Math-Net.Ru

Общероссийский математический портал

В. В. Борисенко, k -распавшиеся и k -однородные латинские квадраты и их трансверсали, *Матем. вопр. криптогр.*, 2020, том 11, выпуск 3, 5–19

DOI: <https://doi.org/10.4213/mvk328>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 34.229.108.108

26 апреля 2023 г., 07:33:32

k -распавшиеся и k -однородные латинские квадраты и их трансверсали

В. В. Борисенко

ООО «Центр сертификационных исследований», Москва

Получено 15.V.2020

Аннотация. Рассматриваются k -распавшиеся латинские квадраты, т.е. латинские квадраты порядка kn , построенные на множестве чисел $\{0, \dots, kn - 1\}$, которые при приведении по модулю n дают $(kn \times kn)$ -матрицу, состоящую из k^2 латинских квадратов порядка n . Если эти k^2 латинских квадратов одинаковы, то исходный квадрат называется k -однородным. Найдены точное число k -однородных латинских квадратов и нижняя оценка для числа k -распавшихся латинских квадратов. Изучены некоторые свойства трансверсалей k -однородных латинских квадратов.

Ключевые слова: латинский квадрат, трансверсаль, ориентированный граф

k -splitted and k -homogeneous Latin squares and their transversals

V. V. Borisenko

LLC «Sertification Research Center», Moscow

Abstract. We consider the k -splitted Latin squares, i.e. Latin squares of order kn with elements from $\{0, \dots, kn - 1\}$ such that after reducing modulo n we obtain $(kn \times kn)$ -matrix consisting of k^2 Latin squares of order n . If these k^2 Latin squares of order n are identical, the original Latin square of order kn is called k -homogeneous. The precise number of all k -homogeneous and lower bound for the number of all k -splitted Latin squares are found. Some characteristics of transversals for k -splitted Latin squares are described.

Keywords: Latin square, transversal, directed graph

1. Введение

В данной работе, являющейся продолжением работ автора [5–7], рассматривается задача описания *k-распавшихся* (*k-однородных*) латинских квадратов и множеств их трансверсалей. Необходимые понятия, относящиеся к латинским квадратам (для краткости далее – ЛК), можно найти в учебнике [1] и книге [2], а понятия и обозначения для распавшихся ЛК – в [5]. Здесь они не приводятся, чтобы не повторять несколько страниц текста. Некоторые понятия и определения, не являющиеся общеизвестными, в дальнейшем изложении будут воспроизводиться по мере необходимости. Далее множество всех целых чисел, начиная с числа m и заканчивая числом n , будем обозначать $[m, n] = \{a \in \mathbb{Z} \mid m \leq a \leq n\} = \{m, m+1, \dots, n\}$.

Описание множеств всех трансверсалей латинских квадратов, относящихся к тем или иным классам, является актуальной задачей в теории латинских квадратов. Это в первую очередь связано с задачей о построении квадратов, ортогональных к заданному латинскому квадрату, и более общо – задачей о построении максимальных систем ортогональных латинских квадратов (СОЛК), которым принадлежит заданный квадрат. Обзор дальнейших результатов и литературы по трансверсальям и их возможным обобщениям дан в [9–13].

В работах автора [5–7] введены классы *распавшихся* и *однородных* латинских квадратов, а именно: распавшимся квадратом порядка $2n$ называется латинский квадрат, построенный на множестве чисел $[0, 2n-1]$, который при приведении по модулю n дает $2n \times 2n$ -матрицу, состоящую из четырех латинских квадратов порядка n на множестве чисел $[0, n-1]$; распавшийся квадрат называется однородным, если эти четыре латинских квадрата одинаковы. В указанных работах автора дано общее описание множеств трансверсалей распавшихся и однородных латинских квадратов.

Следует отметить, что ранее в [14] были рассмотрены частные случаи однородных латинских квадратов порядка $2n$, это так называемые *turn-squares*, получаемые из таблицы Кэли группы $\mathbb{Z}_2 \oplus \mathbb{Z}_n$ заменой символов, находящихся в четырех специально выбираемых латинских подквадратах порядка 2 (см. обзор [11] и учебник [4] в части теории групп).

2. *k*-однородные и *k*-распавшиеся латинские квадраты порядка kn , существование и оценка их числа

В [5] были введены следующие определения распавшегося и однородного ЛК порядка $2n$.

Определение. ЛК $F = (f_{ij})_{2n \times 2n}$ порядка $2n$ на множестве $[0, 2n - 1]$ называется *распавшимся*, если после приведения его элементов по модулю n из него получается матрица $G = \begin{pmatrix} A & C \\ B & D \end{pmatrix} = (g_{ij})_{2n \times 2n}$, в которой подматрицы A, B, C, D являются латинскими квадратами порядка n . Если $A = B = C = D$, то ЛК F называется *однородным*.

Введем следующее определение *k*-распавшихся и *k*-однородных ЛК порядка kn .

Определение. ЛК $F = (f_{ij})_{kn \times kn}$ порядка kn на множестве $[0, kn - 1]$ называется *k-распавшимся*, если после приведения его элементов по модулю n из него получается матрица

$$G = (g_{ij})_{kn \times kn} = \begin{pmatrix} A_{11} & \cdots & A_{1k} \\ \vdots & \ddots & \vdots \\ A_{k1} & \cdots & A_{kk} \end{pmatrix}_{kn \times kn},$$

в которой каждая из подматриц A_{ij} , $i, j \in [1, k]$, является латинским квадратом порядка n на множестве $[0, n - 1]$. Если все эти подматрицы одинаковы: $A = A_{ij}$, $i, j \in [1, k]$, то ЛК F называется *k-однородным*.

Ответ на вопрос о существовании и числе *k*-однородных ЛК порядка kn , которые после приведения всех их элементов по модулю n превращаются в заданную матрицу G указанного в определении вида, дает следующее утверждение.

Утверждение 1. Пусть в матрице

$$G = (g_{ij})_{kn \times kn} = \begin{pmatrix} A_{11} & \cdots & A_{1k} \\ \vdots & \ddots & \vdots \\ A_{k1} & \cdots & A_{kk} \end{pmatrix}_{kn \times kn}$$

все подматрицы A_{ij} , $i, j \in [1, k]$, являются одинаковыми латинскими квадратами порядка n на множестве $[0, n - 1]$, совпадающими с заданным ЛК $A_{n \times n}$. Обозначим через $N(k)$ число различных ЛК порядка k .

Тогда существует ровно $N(k)^{n^2}$ различных k -однородных ЛК порядка kn , которые после приведения их элементов по модулю n дают матрицу G .

Доказательство. Заметим, что доказательство данного утверждения основано на использовании одного ЛК порядка n , а именно $A_{n \times n}$ и упорядоченного набора из n^2 ЛК (произвольных и не обязательно различных) порядка k для построения нового ЛК порядка nk .

Рассмотрим матрицу $G = (g_{ij})_{kn \times kn}$ указанного в формулировке утверждения вида и произвольный ее элемент a_{st} , $s, t \in [1, n]$, находящийся в подматрице A_{11} . Будем говорить, что элемент $g_{s+(i-1)n, t+(j-1)n}$, $i, j \in [1, k]$, находящийся в подматрице A_{ij} , соответствует элементу a_{st} . Все элементы матрицы G , соответствующие элементу a_{st} , образуют $k \times k$ -подматрицу в G , содержащую k^2 одинаковых чисел, равных числу a_{st} в силу того, что по условию все латинские квадраты порядка n совпадают. Рассмотрим произвольный набор из n^2 ЛК порядка k , составленных из чисел $[0, k-1] : \left\{ B^{(s,t)} = \left(b_{ij}^{(s,t)} \right) \middle| i, j \in [1, k], s, t \in [1, n] \right\}$. В матрице G каждое число

$$g_{s+(i-1)n, t+(j-1)n} = a_{st}, \quad s, t \in [1, n], \quad i, j \in [1, k],$$

заменяем числом $a_{st} + n \cdot b_{ij}^{(s,t)}$. Легко показать, что получится матрица $F_{kn \times kn} = \left(f_{s+(i-1)n, t+(j-1)n} = a_{st} + n \cdot b_{ij}^{(s,t)} \right)_{kn \times kn}$, являющаяся ЛК порядка kn на множестве $[0, kn-1]$. Действительно, числа a_{st} и $b_{ij}^{(s,t)}$ удовлетворяют условиям: $a_{st} \in [0, n-1]$, $b_{ij}^{(s,t)} \in [0, k-1]$, поэтому $f_{s+(i-1)n, t+(j-1)n} \in [0, kn-1]$. При приведении элементов матрицы F по модулю n , очевидно, получается матрица G . Если теперь числа f_{lm} и f_{lv} лежат в одной строке матрицы F , то возможны два варианта. Элементы g_{lm} и g_{lv} соответствуют друг другу, т. е. $g_{lm} = g_{lv} = a_{st}$. Но тогда при получении из них элементов f_{lm} и f_{lv} к числу a_{st} будут прибавлены два разных числа $n \cdot b_{ij}^{(s,t)} \neq n \cdot b_{ij'}^{(s,t)}$, поскольку $b_{ij}^{(s,t)} \neq b_{ij'}^{(s,t)}$ — два разных элемента, стоящих в ЛК $B^{(s,t)}$ в одной строке, т. е. $f_{lm} \neq f_{lv}$. Если элементы g_{lm} и g_{lv} не являются соответствующими друг другу, то $g_{lm} \neq g_{lv}$, так как они равны двум различным элементам в одной и той же строке ЛК $A_{n \times n}$ и тогда тем более $f_{lm} \neq f_{lv}$, поскольку f_{lm} и f_{lv} при делении на n дают разные остатки $g_{lm} \neq g_{lv}$. Аналогичные рассуждения проводятся для элементов f_{vm} и f_{lm} , стоящих в матрице F в одном столбце. Таким образом, доказано, что, отталкиваясь от любой

матрицы $G = (g_{ij})_{kn \times kn}$ указанного в условии вида, можно построить соответствующий ей k -однородный ЛК порядка kn .

Очевидно, что для различных наборов ЛК порядка k вида $\left\{ B^{(s,t)} = (b_{ij}^{(s,t)})_{k \times k} \mid i, j \in [1, k], s, t \in [1, n] \right\}$ получаются различные ЛК F . Осталось проверить, что любой k -однородный ЛК F порядка kn , после приведения его элементов по модулю n превращающийся в матрицу G , может быть построен рассмотренным способом. Пусть при приведении по модулю n ЛК F превращается в матрицу G указанного в условии вида. Рассмотрим в матрице G подматрицу D порядка k , состоящую из всех элементов, соответствующих какому-то элементу $a_{st} \in [0, n-1]$, $s, t \in [1, n]$, из подматрицы A_{11} . Тогда элементы D все равны между собой и равны числу a_{st} . Рассмотрим в матрице F подматрицу H порядка k , стоящую на тех же местах, что и матрица D в G . Тогда по условию в каждой строке и в каждом столбце матрицы H стоит ровно k различных элементов из множества $[0, kn-1]$. При приведении по модулю n из H получается G , все элементы которой одинаковы и равны числу a_{st} . Поэтому для разности матриц $H - G$ верны следующие факты: все элементы $H - G$ делятся на n и в каждой строке, и в каждом столбце матрицы $H - G$ стоит ровно k различных элементов из множества $[0, kn-1]$. Поэтому матрица $1/n (H - G) = B^{(s,t)}$ является ЛК порядка k на множестве чисел $[0, k-1]$. Теперь ясно, что ЛК F получен из матрицы G с помощью описанной в начале доказательства конструкции. Из изложенного ясно, что, отталкиваясь от фиксированной матрицы G , можно получить всего $N(k)^{n^2}$ различных k -однородных ЛК порядка kn . $\square$

Замечание. Рассмотренная в доказательстве утверждения 1 конструкция построения k -однородных ЛК является частным случаем конструкции w -сплетения t -квазигрупп, введенной автором статьи в 1979 г. при построении неприводимых t -квазигрупп составного порядка [8]. Рассмотрим это понятие и его связь с k -однородными ЛК. Допуская вольность речи, не будем различать понятия t -квазигруппы и t -квазигрупповой операции.

Определение. Пусть A и B — два непустых множества, $t \in \mathbb{N}$ — натуральное число, $f : A^t \rightarrow A$ — произвольная t -квазигруппа на A , $Q_t[B]$ — множество всех t -квазигрупп на B и $w : A^t \rightarrow Q_t[B]$ — произвольное отображение; в этом случае w -сплетением t -квазигруппы f

называется отображение

$$f^{(w)} : (A \times B)^t \rightarrow A \times B,$$

для которого

$$f^{(w)}((a_1, b_1), \dots, (a_t, b_t)) = (f(a_1, \dots, a_t), w(a_1, \dots, a_t)(b_1, \dots, b_t)).$$

Легко показать, что $f^{(w)} \in Q_t[A \times B]$ является t -квазигруппой на множестве $A \times B$ и рассмотренная в доказательстве утверждения 1 конструкция является частным случаем w -сплетения бинарных ($t = 2$) квазигрупп, при этом $A = [0, n - 1]$, $B = [0, k - 1]$. Данное замечание показывает, что понятие k -однородных латинских квадратов обобщается на квазигруппы арности больше двух.

Рассмотрим теперь случай k -распавшегося ЛК F на множестве чисел $[0, kn - 1]$, который после приведения всех его элементов по модулю n дает указанную в определении матрицу G . Следующее утверждение решает вопрос о существовании k -распавшихся ЛК и нижней оценке для их числа.

Утверждение 2. Пусть в матрице

$$G = (g_{ij})_{kn \times kn} = \begin{pmatrix} A_{11} & \cdots & A_{1k} \\ \vdots & \ddots & \vdots \\ A_{k1} & \cdots & A_{kk} \end{pmatrix}_{kn \times kn}$$

все подматрицы A_{ij} , $i, j \in [1, k]$, являются латинскими квадратами порядка n на множестве $[0, n - 1]$. Пусть, как и раньше, $N(k)$ — число различных ЛК порядка k . Тогда существует по крайней мере $N(k)^n$ различных k -распавшихся ЛК порядка kn , которые после приведения их элементов по модулю n дают матрицу G .

Доказательство. Пусть $a \in [0, n - 1]$ — произвольное число и $\delta_a^{(i,j)} = \{(s, t) \in [1, n]^2 \mid (A_{ij})_{s,t} = a\}$, $i, j \in [1, k]$, — множество позиций в ЛК (подматрице) A_{ij} , на которых стоит элемент a . Относительно позиционирования элементов подматриц см. [4, с. 101, определение 7]. Напомним, что в теории латинских квадратов такое множество позиций называется *диагональю ЛК A_{ij} , отвечающей элементу a* , и это множество имеет ровно один элемент в каждой строке и в каждом столбце ЛК A_{ij} . Пусть теперь задан произвольный набор $(B^{(1)}, \dots, B^{(n)})$ латинских квадратов порядка k на множестве $[0, k - 1]$. Если элемент g_{lm}

матрицы G находится в клетке A_{ij} и принадлежит диагонали $\delta_a^{(i,j)}$, $a \in [0, n-1]$, этого ЛК, то положим $f_{lm} = a + n \cdot b_{ij}^{(a+1)}$. Тогда очевидно, что в матрице $F = (f_{lm})_{kn \times kn}$ все элементы являются числами из множества $[0, kn-1]$, и при приведении всех элементов этой матрицы по модулю n получается матрица G . Пусть теперь элементы f_{lm} и f_{lv} находятся в матрице F в одной строке на несовпадающих местах, $m \neq v$. Рассмотрим стоящие на тех же местах элементы g_{lm} и g_{lv} матрицы G . Они содержатся в клетках A_{ij} и $A_{ij'}$ этой матрицы с одинаковым первым номером i (эти клетки могут и совпадать!). Тогда возможны два варианта. Первый вариант: $g_{lm} = g_{lv} = a \in [0, n-1]$. В этом случае, поскольку клетки являются латинскими квадратами, $j \neq j'$ и тогда

$$f_{lm} = a + n \cdot b_{ij}^{(a+1)} \neq f_{lv} = a + n \cdot b_{ij'}^{(a+1)},$$

так как $B^{(a+1)}$ является латинским квадратом и в нем $b_{ij}^{(a+1)} \neq b_{ij'}^{(a+1)}$. Второй вариант состоит в том, что $g_{lm} \neq g_{lv}$, тогда, очевидно, и $f_{lm} \neq f_{lv}$. Таким образом, доказано, что построенная матрица F является k -распавшимся ЛК порядка kn , дающим при приведении всех его элементов по модулю n наперед заданную матрицу G , клетки которой являются латинскими квадратами порядка n . Из построения следует, что число таких k -распавшихся ЛК не меньше, чем $N(k)^n$, поскольку различные наборы $(B^{(1)}, \dots, B^{(n)})$ дают разные ЛК. $\square$

В утверждении 2 установлено существование k -распавшихся ЛК и получена общая нижняя оценка их числа для любого задания матрицы G . В следующем утверждении будет получена нижняя оценка числа k -распавшихся ЛК для любой конкретной матрицы G , которая в общем случае может улучшать оценку утверждения 2, поскольку в получаемой нижней оценке будет учтена специфика этой конкретной матрицы G . Таким образом, оценка утверждения 2 является глобальной, верной для всех матриц G , в то время как оценка утверждения 3 является локальной для каждой конкретной матрицы.

Сопоставим матрице G обыкновенный неориентированный граф $\Gamma = \{V, E\}$ с множеством вершин V и ребер E следующим образом. Каждой подматрице A_{ij} поставим в соответствие вершину v_{ij} , $V = \{v_{ij} | i, j \in [1, k]\}$, две вершины v_{ij} , $v_{i'j'}$ соединены ребром, если подматрицы A_{ij} , $A_{i'j'}$ являются смежными в G , т.е. стоят рядом по горизонтали или вертикали. Таким образом, граф Γ представляет собой плоскую $k \times k$ решетку.

Рассмотрим множество всех циклов $\{\Delta\}$ (т.е. замкнутых маршру-

тов без повторения ребер), проходящих через вершину v_{11} . Каждому циклу Δ сопоставим подстановку χ_Δ на множестве $[1, n]^2$, которое интерпретируется как множество позиций в матрице A_{11} , следующим образом. Выберем произвольную позицию $(s, t) \in [1, n]^2$ в A_{11} , пусть $a_{s,t}^{(1,1)} = a \in [0, n-1]$ — элемент матрицы A_{11} на этой позиции. Перейдем от элемента $a_{s,t}^{(1,1)} = a$ по циклу Δ в соседнюю подматрицу вдоль той же строки или того же столбца, в котором стоит $a_{s,t}^{(1,1)}$, и найдем в соседней подматрице в той же строке (том же столбце) элемент, равный a . Затем от этого элемента по циклу Δ переходим в следующую соседнюю подматрицу по строке или столбцу, находим в этой строке или в этом столбце элемент, равный a , и так, пройдя весь цикл Δ , возвращаемся в подматрицу A_{11} и находим там элемент $a_{p,q}^{(1,1)} = a$. Полагаем $\chi_\Delta(s, t) = (p, q)$. Прделав эту процедуру для всех позиций $(s, t) \in [1, n]^2$, получаем подстановку χ_Δ . Перебрав все циклы $\{\Delta\}$, получим соответствующее им множество подстановок $\{\chi_\Delta\}$.

Очевидно, что любая диагональ ЛК A_{11} (т.е. множество позиций в A_{11} , содержащих фиксированный элемент $a \in [0, n-1]$) является блоком для любой подстановки χ_Δ , и поэтому для каждой из этих подстановок циклами будут являться некоторые подмножества диагоналей. Определим отношение эквивалентности ρ_G на множестве $[1, n]^2$ как транзитивное замыкание отношения «принадлежать одному циклу для некоторой подстановки χ_Δ ». Тогда все множество позиций $[1, n]^2$ разбивается на некоторое число $\tau(G)$ классов этой эквивалентности, причем в силу предыдущих рассуждений классы являются подмножествами в n диагоналях ЛК A_{11} . Поэтому верны неравенства $n \leq \tau(G) \leq n^2$. Заметим, что в частном случае k -однородного ЛК все подстановки χ_Δ являются тождественными и для этого случая $\tau(G) = n^2$.

Замечание. При практическом построении отношения ρ_G достаточно использовать не все множество циклов $\{\Delta\}$ графа Γ , которые начинаются и заканчиваются в вершине v_{11} , а ограничиться рассмотрением только $2k-2$ циклов: $k-1$ циклов проходят соответственно первую и вторую, первую и третью, ..., первую и k -ю строки и $k-1$ циклов проходят соответственно первый и второй, первый и третий, ..., первый и k -й столбцы графа-решетки Γ .

Утверждение 3. Пусть

$$G = (g_{ij})_{kn \times kn} = \begin{pmatrix} A_{11} & \cdots & A_{1k} \\ \vdots & \ddots & \vdots \\ A_{k1} & \cdots & A_{kk} \end{pmatrix}_{kn \times kn}$$

— матрица, в которой подматрицы $A = A_{ij}$, $i, j \in [1, k]$, являются латинскими квадратами порядка n на множестве $[0, n - 1]$. Пусть, как и раньше, $N(k)$ — число различных ЛК порядка k . Тогда существует по крайней мере $N(k)^{\tau(G)}$ различных k -распавшихся ЛК порядка kn , которые после приведения их элементов по модулю n дают матрицу G . Здесь $n \leq \tau(G) \leq n^2$, $\tau(G)$ — число классов эквивалентности ρ_G на множестве $[1, n]^2$ позиций ЛК A_{11} .

Доказательство. Занумеруем классы эквивалентности ρ_G числами $[1, \tau(G)]$ и пометим этими числами элементы множества позиций $[1, n]^2$: каждая позиция (s, t) получает номер того класса, которому она принадлежит. Для каждой подстановки χ_Δ назовем *маршрутом перехода* $\chi_\Delta(s, t) = (p, q)$ подстановки χ_Δ упорядоченный набор позиций в матрице G , которые были последовательно пройдены от (s, t) до (p, q) в рассмотренном выше процессе построения χ_Δ . Присвоим каждой позиции из маршрута перехода метку начальной позиции (s, t) . Прделаем это для всех переходов всех подстановок $\{\chi_\Delta\}$. Тогда каждая позиция в матрице G получит ровно одну метку из множества $[1, \tau(G)]$. При этом будет, очевидно, выполняться следующее свойство: если $g_{lm} = g_{lv} = a \in [0, n - 1]$ — одинаковые элементы в одной строке G или $g_{ml} = g_{vl} = a \in [0, n - 1]$ — одинаковые элементы в одном столбце G , то и их метки одинаковы.

Пусть теперь $(B^{(1)}, \dots, B^{(\tau(G))})$, $B^{(\mu)} = (b_{ij}^\mu)_{k \times k}$ — произвольный упорядоченный набор ЛК порядка k на множестве $[0, k - 1]$. Заменим в матрице G каждый элемент $g_{lm} = a \in [0, n - 1]$ элементом $f_{lm} = g_{lm} + n \cdot b_{ij}^{\mu(l, m)}$, где $\mu(l, m)$ — метка, присвоенная позиции (l, m) , а (i, j) — индекс подматрицы A_{ij} , в которой находится элемент g_{lm} матрицы G . Тогда $F = (f_{lm})$ является k -распавшимся ЛК порядка nk , после приведения элементов которого по модулю n получается матрица G . Действительно, если f_{lm} и f_{lv} — два элемента матрицы F , стоящие в одной строке, то возможны два случая. Если соответствующие им элементы $g_{lm} \neq g_{lv}$ не равны, то и $f_{lm} \neq f_{lv}$. Если $g_{lm} = g_{lv} = a \in [0, n - 1]$, то, как указано выше, $\mu(l, m) = \mu(l, v)$ и $f_{lm} = a + n \cdot B_{ij}^{\mu(l, m)} \neq a + n \cdot B_{ij'}^{\mu(l, v)} = f_{lv}$, поскольку элементы

$g_{ml} = g_{vl} = a \in [0, n-1]$ лежат в разных подматрицах A_{ij} и $A_{ij'}$, $j \neq j'$, и в силу этого $B_{ij}^{\mu(l,m)} \neq B_{ij'}^{\mu(l,v)}$ — два элемента в одной строке ЛК $B^{(\mu(l,m))} = B^{(\mu(l,v))}$. Аналогично доказывается, что элементы, лежащие в одном столбце матрицы F , различны. Теперь, поскольку разные наборы $(B^{(1)}, \dots, B^{(\tau(G))})$ порождают различные K -распавшиеся ЛК, верна указанная в формулировке утверждения оценка для их числа. $\square$

3. О трансверсалиях в k -однородных латинских квадратах порядка kn

Напомним понятия из теории латинских квадратов, которые используются в данном разделе.

Пусть $A_{n \times n} = (a_{ij})_{n \times n}$ — ЛК порядка n на множестве $[0, n-1]$ и $\lambda \subset [1, n]^2$ — произвольное подмножество, которое будет рассматриваться как *множество позиций ЛК A* . Через $A_\lambda = \{a_{ij} \mid (i, j) \in \lambda\} \subset [0, n-1]$ обозначим множество всех элементов ЛК A , встречающихся на позициях λ . Множество позиций вида $\rho(i) = \{(i, j) \mid j \in [1, n]\}$, $i \in [1, n]$, называется *i -й строкой*, а $\kappa(j) = \{(i, j) \mid i \in [1, n]\}$, $j \in [1, n]$, — *j -м столбцом ЛК A* . Множество позиций $\sigma \in [1, n]^2$ называется *подстановкой в ЛК A* , если оно имеет ровно один общий элемент с каждой строкой и каждым столбцом ЛК A . *Диагональю ЛК A , соответствующей элементу $a \in [0, n-1]$* , называется множество позиций, которые занимает этот элемент: $\delta_a = \{(i, j) \in [1, n]^2 \mid a_{ij} = a\}$. Очевидно, что для любого $a \in [0, n-1]$ его диагональ δ_a является подстановкой в ЛК A , и объединение $[1, n]^2 = \bigcup_{a=0}^{n-1} \delta_a$ является разбиением множества $[1, n]^2$.

Для $s \in [1, n]$ множество позиций $\tau \subset [1, n]^2$ называется *s -трансверсалью в ЛК A* , если оно имеет ровно s общих элементов с каждой строкой и каждым столбцом, и если любое число $a \in [0, n-1]$ встречается на позициях τ ровно s раз: $|\{(i, j) \in \tau \mid a_{ij} = a\}| = s$ (см. [10]). В частном случае, когда $s = 1$, получаем определение *трансверсали* $\tau \subset [1, n]^2$ — это такая подстановка в ЛК A , для которой $A_\tau = [0, n-1]$. Множество всех s -трансверсалей ЛК A обозначается $\text{Tr}_s(A)$, множество всех трансверсалей — $\text{Tr}(A)$.

Рассмотрим матрицу

$$G = (g_{lm})_{kn \times kn} = \begin{pmatrix} A_{11} & \cdots & A_{1k} \\ \vdots & \ddots & \vdots \\ A_{k1} & \cdots & A_{kk} \end{pmatrix}_{kn \times kn},$$

в которой подматрицы $A_{ij} = A$, $i, j \in [1, k]$, все одинаковы и совпадают с ЛК $A_{n \times n} = (a_{ij})_{n \times n}$ порядка n с элементами $[0, n - 1]$. Пусть $(l, m) \in [1, kn]^2$ — произвольная позиция в матрице G . Тогда ее можно однозначно записать в виде $(l, m) = (s + (i - 1)n, t + (j - 1)n)$, где $(s, t) \in [1, n]^2$, $(i, j) \in [1, k]^2$, причем (i, j) — это номер подматрицы A_{ij} , в которой лежит элемент g_{lm} . Тогда можно определить проекцию позиции (l, m) в подматрицу A_{11} , результатом которой является позиция $(s, t) \in [1, n]^2$ в этой подматрице: $\text{pr}(l, m) = (s, t)$. При этом по построению матрицы G получаем равенство $g_{lm} = g_{st} = a_{st}$. Если теперь $\lambda \subset [1, kn]^2$ — некоторое множество позиций матрицы G , то естественным образом определяется его проекция $\text{pr}(\lambda)$ на A_{11} , которую будем рассматривать как *мультимножество с порождающим множеством* $[1, n]^2$, носителем которого является множество $\overline{\text{pr}}(\lambda) = \{\text{pr}(l, m) \mid (l, m) \in \lambda\}$, а кратность $a(s, t)$ каждого элемента $(s, t) \in [1, n]^2$ этого мультимножества определяется числом «попаданий» в него при проецировании: $a(s, t) = |\{(l, m) \in \lambda \mid \text{pr}(l, m) = (s, t)\}|$ (терминологию см. [3, с. 20]).

В работах [5–7] для изучения трансверсалей в 2-распавшихся и 2-однородных ЛК рассматривались их проекции на подматрицу A_{11} . В частности, в [5, 6] было доказано, что для 2-однородных ЛК проекциями трансверсалей являются только 2-трансверсали ЛК A_{11} , причем в каждую 2-трансверсаль проецируется одно и то же число трансверсалей большого квадрата. Оказалось, что в случае *k*-однородных ЛК порядка kn прямое обобщение указанного факта места не имеет.

Свойства трансверсалей в произвольных *k*-однородных латинских квадратах представлены в следующем утверждении.

Утверждение 4. Пусть F — однородный ЛК порядка kn с матрицей

$$G = (g_{ij})_{kn \times kn} = \begin{pmatrix} A_{11} & \cdots & A_{1k} \\ \vdots & \ddots & \vdots \\ A_{k1} & \cdots & A_{kk} \end{pmatrix}_{kn \times kn}, \text{ в которой подматрицы}$$

$A = A_{ij}$, $i, j \in [1, k]$, являются одинаковыми латинскими квадратами порядка n на множестве $[0, n - 1]$, совпадающими с ЛК $A_{n \times n}$. Тогда для произвольной трансверсали $\tau \in \text{Tr}(F)$ ЛК F имеют место следующие свойства.

1. Проекция $\text{pr}(\tau)$ является *k*-сбалансированным мультимножеством позиций в ЛК A в том смысле, что каждый элемент $a \in [0, n - 1]$ встречается на позициях $\text{pr}(\tau)$ ровно k раз (с учетом кратностей позиций в этом мультимножестве).

2. Если проекция $\text{pr}(\tau)$ является k -сбалансированным мультимножеством, то $\text{pr}(\tau) \subset [1, n]^2$ — k -трансверсаль ЛК A .
3. Если носитель $\overline{\text{pr}}(\tau)$ проекции $\text{pr}(\tau)$ является n -множеством, то $\overline{\text{pr}}(\tau)$ — трансверсаль в ЛК A .

Доказательство. Свойство 1 очевидным образом вытекает из определений, сделанных перед утверждением.

Свойство 2. Поскольку на позициях трансверсали τ в ЛК F стоят все числа $[0, kn - 1]$ ровно по одному разу, то на позициях $\text{pr}(\tau)$ стоят все числа, являющиеся результатом приведения чисел $[0, kn - 1]$ по модулю n , т.е. все числа $[0, n - 1]$, причем каждое по k раз. Далее, трансверсаль τ является подстановкой в ЛК F , т.е. каждая строка и каждый столбец этого ЛК содержат ровно один элемент из τ . По условию свойства 2 отображение проецирования pr является биекцией из τ в $\text{pr}(\tau)$, поэтому в каждой строке и в каждом столбце ЛК A имеется ровно k элементов множества $\text{pr}(\tau)$. Таким образом, $\text{pr}(\tau)$ является k -трансверсалью в ЛК A .

Свойство 3. Поскольку каждая строка и каждый столбец этого ЛК содержит ровно один элемент из трансверсали τ , то элементы носителя проекции $\overline{\text{pr}}(\tau)$ должны присутствовать в каждой строке и в каждом столбце ЛК A . Но мощность $|\overline{\text{pr}}(\tau)| = n$, следовательно, $\overline{\text{pr}}(\tau)$ — подстановка в ЛК A . Далее, на позициях $\overline{\text{pr}}(\tau)$ стоят результаты приведения по модулю n всех чисел из множества $[0, kn - 1]$, т.е. числа $[0, n - 1]$, и поэтому $\overline{\text{pr}}(\tau)$ — трансверсаль в ЛК A . $\square$

Как уже было сказано, в случае 2-однородных ЛК реализуется только случай 2, причем другие варианты для проекций трансверсалей невозможны.

В следующем утверждении описывается общая конструкция, позволяющая реализовать случай 3 при $k \geq 3$.

Утверждение 5. Пусть $3 \leq n \leq k$ — натуральные числа. Тогда существуют такие k -однородный ЛК F порядка nk на множестве $[0, nk - 1]$ и трансверсаль $t \in \text{Tr}(F)$ этого ЛК, что носитель $\overline{\text{pr}}(\tau)$ проекции $\text{pr}(\tau)$ является n -множеством.

Доказательство. Пусть $A_{n \times n} = (a_{ij})_{n \times n}$ — такой ЛК порядка n на множестве $[0, n - 1]$, что в нем существует трансверсаль $\lambda \in \text{Tr}(A)$.

Известно, что при $n \geq 3$ такие ЛК существуют. Построим матрицу

$$G = (g_{ij})_{kn \times kn} = \begin{pmatrix} A_{11} & \cdots & A_{1k} \\ \vdots & \ddots & \vdots \\ A_{k1} & \cdots & A_{kk} \end{pmatrix}_{kn \times kn},$$

в которой подматрицы $A_{ij} = A$, $i, j \in [1, k]$, являются одинаковыми латинскими квадратами порядка n на множестве $[0, n-1]$, совпадающими с ЛК $A_{n \times n}$. Поскольку $3 \leq n \leq k$, существует набор $(\sigma_1, \dots, \sigma_n)$ попарно противоречивых подстановок степени k (см. [3, с. 195]). Установим произвольную биекцию $\varphi : \lambda \rightarrow (\sigma_1, \dots, \sigma_n)$. Теперь рассмотрим набор из n^2 ЛК порядка k , составленных из чисел $[0, k-1]$: $\left\{ B^{(s,t)} = \left(b_{ij}^{(s,t)} \right)_{k \times k} \middle| s, t \in [1, n] \right\}$, в котором для n квадратов выполнено следующее свойство: ЛК $B^{(s,t)}$ при любой $(s, t) \in \lambda$ имеет трансверсаль $\varphi(s, t)$. Остальные $n^2 - n$ ЛК в этом наборе могут быть любыми. Очевидно, что набор из n штук ЛК с указанным свойством может быть построен, например, следующим способом. Возьмем произвольный ЛК B порядка k на множестве $[0, k-1]$, содержащий трансверсаль. Тогда подходящей перестановкой строк и столбцов ЛК B можно получить ЛК B' , в котором трансверсалью будет любая наперед заданная подстановка σ степени k . Построим k -однородный ЛК F с помощью матрицы G и набора $\left\{ B^{(s,t)} = \left(b_{ij}^{(s,t)} \right)_{k \times k} \middle| s, t \in [1, n] \right\}$, как это было сделано в утверждении 1. Рассмотрим произвольную позицию $(s, t) \in \lambda$ и порождаемые ею элементы в ЛК F . Это будут k^2 элементов вида $f_{s+n(i-1), t+n(j-1)} = a_{st} + n \cdot b_{ij}^{(s,t)}$, $i, j \in [1, k]$. Среди них есть k элементов, для которых позиции $(i, j) \in \sigma_u = \varphi(s, t)$ принадлежат трансверсали $\sigma_u = \varphi(s, t)$, поэтому все значения $a_{st} + n \cdot b_{ij}^{(s,t)}$, $(i, j) \in \sigma_u$, различны и сравнимы с a_{st} по модулю n . Сбрав вместе все такие значения по всем $(s, t) \in \lambda$, получим числа $[0, nk-1]$, каждое по одному разу, поскольку λ — трансверсаль в ЛК A . В силу того что $(\sigma_1, \dots, \sigma_n)$ — попарно противоречивые подстановки, позиции, на которых стоят эти значения, образуют подстановку τ в ЛК F . Таким образом, τ — трансверсаль в F . Из построения очевидно, что она проецируется на λ .

□

4. Результаты подсчетов числа трансверсалей для отдельных классов распавшихся латинских квадратов

В заключение данной статьи приводятся все возможные значения числа трансверсалей в 2-распавшихся ЛК порядка 10 с тождественной подстановкой χ_{ACDB} и удовлетворяющих следствию утверждения 9 из работы автора [7], т. е. таких, для которых число трансверсалей вычисляется по соответствующему этому ЛК кодовому слову $(\kappa_1, \dots, \kappa_N)^t$ по формуле $\sum_{i=1}^N \kappa_i w_i$.

Всего, как указано в упомянутых выше утверждении и следствии, из общего числа 4157 наборов ЛК (A, B, C, D) с тождественной подстановкой $\chi_{ACDB} = \text{id}_{[1,n]^2}$ этим условиям удовлетворяют 168 наборов. Для каждого из этих наборов был построен соответствующий ему трансверсальный код, найден весовой спектр этого кода, и по указанной выше формуле вычислены все возможные значения для чисел трансверсалей соответствующих латинских квадратов. Результат представлен в приложении. Следует отметить имеющуюся в последовательности чисел закономерность: все эти числа кратны 8 и, начиная с числа $68 \times 8 = 544$ и заканчивая числом $153 \times 8 = 1224$, они образуют арифметическую прогрессию с разностью 8.

Приложение

Возможные значения числа трансверсалей в 2-распавшихся ЛК порядка 10

{ 0, 144, 160, 192, 224, 240, 256, 288, 320, 336, 384, 416, 432, 448, 480, 496, 512, 528, 544, 552, 560, 568, 576, 584, 592, 600, 608, 616, 624, 632, 640, 648, 656, 664, 672, 680, 688, 696, 704, 712, 720, 728, 736, 744, 752, 760, 768, 776, 784, 792, 800, 808, 816, 824, 832, 840, 848, 856, 864, 872, 880, 888, 896, 904, 912, 920, 928, 936, 944, 952, 960, 968, 976, 984, 992, 1000, 1008, 1016, 1024, 1032, 1040, 1048, 1056, 1064, 1072, 1080, 1088, 1096, 1104, 1112, 1120, 1128, 1136, 1144, 1152, 1160, 1168, 1176, 1184, 1192, 1200, 1208, 1216, 1224, 1248, 1280, 1312, 1320, 1344, 1408, 1472, 1536, 1664, 2816, 3328, 3584, 3968, 4096, 4224, 4352, 4736, 4992, 5504 }

Те же числа, разделенные на 8

{0, 18, 20, 24, 28, 30, 32, 36, 40, 42, 48, 52, 54, 56, 60, 62, 64, 66, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96, 97, 98, 99, 100, 101, 102, 103, 104, 105, 106, 107, 108, 109, 110, 111, 112, 113, 114, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124, 125, 126, 127, 128, 129, 130, 131, 132, 133, 134, 135, 136, 137, 138, 139, 140, 141, 142, 143, 144, 145, 146, 147, 148, 149, 150, 151, 152, 153, 156, 160, 164, 165, 168, 176, 184, 192, 208, 352, 416, 448, 496, 512, 528, 544, 592, 624, 688}

Список литературы

- [1] Сачков В. Н., *Введение в комбинаторные методы дискретной математики*, М.: МЦНМО, 2004, 421 с.
- [2] Сачков В. Н., *Комбинаторные методы дискретной математики*, М.: Наука, 1977, 320 с.
- [3] Сачков В. Н., *Курс комбинаторного анализа*, Ижевск: НИЦ «Регулярная и хаотическая динамика», М., 2013, 336 с.
- [4] Глухов М. М., Елизаров В. П., Нечаев А. А., *Алгебра*, М.: Лань, 2015, 608 с.
- [5] Борисенко В. В., “О трансверсалих распавшихся латинских квадратов четного порядка”, *Математические вопросы криптографии*, **5:1** (2014), 5–25.
- [6] Борисенко В. В., “О трансверсалих однородных латинских квадратов”, *Математические вопросы криптографии*, **6:3** (2015), 5–17.
- [7] Борисенко В. В., “О трансверсалих распавшихся латинских квадратов с тождественной подстановкой χ_{ABCD} ”, *Математические вопросы криптографии*, **11:1** (2020), 9–26.
- [8] Борисенко В. В., “Неприводимые n -квазигруппы составного порядка”, *Математические исследования*, **51** (1979), 38–42.
- [9] *Handbook of combinatorial designs*, 2nd ed., eds. C. J. Colbourn, J. H. Dinitz, Chapman&Hall/CRC Press, 2006, 990 pp.
- [10] Wanless I. M., “A generalization of transversals for Latin squares”, *Electron. J. Comb*, **9:R12** (2002).
- [11] Wanless I. M., “Transversals in Latin squares. Quasigroups and related systems”, *Institute of Mathematics Academy of Sciences Moldova*, **15** (2007), 169–190.
- [12] Wanless I. M., “Transversals in Latin squares: a survey”, Cambr. Univ. Press 2011 (London Math. Soc. Lect. Note Ser.: 392), *Surveys in Combinatorics*, 2011, 447, 403–437.
- [13] McKay B. D., Meynert A., Myrvold W. J., “Small Latin squares, quasigroups and loops”, *J. Combin. Des.*, **15:2** (2007), 98–119.
- [14] Brown J. W., Parker E. T., “More on order 10 turn-squares”, *Ars Combinatoria*, **35** (1993), 125–127.