

Румянцев Константин Евгеньевич – Южный федеральный университет; e-mail: rke2004@mail.ru; г. Таганрог, Россия; тел.: 89281827209; кафедра информационной безопасности телекоммуникационных систем; д.т.н.; профессор, зав. кафедрой.

Миронов Яков Константинович – e-mail: tmiyap117@gmail.com; тел.: +78632184000, доб. 30004; кафедра информационной безопасности телекоммуникационных систем; к.т.н.; старший преподаватель.

Миронова Полина Демьяновна – e-mail: mironova.polina.dem@gmail.com; тел.: 89081924053; кафедра информационной безопасности телекоммуникационных систем; ассистент.

Rumyantsev Konstantin Yevgenievich – Southern Federal University; e-mail: rke2004@mail.ru; Taganrog, Russia; phone: +79281827209; the Department of Information Security of Telecommunication Systems; dr. of eng. sc.; professor; head of department.

Mironov Yakov Konstantinovich – e-mail: tmiyap117@gmail.com; phone: +78632184000 (30004); the Department of Information Security of Telecommunication Systems; cand. of eng. sc.; senior lecturer.

Mironova Polina Demyanovna – e-mail: mironova.polina.dem@gmail.com; phone: +79081924053; the Department of Information Security of Telecommunication Systems; assistant.

УДК 519.143

DOI 10.18522/2311-3103-2024-3-126-137

А.О. Новиков, Э.И. Ватутин, С.И. Егоров, В.С. Титов

ИССЛЕДОВАНИЕ АЛГОРИТМА ДАББАГЯНА-ВУ ДЛЯ ПОСТРОЕНИЯ НЕЦИКЛИЧЕСКИХ ПАНДИАГОНАЛЬНЫХ ЛАТИНСКИХ КВАДРАТОВ

Рассматривается математическая модель и базирующийся на ней алгоритм Даббагяна-Ву, предназначенный для построения нециклических пандиагональных латинских квадратов. Показано, что из-за высокой вычислительной сложности и факта существования других разновидностей пандиагональных квадратов, применение классических алгоритмов, таких как полный перебор и циклических сдвигов, недостаточно для построения полного перечня пандиагональных латинских квадратов. Этим подтверждается цель работы – исследование и экспериментальная апробация математических моделей и алгоритмов, предназначенных для задачи построения за приемлемое время. Здесь производится исследование алгоритма, представленного Даббагяном В. и Ву. Т, который предназначен для построения пандиагональных латинских квадратов простых порядков p , определяемых выражением $p=6n+1$. Можно сказать, что он является модификацией алгоритма циклического построения. То есть, позволяет получить из исходного циклического квадрата пандиагональный нециклический. Преобразование выполняется путем циклических сдвигов в определенных ячейках в каждой строке исходного квадрата. Была разработана программная реализация алгоритма Даббагяна-Ву. Результат экспериментов подтвердил корректность предложенной Даббагяном В. и Ву. Т. методики построения. Таким образом, для порядка 13 удалось найти 72 уникальных квадрата. К тому же, проведена попытка построения для порядка, не являющегося нечетным простым числом, например 25. В данном случае удалось получить 4 корректных пандиагональных латинских квадрата. Путем дополнительных преобразований полученных наборов увеличить количество квадратов, так, для порядка 13 коллекция расширена до 1570, а для 25 – до 210. Исследование позволило углубленно ознакомиться с алгоритмом Даббагяна-Ву и сделать вывод о его особенностях – к достоинствам относится его относительно низкая вычислительная сложность, а к недостаткам – полноценная корректность построений только для нечетных простых порядков. Полученные наборы квадратов в дальнейшем будут задействованы для получения их числовых характеристик при помощи распределенных вычислений.

Пандиагональные латинские квадраты; нециклические латинские квадраты; циклический сдвиг; построение; алгоритм; математическая модель; вычислительная сложность.

A.O. Novikov, E.I. Vatutin, S.I. Egorov, V.S. Titov

RESEARCH OF THE DABBAGHIAN-WU ALGORITHM FOR CONSTRUCTING NON-CYCLIC PANDIAGONAL LATIN SQUARES

In this paper we consider a mathematical model and the Dabbaghian-Wu algorithm based on it, designed to construct non-cyclic pandiagonal Latin squares. It is shown that due to the high computational complexity and the fact of existence of other varieties of pandiagonal squares, the application of classical algorithms, such as brute force and cyclic shifts, is insufficient to construct a complete list of pandiagonal Latin squares. This

confirms the purpose of the work – the research and experimental approbation of mathematical models and algorithms for the task of construction in an acceptable time. We perform research of the algorithm presented by Dabbaghian and Wu, which is intended for constructing pandiagonal Latin squares of prime order p , defined by the expression $p=6n+1$. It is a modification of the cyclic construction algorithm and allows to obtain a pandiagonal non-cyclic square from the original cyclic square. The conversion is done by cyclic shifts in specific cells in each row of the original square. A software implementation of the Dabbaghian-Wu algorithm was developed. The results of the experiments confirmed the correctness of the construction methodology proposed by Dabbaghian and Wu. Thus, for order 13, 72 unique squares were found. In addition, an attempt was made to construct for an order that is not an odd prime number, for example 25. In this case, it was possible to obtain 4 correct pandiagonal Latin squares. By additional conversions of the resulting sets, increase the number of squares, so for order 13 the collection is expanded to 1570, and for 25 to 210. The research made it possible to research the Dabbaghian-Wu algorithm in depth and draw a conclusion about its features, the advantages include its relatively low computational complexity, and the disadvantages are the full correctness of the constructions only for odd prime orders. The resulting sets of squares will be used in the future to obtain their numerical characteristics using distributed computing.

Pandiagonal Latin squares; non-cyclic Latin squares; cyclic shift; construction; algorithm; mathematical model; computational complexity.

Введение. В комбинаторике довольно широко известна структура, называемая латинским квадратом [1, 2].

Одним из редких типов латинских квадратов, представляющих научный интерес, являются так называемые пандиагональные латинские квадраты (далее по тексту – ПДЛК, PDLs). Они определяются следующим образом: латинский квадрат порядка N является пандиагональным, если элементы каждой строки, каждого столбца, главной и побочной диагонали, параллельных им ломаных диагоналей образуют множества, равные $\mathbb{Z}_N$, где $\mathbb{Z}_N = \{0, \dots, N-1\}$. Ломанная k -я диагональ, параллельная главной диагонали, определяется как множество элементов квадрата

$$\{D_k\} = x_{k,(k+i) \bmod N}, i \in \{0, \dots, N-1\},$$

а побочная ломанная k -я диагональ, параллельная побочной диагонали (ломаная k -я антидиагональ), как

$$\{D_k\} = x_{k,(N-k+i) \bmod N}, i \in \{0, \dots, N-1\},$$

где x – ячейка латинского квадрата. Иными словами, в ПДЛК все ломаные диагонали и антидиагонали являются трансверсальями [1].

Известно, что ПДЛК существуют только для нечетных порядков, не кратных 3 [2].

Множество всех латинских квадратов заданного типа и порядка N , в том числе множество всех пандиагональных ЛК, генерируются при помощи алгоритма полного перебора, но за счет чрезмерно большой вычислительной сложности его применение на практике возможно только для порядков $N < 10$ с рядом алгоритмических особенностей и оптимизаций соответствующих параллельных и/или распределенных программных реализаций [3–6].

Это обусловлено тем, что далее с ростом размерности задачи происходит так называемый «комбинаторный взрыв», вычислительная сложность резко возрастает и построение ЛК для больших N данным методом попросту невозможно за приемлемое время.

Таким образом, задача исследования и разработки алгоритмов для построения ПДЛК больших порядков является актуальной.

Постановка задачи. Известно, все ПДЛК порядков $N \leq 11$ являются циклическими, чего нельзя сказать о порядках $N > 11$, поэтому для $N \leq 11$ генерация может быть выполнена при помощи алгоритма, базирующегося на циклических сдвигах строк формируемого квадрата и обладающего полиномиальной временной асимптотикой. Данный алгоритм описывается следующим образом: пусть K – циклический латинский квадрат порядка N , где значение каждой его ячейки выражается как

$$K_{i,j} = [\lambda i + j] \bmod N,$$

где $i, j \in \{0, \dots, N-1\}$ – ячейки латинского квадрата, λ – величина циклического сдвига [7].

К. Вик доказал, что полученный таким методом квадрат является пандиагональным в том случае, когда величина сдвига λ равна $2 \leq \lambda \leq N - 2$ [3, 4] (для $\lambda = 0$ получаемый ЛК является некорректным ввиду того, что все его строки совпадают, для $\lambda = 1$ и $\lambda = N - 1$ получаемые квадраты являются циклическими ЛК, но не ДЛК и не ПДЛК ввиду наличия дублирующихся значений на главной и побочной диагонали соответственно).

По формуле видно, что асимптотическая временная сложность данного алгоритма определяется как $t \approx O(N^2(N - 3)) \approx O(N^3)$.

На рис. 1 представлен пример латинского квадрата порядка 11, который является циклическим и пандиагональным.

0	1	2	3	4	5	6	7	8	9	10
2	3	4	5	6	7	8	9	10	0	1
4	5	6	7	8	9	10	0	1	2	3
6	7	8	9	10	0	1	2	3	4	5
8	9	10	0	1	2	3	4	5	6	7
10	0	1	2	3	4	5	6	7	8	9
1	2	3	4	5	6	7	8	9	10	0
3	4	5	6	7	8	9	10	0	1	2
5	6	7	8	9	10	0	1	2	3	4
7	8	9	10	0	1	2	3	4	5	6
9	10	0	1	2	3	4	5	6	7	8

Рис. 1. Пример циклического пандиагонального латинского квадрата порядка 11 для значения $\lambda=2$

Из рисунка видно, что строки квадрата получены при помощи циклического сдвига предыдущей строки на величину λ , а все столбцы – циклическим сдвигом предыдущего столбца на некоторую величину λ' , ввиду чего в некоторых источниках подобные квадраты называются дважды циклическими. Между значениями величин λ и λ' для заданного порядка квадрата N имеется взаимно однозначное соответствие.

Для порядков $N > 11$ помимо циклических существуют также другие разновидности ПДЛК с определенными свойствами, например полуциклические и нециклические квадраты [8].

Полуциклический латинский квадрат определяется следующим образом: либо все строки i являются циклическими перестановками первой строки на некоторое значение λ_i , либо столбцы j являются циклическими перестановками первого столбца на некоторое значение λ'_j , но не одновременно [6].

В нециклическом латинском квадрате ни его строки, ни его столбцы не являются циклическими сдвигами первой строки и столбца соответственно.

Из вышеописанного можно сделать вывод о том, что применение данного алгоритма также недостаточно для построения полного перечня ПДЛК порядков $N > 11$.

Задачей исследования методик генерации ПДЛК занимались такие ученые как А.О.Л. Аткин, Л. Хэй, Р.Г. Ларсон, Дж. Белл, Б. Стивенс, В. Даббаган, Т. Ву, А. Хедаят, А. Стоффель, К. Вик [8–14].

Алгоритм формирования всех ПДЛК с приемлемой временной сложностью неизвестен, ввиду чего на практике известен ряд частных решений данной задачи, сводящихся к получению ПДЛК некоторых типов [15, 16].

Метод решения. Одно из решений данной проблемы было найдено В. Даббаганом и Т. Ву – ими была предложена математическая модель и алгоритм построения нециклических ПДЛК простых порядков $p = 6m + 1$, где m – целое положительное число [11, 14]. Данный алгоритм опирается на теорию модульной арифметики и, по сути, представляет собой модификацию метода построения при помощи циклических сдвигов [7].

Алгоритм Даббагяна-Ву позволяет построить нециклический ПДЛК порядка p из исходного циклического ПДЛК и состоит из нескольких этапов [14].

1. Сперва необходимо найти неупорядоченные пары целых чисел a и b , $a, b \in \{1, \dots, p-1\}$, $a < b$, такие, что выполняется следующее сравнение по модулю:

$$a^2 + b^2 \equiv ab \pmod{p}.$$

2. Для каждой найденной пары чисел a и b необходимо найти значение $c = a - b$ и такое l , что

$$(a + b)l \equiv a^2 \pmod{p}.$$

3. Для каждой пары a и b найти 6 пар целых чисел λ и u таких, что

$$(\lambda, u) \in \left\{ \left(\frac{b-a}{a+b}, -\frac{1}{3} \right), \left(\frac{a-b}{a+b}, \frac{1}{3} \right), \left(\frac{a+b}{b-a}, 1 \right), \right. \\ \left. \left(\frac{a+b}{a-b}, -1 \right), \left(-\frac{b}{a}, 1 \right), \left(\frac{b}{a}, -1 \right) \right\} \pmod{p}.$$

Говоря иначе, следует решить 6 пар сравнений по модулю:

$$Lx \equiv R \pmod{p}.$$

Перепишем задачу согласно данной формуле:

$$(\lambda, u) \in \left\{ \begin{array}{l} ((a+b)\lambda \equiv b-a, 3u \equiv -1), \\ ((a+b)\lambda \equiv a-b, 3u \equiv 1), \\ ((b-a)\lambda \equiv a+b, 1u \equiv 1), \\ ((a-b)\lambda \equiv a+b, 1u \equiv -1), \\ (a\lambda \equiv -b, 1u \equiv 1), \\ (a\lambda \equiv b, 1u \equiv -1) \end{array} \right\} \pmod{p}.$$

4. Построить исходный циклический ПДЛК K порядка p согласно выражению для каждой величины сдвига λ из полученного набора.

5. В каждой i -ой строке, $i \in \{0, \dots, p-1\}$, циклического ПДЛК необходимо помещать местами значения в определенных ячейках по следующим правилам:

$$temp = K[i][iu];$$

$$1. K[i][iu] = K[i][iu + b];$$

$$2. K[i][iu + b] = K[i][iu + a];$$

$$3. K[i][iu + a] = temp;$$

$$temp = K[i][iu + l];$$

$$4. K[i][iu + l] = K[i][iu + c + l];$$

$$5. K[i][iu + c + l] = K[i][iu + b + l]$$

$$6. K[i][iu + b + l] = temp.$$

При выполнении вышеописанных этапов формируется корректный нециклический ПДЛК [14, 15].

Рассмотрим данный алгоритм на примере. Возьмем порядок построения $p = 13 = 2 \cdot 6 + 1$.

Сперва выполняется поиск пар значений (a, b) , удовлетворяющих выражению. Для порядка 13 полученный набор представлен ниже:

$$\left\{ \begin{array}{l} (1, 4), (1, 10), (2, 7), (2, 8), (3, 4), \\ (3, 12), (5, 7), (5, 11), (6, 8), \\ (6, 11), (9, 10), (9, 12) \end{array} \right\}.$$

Для дальнейших преобразований в качестве примера используется $(a, b) = (5, 7)$. В данном случае $l = 1$, $c = b - a = 7 - 5 = 2$.

Далее выполняется поиск значений (λ, u) согласно выражениям. Паре $(a, b) = (5, 7)$ соответствует следующий набор (λ, u) :

$$\{(11, 4), (2, 9), (6, 1), \} \\ \{(7, 12), (9, 1), (4, 12)\}.$$

Следующим шагом выполняется построение исходного циклического квадрата по выражению. Для примера $(\lambda, u) = (7, 12)$. Полученный таким образом циклический квадрат представлен на рис. 2.

0	1	2	3	4	5	6	7	8	9	10	11	12
7	8	9	10	11	12	0	1	2	3	4	5	6
1	2	3	4	5	6	7	8	9	10	11	12	0
8	9	10	11	12	0	1	2	3	4	5	6	7
2	3	4	5	6	7	8	9	10	11	12	0	1
9	10	11	12	0	1	2	3	4	5	6	7	8
3	4	5	6	7	8	9	10	11	12	0	1	2
10	11	12	0	1	2	3	4	5	6	7	8	9
4	5	6	7	8	9	10	11	12	0	1	2	3
11	12	0	1	2	3	4	5	6	7	8	9	10
5	6	7	8	9	10	11	12	0	1	2	3	4
12	0	1	2	3	4	5	6	7	8	9	10	11
6	7	8	9	10	11	12	0	1	2	3	4	5

Рис. 2. Циклический ПДЛК порядка $N=13$ и величиной сдвига $\lambda=7$

Теперь необходимо выполнить преобразования каждой i -ой строке, $i \in \{0, \dots, p-1\}$, циклического ПДЛК по выражениям.

Для строки $i = 0$.

$$temp = K_{0,0} = 0;$$

$$1. K_{0,0} = K_{0,7} = 7;$$

$$2. K_{0,7} = K_{0,5} = 5;$$

$$3. K_{0,5} = temp = 0;$$

$$temp = K_{0,1} = 1;$$

$$4. K_{0,1} = K_{0,3} = 3;$$

$$5. K_{0,3} = K_{0,8} = 8;$$

$$6. K_{0,8} = temp = 1;$$

Аналогичные преобразования выполняются и для остальных строк квадрата. Например, для второй строки ($i = 1$) получим:

$$temp = K_{1,12} = 6;$$

$$1. K_{1,12} = K_{1,6} = 0;$$

$$2. K_{1,6} = K_{1,4} = 11;$$

$$3. K_{1,4} = temp = 6;$$

$$temp = K_{1,0} = 7;$$

$$4. K_{1,0} = K_{1,2} = 9;$$

$$5. K_{1,2} = K_{1,7} = 1;$$

$$6. K_{1,7} = temp = 7;$$

Остальные строки квадрата обрабатываются таким же образом. В результате преобразований построен нециклический ПДЛК, который представлен ниже (рис. 3).

7	3	2	8	4	0	6	5	1	9	10	11	12
9	8	1	10	6	12	11	7	2	3	4	5	0
1	7	3	12	5	4	0	8	9	10	11	6	2
0	9	5	11	10	6	1	2	3	4	12	8	7
2	11	4	3	12	7	8	9	10	5	1	0	6
4	10	9	5	0	1	2	3	11	7	6	12	8
3	2	11	6	7	8	9	4	0	12	5	1	10
8	4	12	0	1	2	10	6	5	11	7	3	9
10	5	6	7	8	3	12	11	4	0	9	2	1
11	12	0	1	9	5	4	10	6	2	8	7	3
5	6	7	2	11	10	3	12	8	1	0	9	4
12	0	8	4	3	9	5	1	7	6	2	10	11
6	1	10	9	2	11	7	0	12	8	3	4	5

Рис. 3. Нециклический ПДЛК, полученный при помощи преобразований

Первая часть преобразований строк фактически выполняет циклическое перемещение вправо записей ячеек, которые определяются уравнениями замен. Соответственно, вторая часть отвечает за циклический сдвиг влево определенных ячеек в квадрате. То есть, циклически перемещаются только значения в указанных индексах, при этом остальные ячейки строки квадрата не изменяются.

Процесс подробно изображен на рис. 4.

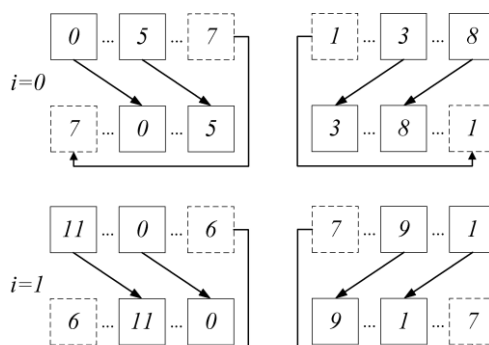


Рис. 4. Преобразования в строках квадрата в виде циклических сдвигов определенных ячеек (на примере первой и второй строки квадрата)

Данные преобразования в строках представлены на рис. 5 ниже. Циклическим сдвигам влево и вправо соответствует определенный рисунок штриховки в ячейках.

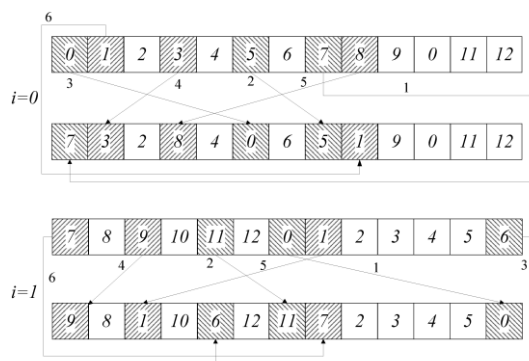


Рис. 5. Циклические сдвиги в строках латинского квадрата

После выполнения смещения ячеек изменяются значения в определенных столбцах квадрата, при этом одно из них отсутствует, а другое дважды повторяется за счет сдвигов. К тому же, аналогичное явление возникает и на соответствующих ломаных диагоналях.

В столбцах данные нарушения исправляются при помощи циклического сдвига влево ячеек в тех строках, где имеется несоответствие. После выполнения в первой строке циклического сдвига вправо одно число повторяется дважды, а другое отсутствует, как видно, это относится и к столбцам, и к ломаным диагоналям. При сдвигах значений ячеек влево в последующих строках, где обнаружено удвоение, устраняется данное противоречие. К примеру, после замен в строке $i = 1$ исчезает цифра 7, дважды повторяющаяся в столбце $j = 0$ [14].

По ломаным диагоналям нарушение исправляется тем же видом сдвига, которым оно и вызвано. Например, удвоения на ломаных главных и побочных устраняются при совершении сдвигов вправо в строках, где они были зафиксированы.

В свою очередь, выполнение сдвигов далее также вызывает такие же нарушения в столбцах и ломаных диагоналях, которые, по аналогии, исправляются новыми сдвигами. То есть, в процессе преобразований в строках происходит пошаговое исправление ошибок, вызванных предыдущими смещениями. После выполнения смещений во всех строках исходного квадрата будет построен нециклический ПДЛК. Поэтапная карта преобразований при помощи сдвигов показана на рис 6 и 7.

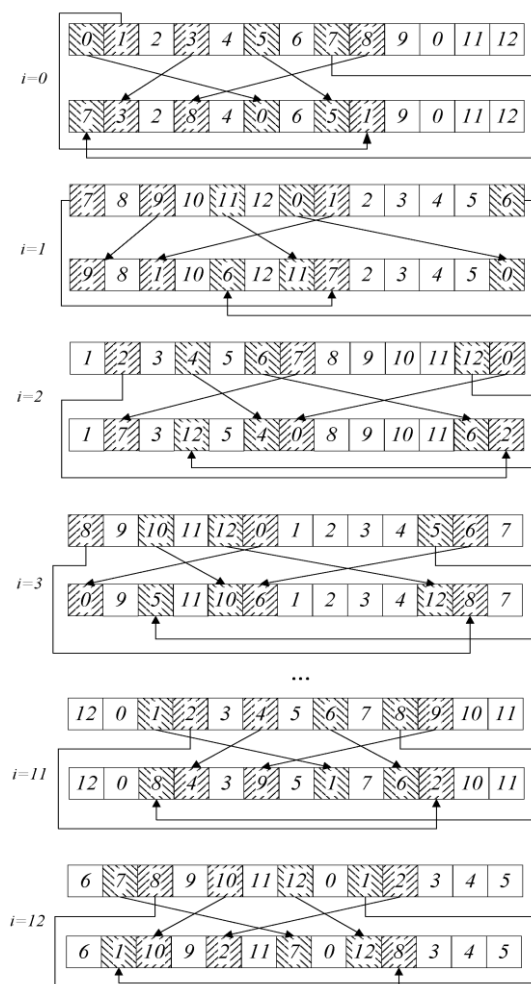


Рис. 6. Карта пошаговых преобразований исходного циклического квадрата

7	3	2	8	4	0	6	5	1	9	10	11	12
9	8	1	10	6	12	11	7	2	3	4	5	0
1	7	3	12	5	4	0	8	9	10	11	6	2
0	9	5	11	10	6	1	2	3	4	12	8	7
2	11	4	3	12	7	8	9	10	5	1	0	6
4	10	9	5	0	1	2	3	11	7	6	12	8
3	2	11	6	7	8	9	4	0	12	5	1	10
8	4	12	0	1	2	10	6	5	11	7	3	9
10	5	6	7	8	3	12	11	4	0	9	2	1
11	12	0	1	9	5	4	10	6	2	8	7	3
5	6	7	2	11	10	3	12	8	1	0	9	4
12	0	8	4	3	9	5	1	7	6	2	10	11
6	1	10	9	2	11	7	0	12	8	3	4	5

Рис. 7. Итоговая карта преобразований для анализируемого ПДЛК

Следует отметить, что построение квадрата единственным образом определяется набором пар параметров (a, b) и соответствующим каждой такой паре значений набором (λ, u) , то есть, для каждой связки этих переменных ПДЛК является уникальным [14].

Несложно показать, что зависимость количества M генерируемых алгоритмом нециклических ПДЛК от их порядка p определяется следующим образом:

$$M = 6(p - 1).$$

Например, для порядка 13 можно построить 72 уникальных ПДЛК.

Вычислительную сложность алгоритма Даббагьяна-Ву можно представить так:

$$t \approx O(6 + (p - 1)^2 + (p - 1) \cdot 6 \cdot p^2 \cdot (6p)) \approx O(p^5).$$

Рассмотрим каждый элемент выражения:

6 – количество параметров u , которые достаточно вычислить единожды, их значения зависят только от порядка p ;

$(p - 1)^2$ – подбор пар параметров a, b и соответствующих им параметрам c, l ;

$(p - 1)$ – для построения ПДЛК берется каждая из подобранных пар a, b ;

6 – для пары a, b подбирается 6 значений величин сдвига λ ;

p^2 – для каждой величины сдвига λ строится исходный циклический латинский квадрат;

$(6p)$ – для каждого исходного циклического квадрата во всех строках выполняется цепочка преобразований.

При работе алгоритма затраты памяти, зависящие от размерности задачи, связаны лишь с хранением формируемого квадрата и составляют величину $m \approx O(p^2)$.

Результаты и обсуждение. В ходе исследования выполнена программная реализация вышеописанного алгоритма. Для порядка $p=13$ удалось найти 72 нециклических ПДЛК, для $p=19$ – 108, что соответствует выражению (10).

Для нечетных порядков, не являющихся простыми и не удовлетворяющих условию $p = 6t + 1$ также возможно построение нециклических ПДЛК. Однако часть результатов является некорректной, другая часть удовлетворяет условиям пандиагональности и нециклическости. На рис. 8 и 9 показаны примеры построений.

Для порядка 25 было найдено 4 ПДЛК, которые удовлетворяют условиям.

Была проведена попытка построения ПДЛК других нечетных порядков, определяемых как $p=2k+1$. Результат, показывающий количество верных построений в зависимости от порядка представлен ниже в виде числового ряда:

$$\{1, 0, 0, 24, 0, 72, 0, 0, 108, 0, 0, 4, 0, 0, \dots\}$$

$$\{180, 0, 3, 216, 0, 0, 252, 0, 0, 264, \dots\}$$

[illegible]

Рис. 8. Некорректный ПДЛК порядка 25

10	1	2	3	4	5	6	7	8	9	15	11	12	13	14	0	16	17	18	19	20	21	22	23	24
2	3	4	5	6	7	8	9	20	11	12	13	14	15	16	17	18	19	0	21	22	23	24	10	1
4	10	6	7	8	9	20	11	12	13	14	15	16	17	18	19	5	21	22	23	24	0	1	2	3
6	7	8	9	10	11	12	13	14	20	16	17	18	19	5	21	22	23	24	0	1	2	3	4	15
8	9	10	11	12	13	14	0	16	17	18	19	20	21	22	23	24	5	1	2	3	4	15	6	7
15	11	12	13	14	0	16	17	18	19	20	21	22	23	24	10	1	2	3	4	5	6	7	8	9
12	13	14	15	16	17	18	19	0	21	22	23	24	10	1	2	3	4	5	6	7	8	9	20	11
14	15	16	17	18	19	5	21	22	23	24	0	1	2	3	4	10	6	7	8	9	20	11	12	13
16	17	18	19	5	21	22	23	24	0	1	2	3	4	15	6	7	8	9	10	11	12	13	14	20
18	19	20	21	22	23	24	5	1	2	3	4	15	6	7	8	9	10	11	12	13	14	0	16	17
20	21	22	23	24	10	1	2	3	4	5	6	7	8	9	15	11	12	13	14	0	16	17	18	19
22	23	24	20	1	2	3	4	5	6	7	8	9	20	11	12	13	14	15	16	17	18	19	0	21
24	0	1	2	3	4	10	6	7	8	9	20	11	12	13	14	15	16	17	18	19	5	21	22	23
1	2	3	4	15	6	7	8	9	10	11	12	13	14	20	16	17	18	19	5	21	22	23	24	0
3	4	15	6	7	8	9	10	11	12	13	14	0	16	17	18	19	20	21	22	23	24	5	1	2
5	6	7	8	9	15	11	12	13	14	0	16	17	18	19	20	21	22	23	24	10	1	2	3	4
7	8	9	20	11	12	13	14	15	16	17	18	19	0	21	22	23	24	10	1	2	3	4	5	6
9	20	11	12	13	14	15	16	17	18	19	5	21	22	23	24	0	1	2	3	4	10	6	7	8
11	12	13	14	20	16	17	18	19	5	21	22	23	24	0	1	2	3	4	15	6	7	8	9	10
13	14	0	16	17	18	19	20	21	22	23	24	5	1	2	3	4	15	6	7	8	9	10	11	12
0	16	17	18	19	20	21	22	23	24	10	1	2	3	4	5	6	7	8	9	15	11	12	13	14
17	18	19	0	21	22	23	24	10	1	2	3	4	5	6	7	8	9	20	11	12	13	14	15	16
19	5	21	22	23	24	0	1	2	3	4	10	6	7	8	9	20	11	12	13	14	15	16	17	18
21	22	23	24	0	1	2	3	4	15	6	7	8	9	10	11	12	13	14	15	16	17	18	19	5
23	24	5	1	2	3	4	15	6	7	8	9	10	11	12	13	14	0	16	17	18	19	20	21	22

Рис. 9. Корректный ПДЛК порядка 25

К тому же, при помощи следующих преобразований набора построенных нециклических ПДЛК порядка 13 удалось увеличить их количество до 1570 уникальных квадратов:

- ◆ поворот ПДЛК на углы, кратные 45;
- ◆ внесение в исходный набор циклических диагональных латинских квадратов;
- ◆ внесение в набор повернутых полуциклических диагональных латинских квадратов;
- ◆ преобразование в виде отражения и транспонирования ПДЛК;
- ◆ вращение на тороидальной решетке N^2 способами [16, 17].

Ход расширения коллекции ПДЛК порядка 13 путем описанных преобразований можно представить таким образом:

$$72 \rightarrow 264 \rightarrow 274 \rightarrow 1458 \rightarrow 1554 \rightarrow 1570.$$

Аналогичные действия были проведены для порядков 19 и 25. Следует указать, что для порядка $p=25$ не было проведено внесение полуматричных латинских квадратов ввиду сложности их построения для данного p .

Расширение коллекции ПДЛК порядка 19:

$$108 \rightarrow 546 \rightarrow 262 \rightarrow 172892 \rightarrow 173148 \rightarrow 173600.$$

Для порядка 25:

$$4 \rightarrow 16 \rightarrow 26 \rightarrow 210.$$

Данные преобразования позволили найти нижние оценки количества ПДЛК в числовой последовательности OEIS A338620:

$$\begin{aligned} A(13) &\geq 1570; \\ A(19) &\geq 173600; \\ A(25) &\geq 210. \end{aligned}$$

Найденные нижние оценки количества ПДЛК позволяют оценить масштабы и эффективность применения исследуемого алгоритма Даббагьяна-Ву и представленных выше преобразований полученных коллекций. Описанные методы могут быть использованы для поиска новых решений на больших порядках.

Анализ результатов указывает на потенциал для дальнейших исследований, направленных на более точное определение общего количества ПДЛК и исследование их свойств.

Выводы. Таким образом, в статье была проведена апробация алгоритма Даббагьяна-Ву для построения нециклических пандиагональных латинских квадратов, разработанная программная реализация и экспериментальные исследования с ее использованием подтвердили корректность рассмотренных выше математических построений.

Стоит отметить, что к достоинствам алгоритма Даббагьяна-Ву можно отнести его относительно низкую вычислительную сложность, а к недостаткам – полноценную корректность построений только для нечетных простых порядков, удовлетворяющих выражению $p = 6m + 1$, где m – целое положительное число.

В перспективе планируется дальнейший анализ пандиагональных латинских квадратов, расчет их числовых характеристик при помощи распределенных вычислительных систем на базе грид-технологий, исследование других математических моделей, методов и алгоритмов для их построения [18–20].

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Colbourn C.J., Dinitz J.H. Handbook of Combinatorial Designs. – Second ed. – Chapman & Hall/CRC, 2006. – 1016 p.
2. Keedwell A.D., Dénes J. Latin Squares and their Applications. – Elsevier, 2015. – 438 p.
3. Ватутин Э.И. О перечислении циклических латинских квадратов и расчете значения функции Эйлера с их использованием // Высокопроизводительные вычислительные системы и технологии. – 2020. – Т. 4, № 2. – С. 40-48.
4. Vatutin E.I., Kochemazov S.E., Zaikin O.S. Applying volunteer and parallel computing for enumerating diagonal Latin squares of order 9 // Proc. of The Eleventh International Conference on Parallel Computational Technologies, Vol. 753 of Communications in Computer and Information Science. – Springer, 2017. – P. 114-129.
5. Kochemazov S., Zaikin O., Vatutin E., Belyshev A. Enumerating diagonal latin squares of order up to 9 // Journal of Integer Sequences. – 2020. – Vol. 23, No. 1. – P. 2012.
6. Ватутин Э.И., Бельшев А.Д., Никитина Н.Н., Манзюк М.О. Использование X-образных диагональных заполнений и ESODLS CMS схем для перечисления главных классов диагональных латинских квадратов // Телекоммуникации. – 2023. – № 1. – С. 2-16.
7. Ватутин Э.И. О подсчете главных классов циклических диагональных и пандиагональных латинских квадратов // Оптико-электронные приборы и устройства в системах распознавания образов и обработки изображений. – 2021. – С. 77-79.

8. Bell J., Stevens B. Constructing orthogonal pandiagonal Latin squares and panmagic squares from modular n-queens solutions // *Journal of Combinatorial Designs*. – 2007. – No. 15 (3). – P. 221-234.
9. Hedayat A. A complete solution to the existence and nonexistence of Knut Vik designs and orthogonal Knut Vik designs // *Journal of Combinatorial Theory, Series A*. – 1977. – No. 22 (3). – P. 331-337.
10. Atkin A.O.L., Hay L., Larson R.G. Enumeration and construction of pandiagonal Latin squares of prime order // *Computers & Mathematics with Applications*. – 1983. – No. 9 (2). – P. 267-292.
11. Vik K. Bedømmelse av feilene på forsøksfelter med og uten målestokk. – 1924.
12. Stoffel A. Totally diagonal Latin squares // *Stud Cerc Mat*. – 1976. – Vol. 28. – P. 113-119.
13. Chang G.J., Hwang F.K. Diagonal and Pandiagonal Tournament Latin Squares // *European Journal of Combinatorics*. – 1985. – Vol. 6, No. 2. – P. 149-155.
14. Dabbagian V., Wu T. Constructing non-cyclic pandiagonal Latin squares of prime orders // *Journal of Discrete Algorithms*. – 2015. – No. 30. – P. 70-77.
15. Ватутин Э.И. Специальные виды диагональных латинских квадратов // *Облачные и распределенные вычислительные системы в электронном управлении ОРВСЭУ - 2022 в рамках Национального суперкомпьютерного форума (НСКФ - 2022)*. – 2022. – С. 9-18.
16. Vatutin E., Nikitina N., Belyshev A., Manzyuk M. On polynomial reduction of problems based on diagonal Latin squares to the exact cover problem // *CEUR Workshop*. – 2020. – P. 289-297.
17. Vatutin E., Belyshev A., Manzyuk M., Nikitina N. Evaluation of Efficiency of Using Simple Transformations When Searching for Orthogonal Diagonal Latin Squares of Order 10 // *Communications in Computer and Information Science*. – 2020. – Vol. 1304. – P. 127-146.
18. Альбертьян А.М., Курочкин И.И., Ватутин Э.И. Использование гетерогенных вычислительных комплексов в грид-системах из персональных компьютеров // *XIV Всероссийская мультikonференция по проблемам управления МКПУ-2021*. – 2021. – С. 90-93.
19. Никитина Н.Н., Ватутин Э.И., Манзюк М.О. [и др.]. Показатели и технологическая основа проектов распределённых вычислений Rakesearch и Sidock@home // *Облачные и распределенные вычислительные системы в электронном управлении ОРВСЭУ - 2022 в рамках Национального суперкомпьютерного форума (НСКФ - 2022)*. – 2022. – С. 38-46.
20. Manzyuk M., Nikitina N., Vatutin E. Start-up and the Results of the Volunteer Computing Project RakeSearch // *Communications in Computer and Information Science*. – 2019. – Vol. 1129. – P. 725-734.

REFERENCES

1. Colbourn C.J., Dinitz J.H. *Handbook of Combinatorial Designs*. Second ed. Chapman & Hall/CRC, 2006, 1016 p.
2. Keedwell A.D., Dénes J. *Latin Squares and their Applications*. Elsevier, 2015, 438 p.
3. Vatutin E.I. O perechislenii tsiklicheskikh latinskikh kvadratov i raschete znacheniya funktsii Eylera s ikh ispol'zovaniem [On enumerating cyclic Latin squares and calculating the value of the Euler function using them], *Vysokoproizvoditel'nye vychislitel'nye sistemy i tekhnologii* [High-performance computing systems and technologies], 2020, Vol. 4, No. 2, pp. 40-48.
4. Vatutin E.I., Kochemazov S.E., Zaikin O.S. Applying volunteer and parallel computing for enumerating diagonal Latin squares of order 9, *Proc. of The Eleventh International Conference on Parallel Computational Technologies, Vol. 753 of Communications in Computer and Information Science*. Springer, 2017, pp. 114-129.
5. Kochemazov S., Zaikin O., Vatutin E., Belyshev A. Enumerating diagonal latin squares of order up to 9, *Journal of Integer Sequences*, 2020, Vol. 23, No. 1, pp. 2012.
6. Vatutin E.I., Belyshev A.D., Nikitina N.N., Manzyuk M.O. Ispol'zovanie X-obraznykh diagonal'nykh zapolneniy i ESODLS CMS skhem dlya perechisleniya glavnykh klassov diagonal'nykh latinskikh kvadratov [Use of X-based diagonal fillings and ESODLS CMS schemes for enumeration of main classes of diagonal Latin squares], *Telekommunikatsii* [Telecommunications], 2023, No. 1, pp. 2-16.
7. Vatutin E.I. O podschete glavnykh klassov tsiklicheskikh diagonal'nykh i pandiagonal'nykh latinskikh kvadratov [On the calculation of the main classes of cyclic diagonal and pandiagonal Latin squares], *Optiko-elektronnye pribory i ustroystva v sistemakh raspoznavaniya obrazov i obrabotki izobrazheniy* [Optical-electronic instruments and devices in pattern recognition and image processing systems], 2021, pp. 77-79.
8. Bell J., Stevens B. Constructing orthogonal pandiagonal Latin squares and panmagic squares from modular n-queens solutions, *Journal of Combinatorial Designs*, 2007, No. 15 (3), pp. 221-234.
9. Hedayat A. A complete solution to the existence and nonexistence of Knut Vik designs and orthogonal Knut Vik designs, *Journal of Combinatorial Theory, Series A*, 1977, No. 22 (3), pp. 331-337.
10. Atkin A.O.L., Hay L., Larson R.G. Enumeration and construction of pandiagonal Latin squares of prime order, *Computers & Mathematics with Applications*, 1983, No. 9 (2), pp. 267-292.

11. Vik K. Bedømmelse av feilene på forsøksfelter med og uten målestokk. – 1924.
12. Stoffel A. Totally diagonal Latin squares, *Stud Cerc Mat.*, 1976, Vol. 28, pp. 113-119.
13. Chang G.J., Hwang F.K. Diagonal and Pandiagonal Tournament Latin Squares, *European Journal of Combinatorics*, 1985, Vol. 6, No. 2, pp. 149-155.
14. Dabbagian V., Wu T. Constructing non-cyclic pandiagonal Latin squares of prime orders, *Journal of Discrete Algorithms*, 2015, No. 30, pp. 70-77.
15. Vatutin E.I. Spetsial'nye vidy diagonal'nykh latinskikh kvadratov [Special types of diagonal Latin squares], *Oblachnye i raspredelennye vychislitel'nye sistemy v elektronnom upravlenii ORVSEU - 2022 v ramkakh Natsional'nogo superkomp'yuternogo foruma (NSKF – 2022)* [Cloud and distributed computing systems in the electronic management of ORVSEU - 2022 within the framework of the National Supercomputing Forum (NSCF - 2022)], 2022, pp. 9-18.
16. Vatutin E., Nikitina N., Belyshev A., Manzyuk M. On polynomial reduction of problems based on diagonal Latin squares to the exact cover problem, *CEUR Workshop*, 2020, pp. 289-297.
17. Vatutin E., Belyshev A., Manzyuk M., Nikitina N. Evaluation of Efficiency of Using Simple Transformations When Searching for Orthogonal Diagonal Latin Squares of Order 10, *Communications in Computer and Information Science*, 2020, Vol. 1304, pp. 127-146.
18. Al'bert'yan A.M., Kurochkin I.I., Vatutin E.I. Ispolzovanie geterogennykh vychislitel'nykh kompleksov v grid-sistemakh iz personal'nykh komp'yuteroi [The use of heterogeneous computing complexes in grid systems of personal computers], *XIV Vserossiyskaya mul'tikonferentsiya po problemam upravleniya MKPU-2021* [XIV All-Russian Multiconference on Control Problems MKPU-2021], 2021, pp. 90-93.
19. Nikitina N.N., Vatutin E.I., Manzyuk M.O. [i dr.]. Pokazateli i tekhnologicheskaya osnova proektov raspredelennykh vychisleniy Rakesearch i Sidock@home [Metrics and technological basis of distributed computing projects Rakesearch and Sidock@home], *Oblachnye i raspredelennye vychislitel'nye sistemy v elektronnom upravlenii ORVSEU - 2022 v ramkakh Natsional'nogo superkomp'yuternogo foruma (NSKF - 2022)* [Cloud and distributed computing systems in the electronic management of ORVSEU - 2022 within the framework of the National Supercomputing Forum (NSCF - 2022)], 2022, pp. 38-46.
20. Manzyuk M., Nikitina N., Vatutin E. Start-up and the Results of the Volunteer Computing Project RakeSearch, *Communications in Computer and Information Science*, 2019, Vol. 1129, pp. 725-734.

Статью рекомендовал к опубликованию д.т.н., профессор Ю.А. Кравченко.

Новиков Александр Олегович – Юго-Западный государственный университет; e-mail: alexnov4616@gmail.com; г. Курск, Россия; кафедра вычислительной техники; магистрант.

Ватутин Эдуард Игоревич – e-mail: evatutin@rambler.ru; кафедра вычислительной техники; д.т.н.; профессор.

Егоров Сергей Иванович – e-mail: sie58@mail.ru; кафедра вычислительной техники; д.т.н.; профессор.

Титов Виталий Семенович – e-mail: vt.swsu@yandex.ru; кафедра вычислительной техники; д.т.н.; профессор.

Novikov Aleksandr Olegovich – South-West State University; e-mail: alexnov4616@gmail.com; Kursk, Russia; the Department of Computer Science; master student.

Vatutin Eduard Igorevich – e-mail: evatutin@rambler.ru; the Department of Computer Science; dr. of eng. sc.; professor.

Egorov Sergei Ivanovich – e-mail: sie58@mail.ru; the Department of Computer Science; dr. of eng. sc.; professor.

Titov Vitalii Semenovich – e-mail: vt.swsu@yandex.ru; the Department of Computer Science; dr. of eng. sc.; professor.