Math-Net.Ru

Общероссийский математический портал

В. В. Борисенко, О трансверсях распавшихся латинских квадратов с тождественной подстановкой χ_{ACDB} , *Матем. вopr. криптогр.*, 2020, том 11, выпуск 1, 9–26

DOI: <https://doi.org/10.4213/mvk312>

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: 54.166.219.16

26 апреля 2023 г., 17:41:16

О трансверсальных распавшихся латинских квадратов с тождественной подстановкой χ_{ACDB}

В. В. Борисенко

ООО «Центр сертификационных исследований», Москва

Получено 29.IV.2019

Аннотация. Рассматриваются распавшиеся латинские квадраты, т. е. латинские квадраты порядка $2n$, построенные на множестве чисел $\{0, \dots, 2n - 1\}$, которые при приведении по модулю n дают $(2n \times 2n)$ -матрицу, состоящую из четырех латинских квадратов (A, B, C, D) порядка n и имеющую тождественную подстановку χ_{ACDB} . Разработан метод нахождения всех возможных значений для числа трансверсальных в таких латинских квадратах фиксированного порядка $2n$, основанный на использовании вводимого автором понятия трансверсального кода.

Ключевые слова: латинский квадрат, трансверсаль, изотопия, линейный код

On transversals of splitted Latin squares with identical substitution χ_{ACDB}

V. V. Borisenko

LLC «Certification Research Center», Moscow

Abstract. We consider the splitted homogeneous Latin squares, i.e. Latin squares of order $2n$ with elements from $\{0, \dots, 2n - 1\}$ such that reducing modulo n leads to a $(2n \times 2n)$ -matrix consisting of four Latin squares (A, B, C, D) of order n with identity χ_{ACDB} permutation. The method for finding all possible numbers of transversals for Latin Squares of this kind of order $2n$ was described. This method is based on the notion of transversal code introduced in the paper.

Keywords: Latin square, transversal, isotopism, linear code

1. Введение

В данной работе, являющейся продолжением работ автора [3] и [4], рассматривается задача описания множеств трансверселей распавшихся латинских квадратов с тождественной подстановкой χ_{ACDB} . Необходимые понятия, относящиеся к латинским квадратам (для краткости далее – ЛК), можно найти в книгах [1, 2], а понятия и обозначения для распавшихся ЛК – в [3]. Здесь они не приводятся, чтобы не повторять несколько страниц текста. В дальнейшем множество всех целых чисел, начинающееся с числа m и заканчивающееся числом n , будем обозначать $[m, n] = \{a \in \mathbb{Z} \mid m \leq a \leq n\} = \{m, m+1, \dots, n\}$.

Напомним определения распавшегося и однородного латинских квадратов из [3].

Определение 1. 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 квадратные подматрицы A, B, C, D являются латинскими квадратами порядка n на множестве $[0, n-1]$. Если при этом $A = B = C = D$, то ЛК F называется *однородным*.

Подстановка χ_{ACDB} на множестве $[0, n-1]^2$ строится по латинским квадратам $A = \|a_{ij}\|$, $C = \|c_{ij}\|$, $D = \|d_{ij}\|$, $B = \|b_{ij}\|$ ($i, j \in [0, n-1]$) следующим образом. Чтобы определить, в какую пару подстановка χ_{ACDB} переводит пару (i, j) , нужно найти решения x, y, z, w уравнений

$$a_{ij} = c_{ix} = d_{yx} = b_{yz} = a_{wx}$$

и положить $\chi_{ACDB}(i, j) = (w, z)$.

Следует отметить, что ранее в [7] были рассмотрены частные случаи однородных латинских квадратов порядка $2n$: так называемые turn-squares, получаемые из таблицы Кэли группы $\mathbb{Z} \oplus \mathbb{Z}_n$ заменой символов, находящихся в четырех специально выбираемых латинских подквадратах порядка 2 (см. обзор [8]). Очевидно, что указанные латинские квадраты типа turn-squares являются однородными, строящимися по одному и тому же фиксированному набору (A, A, A, A) латинских квадратов порядка n , в котором ЛК A является таблицей Кэли группы $\mathbb{Z}_n$, и по некоторому ограниченному методу построения множеству трафаретов. Спектр возможных значений для числа трансверселей во всех однородных латинских квадратах порядка 10, построенных с помощью таблицы Кэли группы $\mathbb{Z}_5$, указан в [4, табл. 1 на с. 16]. Там как

частные случаи содержатся и все латинские turn-squares порядка 10. В [4, табл. 2 на с. 17] представлены данные для однородных ЛК порядка 10, строящихся по латинскому квадрату порядка 5 из второго (их всего 2) изотопического класса, отличного от $\mathbb{Z}_5$. Эти однородные ЛК порядка 10 заведомо не могут относиться к типу turn-squares.

Пусть $F = (A, B, C, D, T)$ — распавшийся ЛК порядка $2n$, заданный произвольными ЛК (A, B, C, D) порядка n на множестве $[0, n-1]$ и произвольным трафаретом

$$T = (t_{ij})_{n \times n} \in \{0, 1\}^{n^2}, \quad t_{ij} = 1 \Leftrightarrow g_{ij} = f_{ij}, \quad i, j \in [1, n].$$

Сформулируем в виде замечаний основные результаты, полученные в [3], применительно к рассматриваемому случаю распавшихся ЛК с тождественной подстановкой χ_{ACDB} .

Замечания. Если подстановка $\chi_{ACDB} = \text{id}$ тождественна, то:

- 1) Любой трафарет $T \in \{0, 1\}^{n^2}$ согласован с набором ЛК (A, B, C, D) . Число различных распавшихся ЛК $F = (A, B, C, D, T)$ при заданном наборе ЛК (A, B, C, D) равно числу трафаретов T , т.е. числу 2^{n^2} , см. [3, замечание перед утверждением 2 на с. 11].
- 2) Проекция $\pi_A(\tau)$ любой трансверсали $\tau \in \text{Tr}(F)$ латинского квадрата F на ЛК A является подстановочным 2-сбалансированным множеством позиций ЛК A . Подстановочным 2-сбалансированным множеством позиций ЛК A является любое 2-сбалансированное множество его позиций, являющееся проекцией подстановки степени $2n$ на ЛК A , см. [3, утверждение 3 и замечание 1 перед утверждением 4, с. 13 и 15].
- 3) Для любого множества позиций λ в ЛК A накрывающим будет любой трафарет T , у которого $t_{ij} = 0$ для всех позиций $(i, j) \notin \lambda$, см. [3, замечание 2 на с. 17]. Отсюда следует, что число таких трафаретов равно $2^{|\lambda|}$, и если λ — это 2-сбалансированное множество позиций, то $|\lambda| = 2n$, и тогда число накрывающих трафаретов для λ равно 2^{2n} .
- 4) Пусть λ — это подстановочное 2-сбалансированное множество позиций в ЛК A , и $\alpha \in S_{2n}$ порождает λ , т.е. $\lambda = \pi_A(\alpha)$. Тогда существует ровно 2^n таких трафаретов T , накрывающих λ , что $\alpha \in \text{Tr}(F, \lambda)$, $F = (A, B, C, D, T)$, см. [3, утверждение 5, с. 19].

- 5) В соответствии со следствием к указанному в предыдущем пункте утверждению, см. [3, с. 21], все множество подстановок, порождающих заданное подстановочное 2-сбалансированное множество позиций λ в ЛК A :

$$S_{2n}(\lambda) = \{a \in S_{2n} \mid \pi_A(a) = \lambda\},$$

разбивается на такие подмножества $N_1, \dots, N_t$:

$$S_{2n}(\lambda) = \bigcup_{i=1}^t N_i, \quad N_i \cap N_j = \emptyset \text{ при } i \neq j,$$

что для любого трафарета T и любой подстановки $\alpha \in S_{2n}(\lambda)$ из того, что $a \in \text{Tr}(F)$, $F = (A, B, C, D, T)$, следует, что множество всех трансверсалий ЛК F , проецирующихся на λ , совпадает с тем N_i , которому принадлежит подстановка α : $\text{Tr}(F, \lambda) = N_i$, где $\alpha \in N_i$.

- 6) Если вес трафарета T относительно λ и n имеют различную четность, то множество $\text{Tr}(F, \lambda)$ трансверсалий ЛК F , проецирующихся на λ , пусто:

$$w_\lambda(T) = w(T * \Pi_\lambda) \not\equiv n \pmod{2} \Rightarrow \text{Tr}(F, \lambda) = \emptyset,$$

см. [3, следствие к лемме 2, с. 22].

В данной работе рассматриваются следующие основные задачи: для данного натурального числа $n \in \mathbb{N}$ найти все наборы ЛК (A, B, C, D) порядка n с тождественной подстановкой $\chi_{ACDB} = \text{id}$, задающие все с точностью до изотопии распавшиеся ЛК порядка $2n$; разработать алгоритм, позволяющий для каждого такого ЛК найти все его трансверсалии.

2. Построение наборов ЛК (A, B, C, D) порядка n , задающих все с точностью до изотопии распавшиеся ЛК порядка $2n$ с тождественной подстановкой χ_{ACDB}

Начнем со следующего очевидного замечания, вытекающего непосредственно из определения распавшихся ЛК и их простейших свойств, см. [3, раздел 2, с. 8–12]. Пусть $F = (A, B, C, D, T)$ — распавшийся ЛК

порядка $2n$, заданный произвольным набором ЛК (A, B, C, D) порядка n на $[0, n-1]$ и произвольным трафаретом T . Пусть $G = \begin{pmatrix} A & C \\ B & D \end{pmatrix} = (g_{ij})_{2n \times 2n}$ — результат его приведения по модулю n . Возьмем произвольный набор подстановок $(\alpha_1, \alpha_2, \beta_1, \beta_2, \varphi)$ степени n и построим матрицу $G' = \begin{pmatrix} A' & C' \\ B' & D' \end{pmatrix} = (g'_{ij})_{2n \times 2n}$, переставив в G первые n строк по подстановке α_1 , оставшиеся n строк по подстановке α_2 , затем первые n столбцов по подстановке β_1 , оставшиеся n столбцов по подстановке β_2 , затем все элементы полученной матрицы заменяются по подстановке φ . Теперь по трафарету T построим новый трафарет T' , переставив строки T по подстановке α_1 , а столбцы — по подстановке β_1 . Тогда, очевидно, ЛК $F' = (A', B', C', D', T')$ порядка $2n$ будет изотопен исходному ЛК F . Следующее утверждение описывает, как изменяется подстановка χ_{ACDB} при описанном выше преобразовании матрицы G в матрицу G' .

Утверждение 1. Пусть $G = \begin{pmatrix} A & C \\ B & D \end{pmatrix} = (g_{ij})_{2n \times 2n}$ — матрица, в которой подматрицы A, B, C, D являются латинскими квадратами порядка n , составленными из элементов $0, 1, \dots, n-1$, и χ_{ACDB} — подстановка степени n^2 , соответствующая матрице G . Тогда:

- 1) Применение ко всем элементам G биекции $\varphi: [0, n-1] \rightarrow [0, n-1]$ не изменяет подстановку χ_{ACDB} .
- 2) Любые перестановки строк и столбцов с номерами $n+1, \dots, 2n$ не изменяют подстановку χ_{ACDB} .
- 3) Перестановка строк и столбцов с номерами $1, \dots, n$ по подстановкам $\alpha, \beta \in S_n$ соответственно приводит к матрице $G = \begin{pmatrix} A' & C' \\ B' & D' \end{pmatrix}$, для которой $\chi_{A'C'DB'} = \gamma^{-1} \chi_{ACDB} \gamma$, где $\gamma \in S_{n^2}$, $\gamma(i, j) = (\alpha(i), \beta(j))$. В частности, в этом случае подстановки $\chi_{A'C'DB'}$ и χ_{ACDB} сопряжены.

Доказательство. Первые два пункта утверждения очевидны в силу определения подстановки χ_{ACDB} .

Для доказательства третьего пункта рассмотрим $A = (a_{ij})$, $A' = (a'_{ij})$. Тогда по построению $a'_{ij} = a_{\alpha^{-1}(i)\beta^{-1}(j)} = a_{\gamma^{-1}(i,j)}$, и при действии на эти элементы подстановок $\chi_{A'C'DB'}$ и χ_{ACDB} соответственно

получим:

$$a'_{ts} = a'_{\chi_{A'C'DB'}(i,j)} = a_{(\gamma^{-1}\chi_{ACDB}\gamma)(i,j)} = a_{\gamma^{-1}(t,s)}.$$

Поэтому $(t, s) = \chi_{A'C'DB'}(i, j) = (\gamma^{-1} \cdot \chi_{ACDB} \cdot \gamma)(i, j)$ таким образом,

$$\chi_{A'C'DB'} = \gamma^{-1} \cdot \chi_{ACDB} \cdot \gamma.$$

□

Будем считать, что все множество ЛК порядка n разбито на классы изотопных латинских квадратов, и в каждом таком классе выделен стандартный представитель; как правило, в качестве такого представителя берут какой-нибудь из *нормализованных* квадратов этого класса (ЛК называется *нормализованным*, если в его первой строке и в первом столбце элементы расположены в порядке их возрастания, см. [2, с. 35]).

В книгах [1, с. 389] и [2, с. 36] вводится понятие полунормализованного ЛК, у которого первая строка содержит элементы в порядке их возрастания. В данной работе будем называть такие ЛК *полунормализованными по столбцам*. Аналогично, *полунормализованным по строкам* будем называть ЛК, у которого в первом столбце элементы расположены в порядке возрастания.

Следующее утверждение, непосредственно вытекающее из определений и рассуждений, приведенных в начале данного раздела, и утверждения 1, позволяет набирать четверки латинских квадратов с ограничением на подстановку χ_{ACDB} так, чтобы из набранных четверок заведомо можно было бы построить все с точностью до изотопии распавшиеся ЛК, для которых выполнено заданное ограничение на подстановку χ_{ACDB} .

Утверждение 2. Пусть F — распавшийся ЛК порядка $2n$, которому соответствует набор (A, B, C, D) латинских квадратов порядка n . Тогда существует изотопный ему распавшийся ЛК F' порядка $2n$ с набором (A', B', C', D') латинских квадратов порядка n , в котором:

- $A' \in [A]$ — стандартный представитель класса изотопии, к которому относится исходный ЛК A ,
- C' — полунормализованный по столбцам ЛК, изотопный латинскому квадрату C ,
- D' — полунормализованный по строкам ЛК, изотопный латинскому квадрату D ,

– B' изотопен B .

При этом подстановки $\chi_{A'C'D'B'}$ и χ_{ACDB} сопряжены.

Следствие 1. Если условия утверждения 2 выполнены и подстановка $\chi_{ACDB} = \text{id}_{[1,n]^2}$ тождественна, то и $\chi_{A'C'D'B'} = \text{id}_{[1,n]^2}$ тождественна.

Таким образом, нужно найти все наборы ЛК (A, B, C, D) порядка n , в которых A принимает значения из множества стандартных нормализованных представителей классов изотопных ЛК порядка n , C, D — полунормализованные по столбцам и строкам ЛК порядка n , а ЛК B подобран так, чтобы подстановка $\chi_{ACDB} = \text{id}_{[1,n]^2}$ была тождественной.

Найдем условия, при которых для заданных ЛК A, C, D существует такой ЛК B , что подстановка $\chi_{ACDB} = \text{id}_{[1,n]^2}$ тождественна.

Утверждение 3. Пусть A, C, D — произвольные ЛК порядка n на множестве $[0, n-1]$. Для существования такого ЛК B порядка n на множестве $[0, n-1]$, что $\chi_{ACDB} = \text{id}_{[1,n]^2}$, необходимо и достаточно, чтобы образы элементов из любого столбца $A_i^\downarrow$ латинского квадрата A при переходе в ЛК D по изображенной на рисунке схеме стояли там в разных строках. При выполнении этого условия ЛК B определен однозначно.

Доказательство. На рисунке показано действие подстановки χ_{ACDB} на элемент $(i, j) \in [1, n]^2$: если элемент a_{ij} ЛК A равен числу $a \in [0, n-1]$, то находим в ЛК C в строке с тем же номером i равный ему элемент $c_{is} = a$, затем находим в ЛК D в столбце с тем же номером s равный ему элемент $d_{ls} = a$, затем находим в ЛК B в строке с тем же номером l равный ему элемент $b_{lt} = a$, затем находим в ЛК A в столбце с тем же номером t равный ему элемент $a_{kt} = a$. В результате значением подстановки χ_{ACDB} на элементе $(i, j) \in [1, n]^2$ является элемент $(k, t) \in [1, n]^2$: $\chi_{ACDB}(i, j) = (k, t)$.

Отсюда легко следует, что если латинские квадраты A, C, D заданы, то для существования такого ЛК B , что подстановка χ_{ACDB} тождественна, необходимо и достаточно выполнение условия, указанного в утверждении. И если это условие выполнено, то ЛК B определен однозначно. $\square$

Теперь можно описать алгоритм построения множества четверок (A, B, C, D) латинских квадратов порядка n , которые с точностью до изотопии определяют все распавшиеся ЛК порядка $2n$ с тождественной подстановкой $\chi_{A'C'D'B'} = \text{id}_{[1,n]^2}$.

Для работы алгоритма потребуются следующие три массива латинских квадратов:

- массив $A_1, \dots, A_N$ стандартных представителей всех классов изотопии ЛК порядка n ,
- массив $C_1, \dots, C_M$ всех полунормализованных по столбцам ЛК порядка n ,
- массив $D_1, \dots, D_M$ всех полунормализованных по строкам ЛК порядка n (т. е. $D_i = C_i^T, i \in [1, M]$).

Алгоритм состоит в переборе всех $N \times M^2$ троек $\{(A_i, C_j, D_k) \mid i \in [1, N], j, k \in [1, M]\}$, проверке для каждой тройки выполнения условий утверждения 3 и построении ЛК B , если условия выполнены.

Данный алгоритм был реализован для $n = 5$. Известно (см. [6, с. 137, 142]), что существуют 2 класса изотопии ЛК порядка $n = 5$, т. е. в этом случае $N = 2$, число нормализованных ЛК порядка 5 равно $L(n) = 56$, и следовательно, число полунормализованных ЛК равно $M = (n - 1)!L(n) = 24 \times 56 = 1344$. Таким образом, при $n = 5$ было проверено $2 \times 1344^2 = 3\,612\,672$ варианта, из которых утверждению 3 удовлетворяют 7896. В таблице приведены результаты распределения построенных наборов по изотопическим типам подквадратов пятого порядка, например тип $\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$ означает, что квадраты A, B имеют первый изотопический тип, а квадраты C, D — второй.

В графе «отобранные варианты» указаны изотопические типы с наименьшим числом наборов, из которых остальные варианты получаются поворотом, что равносильно повороту распавшегося ЛК порядка 10. Очевидно, что латинские квадраты, получающиеся друг из друга по-

Изотопический тип	$\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$	$\begin{pmatrix} 1 & 1 \\ 2 & 2 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$	$\begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$	$\begin{pmatrix} 2 & 2 \\ 1 & 1 \end{pmatrix}$	$\begin{pmatrix} 2 & 1 \\ 2 & 1 \end{pmatrix}$	$\begin{pmatrix} 2 & 2 \\ 2 & 2 \end{pmatrix}$
Число наборов	398	1600	1600	350	42	192	192	3525
Отобранные варианты	✓				✓		✓	✓

воротом вокруг их центров, имеют одинаковые с точностью до такого же поворота множества трансверсалей.

3. Аддитивные группы трафаретов, отвечающие набору (A, B, C, D) ЛК порядка n с тождественной подстановкой χ_{ACDB}

В [3, с. 22–23] описан метод, позволяющий для каждого набора (A, B, C, D) ЛК порядка n (после некоторой предварительной работы, проводимой для этого набора) для любого согласованного с этим набором трафарета T с небольшой трудоемкостью строить множество $\text{Tr}(F)$ всех трансверсалей распавшегося ЛК $F = (A, B, C, D, T)$ порядка $2n$, построенного по набору (A, B, C, D) и трафарету T . В данном разделе этот метод будет уточнен для случая, когда распавшиеся ЛК $F = (A, B, C, D, T)$ порядка $2n$ строятся по набору (A, B, C, D) ЛК порядка n с тождественной подстановкой χ_{ACDB} .

Пусть (A, B, C, D) — произвольный фиксированный набор ЛК порядка n с тождественной подстановкой χ_{ACDB} . Обозначим через $\mathcal{T}_n$ множество всех трафаретов $((0, 1)$ -матриц) порядка n , которое будем рассматривать как аддитивную группу кольца $GF(2)_{n,n}$ квадратных матриц порядка n над полем из двух элементов $GF(2)$. Пусть $\lambda \in [1, n]^2$ — произвольное множество позиций в ЛК A . Обозначим через $\mathcal{T}_n(\lambda)$ множество всех трафаретов, у которых на позициях вне λ стоят нули: $\mathcal{T}_n(\lambda) = \{T \in \mathcal{T}_n \mid t_{ij} = 0 \forall (i, j) \notin \lambda\}$. Тогда очевидно, что $\mathcal{T}_n = \mathcal{T}_n(\lambda) \oplus \mathcal{T}_n(\bar{\lambda})$ — прямая сумма подгрупп, где $\bar{\lambda} = [1, n]^2 \setminus \lambda$ — дополнение к множеству позиций λ . В соответствии с этим любой трафарет $T \in \mathcal{T}_n$ однозначно раскладывается в сумму $T = T_\lambda + T_{\bar{\lambda}}$, где $T_\lambda \in \mathcal{T}_n(\lambda)$, $T_{\bar{\lambda}} \in \mathcal{T}_n(\bar{\lambda})$.

Пусть теперь с этого момента λ — подстановочное 2-сбалансированное множество позиций ЛК A (см. [3, с. 15, определение и замечание 1]). В этом случае $|\lambda| = 2n$, $|\mathcal{T}_n(\lambda)| = 2^{2n}$ и $\mathcal{T}_n(\lambda)$ — в точности множество всех трафаретов, накрывающих λ (см. [3, с. 16–17, определение и замечание 2]).

Для множества λ определим его характеристическую матрицу:

$$C_\lambda = (c_{ij})_{n \times n}, \quad c_{ij} = \begin{cases} 1, & (i, j) \in \lambda, \\ 0, & (i, j) \notin \lambda. \end{cases}$$

Рассмотрим теперь $\mathcal{T}_n[A] < \mathcal{T}_n$ — подгруппу всех трафаретов, постоянных на диагоналях ЛК A , $|\mathcal{T}_n[A]| = 2^n$. С ее помощью построим следующую подгруппу в $\mathcal{T}_n(\lambda)$:

$$\mathcal{T}_n(\lambda, A) = \mathcal{T}_n[A] * C_\lambda = \{T * C_\lambda \mid T \in \mathcal{T}_n[A]\}, \quad \mathcal{T}_n(\lambda, A) < \mathcal{T}_n(\lambda).$$

Здесь $*$ — операция поэлементного произведения $(0, 1)$ -матриц. Поскольку λ — 2-сбалансированное множество позиций ЛК A , то λ пересекается ровно по двум элементам с каждой диагональю этого ЛК. Тогда трафареты из подгруппы $\mathcal{T}_n(\lambda, A)$ характеризуются следующим свойством: они являются накрывающими для λ и принимают одинаковые значения на позициях, отвечающих равным элементам ЛК $A = (a_{ij})_{n \times n}$:

$$\begin{aligned} T \in \mathcal{T}_n[\lambda, A] &\Leftrightarrow (\forall (i, j) \notin \lambda: t_{ij} = 0) \\ &\wedge (\forall (i, j), (i', j') \in \lambda: a_{ij} = a_{i'j'} \rightarrow t_{ij} = t_{i'j'}). \end{aligned}$$

Очевидно, что $|\mathcal{T}_n(\lambda, A)| = 2^n$ и поэтому ее индекс в группе $\mathcal{T}_n(\lambda)$ равен $|\mathcal{T}_n(\lambda) : \mathcal{T}_n(\lambda, A)| = 2^{2n}/2^n = 2^n$. Из приведенных определений групп и их свойств очевидным образом вытекает справедливость следующего утверждения.

Утверждение 4. Пусть $\tau \subset \lambda$ — такое n -подмножество в множестве λ , что на позициях τ в ЛК A встречаются все n элементов из множества $[0, n-1]$ (и ровно по одному разу). Тогда имеет место разложение групп $\mathcal{T}_n(\lambda)$ и $\mathcal{T}_n$ в прямые суммы их подгрупп:

$$\begin{aligned} \mathcal{T}_n(\lambda) &= \mathcal{T}_n(\lambda, A) \oplus \mathcal{T}_n(\tau), \\ \mathcal{T}_n &= \mathcal{T}_n(\lambda) \oplus \mathcal{T}(\bar{\lambda}) = \mathcal{T}_n(\lambda, A) \oplus \mathcal{T}_n(\tau) \oplus \mathcal{T}_n(\bar{\lambda}). \end{aligned}$$

Отсюда следует, что для любого трафарета $T \in \mathcal{T}_n$ имеет место однозначное разложение:

$$T = T_\lambda + T_{\bar{\lambda}} = T_{\lambda, A} + T_\tau + T_{\bar{\lambda}}, \quad T_{\lambda, A} \in \mathcal{T}_n(\lambda, A), \quad T_\tau \in \mathcal{T}_n(\tau), \quad T_{\bar{\lambda}} \in \mathcal{T}_n(\bar{\lambda}).$$

Пусть $F = (A, B, C, D, T)$ — распавшийся ЛК порядка $2n$, построенный по набору (A, B, C, D) ЛК порядка n и трафарету $T \in \mathcal{T}_n$. Обозначим через $S_{2n}(\lambda)$ множество всех подстановок $\alpha \in S_{2n}$ степени $2n$,

порождающих множество λ (т.е. проецирующихся на λ : $\pi_A(\alpha) = \lambda$, см. [3, с. 17]) и через $\text{Tr}(F, \lambda) = \text{Tr}(F) \cap S_{2n}(\lambda)$ — множество тех из них, которые являются трансверсалиями ЛК F . Аналогично для другого произвольного трафарета $T' \in \mathcal{T}_n$:

$$F' = (A, B, C, D, T'), \quad \text{Tr}(F', \lambda) = \text{Tr}(F') \cap S_{2n}(\lambda),$$

$$T' = T'_\lambda + T'_\tau = T'_{\lambda, A} + T'_\tau + T'_{\bar{\lambda}}, \quad T'_{\lambda, A} \in \mathcal{T}_n(\lambda, A), \quad T'_\tau \in \mathcal{T}_n(\tau), \quad T'_{\bar{\lambda}} \in \mathcal{T}_n(\bar{\lambda}).$$

Пусть T_λ и T'_λ — накрывающие λ трафареты, соответствующие трафаретам T и T' . Через $F_\lambda = (A, B, C, D, T_\lambda)$, $F'_\lambda = (A, B, C, D, T'_\lambda)$ обозначим распавшиеся ЛК порядка $2n$, задаваемые этими трафаретами и набором (A, B, C, D) ЛК порядка n . Известно (см. [3, с. 17, замечание 1]), что

$$\text{Tr}(F, \lambda) = \text{Tr}(F_\lambda, \lambda), \quad \text{Tr}(F', \lambda) = \text{Tr}(F'_\lambda, \lambda).$$

Отсюда следует, что $\text{Tr}(F, \lambda) = \text{Tr}(F', \lambda)$ тогда и только тогда, когда $\text{Tr}(F_\lambda, \lambda) = \text{Tr}(F'_\lambda, \lambda)$. А из доказательства п. 2 утверждения 5 в [3, с. 20] следует, что последнее равенство выполняется в том и только том случае, когда $T_\lambda + T'_\lambda \in \mathcal{T}_n(\lambda, A)$, т.е. когда $T_\tau = T'_\tau \in \mathcal{T}_n(\tau)$. Приведенные рассуждения доказывают следующее утверждение.

Утверждение 5. Пусть (A, B, C, D) — произвольный набор ЛК порядка n с тождественной подстановкой χ_{ACDB} . Пусть $\lambda \in [1, n]^2$ — произвольное подстановочное 2-сбалансированное множество позиций ЛК A , трафареты $T, T' \in \mathcal{T}_n$ — произвольные, $T_\lambda, T'_\lambda \in \mathcal{T}_n(\lambda)$ — соответствующие им трафареты, накрывающие λ , и пусть $\tau \subset \lambda$ — n -подмножество в λ , на позициях которого в ЛК A встречаются все числа из $[0, n-1]$. Множества трансверсалий распавшихся ЛК $F = (A, B, C, D, T)$, $F' = (A, B, C, D, T')$, проецирующихся на λ , совпадают тогда и только тогда, когда $T_\tau = T'_\tau$, или, что то же самое, когда T_λ, T'_λ лежат в одном смежном классе группы $\mathcal{T}_n(\lambda)$ по ее подгруппе $\mathcal{T}_n(\lambda, A)$.

Рассмотрим смежные классы $H_1, \dots, H_{2^{n-1}}, \dots, H_{2^n}$ группы $\mathcal{T}_n(\lambda)$ по ее подгруппе $\mathcal{T}_n(\lambda, A)$. Внутри каждого класса четность веса трафаретов одинакова, так как они отличаются друг от друга слагаемыми из группы $\mathcal{T}_n(\lambda, A)$, в которой все трафареты, очевидно, имеют четные веса. Тогда получается, что половина смежных классов (пусть $H_1, \dots, H_{2^{n-1}}$) состоит из трафаретов с весами, четность которых совпадает с четностью числа n , а другая половина (пусть $H_{2^{n-1}+1}, \dots, H_{2^n}$)

состоит из трафаретов с весами, четность которых противоположна четности числа n . В соответствии со следствием к лемме 2 в [3, с. 22] всем трафаретам T , для которых накрывающий λ трафарет T_λ лежит в одном из классов $H_{2^{n-1}+1}, \dots, H_{2^n}$, соответствуют распавшиеся ЛК $F = (A, B, C, D, T)$, у которых $\text{Tr}(F, \lambda) = \emptyset$. Таким образом, остаются смежные классы $H_1, \dots, H_{2^{n-1}}$, содержащие накрывающие λ трафареты с весами той же четности, что и у числа n . Для трафаретов T , для которых накрывающий λ трафарет T_λ лежит в одном из классов $H_1, \dots, H_{2^{n-1}}$, в распавшемся ЛК $F = (A, B, C, D, T)$ возможно соотношение $\text{Tr}(F, \lambda) = \emptyset$, т.е. в нем может быть некоторое число трансверсалей, проецирующихся на λ .

В соответствии со следствием к утверждению 5 в [3, с. 21] множество всех подстановок степени $2n$, проецирующихся на λ , разбивается на подмножества: $S_{2n}(\lambda) = \bigcup_{i=1}^t N_i$, $N_i \cap N_j = \emptyset$ при $i \neq j$, причем для любой подстановки $\alpha \in S_{2n}(\lambda)$ и любого трафарета T из того, что подстановка α является трансверсалью в ЛК $F = (A, B, C, D, T)$, $\alpha \in \text{Tr}(F)$, следует, что все множество трансверсалей этого ЛК, проецирующихся на λ , равно $\text{Tr}(F, \lambda) = N_k$, где N_k определено принадлежностью $\alpha \in N_k$.

Отсюда вытекает, что некоторым t смежным классам из $H_1, \dots, H_{2^{n-1}}$ (пусть это будут $H_1, \dots, H_t$) соответствуют множества $N_1, \dots, N_t$ и выполнено условие

$$\forall T \in \mathcal{T}_n \forall k \in [1, t] \quad (T_\lambda \in H_k) \rightarrow \text{Tr}(F, \lambda) = N_k,$$

где $F = (A, B, C, D, T)$. При этом, очевидно, $t \leq 2^{n-1}$. Если $t < 2^{n-1}$, то смежным классам из числа $H_{t+1}, \dots, H_{2^{n-1}}$ отвечают пустые множества трансверсалей, проецирующихся на λ .

Заметим, что поскольку имеет место разложение в прямую сумму

$$\mathcal{T}_n(\lambda) = \mathcal{T}_n(\lambda, A) \oplus \mathcal{T}_n(\tau),$$

то каждому смежному классу H_i , $i \in [1, 2^n]$, группы $\mathcal{T}_n(\lambda)$ по ее подгруппе $\mathcal{T}_n(\lambda, A)$ однозначно соответствует элемент $T_i(i) \in \mathcal{T}_n(\tau)$, $i \in [1, 2^n]$. Тогда указанным выше смежным классам $H_1, \dots, H_t$, которым соответствуют непустые множества $N_1, \dots, N_t$, соответствуют трафареты $T_\tau(1), \dots, T_\tau(t)$.

Полученные результаты позволяют уточнить метод построения множеств трансверсалей распавшихся ЛК (см. [3, с. 22–23]) для рассматриваемого в данной работе случая, когда подстановка χ_{ACDB} тождественна.

Пусть дан произвольный набор (A, B, C, D) ЛК порядка n с тождественной подстановкой χ_{ACDB} . Сначала для этого набора ЛК проведем следующую предварительную работу:

- П1) Перебором всех подстановок $\alpha \in S_{2n}$ степени $2n$ построим все подстановочные 2-сбалансированные множества позиций ЛК A : $\Lambda = \{\lambda_1, \dots, \lambda_V\}$ и наборы порождающих их подстановок $\{S_{2n}(\lambda_1), \dots, S_{2n}(\lambda_V)\}$.
- П2) Для каждого 2-сбалансированного множества $\lambda_i, i \in [1, V]$, строим его n -подмножество $\tau_i \subset \lambda_i, i \in [1, V]$, на позициях которого в ЛК A содержатся все числа из $[0, n-1]$. Для множества τ_i строим соответствующую ему группу накрывающих трафаретов $\mathcal{T}_n(\tau_i) = \{T_{\tau_i}(1), \dots, T_{\tau_i}(2^n)\}$. Из этого множества удалим все трафареты, четности весов которых не совпадают с четностью числа n , получим множество трафаретов $\{T_{\tau_i}(1), \dots, T_{\tau_i}(2^n - 1)\}$.
- П3) Для каждого 2-сбалансированного множества $\lambda_i, i \in [1, V]$, по набору (A, B, C, D) ЛК порядка n и полученным в предыдущем пункте трафаретам строим 2^{n-1} распавшихся ЛК порядка $2n$:

$$\{F_1(\lambda_1), \dots, F_{2^{n-1}}(\lambda_i) \mid F_k = (A, B, C, D, T_{\tau_i}(k))\}.$$

- П4) Для каждого 2-сбалансированного множества $\lambda_i, i \in [1, V]$, перебираем подстановки $\alpha \in S_{2n}(\lambda_i)$ и формируем множества

$$\{N_1(\lambda_1), \dots, N_{2^{n-1}}(\lambda_i) \mid N_k(\lambda_i) \subset \text{Tr}(A, B, C, D, T_{\tau_i}(k))\},$$

пусть $N_1(\lambda_1), \dots, N_{t_i}(\lambda_i) \neq \emptyset$ — те из них, которые оказались непустыми. Эти множества удовлетворяют условиям

$$S_{2n}(\lambda_i) = \bigcup_{k=1}^{t_i} N_k(\lambda_i), \quad N_k(\lambda_i) \cap N_s(\lambda_i) = \emptyset \text{ при } k \neq s.$$

- П5) Для каждого 2-сбалансированного множества $\lambda_i, i \in [1, V]$, формируем два массива: массив множеств подстановок степени $2n$ $\{N_1(\lambda_1), \dots, N_{t_i}(\lambda_i)\}$ и массив соответствующих этим множествам трафаретов $\{T_{\tau_i}(1), \dots, T_{\tau_i}(t_i)\}$.

На этом предварительная работа завершается, в результате чего получаются массивы:

- 1) Массив $\Lambda = \{\lambda_1, \dots, \lambda_V\}$ подстановочных 2-сбалансированных множеств позиций ЛК A и их подмножеств $T = \{\tau_1, \dots, \tau_V\}$.
- 2) Массив подстановок степени $2n$

$$S_{2n}(\Lambda) = \bigcup_{i=1}^V S_{2n}(\lambda_i) = \bigcup_{i=1}^V \bigcup_{k=1}^{t_i} N_k(\lambda_i).$$

- 3) Массив трафаретов $\{\{T_{\tau_1}(1), \dots, T_{\tau_1}(t_1)\}, \dots, \{T_{\tau_V}(1), \dots, T_{\tau_V}(t_V)\}\}$.

Теперь с помощью построенных массивов легко строится множество трансверселей для любого распавшегося ЛК $F = (A, B, C, D, T)$:

- 1) Для каждого $i \in [1, V]$ по трафарету T строится соответствующий ему трафарет T_{τ_i} , накрывающий τ_i . Если $T_{\tau_i} = T_{\tau_i}(k)$, $k \in [1, t_i]$, то на этом этапе формируется добавляемое множество трансверселей $M_i = N_k(\lambda_i)$. Если такого совпадения не найдено, то полагаем $M_i = \emptyset$.
- 2) После завершения цикла в п. 1) получаем множество всех трансверселей ЛК F : $\text{Tr}(F) = \bigcup_{i=1}^V M_i$.

4. Группа инерции функции Tr числа трансверселей для распавшегося ЛК порядка $2n$, задаваемых набором (A, B, C, D) с тождественной подстановкой χ_{ACDB}

Пусть (A, B, C, D) — произвольный фиксированный набор ЛК порядка n с тождественной подстановкой χ_{ACDB} и $\mathcal{F}_{A,B,C,D} = \{F = (A, B, C, D, T) \mid T \in \mathcal{T}\}$ — множество всех распавшихся ЛК порядка $2n$, построенных по указанному набору. Тогда определено действие группы $\mathcal{T}_n$ на множестве $\mathcal{F}_{A,B,C,D}$: для любого ЛК $F = (A, B, C, D, T) \in \mathcal{F}_{A,B,C,D}$ и любого трафарета $T' \in \mathcal{T}_n$

$$F \cdot T' = \tilde{F} = (A, B, C, D, T + T') \in \mathcal{F}_{A,B,C,D}.$$

Очевидно, что группа $\mathcal{T}_n$ действует на множестве $\mathcal{F}_{A,B,C,D}$ регулярно (см. [5, с. 496]). Рассмотрим функцию $\text{Tr}: \mathcal{F}_{A,B,C,D} \rightarrow 2^{S_{2n}}$, ставящую в соответствие каждому ЛК $F \in \mathcal{F}_{A,B,C,D}$ множество его трансверселей $\text{Tr}(F) \subset S_{2n}$. Тогда можно определить группу инерции функции Tr в группе $\mathcal{T}_n$, действующей на множестве $\mathcal{F}_{A,B,C,D}$:

$$\mathcal{T}_n^{\text{Tr}} = \{T' \in \mathcal{T}_n \mid \forall T \in \mathcal{T}_n: \text{Tr}(A, B, C, D, T) = \text{Tr}(A, B, C, D, T + T')\}.$$

Утверждение 6. *Справедливо представление*

$$\mathcal{T}_n^{\text{Tr}} = \mathcal{T}_n(\eta, A) \oplus \mathcal{T}_n(\bar{\eta}),$$

где $\eta = \bigcup \lambda$ — объединение всех 2-сбалансированных подстановочных множеств в ЛК A , $\bar{\eta} = [1, n]^2 \setminus \eta$ — дополнение к множеству η и $\mathcal{T}_n(\eta, A) = \mathcal{T}_n[A] * C_\eta$, C_η — характеристическая матрица для множества η , $\mathcal{T}_\eta[A]$ — группа трафаретов, постоянных на диагоналях ЛК A .

Доказательство. Пусть $F = (A, B, C, D, T)$ — произвольный распавшийся ЛК, $T' \in \mathcal{T}_n$ — произвольный трафарет и $\tilde{F} = (A, B, C, D, T + T')$.

Пусть $\lambda \subset [1, n]^2$ — произвольное 2-сбалансированное подстановочное множество позиций в ЛК A , $\tau \subset \lambda$ — произвольное n -подмножество в множестве λ , на позициях которого в ЛК A встречаются все числа из $[0, n - 1]$.

Рассмотрим разложения

$$T = T_\lambda + T_{\bar{\lambda}} = T_{\lambda, A} + T_\tau + T_{\bar{\lambda}}, \quad T_{\lambda, A} \in \mathcal{T}_n(\lambda, A), \quad T_\tau \in \mathcal{T}_n(\tau), \quad T_{\bar{\lambda}} \in \mathcal{T}_n(\bar{\lambda}),$$

$$T' = T'_\lambda + T'_{\bar{\lambda}} = T'_{\lambda, A} + T'_\tau + T'_{\bar{\lambda}}, \quad T'_{\lambda, A} \in \mathcal{T}_n(\lambda, A), \quad T'_\tau \in \mathcal{T}_n(\tau), \quad T'_{\bar{\lambda}} \in \mathcal{T}_n(\bar{\lambda}).$$

Для $T + T'$ имеем:

$$T + T' = (T_{\lambda, A} + T'_{\lambda, A}) + (T_\tau + T'_\tau) + (T_{\bar{\lambda}} + T'_{\bar{\lambda}}).$$

Как показано в утверждении 5, множества трансверсалей ЛК F и $\tilde{F}$, проецирующихся на множество λ , совпадают тогда и только тогда, когда $T_\tau = T'_\tau$, т.е. $T'_\tau = (0)_{n \times n}$ и, значит, когда $T'_\lambda = T'_{\lambda, A} \in \mathcal{T}_n(\lambda, A)$. Трафарет T' принадлежит группе инерции $\mathcal{T}_n^{\text{Tr}}$ тогда и только тогда, когда предыдущее равенство выполнено для всех 2-сбалансированных подстановочных множеств позиций; поэтому для такого трафарета $T'_\eta = T'_{\eta, A} \in \mathcal{T}_n(\eta, A)$, где $\eta = \bigcup \lambda$ — указанное в условии объединение. Поскольку каждая трансверсаль ЛК F дает в проекции на ЛК A какое-то 2-сбалансированное подстановочное множество позиций, то значение T'_η в разложении $T' = T'_\eta + T'_{\bar{\eta}}$ может быть любым, поэтому $T' = T'_{\eta, A} + T'_{\bar{\eta}}$, что доказывает утверждение. $\square$

Следствие 2. *Группа инерции $\mathcal{T}_n^{\text{Tr}}$ совпадает с группой трафаретов, постоянных на диагоналях ЛК A , $\mathcal{T}_n^{\text{Tr}} = \mathcal{T}_n[A]$ тогда и только тогда, когда 2-сбалансированные подстановочные множества в ЛК A все вместе покрывают все его позиции: $\eta = \bigcup \lambda = [1, n]^2$.*

5. О числе трансверсалей в произвольных распахшихся ЛК порядка $2n$ с тождественной подстановкой χ_{ACDB}

В разделе 2 данной работы показано, что для заданного значения n можно отобрать относительно небольшое множество $M(n)$ наборов (A, B, C, D) ЛК порядка n , задающих с точностью до изотопии все распахшиеся латинские квадраты порядка $2n$ с тождественной подстановкой χ_{ACDB} . Так, при $n = 5$ было отобрано всего 4157 таких наборов, задающих все с точностью до изотопии и поворотов распахшиеся ЛК порядка $2n = 10$ с тождественной подстановкой χ_{ACDB} .

Теперь, перебирая $|M(n)| \times 2^{n^2}$ распахшихся ЛК порядка $2n$, задаваемых всеми этими наборами, с помощью быстрого алгоритма построения множеств трансверсалей, описанного в разделе 3, можно найти спектр значений для числа трансверсалей всех таких квадратов.

Однако уже при $n = 5$ получается число $|M(n)| \times 2^{n^2} = 139\,485\,773\,824$, оно недопустимо велико для перебора.

В этом разделе рассматривается подход к определению числа трансверсалей в распахшихся ЛК с помощью трансверсальных кодов, введенных автором в [4] для частного случая *однородных* латинских квадратов.

Пусть (A, B, C, D) — набор ЛК порядка n с тождественной подстановкой χ_{ACDB} и $\lambda_1, \dots, \lambda_N$ — все 2-сбалансированные подстановочные множества позиций в ЛК A для этого набора, а $\Pi_1, \dots, \Pi_N$ — соответствующие им характеристические $(0, 1)$ -матрицы порядка n (в Π_i единицы стоят на местах позиций множества λ_i).

Определение 2. Трансверсальным кодом, соответствующим набору (A, B, C, D) , называется линейный код $K_{A,B,C,D}$ с порождающей матрицей $H_{N \times n^2}$, строки которой получены в результате конкатенации строк в каждой из матриц $\Pi_1, \dots, \Pi_N$:

$$K_{A,B,C,D} = \left\{ H_{N \times n^2} T^\downarrow \mid T^\downarrow \in GF(2)^{(n^2)} \right\}.$$

Здесь матрица $H_{N \times n^2}$ рассматривается как матрица над полем из двух элементов и $GF(2)^{(n^2)}$ обозначает арифметическое векторное пространство столбцов длины n^2 над этим полем.

Утверждение 7. Определена функция $\kappa: \mathcal{F}_{A,B,C,D} \rightarrow K_{A,B,C,D}$, ставящая в соответствие каждому ЛК $F = (A, B, C, D, T) \in \mathcal{F}_{A,B,C,D}$

кодировое слово $k(F) = H_{N \times n^2} \bar{T}^\downarrow \in K_{A,B,C,D}$, где столбец $\bar{T}^\downarrow$ получен из трафарета T конкатенацией его строк и транспонированием. В этом кодировом слове $\kappa(F) = (\kappa_1, \dots, \kappa_N)^t$ координата $\kappa_i = 0$, если вес $\omega_{\lambda_i}(T)$ трафарета T относительно λ_i четен, и $\kappa_i = 1$, если этот вес нечетен.

Доказательство утверждения немедленно следует из определений использующихся в нем понятий.

Утверждение 8. Для ранга порождающей матрицы трансверсального кода выполняется неравенство $rk(H_{N \times n^2}) \leq n^2 - n$.

Доказательство. Если $T \in \mathcal{T}_n[A]$, то очевидно, что $H_{N \times n^2} \bar{T}^\downarrow = 0^\downarrow$, поэтому $\mathcal{T}_n[A] \subset \text{Ker}(\kappa)$. Переходя к мощностям, получаем $2^n \leq 2^{n^2 - rk(H)}$, значит, $rk(H_{N \times n^2}) \leq n^2 - n$. $\square$

В [3, лемма 2 и ее следствие, с. 21, 22] доказано, что множество трансверсалей, проецирующихся на λ_i , может быть непустым только при совпадении четностей числа n и веса $\omega_{\lambda_i}(T)$, т.е. при выполнении сравнения $n \equiv \kappa_i \pmod{2}$, таким образом, при нечетном n единицы, а при четном n нули указывают в кодировом слове те 2-сбалансированные множества, которые могут вносить вклад в множество трансверсалей данного ЛК.

Утверждение 9. При $n = 5$ для любого распавшегося ЛК, отвечающего четверке (A, B, C, D) ЛК порядка 5 с тождественной подстановкой χ_{ACDB} , и для соответствующего ему кодирового слова $(\kappa_1, \dots, \kappa_N)^t$ при выполнении равенства $\kappa_i = 1$ число трансверсалей, вносимых множеством λ_i , может быть либо равно 0, либо некоторому числу w_i , которое зависит только от номера i и одинаково для всех указанных ЛК.

Доказательство. Доказательство утверждения проведено путем реализации на вычислительной технике предварительного этапа работы метода нахождения множества трансверсалей $\text{Tr}(F)$, описанного в завершающей части раздела 3 данной работы (пп. П1–П5), для каждого из 4157 наборов ЛК (A, B, C, D) с тождественной подстановкой $\chi_{ACDB} = \text{id}_{[1,n]^2}$, полученных в разделе 2. При этом оказалось, что ранги порождающих матриц принимают значения от 12 до 20, таким образом, число кодовых слов в трансверсальном коде, равное $2^{rk(H)}$, значительно меньше числа ЛК 2^{5^2} , т.е. перебор кодовых слов вместо квадратов существенно сокращает число опробований. $\square$

Следствие 3. При проведении доказательства утверждения были найдены 168 наборов ЛК (A, B, C, D) с тождественной подстановкой $\chi_{ACDB} = \text{id}_{[1,n]^2}$ (из общего числа 4157 всех перебранных наборов), для которых при выполнении равенства $\alpha_i = 1$ число трансверсалей, вносимых множеством λ_i , не может быть равно 0. В этом случае для каждого распавшегося ЛК число трансверсалей вычисляется по соответствующему ему кодовому слову $(\kappa_1, \dots, \kappa_N)^t$ по формуле $\sum_{i=1}^N \kappa_i w_i$. Для таких ЛК вопрос о возможных значениях числа трансверсалей в них может быть полностью решен перебором слов трансверсальных кодов и подсчетом указанного веса каждого слова.

В заключение следует отметить, что реализация на вычислительной технике методов, изложенных в данном разделе, оказалась весьма трудоемкой, в связи с чем результаты по подсчету возможных значений числа трансверсалей в рассматриваемых ЛК будут представлены в следующей статье.

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] Борисенко В. В., “О трансверсалиях распавшихся латинских квадратов четного порядка”, *Математические вопросы криптографии*, **5:1** (2014), 5–25.
- [4] Борисенко В. В., “О трансверсалиях однородных латинских квадратов”, *Математические вопросы криптографии*, **6:3** (2015), 5–17.
- [5] Глухов М. М., Елизаров В. П., Нечаев А. А., *Алгебра*, М.: Лань, 2015, 608 с.
- [6] *Handbook of combinatorial designs*, 2nd, eds. Colbourn C. J., Dinitz J. H., CRC Press Taylor & Francis Group, 2007, 990 pp.
- [7] Brown J. W., Parker E. T., “More on order 10 turn-squares”, *Ars Combinatoria*, **35** (1993), 125–127.
- [8] Wanless I. M., “Transversals in latin squares: a survey”, London Math. Soc. Lect. Note Series: 392, Cambridge Univ. Press, 2011, 403–437.