Для цитирования: *П.А. Кадиев, И.П. Кадиев. Формирование ортогональных латинских квадратов методом индексной структуризации таблиц умножения n– множеств. Вестник Дагестанского государственного технического университета. Технические науки. 2020; 47(3): 71-80. DOI:10.21822/2073-6185-2020-47-3-71-80*
For citation: *P.A. Kadiev, I.P. Kadiev. Formation of orthogonal latin squares by index structuring of n-set multiplication tables. Herald of Daghestan State Technical University. Technical Sciences. 2020; 47 (3): 71-80. (In Russ.) DOI:10.21822/2073-6185-2020-47-3-71-81*

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ
COMPUTER SCIENCE, COMPUTER ENGINEERING AND MANAGEMENT

УДК 519.5
DOI: 10.21822/2073-6185-2020-47-3-71-80

ФОРМИРОВАНИЕ ОРТОГОНАЛЬНЫХ ЛАТИНСКИХ КВАДРАТОВ МЕТОДОМ ИНДЕКСНОЙ СТРУКТУРИЗАЦИИ ТАБЛИЦ УМНОЖЕНИЯ n– МНОЖЕСТВ

П.А. Кадиев, И.П. Кадиев
Дагестанский государственный технический университет,
367026, г. Махачкала пр.И.Шамиля, 70, Россия

Резюме. Цель. *Целью исследования является формирование структурно совершенных ортогональных латинских квадратов (ОЛК) методом индексно упорядоченного расположения элементов таблицы умножения* ***n****-множеств на основе таблицы умножения.* ***Метод.*** *Формирование ортогональных латинских квадратов произведено методом индексной структуризации таблиц умножения* n *– множеств.* ***Результат.*** *Предлагается метод построения структурно совершенных ортогональных латинских квадратов пар индексированных конечных множеств нечетной размерности, на основе индексного упорядочения* nxn- *массива элементов таблицы умножения. Отличительная особенность предлагаемого метода построения структурно совершенных ортогональных квадратов из элементов двух индексированных множеств, одинаковой размерности, заключается в использовании авторами, разработанного ими метода перестановок элементов исходных* nxn- *матричных конфигураций, с формированием индексно упорядоченных или индексно структурированных комбинаторных конфигураций.* ***Вывод.*** *Использование метода построения семейства ортогональных латинских квадратов для пар индексированных конечных множеств одинаковой нечетной размерности по элементам, образующим их таблицу умножения, методом индексной структуризации по принципу функциональных зависимостей значений индексов пар элементов множеств и значений индексов пар элементов её окружения позволяет формировать ортогональные конфигурации определенного класса, в которых, оперируя индексами элементов, легко демонстрируется их ортогональность.*

Ключевые слова: *ортогональные латинские квадраты, таблица умножения, комбинаторные конфигурации, индексная структуризация*

FORMATION OF ORTHOGONAL LATIN SQUARES BY INDEX STRUCTURING OF N-SET MULTIPLICATION TABLES

P.A. Kadiev, I. P. Kadiev
Daghestan State Technical University,
70 I. Shamil Ave., Makhachkala 367026, Russia

Abstract. Objective. *Formation of structurally perfect orthogonal Latin squares by the method of index ordering of the multiplication table elements of* ***n****-sets based on the multiplication table.* ***Methods.*** *Orthogonal Latin squares are formed by the method of index structuring of n-set multiplication tables.* ***Results.*** *A method is proposed for constructing structurally perfect orthogonal Latin squares of pairs of indexed finite sets of odd dimension, based on the index ordering of an nxn-array*

of elements in the multiplication table. A distinctive feature of the proposed method for constructing structurally perfect orthogonal squares from elements of two indexed sets of the same dimension is the use by the authors of the method of permutations of elements of the original nxn-matrix configurations, with the formation of index-ordered or index-structured combinatorial configurations. ***Conclusion.*** *The use of the method for constructing a family of orthogonal Latin squares for pairs of indexed finite sets of the same odd dimension by the elements forming their multiplication table by the method of index structuring based on the principle of functional dependency of the index values on pairs of set elements and index values on pairs of elements from its environment allows creating a specific class orthogonal configuration, which, in terms of element indices, easily demonstrates their orthogonality.*

Keywords: *orthogonal Latin squares, multiplication table, combinatorial configurations, index structuring*

Введение. Для последних десятилетий характерно быстрое повышение интереса к дискретной математике, в том числе разделу – комбинаторике. Это объяснимо тем, что одной из центральных задач комбинаторики является исследование возможности различных вариантов формирования комбинаторных конфигураций из элементов конечных множеств, обладающих теми или иными свойствами. Если учесть, что при системном подходе все объекты – это системы, состоящие из компонентов, абстрактными моделями которых часто выступают множества и структуры, формируемых из их элементов конфигураций, возможные варианты расположения элементов, среди которых есть лучшие и наилучшие. Задача отбора варианта из числа возможных является одним из этапов принятия управленческого решения. Таким образом, методы комбинаторики – это основа выработки предложений по решению поставленных задач, один из факторов, обуславливающих интерес использования и рост внимания к методам комбинаторики.

Среди других проблем в век информационных технологий невозможно обойти вниманием вопросы требования к информации, представляемой для принятия решений: необходимость обеспечения оперативности ее доставки, полноты и достоверности информации, обеспечение конфиденциальности. И здесь, значительна роль методов комбинаторики при решении этих задач.

Так, известны комбинаторная ветвь теории информации, предлагающая меры количества информации, как количество разнообразий и связанных с ними неопределенности; меры оценки избыточности и методы сжатия информации, методы построения помехоустойчивых кодов, обнаруживающих и исправляющих ошибки при передаче и хранении информации; отдельная группа комбинаторных методов шифрования, для обеспечения конфиденциальности. Не остались без внимания и ранее решаемые задачи комбинаторикой задачи, такие как составление расписаний, календарное планирование, планирование экспериментов. Практически при решении большинства задач в указанных выше областях применения методов, в комбинаторике отведено определенное место конфигурациям, известным как латинские и греко-латинские квадраты, а также и вопросам их ортогонализации.

По определению «латинским квадратом» называется комбинаторная конфигурация nxn - размерности**,** строки и столбцы которых образованы элементами одного и того же множества, и содержат все его элементы [1,2]. Конфигурация была предложена Леонардом Эйлером в 1872 году, её строки и столбцы содержали все элементы латинского алфавита. Позже Эйлером была предложена конфигурация, получившая название греко-римского квадрата, строки и столбцы которой, образованы всеми упорядоченными парами символов греческого и латинского алфавитов. Обобщением этих открытий, особенно греко – римского квадрата, в комбинаторике стало понятие ортогональных латинских квадратов. Этим комбинаторным конфигурациям посвящены отдельные разделы комбинаторного анализа. Понятия «латинский» и «греко-латинский» квадрат сохранилось для комбинаторных конфигураций, строки и столбцы которых образованы элементами множества или парами элементов двух конечных множеств [3].

Ортогональными называются nxn-конфигурации в виде таблиц, в каждой ячейке которой расположена одна из возможных пар элементов исходных множеств, представленных латинскими квадратами, если строки и столбцы их содержат все упорядоченные пары элементов исходных конфигураций a_ib_j, где i, j принимают значения от 1 до n [4, 5], принадлежащих множествам A и B.

Построение ортогональных квадратов рассматривается в комбинаторике как сложная задача. Общий метод формализации процесса построения этих конфигураций не предложен. Для её решения применяются как алгебраические конструкции, так и комбинаторные (трансверсали, ортогональные массивы, дизайны, блок-схемы, тройки Штейнера и др.) [6-19].

Существует несколько подходов к решению этих задач, их часто сводят в две группы. К первой группе относятся методы, основанные на выборе «базового» латинского квадрата из элементов одного множества, которому отыскиваются ортогональные с ним латинские квадраты, образованные элементами другого множества. Ко второй группе относятся методы, использующие для построения ортогональных латинских квадратов различные комбинаторные объекты (включая сами латинские квадраты) меньших порядков [20-22].

Постановка задачи. Известно, что ортогональный квадрат образует таблица умножения конечных множеств одной размерности [22]. Основанием является то, что таблицу умножения множеств составляют все пары их элементов, каждая из которых занимают отдельную клетку квадрата. Утверждение о том, что полученная таблица это конфигурация, образованная наложением двух латинских квадратов, слабо аргументировано. Особенно лишает конфигурации этих свойств, при использовании в качестве элементов исходных множеств цифр, что чаще всего и используется авторами в приводимых примерах латинских и ортогональных латинских квадратов.

Для обозначения элементов множеств могут использоваться различные символы, требование к ним одно – их различимость. Одним из методов обозначения элементов множеств является использование общего символа, с присвоением ему дополнительного атрибута – индекса, указывающего его местоположения при классической системе индексации. Изменение местоположения элемента, при формировании из них комбинаторных конфигураций, сохраняет его различимость и информацию о предшествующем местоположении. В ряде случаев эта информация важна, так как характеризует изменения структуры множества или их совокупности [13,14].

Для иллюстрации справедливости утверждения о том, что таблицу умножения множеств можно рассматривать как ортогональный квадрат, образованный из элементов этих множеств, предлагается перестановками элементов по алгоритмам метода индексной структуризации представить её в более наглядной форме. Эта форма представления таблицы умножения после перестановок методом индексного упорядочения расположения элементов исходных множеств и их элементов, отражает структуру, сформированную наложением друг на друга двух латинских квадратов, подтверждая приведенное выше утверждение, что таблица содержит все элементы ортогонального латинского квадрата. Предложенный метод формирования ортогональных латинских квадратов можно рассматривать как метод построения ортогональных квадратов двух произвольно взятых индексированных множеств одинаковой размерности с индексной структуризацией их таблиц умножения.

Методы исследования. Для построения ортогональных латинских квадратов из элементов двух n- множеств A и B, необходимо сформировать все пары элементов множеств- a_ib_j. Этот процесс представляет собой составление таблицы их умножения.

При заданных n- множествах: A = $(a_1,a_2,\ldots, a_n)$ и B = $(b_1,b_2,\ldots, b_n)$ указанные пары образуют множество C , являющееся таблицей умножениям: A x B = C. Первым элементов в этих парах является элемент множества A, вторыми – элемент множества B. Множество C содержит все пары символов и представляют собой таблицу умножение множеств A и B. Общее число пар равно nxn: $C = [(a_1b_1),(a_1b_2),\ldots, (a_1b_n),(a_2b_1),(a_2b_2),\ldots,(a_2b_n), \ldots,(a_nb_1), (a_nb_2),\ldots,(a_nb_n)]$. В качестве примера приведена табл. 1 умножения множеств A и B, размерности **n** = 5.

Таблица 1. Умножения множеств A и B
Table 1. Multiplication of sets A and B

ai/bj	b_1	b_2	b_3	b_4	b_5
a1	a_1b_1	a_1b_2	a_1b_3	$a_1\ b_4$	$a_1\ b_5$
a 2	a_2b_1	a_2b_2	a_2b_3	$a_2\ b_4$	$a_2\ b_5$
a 3	a_3b_1	a_3b_2	a_3b_3	$a_3\ b_4$	$a_3\ b_5$
a 4	a_4b_1	a_4b_2	a_4b_3	$a_4\ b_4$	$a_4\ b_5$
a 5	a_5b_1	a_5b_2	a_5b_3	$a_5\ b_4$	$a\ b_5$

Для упрощения представления и анализа результатов может быть использовано соответствие $a_i\, b_j : c_{ij}$.

Таблицу 1 умножения множеств сводим в матричную nxn - конфигурацию $C = ||c_{ij}||$, приведенную на рис. 1, где установлено соответствие $c_{ij} : a_i\, b_j$, при $i,j \in 1,2,\ldots,n$, которую образуют все nxn- пар индексов.

В полученной конфигурации C могут быть выполнены перестановки элементов методом индексной структуризации, предложенным в [13,15].

Для индексной структуризации формируемой конфигурации нами использована

$$C = \begin{matrix} c_{11}c_{12}\ldots..c_{1n} \\ c_{21}c_{22}\ldots..c_{2n} \\ c_{31}c_{32}\ldots..c_{3n} \\ \ldots\ldots\ldots\ldots\ldots\ldots.. \\ c_{n1}c_{n2}\ldots c_{nn} \end{matrix}$$

Рис.1. Комбинаторная конфигурация - таблица умножения, n- множеств A x B = C
Fig. 1. Combinatorial configuration - multiplication table, n-sets A x B = C

В полученной конфигурации C могут быть выполнены перестановки элементов методом индексной структуризации, предложенным в [13,15].

Для индексной структуризации формируемой конфигурации нами использована система рекуррентных соотношений на множестве пар индексов элементов, которые определены как система индексно-функционального окружения элемента, предложенная в [14], приведенная на рис. 2 .

$$\begin{matrix} c_{i-(k+1),j-k}\cdots \\ \ldots,c_{i-k,j-(k+1)},\ c_{i,j},\ c_{i+k,j+(k+1)},\ldots \\ \ldots c_{i+(k+1),j+k}\cdots, \end{matrix} \quad (\text{mod } n)$$

Рис.2. Система индексно-функциональной структуризации окружения элемента
Fig.2. The system of index-functional structuring of the element's environment

Приведенная система индексно-функциональной структуризации окружения элементов является системой индексации, которая построена на принципе функциональных зависимостей значений индексов элементов окружения любого элемента комбинаторной конфигурации от значений индексов окруженного элемента.

По принятой на рис. 2 системе индексно - функционального окружения элементов выполняются перестановки элементов в матрице C. Для формирования перестановками элементов конфигурации C индексно структурированной конфигурации C*, в ней выбирается «базовый» элемент и его местоположение в формируемой перестановками конфигурации. Местоположение «базового» элемента будет определять структуру формируемой конфигурации.

В качестве «базового» элемента может быть выбран любой из *nxn* элементов матрицы C, с расположением его на любой из *nxn*-позиций в формируемой перестановками конфигурации C*. Отсюда следует, что располагая выбранный «базовый» элемент поочередно на всех nxn-

позициях формируемых конфигураций, могут быть построены nxn различных «базовых» индексно структурированных конфигураций.

Система индексации (рис.2), использованная при сформировании конфигурации С*, позволяет различать свойства, характерные для ортогональных латинских квадратов: индексы элементов на одноименных позициях в строках и столбцах принимают значения от 1 до *n*, свидетельствуя наличие в них «представителей» каждой строки и каждого столбца исходной конфигурации С.

Обсуждение результатов. В результате перестановок по выбранной системе расположения элементов формируется конфигурация С* с индексно упорядоченной структурой, приведенная для частного случая n = 7, на рис. 3 при значениях коэффициента индексной удаленности окружения k = 1.

Индексная упорядоченность в сформированной конфигурации заключается в том, что в каждой строке и каждом столбце индексы элементов принимают значения от 1 до n. В каждом из них имеет место «индексное представительство» строк и столбцов исходной матрицы С. Ниже рассмотрен пример выполнения указанных преобразований для исходных множеств A= $\{a_i\}$ и B = $\{b_j\}$ размерности *n=7*. Результат умножения сведен к матрице C_{7x7}, приведенной на рис.3.

$$C_{7x7} = \begin{matrix} c_{11}c_{12}c_{13}c_{14}c_{15}c_{16}c_{17} \\ c_{21}c_{22}c_{23}c_{24}c_{25}c_{26}c_{27} \\ c_{31}c_{32}c_{33}c_{34}c_{35}c_{36}c_{37} \\ c_{41}c_{42}c_{43}c_{44}c_{45}c_{46}c_{47} \\ c_{51}c_{52}c_{53}c_{54}c_{55}c_{56}c_{57} \\ c_{61}c_{62}c_{63}c_{64}c_{65}c_{66}c_{67} \\ c_{71}c_{72}c_{73}c_{74}c_{75}c_{76}c_{77} \end{matrix}$$

Рис.3. Конфигурация произведения множеств A_{7x7} x B_{7x7}
Fig. 3. Configuration of the product of sets A7x7 x B7x7

Перестановками по системе индексно - функциональной структуризации окружения элемента, приведенной на рис. 2, при значениях k = 1 и выбранном «базовом» элементе c_{11}, местоположение которого сохранили как в исходной конфигурации $C_{7x7,}$ приведенные на рис. 3, и расположили элемент его в другой позиции, формируются индексно структурированные конфигурации C_{7x7}*и C_{7x7}**, приведенные на рис.4, которые отличаются структурой строк и столбцов.

$$C_{7x7}{*} = \begin{matrix} c_{11}c_{23}c_{35}c_{47}c_{52}c_{64}c_{76} \\ c_{32}c_{44}c_{56}c_{61}c_{73}c_{15}c_{27} \\ c_{53}c_{65}c_{77}c_{12}c_{24}c_{36}c_{41} \\ c_{72}c_{16}c_{21}c_{33}c_{45}c_{57}c_{62} \\ c_{24}c_{37}c_{42}c_{54}c_{66}c_{71}c_{13} \\ c_{46}c_{51}c_{63}c_{75}c_{17}c_{22}c_{34} \\ c_{67}c_{72}c_{14}c_{26}c_{31}c_{73}c_{55} \end{matrix} \qquad C_{7x7}{**} = \begin{matrix} c_{53}c_{65}c_{77}c_{12}c_{24}c_{36}c_{41} \\ c_{72}c_{16}c_{21}c_{33}c_{45}c_{57}c_{62} \\ c_{24}c_{37}c_{42}c_{54}c_{66}c_{71}c_{13} \\ c_{46}c_{51}c_{63}c_{75}c_{17}c_{22}c_{34} \\ c_{67}c_{72}c_{14}c_{26}c_{31}c_{43}c_{55} \\ \mathbf{c_{11}}c_{23}c_{35}c_{47}c_{52}c_{64}c_{76} \\ c_{32}c_{44}c_{56}c_{61}c_{73}c_{15}c_{27} \end{matrix}$$

Рис.4. Конфигурации, образованные перестановками элементов методом индексно - функциональной структуризации множества C_{7x7}
Fig. 4. Configurations formed by permutations of elements by the method of index-functional structuring of the C7x7 set

Индексно-функциональная структура конфигурации C_{7x7}* отражена в особенности индексации элементов строк и столбцов. В них значения индексов меняются от 1 до n, каждый элемент в строках и столбцах исходного массива С занимает различную позицию.

Конфигурациями этого класса были нами приведены в работе [12,13] и определены нами как конфигурации нового типа - двух индексные латинские квадраты, формируемые из исходной n x n - совокупности множеств циклическими сдвигами строк и столбцов по заданному алгоритму.

Для исследования свойств полученной конфигурации, как ортогонального латинского квадрата, целесообразно перейти к символике обозначения элементов исходных множеств А и В, обратной заменой соответствий c_{ij}: a_ib_j. При этом формируется конфигурация, приведенная на рис.5.

Конфигурация, приведенная на рис.5 является ортогональным квадратом, образованным парами элементов множеств А и В.

Каждый элемент этой конфигурации представляет пару из элементов произведения множеств А x В, индексы и элементы которых не повторяются. Все это достаточно наглядно отображено на системе индексации элементов в строках и столбцах конфигурации на рис. 5.

$$A \times B = \begin{matrix} a_1b_1 & a_2b_3 & a_3b_5 & a_4b_7 & a_5b_2 & a_6b_4 & a_7b_6 \\ a_3b_2 & a_4b_4 & a_5b_6 & a_6b_1 & a_7b_3 & a_1b_5 & a_2b_7 \\ a_5b_3 & a_6b_5 & a_7b_7 & a_1b_2 & a_2b_4 & a_3b_6 & a_4b_1 \\ a_7b_2 & a_1b_6 & a_2b_1 & a_3b_3 & a_4b_5 & a_5b_7 & a_6b_2 \\ a_2b_4 & a_3b_7 & a_4b_2 & a_5b_4 & a_6b_6 & a_7b_1 & a_1b_3 \\ a_4b_6 & a_5b_1 & a_6b_3 & a_7b_5 & a_1b_7 & a_2b_2 & a_3b_4 \\ a_6b_7 & a_7b_2 & a_1b_4 & a_2b_6 & a_3b_1 & a_7b_3 & a_5b_5 \end{matrix}$$

Рис.5. Ортогональный латинский квадрат, образованный элементами таблицы умножения множеств А и В
Fig. 5. Orthogonal Latin square formed by the elements of the multiplication table of sets A and B

Для демонстрации приведенного выше утверждения о том, что таблица умножения множеств одинаковой размерности является ортогональным квадратом, можно провести преобразование полученной конфигурации.

Так, если в полученной конфигурации, приведенной на рис.5, образованной всеми парами элементов произведения множеств – $a_ib_j : c_{ij}$, выполнить операцию удаления первых элементов в парах, являющихся, по условию умножения множеств, элементами множества А, то формируется латинский квадрат, образованный элементами второго множества – Влк (рис.6).

$$B_{лк} = \begin{matrix} b_1b_3b_5b_7 & b_2b_4b_6 \\ b_2b_4b_6b_1 & b_3b_5b_7 \\ b_3b_5b_7b_2 & b_4b_6b_1 \\ b_2b_6b_1b_3 & b_5b_7b_2 \\ b_4b_7b_2b_4 & b_6b_1b_3 \\ b_6b_1b_3b_5 & b_7b_2b_4 \\ b_7b_2b_4b_6 & b_1b_3b_5 \end{matrix}$$

Рис.6. Латинский квадрат, образованный из C_{7x7}* элементами множества В
Fig. 6. Latin square formed from C7x7 * by elements of set B

При удалении вторых элементов в парах, элементов второго множества, формируется латинский квадрат, образованный элементами множества А (рис.7).

$$A_{лк} = \begin{matrix} a_1a_2a_3a_4 & a_5a_6a_7 \\ a_3a_4a_5a_6 & a_7a_1a_2 \\ a_5a_6a_7a_1 & a_2a_3a_4 \\ a_7a_1a_2a_3 & a_4a_5a_6 \\ a_2a_3a_4a_5 & a_6a_7a_1 \\ a_4a_5a_6a_7 & a_1a_2a_3 \\ a_6a_7a_1a_2 & a_3a_7a_5 \end{matrix}$$

Рис.7. Латинский квадрат, образованный из $C7_{x7}$*, элементами множества А
Fig. 7. Latin square formed from C7x7 *, elements of set A

Подобное преобразование в таб.1 умножения множеств или матричной конфигурации C, образованной элементами таблицы, приведенное в табл. 2, не позволяет убедиться, что эти конфигурации являются ортогональными конструкциями.

Таблица 2. Таблица умножения при устранении элементов множества A
Table 2. Multiplication table when eliminating elements of set A

ai/bj	b_1	b_2	b_3	b_4	b_5
a1	b_1	b_2	b_3	b_4	b_5
a 2	b_1	b_2	b_3	b_4	b_5
a 3	b_1	b_2	b_3	b_4	b_5
a 4	b_1	b_2	b_3	b_4	b_5
a 5	b_1	b_2	b_3	b_4	b_5

Следовательно, выполненные выше преобразования таблицы умножения множеств, построение массива из элементов произведения, и перестановки элементов методом индексной структуризации, формируют конфигурация C*, которая представляет собой ортогональный латинский квадрат, полученный наложением двух латинских квадратов, образованных сомножителями-множествми.

Её структура, удовлетворяет условиям ортогональности латинских квадратов, которые образованы структуризацией перестановками массива элементов произведения двух n-множеств.

Кроме того, подтверждением ортогональности является и то, что строки и столбцы конфигурации являются непересекающимися трансверсалями. Это отражает сущность предлагаемого метода: получение ортогональных латинских квадратов из элементов двух конечных множеств одинаковой размерности по приведенному алгоритму последовательности преобразований.

Следует отметить, что в конфигурации C*, как «базовой» конфигурации, подставляя любой из элементов c_{ij}: a_ib_j, таблицы умножения последовательно на все n x n - позиций, может быть сформировано семейство изотопных ортогональных латинских квадратов, образованных парой множеств A и B, которые отличаются изменением местоположения его элементов, различием структуры, но с сохранением свойств индексного представительства в строках и столбцах.

Конфигурации, полученные из «базовой» перестановками строк или столбцов являются изотопными вариантами построения ортогональных латинских квадратов из элементов множеств A и B.

Они являются результатом наложения изотопных латинских квадартов, полученных перестановками элементов строк и столбцов «базовых» латинских квадратов множества A и B.

Наложением изотопных латинских квадратов, образованных «базовыми» латинскими квадратами исходных множеств могут быть сформированы семейства ортогональных латинских квадратов этих множеств.

В итоге может быть сформулировано, практически доказанное приведенным примером, следующее утверждение:

ортогональный латинский квадрат для двух конечных множеств A и B может быть построен из пар элементов a_ib_j таблицы умножения, где i, j принимают значения от 1 до n, если расположить их в клетках *n x n* - таблицы по рекуррентным соотношением между индексами любой пары и значениями индексов элементов пар её окружения по функциональным зависимостям между ними вида (1), приведенным на рис. 8, при следующих ограничениях:

- n – число нечетное; - k- число простое, не является делителем числа n;
- значения индексов элементов окружения по суммам, при их значения больших, чем n, определяются по модулю mod n;

– при отрицательных значениях результатов выполнения операций по определению значений индексов пар элементов окружения, равных (– m), значения индекса определяется по формуле (n-m), если оно равно нулю, то значение индекса выбирается равным числу n.

$$\begin{matrix} \dots\ ,\ a_{i-(k+1)}\,b_{j-k},\dots \\ \dots\ ,a_{i-k}\,b_{,j-(k+1)},\ \underline{\boldsymbol{a_i\ b_j}},\ a_{i+k}\,b_{,j+2},\dots \\ \dots,a_{i+(k+1)}\,b_{,j+k},\dots, \end{matrix} \quad (\text{mod } n) \qquad (1)$$

Рис.8. Система индексно – функциональной структуризации окружения элемента $\underline{a_i\ b_j}$
Fig. 8.System of index - functional structuring of the environment of the element $\underline{a_i\ b_j}$

Ортогональные латинские квадраты двух множеств могут быть сформированы наложением изотопных латинских квадратов, образованных из «базовых» латинских квадратов исходных множеств.

Сформулированное утверждение может рассматриваться как алгоритм формализации процесса формирования ортогональных латинских квадратов из элементов двух множеств равной конечной размерности, удовлетворяющих приведенным выше ограничениям к размерности и системе индексации.

Вывод. Отличительная особенность предлагаемого метода построения ортогональных квадратов из элементов двух индексированных множеств, одинаковой размерности, заключается в использовании авторами разработанного ими метода перестановок элементов исходных nxn- матричных конфигураций, с формированием индексно упорядоченных или индексно структурированных комбинаторных конфигураций.

Его использование для формирования ортогональных конфигураций позволяет формировать ортогональные конфигурации определенного класса, в которых, оперируя индексами элементов, легко демонстрируется их ортогональность. Эти конфигурации обладают свойством, которое позволяет их рассматривать как отдельный класс или семейство ортогональных латинских квадратов, а именно структурно совершенных, со свойством индексного «представительства» отдельных пар элементов.

Анализ структуры формируемых комбинаторных конфигураций показал, что характерные для ортогональных конфигураций свойства у них сохраняются при любых перестановках между собой строк и столбцов.

При построении конфигурации любая пара из *nxn* элементов, может быть расположена на любой из *nxn*-позиции, формируя структурно различимые ортогональные латинские квадраты. Это позволяет определить число возможных вариантов построения пар латинских квадратов, образующих «семейство», образованное множествами A и B, как число возможных перестановок строк и столбцов полученной конфигурации.

Полученная перестановками элементов конфигурации C (рис.3) конфигурации C* и C** (рис.4), могут быть рассмотрены как «базовые». Перестановками строк и столбцов этих матриц могут быть сформированы изотопные конфигурации (C**- изотопна конфигурации C*, так как получена перестановками ее строк), которые каждая может быть получена определенными операциями перестановок строк и столбцов.

Следует отметить и то обстоятельство, что из элементов множеств A и B могут быть сформированы «базовые» латинские квадраты, перестановками строк и столбцов которых также могут быть сформированы изотопные ортогональные латинские квадраты. Существует понятие семейства латинских квадратов, которое образуют квадраты, любая пара которых взаимно ортогональны.

Каждый латинский квадрат, образованный из «базовых» для множества A (B), является ортогональным с изотопными квадратами, образованными из базовой конфигурации латинского квадрата множества B (A).

Ортогональный латинский квадрат может быть получен наложением изотопных латинских квадратов, образованных базовыми латинскими квадратами из этих множеств, также как из базового ортогонального квадрата C*, путем изменения её структуры перестановками строк или столбцов и значений индексов aij : aji .

Предлагаемый метод формирования ортогональных латинских квадратов для любой пары индексированных конечных множеств одинаковой нечетной размерности является более общим, чем построение их на основе подбора к выбранному латинскому квадрату ортогональных с ним, и построение их наложением элементов двух выбранных латинских квадратов друг на друга.

Достоинством метода является и то, что он обладает определенной универсальностью, может рассматриваться как формализованный метод построения ортогональных латинских квадратов для множеств, удовлетворяющих определенным требованиям.

По аналогии с ортогональными греко - латинскими квадратами могут быть составлены конфигурации, содержащие в себе все возможные пары элементов двух информационных массивов, с которыми встречаемся при решении ряда практических задач в криптографии.

Эта задача к криптографии может быть сформулирована как задача «рассеивания» пар элементов информационных массивов с индексным упорядочением структур с целью обеспечения конфиденциальности содержимого.

Метод может быть использован для решения ряда практических задач, таких как шифрование данных в информационных массивах подстановками и перестановками элементов, борьбы с сосредоточенными ошибками большой кратности «пакетами ошибок», рассеивание их по информационному массиву в виде ошибок малой кратности, построение таких комбинаторных систем как системы различных представительств, числовых магических квадратов, решению таких классических задач комбинаторики, как составление расписаний, календарное планирование и планирование экспериментов и др.

Библиографический список:

1. Виленкин Н.Я. Комбинаторика. - М.: «Наука»,1969г.,328с.
2. Тараканов В.Е., Айгнер М. А. Комбинаторная теория.- М.: Мир,1982, 362с.
3. Холл М. Комбинаторика. / Перевод с английского С.А. Широкова под ред. А.О. Гельфанда А.О.и Тараканова В.Е // М.: Мир,1970г.
4. Стенли Р. Перечислительная комбинаторика М.: Мир, 1990г.
5. Рыбников К.А. Введение в комбинаторный анализ. М.: изд. МГУ, 1994г.
6. http://www. google/ ru. Алгоритмы индексной сортировки массивов данных.
7. Леонтьев В.К. Избранные задачи комбинаторного анализа. - М.: изд-во МГТУ им. Н.Э. Баумана, 2001
8. Волкова В.Н. Теория систем и системный анализ. Учебник / В. Н. Волкова, А. А. Денисов // М.: Юрайт, 2015.615с.
9. Dénes J. H., Keedwell A. D. Latin squares: New developments in the theory and applications. Annals of Discrete Mathematics vol. 46. Academic Press. Amsterdam. 1991.
10. Рыбников К. А. Комбинаторный анализ. Очерки истории. Текст// М.: Изд. Мехмата МГУ, 1996. 124 с.
11. Андерсен Дж.А. Дискретная математика и комбинаторика. Текст //пер. с англ. М.: Вильямс, 2003.
12. Кадиев П.А., Кадиев И.П. Алгоритмы преобразования «классических» матриц в 2-х индексные латинские квадраты. Текст. / П.А Кадиев, И.П. Кадиев, М.З. Зейналов// Вестник Дагестанского государственного технического университета. Технические науки. Т17. 2010. с.93-99
13. Кадиев П.А. Программа преобразования матриц методом латинских квадратов. Текст. / П.А. Кадиев, М.З. Зейналов. // Свидетельство о государственной регистрации программ для ЭВМ №2009616143 от 09.11.2009г.
14. Кадиев И.П. Рассеивание элементов «пакетов ошибок» в информационном массиве методом индексной структуризации. Текст / П.А Кадиев, И.П. Кадиев, Кудаев Р.Б. // Вестник Дагестанского государственного технического университета. Технические науки. Том 46. №4, 2019. с.81-89
15. Кадиев И.П. Система индексной структуризации комбинаторных конфигураций методом рекуррентных функциональных соотношений для защиты передаваемых по каналам связи данных. Текст./ Кадиев И.П., Мелехин В. Б. // ж. Приборы и системы. Управление, контроль, диагностика. № 2 ,2019г. с.37- 43
16. Laywine C. F. and Mullen G. L. Discrete mathematics using Latin squares. New York: Wiley, 1998.
17. Chum C.S. and Zhang X. The Latin squares and the secret sharing schemes // Groups Complex. Cryptol. 2010. V. 2. P. 175-202.

18. Laywine C. F. and Mullen G. L. Discrete mathematics using Latin squares. New York: Wiley, 1998.
19. Глухов М. М. О применениях квазигрупп в криптографии. Статья. // Прикладная дискретная математика. 2008. №2(2). С. 28-32.
20. Малых А.Е Об историческом процессе развития теории латинских квадратов и некоторых их приложениях. Текст/Малых А.Е., Данилова В. И. // Вестник Пермского университета. 2010. Вып. 4(4). С. 95-104.
21. Тришин А.Е. Способ построения ортогональных латинских квадратов на основе подстановочных двучленов конечных полей. Текст.//– М.: ТВП.
22. Тужилин М. Э. Об истории исследований латинских квадратов Текст// Обозрение прикладной и промышленной математики. 2012. Том 19, выпуск 2. С. 226-227.

References:

1. Vilenkin N.YA. Kombinatorika. - M.: «Nauka»,1969g.,328s. [Vilenkin N. Ya. Combinatorics. - M .: "Science", 1969, 328s. (In Russ)]
2. Tarakanov V.Ye., Aygner M. A. Kombinatornaya teoriya.- M.: Mir,1982, 362s. [Tarakanov V.E., Aigner M.A., Combinatorial theory, Moscow: Mir, 1982, 362p. (In Russ)]
3. Kholl M. Kombinatorika. / Perevod s angliyskogo S.A. Shirokova pod red. A.O. Gel'fanda A.O.i Tarakanova V.Ye //.- M.: Mir,1970.[Hall M. Combinatorics. / Translated from English by S.A. Shirokova, ed. A.O. Gelfand A.O. and Tarakanova V.E. // M .: Mir, 1970 (In Russ)]
4. Stenli R. Perechislitel'naya kombinatorika. M.: Mir, 1990. [Stanley R. Enumeration combinatorics - M .: Mir, 1990. (In Russ)]
5. Rybnikov K.A. Vvedeniye v kombinatornyy analiz.- M.: izd. MGU, 1994. [Rybnikov K.A. Introduction to combinatorial analysis. Moscow: ed. Moscow State University, 1994. (In Russ)]
6. http: // www. google / ru. Index sorting algorithms for data arrays.
7. Leont'yev V.K. Izbrannyye zadachi kombinatornogo analiza. - M.: izd-vo MGTU im. N.E. Baumana, 2001 [Leontiev V.K. Selected problems of combinatorial analysis. - M .: publishing house of MSTU im. N.E. Bauman, 2001 (In Russ)]
8. Volkova V.N. Teoriya sistem i sistemnyy analiz. Uchebnik / V. N. Volkova, A. A. Denisov //– M.: Yurayt, 2015.-615s. [Volkova V.N. Systems theory and systems analysis. Textbook / V. N. Volkova, A. A. Denisov // - M .: Yurayt, 2015.-615s. (In Russ)]
9. Dénes J. H., Keedwell A. D. Latin squares: New developments in the theory and applications. Annals of Discrete Mathematics vol. 46. Academic Press. Amsterdam. 1991.
10. Rybnikov K. A. Kombinatornyy analiz. Ocherki istorii. Tekst//— M.: Izd. Mekhmata MGU, 1996. — 124 s. [Rybnikov KA Combinatorial analysis. Essays on history. Text // - M .: Ed. Mehmat Moscow State University, 1996. 124 p. (In Russ)]
11. Andersen J.A. Discrete mathematics and combinatorics. Text // lane. from English - M .: Williams, 2003.
12. Kadiyev P.A., Kadiyev I.P. Algoritmy preobrazovaniya «klassicheskikh» matrits v 2-kh indeksnyye latinskiye kvadraty. Tekst. / P.A Kadiyev, I.P. Kadiyev, M.Z. Zeynalov. // Vestnik Dag. Gos. Tekh. Un-ta, T17. 2010. s.93-99 [Kadiev P.A., Kadiev I.P. Algorithms for transforming "classical" matrices into 2-index Latin squares. Text. / P.A. Kadiev, I.P. Kadiev, M.Z. Zeynalov//Herald of Daghestan State Technical University. Technical Sciences. Vol. 17. 2010. pp.93-99 (In Russ)]
13. Kadiyev P.A. Programma preobrazovaniya matrits metodom latinskikh kvadratov. Tekst. / P.A. Kadiyev, M.Z. Zeynalov. // Svidetel'stvo o gosudarstvennoy registratsii programm dlya EVM №2009616143 ot 09.11.2009g. [Kadiev P.A. A program for converting matrices by the method of Latin squares. Text. / P.A. Kadiev, M.Z. Zeynalov. // Certificate of state registration of computer programs No. 2009616143 dated 09.11.2009. (In Russ)]
14. Kadiyev I.P. Rasseivaniye elementov «paketov oshibok» v informatsionnom massive metodom indeksnoy strukturizatsii. Tekst / P.A Kadiyev, I.P. Kadiyev, Kudayev R.B. // Vestnik DGTU. Tekhnicheskiye nauki. Tom 46. №4, 2019.- s.81-89 [Kadiev I.P. Scattering of "error packets" elements in the information array by the method of index structuring. Text / P.A. Kadiev, I.P. Kadiev, Kudaev R.B. // Herald of Daghestan State Technical University. Technical Sciences. Vol. 46. No4, 2019. pp.81-89 (In Russ)]
15. Kadiyev I.P. Sistema indeksnoy strukturizatsii kombinatornykh konfiguratsiy metodom rekurrentnykh funktsional'nykh sootnosheniy dlya zashchity peredavayemykh po kanalam svyazi dannykh. Tekst./ Kadiyev I.P., Melekhin V.B. // zh. Pribory i sistemy. Upravleniye, kontrol', diagnostika. № 2 ,2019. s.37- 43 [Kadiev I.P. The system of index structuring of combinatorial configurations by the method of recurrent functional relations for the protection of data transmitted over communication channels. Text. / Kadiev I.P., Melekhin V.B. // J. Devices and systems. Management, control, diagnostics. No. 2, 2019 pp. 37-43 (In Russ)]
16. Laywine C. F. and Mullen G. L. Discrete mathematics using Latin squares. New York: Wiley, 1998.
17. Chum C.S. and Zhang X. The Latin squares and the secret sharing schemes // Groups Complex. Cryptol. 2010. Vol. 2. pp. 175-202.
18. Laywine C. F. and Mullen G. L. Discrete mathematics using Latin squares. New York: Wiley, 1998.

19. Glukhov M. M. O primeneniyakh kvazigrupp v kriptografii .Stat'ya. // Prikladnaya diskretnaya matematika. 2008. №2(2). s. 28-32. [Glukhov MM On applications of quasigroups in cryptography. Article. // Applied discrete mathematics. 2008. No. 2 (2). pp. 28-32. (In Russ)]
20. Malykh A.Ye Ob istoricheskom protsesse razvitiya teorii latinskikh kvadratov i nekotorykh ikh prilozheniyakh. Tekst. /. Malykh A.Ye., Danilova V. I. // Vestnik Permskogo universiteta. 2010. Vol. 4(4). S. 95-104. [Malykh AE On the historical development of the theory of Latin squares and some of their applications. Text. /. Malykh A.E., Danilova V.I. // Bulletin of Perm University. 2010. Issue. 4 (4). pp. 95-104. (In Russ)]
21. Trishin A.Ye. Sposob postroyeniya ortogonal'nykh latinskikh kvadratov na osnove podstanovochnykh dvuchlenov konechnykh poley . Tekst.// M.: TVP. [Trishin A.E. A method for constructing orthogonal Latin squares based on substitutional binomials of finite fields. Text // M .: TVP. (In Russ)]
22. Tuzhilin M. E. Ob istorii issledovaniy latinskikh kvadratov Tekst. // Obozreniye prikladnoy i promyshlennoy matematiki. 2012. Tom 19, vypusk 2. S. 226—227. [Tuzhilin M. E. On the history of studies of Latin squares Text.// Review of Applied and Industrial Mathematics. 2012. Vol. 19, Issue 2. pp. 226-227. (In Russ)]

Сведения об авторах:

Кадиев Исламудин Пашаевич, соискатель кафедры управления и информатики в технических системах и вычислительной техники; e-mail:islam-kadi@mail.ru

Кадиев Пашай Абдулгамидович, кандидат технических наук, профессор, кафедра управления и информатики в технических системах и вычислительной техники; e-mail:islam-kadi@mail.ru

Information about the authors:

Islamudin P. Kadiev, Applicant, Department of Management and Informatics in Technical Systems and Computer Engineering; e-mail:islam-kadi@mail.ru

Pashay A. Kadiev, Cand. Sci. (Technical), Assoc. Prof., Department of Management and Informatics in Technical Systems and Computer Engineering; e-mail:islam-kadi@mail.ru

Конфликт интересов.
Авторы заявляют об отсутствии конфликта интересов.
Поступила в редакцию 30.07.2020.
Принята в печать 05.09.2020.

Conflict of interest.
The authors declare no conflict of interest.
Received 30.07.2020.
Accepted for publication 05.09.2020.