l'Avancement de Science Naturel. – 1900. – №1. – P. 122-123.
3. Mann H.B. *The construction of orthogonal Latin squares* // Ann. Math. Statistics. –1942. – Vol. 13, №4. – P. 418-423.
4. Paige L.J. *Complete mappings of finite groups* // Pacific J. Math. – 1951. – Vol. 1, №1. – P. 111-116.
5. Белоусов В.Д. *Ассоциативные системы квазигрупп* // Успехи мат. наук. – 1958. – Т. 13, Вып. 3(81). – С. 243.
6. Кузнецов А.В. *О бесповторных контактных схемах и бесповторных суперпозициях функций алгебры логики* // Тр. МИАН СССР. – 1958. – Т. 51. – С. 186-225.
7. Bose R.C., Shrikhande S.S. *On the Falsity of Euler's Conjecture About the Non-Existence of two Orthogonal Latin Squares of order 4t+2* // Proceedings of the National Academy of Sciences. – 1959. – Vol. 45, №5. – P. 734-737.
8. Parker E.T. *Orthogonal latin squares* // Proceedings of the National Academy of Sciences. – 1959. – Vol. 45, №6. – P. 859-862.
9. Aczél J., Belousov V.D., Hosszú M. *Generalized associativity and bisymmetry on quasigroups* // Acta Mathematica Hungarica. – 1960. – Vol. 11, Iss. 1-2. – P. 127–136.
10. Bose R.C., Shrikhande S.S., Parker E.T. *Further results on the construction of mutually orthogonal Latin squares and the falsity of Euler's conjecture* // Canad. J. Math. – 1960. – Vol. 12. – P. 189-203.

11. Сосинский Л.М. *О представлении функций бесповторными суперпозициями в трехзначной логике* // Проблемы кибернетики. – 1964. – Вып. 12. – С. 57-68.

12. Белоусов В. Д., Сандик, М. Д. *n-арные квазигруппы и лупы* // Сибирский математический журнал. – 1966. – Т. 7, №1. – С. 31—54.

13. Белоусов В.Д. *Основы теории квазигрупп и луп.* Москва: Наука, 1967. – 223 с.

14. Белоусов В.Д. *Системы ортогональних операций* // Математический сборник. – 1968. – Т. 77(119), №1. – С. 38-58.

15. Kepka T., Nemec P. *T-quasigroups (Part I)* // Acta Universitatis Carolinae. Mathematica et Physica. – 1971. – Vol. 12, Iss. 1. – P. 39-49.

16. Kepka T., Nemec P. *T-quasigroups (Part II)* // Acta Universitatis Carolinae. Mathematica et Physica. – 1971. – Vol. 12, Iss. 2. – P. 31-49.

17. Белоусов В.Д. *Алгебраические сети и квазигруппы.* Кишинев: Штиинца, 1971. – 176 с.

18. Белоусов В.Д. *n-арные квазигруппы.* Кишинев: Штиинца, 1972. – 227 с.

19. Бектенов А.С. *Алгебраические (k, n)-сети и ортогональные системы n-арных квазигруп* // Изв. АН МССР. Сер. физ.-техн. и мат. наук. – 1974. – №1. – С. 3-11.

20. Бектенов А.С., Якубов Т. *Системы ортогональных n-арных операций* // Изв. АН МССР. Сер. физ.-тех. и мат. наук. – 1974. – №3. – С. 7-14.

21. Якубов Т. *О $(2, n)$-полугруппе n-арных операций* // Изв. АН МССР. Сер. физ.-тех. и мат. наук. – 1974. – №1. – С. 29-46.

22. Белоусов В.Д., Якубов Т. *Ортогональность n-арных операций* // Труды II Всесоюзного семинара по комбинаторной математике. – 1974. – Вып. 16, ч. 1. – С. 3-17.

23. Dénes J., Keedwell A.D. *Latin Squares and their Applications.* New York: Academic Press, 1974. – 547 p.

24. Arkin J., Straus E.G. *Latin k-cubes* // Fibonacci Quart. – 1974. – №12. – P. 288-292.

25. Белявская Г.Б., Руссу А.Ф. *О допустимости квазигрупп* // Мат. исслед. – 1975. – Т. 10, №1(35). – С. 45-57.

26. Белявская Г.Б. *r-ортогональные квазигруппы I* // Сети и квазигруппы: Мат. исслед. – 1976. – Вып. 39. – С. 32-39.

27. Белявская Г.Б. *r-ортогональные квазигруппы II* // Квазигруппы и комбинаторика: Мат. исслед. – 1976. – Вып. 43. – С. 39-48.

28. Belyavskaya G.B., Murathudjae S. *About admissibility of n-ary quasigroups* // Colloquia mathematica societatis Jonos Bolyai. Combinatorics Keszthely (Hungary). – 1976. – P. 101-119.

29. Evans T. *The construction of orthogonal k-skeins and latin k-cubes* // Aequationes Math. – 1976. – Vol. 13, Iss. 3. – P. 485-491.

30. Белявская Г.Б., Муратхуджаев С. *Допустимые n-арные квазигруппы I* // Изв. АН МССР, сер. физ.-техн. и матем. наук. – 1977. – №2. – С. 14-21.

31. Phelps K.T. *Conjugate orthogonal quasigroups* // J. Combin. Theory Ser. A. – 1978. – Vol. 25, Iss. 2. – P. 117-127.

32. Белоусов В.Д., Бектенов А.С. *Пространственные сети и их координатизация:* препринт. – Кишинев, 1979. – 32 с.

33. Белявская Г.Б., Муратхуджаев С. *Допустимые n-арные квазигруппы II* // Квазигруппы и лупы: Мат. исслед. – 1979. – Вып. 51. – С. 27-37.

34. Čupona G., Ušan J., Stojaković Z. *Multiquasigroups and some related structures* // Прилози МАНУ, Скопје. – 1980. – Т. I, №2. – P. 5-12.

35. Čupona G., Stojaković Z., Ušan J. *On finite multiquasigroups* // Publications de L'Institute Mathématique. Nouvelle série. – 1981. – T. 29 (43). – P. 53-59.

36. Белявская Г.Б. *О спектре частичной допустимости конечных квазигрупп (латинских квадратов)* // Мат. заметки. – 1982. – Т. 32, Вып. 6. – С. 777-788.

37. Муратхуджаев С. *Допустимость n-квазигрупп. Связь допустимости и ортогональности* // Исследования по теории бинарных и n-арных квазигрупп: Мат. исслед. – 1985. – Вып. 83. – С. 77-86.

38. Сырбу П.Н. *Об ортогональности и самоортогональности n-арных операций* // Квазигруппы: Мат. исслед. – 1987. – Вып. 95.– С. 121-129.

39. Сырбу П.Н. *О самоортогональности n-арных операций* // Исследование операций и квазигрупп: Мат. исслед. – 1988. – Вып. 102.– С. 92–96.

40. Глухов М.М. *Об α-замкнутых классах и α-полных системах функций k-значной логики* // Дискретная математика. – 1989. – Т.1, Вып.1. – С. 16-21. (Те саме: M. M. Glukhov, α-closed classes and α-complete systems of functions of k-valued logic // Discrete Math. Appl. – 1991. Vol. 1, Iss. 1. – P. 1–7.)

41. Белоусов В.Д. *Скрещенные изотопии квазигрупп* // Квазигруппы и их системы: Мат. исслед. – 1990. – Вып. 113. – С. 14-20.

42. Оной В.И., Урсу Л.А. *n-арные лупы со свойствами обратимости с одним параметром обращения* // Квазигруппы и их системы: Мат. исслед. – 1990. – Вып. 113. – С. 72–82.

43. Сырбу П.Н. *Самоортогональные n-группы* // Квазигруппы и их системы: Мат. исслед. – 1990. – Вып. 113. – С. 100-107.

44. Сырбу П.Н. *Ортогональные и самортогональные n-операций*: дисс. канд. физ.-мат. наук: 01.01.06. – Кишинев: АН Молдавской ССР, 1990. – 100 с.

45. Сохацкий Ф.Н. *Многоместные разделимые квазигруппы со свойством обратимости* // Квазигруппы и их системы: Мат. исслед. – 1990. – Вып. 113. – P. 89-99.

46. Dénes J., Keedwell A.D. *Latin Squares: New Developments in the Theory and Applications.* – Amsterdam: North-Holland, 1991. – xiv+453 p. (Series "Annals of Discrete Mathematics": vol. 46.)

47. Belyavskaya G.B. *Abelian quasigroups are T-quasigroups* // Quasigroups Related Systems. – 1994. – Vol. 1, №1 (1). – P. 1-7.

48. Sokhatskyj F., Syvakivskyj P. *On linear isotopes of cyclic groups* // Quasigroups Related Systems. – 1994. – Vol. 1, №1 (1). – P. 66-76.

49. Colbourn C.J., Zhu L. *The spectrum of r-orthogonal Latin squares* // Combinatorics Advances. Book series: Mathematics and Its Applications. – Boston, MA: Springer, 1995. – Vol. 329 – P. 49-75.

50. Laywine F., Mullen G.L., Whittle G. *D-Dimensional hypercubes and the Euler and MacNeish conjectures* // Mh. Math. – 1995. – Vol. 119, Iss. 3. – P. 223-238.

51. Mullen G.L., Schmid W.Ch. *An Equivalence between (T, M, S)-Nets and Strongly Orthogonal Hypercubes* // J. Combin. Theory. Ser. A. – 1996. – Vol. 76, Iss. 1. – P. 164-174.

52. Sokhatsky F.M. *The deepest repetition-free decompositions of non-singular functions of finite valued logics* // Proceedings of 26th IEEE International Symposium on Multiple-Valued Logic, 29-31 May 1996, Santiago de Compostela, Spain. – P. 279-282.

53. Гонсалес С., Косусело Е., Марков В.Т., Нечаев А.А. *Рекурсивные МДР-коды и рекурсивно дифференцируемые квазигруппы* // Дискрет-

ная математика. – 1998. – Т. 10, Вып. 2. – С. 3-29. (Те саме: Couselo E., Gonzalez S., Markov V., Nechaev A. *Recursive MDS-codes and recursively differentiable quasigroups* // Discrete Math. Appl. – 1998. – Vol. 8, Iss. 3. – P. 217-246.)

54. Zhu L., Zhang H. *A few more r-orthogonal Latin squares* // Discrete Math. – 2001. – Vol. 238, Iss. 1-3. – P. 183-191.

55. Zhu L., Zhang H. *Completing the spectrum of r-orthogonal Latin squares* // Discrete Math. – 2003. – Vol. 268, Iss. 1-3. – P 343-349.

56. Черемушкин А.В. *Бесповторная декомпозиция сильно зависимых функций* // Дискретная математика. – 2004. – Т. 16, Вып. 3. – С. 3-42.

57. Izbash V., Syrbu P. *Recursively differentiable quasigroups and complete recursive codes* // Comment. Math. Univ. Carolin. – 2004. – Vol. 45, №2. – P. 257-263.

58. Mullen G.L., Shcherbacov V. *n-T-quasigroup codes with one check symbol and their error detection capabilities* // Comment. Math. Univ. Carolin. – 2004. – Vol. 45, №2. – P. 321-340.

59. Sokhatsky F.M. *Commutation of operations and its relationship with Menger and Mann superpositions* // Discuss. Math. Gen. Algebra Appl. – 2004. – Vol. 24, Iss. 2. – P. 153-176.

60. Сохацький Ф.М. *Про схрещену ізотопію та схрещений ізоморфізм* // Праці інституту прикладної математики і механіки НАН України. – 2005. – №11. – С. 23-33.

61. Юревич О. *Про схрещену ізотопію поліагруп* // Праці інституту прикладної математики і механіки НАН України. – 2005. – №11. – С. 34-39.

62. Belousov V.D. *Parastrophic-orthogonal quasigroups* // Quasigroups Related Systems. – 2005. – Vol. 13, №1. – P. 25-72.

63. Belyavskaya G. *Pairwise ortogonality of n-ary operations* // Bul. Acad. Ştiinţe Repub. Mold. Mat. – 2005. – №3(49). – P. 5-18.

64. Belyavskaya G., Mullen G.L. *Orthogonal hypercubes and n-ary operations* // Quasigroups Related Systems. – 2005. – Vol. 13, №1. – P. 73-86.

65. Mullen G.L., Shcherbacov V.A. *On orthogonality of binary operations and squares* // Bul. Acad. Ştiinţe Repub. Mold. Mat. – 2005. – №2(48). – P. 3-42.

66. Trenkler M. *On orthogonal latin p-dimensional cubes* // Czechoslovak Math. J. – 2005. – Vol. 55, Iss. 3. – P. 725-728.

67. Belyavskaya G., Mullen G.L. *Strongly orthogonal and uniformly orthogonal many-placed operations* // Algebra Discrete Math. – 2006. – Vol. 5, №1. – P. 1-17.

68. Soedarmadji E. *Latin hypercubes and MDS codes* // Discrete Math. – 2006. – Vol. 306, Iss. 12. – P. 1232-1239.

69. Belyavskaya G. *S-systems of n-ary quasigroups* // Quasigroups Related Systems. – 2007. – Vol. 15, №2. – P. 251-260.

70. Belyavskaya G. *Power sets of n-ary quasigroups* // Bul. Acad. Ştiinţe Repub. Mold. Mat. – 2007. – №1(53). – P. 37-45.

71. Wanless I. *Transversals in Latin Squares* // Quasigroups Related Systems. – 2007. – Vol. 15, №1. – P. 169-190.

72. Dougherty S.T., Szczepanski T.A. *Latin k-hypercubes* // Australas. J. Combin. – 2008. – Vol. 40. – P. 145-160.

73. Krotov D.S. *On irreducible n-ary quasigroups with reducible retracts* // European J. Comb. – 2008. – Vol. 29, Iss. 2. – P. 507-513.

74. Krotov D.S., Potapov V.N., Sokolova P.V. *On reconstructing reducible n-ary quasigroups and switching subquasigroups* // Quasigroups Related Systems. – 2008. – Vol. 16, №1. – P. 55-67.

75. Belyavskaya G.B. *Secret-sharing schemes and orthogonal systems of k-ary operations* // Quasigroups Related Systems. – 2009. – Vol. 17, №2. – P. 161-176.

76. Krotov D.S., Potapov V.N. *n-Ary quasigroups of order* 4 // SIAM J. Discrete Math. – 2008. – Vol. 23, Iss. 2. – P. 561-570.

77. Глухов М.М. *О методах построения систем ортогональных квазигрупп с использованием групп* // Математические вопросы криптографии. – 2011. – Т. 2, №4. – С. 5–24.

78. Sokhatsky F.M., Fryz I.V. *Invertibility of repetition compositions and its connection with orthogonality* // International Mathematical Conference on Quasigroups and Loops "Loops'11" (Trest, Czech Republic, 21-27 July, 2011): Booklet of Abstracts. – Електрон. текст. дані. – URL: http://www.karlin.mff.cuni.cz/∼loops11/ (дата звернення: 20.01.2019).

79. Dudek W.A., Trokhimenko V.S. *Algebras of multiplace functions.* Berlin/Boston: Walter de Gruyter GmbH & Co. KG, 2012. – 399 p.

80. Ethier J.T., Mullen G.L. *Strong forms of orthogonality for sets of hypercubes* // Discrete Math. – 2012. – Vol. 312, Iss. 12-13. – P. 2050-2061.

81. Fryz I.V. *Some construction method of orthogonal n-ary operations and hypercubes* // International Conference dedicated to the 120-th anniversary of Stefan Banach, 17-21 September 2012, Lviv: Abstracts of Reports. – Lviv, 2012. – P. 253.

82. Sokhatsky F.M., Fryz I.V. *Invertibility criterion of composition of two multiary quasigroups* // Comment. Math. Univ. Carolin. – 2012. – Vol. 53, №3. – P. 429-445.

83. Belyavskaya G.B. *Successively orthogonal systems of k-ary operations* // Quasigroups Related Systems. – 2014. – Vol. 22, №2. – P. 165-178.

84. Фриз І.В. *Про побудову n-арних квазігруп* // Вісник Донецького національного університету. Сер. А: Природничі науки. – 2015. – №1/2. – С. 89-96.

85. Fryz I.V. *Block composition algorithm for constructing orthogonal multiary operations* // International Mathematical Conference on Quasigroups

and Loops “Loops'15”, 28 June - 04 July 2015, Ohrid: Book of Extended Abstracts. – Skopje, 2015. – P. 53-53.

86. Keedwell A.D., Dénes J. *Latin Squares and their Applications* (Second Edition). – Amsterdam: North Holland, 2015. – xiv+424 p.

87. Kokkala J.I., Östergård P.R. *Classification of Graeco-Latin Cubes* // J. Combin. Des. – 2015. – Vol. 23, №12. – P. 509-521.

88. Krotov D.S., Potapov V.N. *Constructions of transitive latin hypercubes* // European J. Combin. – 2016. – Vol. 54 – P. 51-64.

89. Fryz I.V. *On construction of n-ary quasigroups* // 7 European Congress of Mathematics, 18-22 July 2016, Berlin: Book of Abstracts. – Berlin, 2016. – P. 524.

90. Fryz I.V., Sokhatsky F.M. *Block composition algorithm for constructing orthogonal n-ary operations* // Discrete Math. – 2017. – Vol. 340, Iss. 8. – P. 1957-1966.

91. Фриз І.В. *Ортогональні доповнення тернарних операцій* // Вісник Донецького національного університету. Сер. А: Природничі науки. – 2017. – №1/2. – С. 119-127.

92. Fryz I.V. *Retract orthogonality and orthogonality of operations and hypercubes* // Fourth Mile High Conference on Nonassociative Mathematics, 29 July - 5 August 2017, Denver: Abstracts of Talks. – Denver, 2017. – P. 9.

93. Markovsky S., Mileva A. *On construction of orthogonal d-ary operations* // Publications de l'institut mathématique, Nouvelle série. – 2017. – №101 (115). – P. 109-119.

94. Shcherbacov V. *Elements of Quasigroup Theory and Applications.* – Chapman and Hall/CRC, 2017. – xxi+576 p.

95. Evans A.B. *Orthogonal Latin Squares Based on Groups.* – Springer International Publishing, 2018. – xv+537 p. (Series “Development in Mathematics”: vol. 57).

96. Fryz I.V. *Orthogonal complements of n-ary operations* // International Conference on Mathematics, Informatics and Information Technologies dedicated to the illustrious scientist Valentin Belousov, 19-21 April 2018, Balti: Communications. – Balti, 2018. – P. 43-44.

97. Fryz I.V.*Orthogonality and retract orthogonality of operations* // Bul. Acad. Ştiinţe Repub. Mold. Mat. – 2018. – №1(86). – P. 24-33.

98. Fryz I.V. *Algorithm for the complement of orthogonal operations* // Comment. Math. Univ. Carolin. – 2018. – Vol. 59, №2. – P. 135-151.

ДОДАТКИ

Список публікацій за темою дисертації

1. Sokhatsky F.M., Fryz I.V. *Invertibility criterion of composition of two multiary quasigroups* // Comment. Math. Univ. Carolin. – 2012. – Vol. 53, №3. – P. 429-445.

2. Фриз І.В. *Про побудову n-арних квазігруп* // Вісник Донецького національного університету. Сер. А: Природничі науки. – 2015. – №1/2. – С. 89-96.

3. Fryz I.V., Sokhatsky F.M. *Block composition algorithm for constructing orthogonal n-ary operations* // Discrete Math. – 2017. – Vol.340, Iss. 8. – P. 1957-1966.

4. Фриз І.В. *Ортогональні доповнення тернарних операцій* // Вісник Донецького національного університету. Сер. А: Природничі науки. – 2017. – №1/2. – С. 119-127.

5. Fryz I.V.*Orthogonality and retract orthogonality of operations* // Bul. Acad. Ştiinţe Repub. Mold. Mat. – 2018. – №1(86). – P. 24-33.

6. Fryz I.V. *Algorithm for the complement of orthogonal operations* // Comment. Math. Univ. Carolin. – 2018. – Vol.59, №2. – P. 135-151.

7. Sokhatsky F.M., Fryz I.V. *Invertibility of repetition compositions and its connection with orthogonality* // International Mathematical Conference on Quasigroups and Loops "Loops'11" (Trest, Czech Republic, 21-27 July, 2011): Booklet of Abstracts. – Електрон. текст. дані. – URL: http://www.karlin.mff.cuni.cz/∼loops11/ (дата звернення: 20.01.2019).

8. Fryz I.V. *Some construction method of orthogonal n-ary operations and hypercubes* // International Conference dedicated to the 120-th anniversary of Stefan Banach, 17-21 September 2012, Lviv: Abstracts of Reports. – Lviv, 2012. – P. 253.

9. Fryz I.V. *Block composition algorithm for constructing orthogonal multi-ary operations* // International Mathematical Conference on Quasigroups and Loops "Loops'15", 28 June - 04 July 2015, Ohrid: Book of Extended Abstracts. – Skopje, 2015. – P. 53-53.

10. Fryz I.V. *On construction of n-ary quasigroups* // 7 European Congress of Mathematics, 18-22 July 2016, Berlin: Book of Abstracts. – Berlin, 2016. – P. 524.

11. Fryz I.V. *Retract orthogonality and orthogonality of operations and hypercubes* // Fourth Mile High Conference on Nonassociative Mathematics, 29 July - 5 August 2017, Denver: Abstracts of Talks. – Denver, 2017. – P. 9.

12. Fryz I.V. *Orthogonal complements of n-ary operations* // International Conference on Mathematics, Informatics and Information Technologies dedicated to the illustrious scientist Valentin Belousov, 19-21 April 2018, Balti: Communications. – Balti, 2018. – P. 43-44.

Результати дисертаційної роботи доповідалися на таких конференціях і семінарах:

1. Міжнародна математична конференція з квазігруп та луп “Loops’11” (м. Трешт, Чехія, 21-27 липня 2011 р.).
2. Міжнародна конференція, присвячена 120-річчю з дня народження Стефана Банаха (м. Львів, Україна, 17-21 вересня 2012 р.).
3. Міжнародна математична конференція з квазігруп та луп “Loops’15” (м. Охрід, Македонія, 28 червня - 4 липня 2015 р.).
4. 7 Європейський конгрес математиків (м. Берлін, Німеччина, 18-22 липня 2016 р.).
5. Четверта конференція з неасоціативної математики (м. Денвер, США, 29 липня - 5 серпня 2017 р.).
6. Міжнародна конференція з математики, інформатики та інформаційних технологій, присвячена відомому вченому Валентину Білоусову (м. Бєльці, Республіка Молдова, 19-21 квітня 2018 р.).
7. Алгебраїчний семінар Інституту математики НАН України (м. Київ, 30 жовтня 2018 р., керівник – доктор фізико-математичних наук, член-кореспондент НАН України Ю.А. Дрозд).
8. Алгебраїчний семінар Київського національного університету імені Тараса Шевченка (м. Київ, 27 вересня 2018 р., керівники – доктор фізико-математичних наук, член-кореспондент НАН України Ю.А. Дрозд, доктор фізико-математичних наук А.П. Петравчук).