ВЕСТНИК ОШСКОГО ГОСУДАРСТВЕННОГО УНИВЕРСИТЕТА
МАТЕМАТИКА, ФИЗИКА, ТЕХНИКА. 2023, №2

МАТЕМАТИКА

УДК 512.643
https://doi.org/10.52754/16948645_2023_2_56

МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ МАГИЧЕСКИХ КВАДРАТОВ ВЫСОКОГО ПОРЯДКА И ИХ ПРИЛОЖЕНИЯ К ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Байзаков Асан Байзакович, д.ф.-м.н., профессор
asan_baizakov@mail.ru
Шаршенбеков Мирлан Маликович, научный сотрудник
Айтбаев Кубат Асаналиевич, к.ф.-м.н.
Момбеков Алымбек Джаманкулович, Академик Академии народной медицины Республики Коми РФ
Институт математики Национальной Академии наук Кыргызской Республики
Бишкек, Кыргызстан

Аннотация: *Выявлено, что основным математическим аппаратом построения магических квадратов (М-матриц) высокого порядка, является арифметическая прогрессия. В силу свойств констант квадратов как члена арифметическая прогрессия получаем возможность построения матриц все более высокого порядка. Возможность получения многообразий М-матриц, например вращением подблоков, дает отличное условие применение магических квадратов высокого порядка к информационной безопасности, в частности в криптографии.*

Ключевые слова: *Магический квадрат, квадратные блочные матрицы, константа квадрата, арифметическая прогрессия, члены арифметической прогрессии как идентификаторы.*

ЖОГОРКУ ТАРТИПТЕГИ МАГИЯЛЫК КВАДРАТТАРДЫН МАТЕМАТИКАЛЫК МОДЕЛДЕШТИРИЛИШИ ЖАНА АЛАРДЫН МААЛЫМАТ КООПСУЗДУГУНДА КОЛДОНУЛУШУ

Байзаков Асан Байзакович, ф.-м.и.д., профессор
asan_baizakov@mail.ru
Шаршенбеков Мирлан Маликович, илимий кызматкер
Айтбаев Кубат Асаналиевич, ф.-м.и.к.,
Момбеков Алымбек Джаманкулович, Академик Академии народной медицины Республики Коми РФ
Кыргыз Республикасынын Улуттук илимдер Академиясы математика Институту
Бишкек, Кыргызстан

Аннотация: *Жогорку тартиптеги магиялык квадраттарды (М-матрицаларды) куруунун негизги математикалык аппараты арифметикалык прогрессия экени аныкталган. Арифметикалык прогрессиянын мүчөсү катары квадраттардын константаларынын касиеттеринин аркасында биз барган сайын жогору даражадагы матрицаларды куруу мүмкүнчүлүгүнө ээ болобуз. М-матрицалардын ар башка түрлөрүн алуу мүмкүнчүлүгү, мисалы, ички блокторду айлантуу жолу менен, маалыматтын коопсуздугуна, атап айтканда криптографияга жогорку тартиптеги магиялык квадраттарды колдонуу үчүн эң сонун шарт түзөт.*

Урунттуу сөздөр: *Магиялык квадрат, квадраттык блок матрицалары, квадраттык константа, арифметикалык прогрессия, идентификатор катары арифметикалык прогрессиянын мүчөлөрү.*

MATHEMATICAL MODELING OF HIGH ORDER MAGIC SQUARES AND THEIR APPLICATIONS TO INFORMATION SECURITY

Baizakov Asan Baizakovich, Doctor of Physical and Mathematical Sciences, Professor
asan_baizakov@mail.ru
Sharshenbekov Mirlan Malikovich, researcher
Aitbaev Kubat Asanalievich, Candidate of Physical and Mathematical Sciences
Mombekov Alymbek Dzhamankulovich,
Academician of the Academy of Traditional Medicine of the Komi Republic of the Russian Federation
Institute of Mathematics of the National Academy of Sciences of the Kyrgyz Republic

Abstract:: *It is revealed that the main mathematical apparatus for constructing magic squares (M-matrices) of high order is an arithmetic progression. By virtue of the properties of the constants of squares as a member of an arithmetic progression, we obtain the possibility of constructing matrices of ever higher order. The possibility of obtaining varieties of M-matrices, for example, by rotating sub-blocks, provides an excellent condition for applying high-order magic squares to information security, in particular in cryptography.*

Keywords: *Magic square, square block matrices, square constant, arithmetic progression, members of an arithmetic progression as identifiers.*

Постановка задачи

Метод декомпозиции широко применяется в науке и практике. Он приводит к достижению цели, если целью удается расчленить на независимые друг от друга части, поскольку в этом случае их отдельное рассмотрение позволяет правильное представление об их вкладе в общий эффект. Французский математик Р. Декарт писал: «Расчлените каждую изучаемую вами задачу на столько частей, сколько потребуется, чтобы их было легко решить».

Наша цель построить M матрицу высокого порядка, например, матрицу 48го порядка применяя вышеуказанный метод, т.е. разместить натуральные числа от 1 до 2304 ($48^2 = 2304$) в M матрицу 48 порядка, так, чтобы S константа квадрата (магическое число) был 55320:

$$S = \frac{n^2+1}{2} \cdot n = \frac{48^2+1}{2} \cdot 48 = 55320 .$$

Будем использовать обозначение: N -множество натуральных чисел; R -множество действительных чисел; C -комплексное поле.

Определение 1. Квадратная матрица $A = (a_{ij})_{i,j=1}^{n}$ называется M матрицей, если $a_{ij} \in N,\ i, j = \overline{1,\ n}$ причем выполнены следующие условия:

1) Все n^2 числа $a_{ij} \in N,\ i, j = \overline{1,\ n}$ различны и являются элементом подмножества $N_m \subset N$, последовательно расположенных n^2 чисел от $m+1$, до $m+n^2$ в множестве N;

2) $\sum_{i=1} a_{ij} = S,\ \forall j = \overline{1,n},\ \sum_{j=1} a_{ij} = S,\ \forall i = \overline{1,n}, \sum_{i=1}^{n} a_{ij} = S,\ \sum_{i+j=n+1} a_{ij} = S$.

Определение 2. Матрица $A = (a_{ij})_{i,j=1}^{n}$ называется M_1 матрицей, если $a_{ij} \in R,\ i, j = \overline{1,\ n}$, причем выполнены следующие условия:

1) Все n^2 числа $a_{ij},\ i, j = \overline{1,\ n}$ различны и является элементом подмножества $R_m \in R$ (множество действительных чисел);

2) $\sum_{i=1} a_{ij} = S,\ \forall j = \overline{1,n},\ \sum_{j=1}^{n} a_{ij} = S,\ \forall i = \overline{1,n}, \sum_{i=1}^{n} a_{ij} = S,\ \sum_{i+j=n+1} a_{ij} = S$.

По определению ясно, что M матрицы являются подмножеством M_1 матриц.

Будем исходить из того, что M матрицы 3 и 4го порядка нами построены, например,

$$\begin{pmatrix} 6 & 7 & 2 \\ 1 & 5 & 9 \\ 8 & 3 & 4 \end{pmatrix}, \text{ (а)} \qquad \begin{pmatrix} 13 & 2 & 12 & 7 \\ 16 & 3 & 9 & 6 \\ 1 & 14 & 8 & 11 \\ 4 & 15 & 5 & 10 \end{pmatrix}. \text{ (б)} \tag{1}$$

Можно будет использовать и другие виды M матриц 3 и 4го порядка. Как известно, количество M матриц 3го порядка -8, а M -матриц 4го порядка -880, а M -матриц 5го порядка -более 1 000 000.

Свойства констант квадратов в M матрицах

Теорема 1. Пусть A - M матрица с константой квадрата S. Тогда число S является собственным значением M матрицы A, с соответствующим собственным вектором

$$\vec{x} = c \cdot colon(1, 1, 1),$$

где c -произвольная константа.

Доказательство.

Для определенности будем считать, что $c = 1$. Тогда равенство

$$A\vec{x} = S\vec{x}$$

будет выполняться в силу определения 1 M матрицы. Что и требовалась доказать.

Например, для M матрицы (1) (или (2)) число 15 (соответственно число 34) является собственным числом, а собственный вектор $\vec{x} = c \cdot colon(1, 1, 1)$ (соответственно $\vec{x} = c \cdot colon(1, 1, 1, 1)$).

Теорема 2. Пусть последовательность, $\{a_i, i \in N\}$ некоторая арифметическая прогрессия, где $a_i \in R$. Выделим из этой арифметической прогрессии подмножество R_m последовательна расположенных n^2 членов: от a_{m+1} до a_{m+n^2}. Тогда из этих членов можно построить M_1 матрицу n го порядка.

Доказательство. Для ясности пусть $m = 0$. Так как $a_j,\ j = \overline{1,\ n^2}$ член арифметической прогрессии то в M матрице nго порядка натуральных чисел от 1 до n^2 вместе натурального числа j расположим член a_j. Тогда константа квадрата полученной M_1 матрица вычисляется по формуле

$$S = \left[\frac{a_1 + a_{n^2}}{2} \cdot n^2 \right] \frac{1}{n}$$

или

$$S = \frac{2a_1 + d(n^2 - 1)}{2} \cdot n\,. \qquad (2)$$

Что и требовалась доказать.

Например, M матрица вида

$$\begin{pmatrix} 32 & 37 & 12 \\ 7 & 27 & 47 \\ 42 & 17 & 22 \end{pmatrix}$$

по формуле (2), где $a_1 = 7,\ d = 5,\ n = 3$ имеет константу квадрата $S = 81$.

Теорема 3. Если A - M матрица, $D_m = (m)_{ij=1}^{n}$ постоянная матрица, то $A \pm D_m$ так же будет M матрицей. В этом случае константа квадрата определяется формулой:

$$S = S_A \pm mn\,, \qquad (3)$$

S_A-константа квадрат матрицы A.

Доказательство данной теоремы проводится с использованием формулы суммы арифметической прогрессии.

Так же следует отметить, что в M_1 матрице элементами могут быть и вещественные (комплексные) числа, являющиеся членами арифметической прогрессии.

Например, матрицы вида

$$\begin{pmatrix} -9 & -16 & -6 & -3 \\ -5 & -4 & -10 & -15 \\ -12 & -13 & -7 & -2 \\ -8 & -1 & -6 & -14 \end{pmatrix};$$

$$\begin{pmatrix} 1,6 & 1,9 & 0,4 \\ 0,1 & 1,3 & 2,5 \\ 2,2 & 0,7 & 1,0 \end{pmatrix};$$

$$\begin{pmatrix} 6+12i & 7+14i & 2+4i \\ 1+2i & 5+10i & 9+18i \\ 2+16i & 3+6i & 4+8i \end{pmatrix},$$

имеют соответственно константы квадрата равные:

$$S = -34;$$

$$S = 3,9;$$

$$S = 15 + 30i,\ \ i = \sqrt{-1}.$$

Построение M матриц высокого порядка

При построении M матриц высокого порядка будет использовать M матрицу низкого порядка и свойства арифметической прогрессии констант квадрата.

Пример 1. Согласно методу декомпозиции определим дерево целей следующим образом

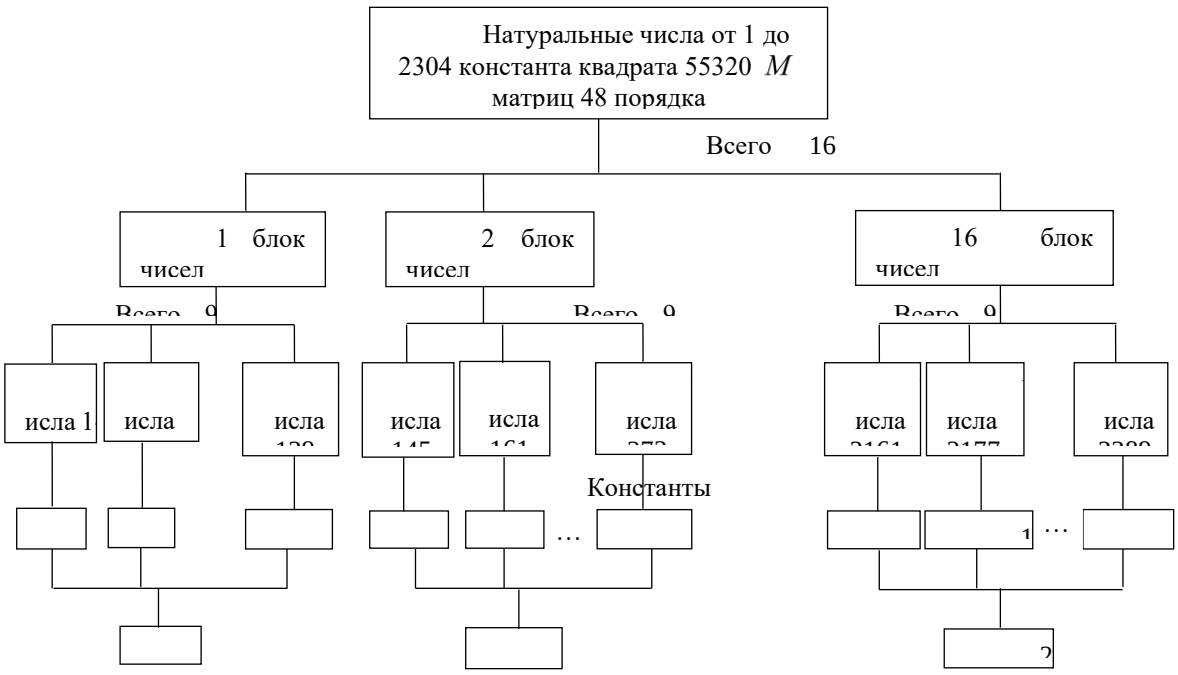

Рис. 1. Блок-схема построения M матрицы 48 порядка

Теперь начинаем с 1го подблока 1го блока. В нем находятся числа от 1 до 16. Из них можно построить M матрицу 4 порядка в частности как (2), с константой квадрата $S = 34$. Далее из 2го подблока 1го блока построим M матрицу в силу теоремы 3 $m = 16$, с константой квадрата

$$S = S_A + 16 \cdot 4 = 34 + 64 = 98,$$

и т.д.

9 подблок 1 блока имеет константу квадрата $S = 34 + 128 \cdot 4 = 546$ и самый последний подблок 9 блока имеет константу квадрата $S = 34 + 2288 \cdot 4 = 9186$. Отметим, что константы квадратов подблоков 1го блока сами образуют арифметическую прогрессию $\{a_i,\ a_1 = 34,\ i = \overline{1, 9},\ A = 64\}$: 34, 98, … , 546. В силу магичности каждая константа квадрата выступает как от имени подблока. Тогда по теореме 2 мы можем построить M матрицу 3го порядка по образцу (1) с константой квадрата равной 870 ($n = 3$): $S = \dfrac{2 \cdot 34 + 64 \cdot 8}{2} \cdot 3 = 870$ (см. рис 1).

Итак, 1 блок есть M блок матрица 12го порядка с общей константой квадрата 870, т.е. 1 блок можно рассмотреть как одно число 870.

Аналогично, константы квадратов подблоков 2го блока так же образуют арифметическую прогрессию $\{a_i,\ a_1 = 610,\ i = \overline{1, 9},\ A = 64\}$. Для констант квадратов подблоков 2го блока можем построить по образцу (1) M матрицу 3го порядка, с константой квадрата

$$S = \frac{2 \cdot 610 + 64 \cdot 8}{2} \cdot 3 = 2598,$$

или по формуле (3)

$$S = S_A \pm mn = 870 + 144 \cdot 12 = 2598.$$

Повторяя точно такие же алгоритмы с константами квадратов во всех остальных 14 M блоков, окончательно получим 16 членов арифметической прогрессии 870, 2598, … ,

26790, т.е. $a_n = a_1 + d(n-1)$, где $a_1 = 870,\ d = 1728,\ n = \overline{1,\ 16}$.

Теперь эти 16 чисел констант квадратов мы расположим, в частности, на M матрицу по образцу (1) (можно их построить в другом виде).

Далее вместо каждой константы квадрата рассматриваем как идентификаторы и выпишем соответствующие M блоки матриц с M_1 матрицами (подблоки) и получим искомую M матрицу 48 порядка.

Так же отметим, что множество значений констант квадратов моделируется разностным уравнением второго порядка вида

$$u_{n+2} = 2u_{n+1} - u_n, \quad n \geq 1 \tag{4}$$

с начальными условиями

$$\begin{aligned} &а) \quad u_1 = 34, \quad u_2 = 98; \\ &б) \quad u_1 = 870, \quad u_2 = 2598. \end{aligned} \tag{5}$$

Согласно методу Эйлера общее решение уравнения (4) имеет вид

$$u(n) = c_1 + c_2 n$$

так как корни характеристического уравнения $\lambda^2 - 2\lambda + 1 = 0:\ \lambda_1 = \lambda_2 = 1$ совпадают.

Тогда, решение задачи Коши (4), (5), а), б) имеет вид

$$\begin{aligned} &а) \quad u(n) = -30 + 64n; \\ &б) \quad u(n) = -858 + 1728n. \end{aligned} \tag{6}$$

В силу (6) а) получаем значения (5)

$u(1) = 34,\ u(2) = 98,\ ...,\ u(143) = 9122,\ u(144) = 9186,$

и в силу (6) б) имеем

$u(1) = 870,\ u(2) = 2598,\ ...,\ u(15) = 25062,\ u(16) = 26790$.

Топологическая структура и свойства M матриц

Пусть нами построена M матрица n-го порядка A. Для ясности в дальнейшем матрицу A представим в виде магического квадрата и обозначим опять через A.

Произведем гомеоморфное отображение $f : A \to B$, где B кольцо и верхняя сторона квадрата взаимно однозначно и непрерывно отображается в границу окружность внешнего круга, а нижняя сторона квадрата отображается в окружность внутреннего круга. Ясно, что при этом строки M матрицы однозначно и непрерывно преобразуется в параллели, а столбцы в меридианы. И поэтому константа квадрата сохраняется для каждой параллели, и для каждой меридианы. Далее, в этом случае обнаруживается новое свойство кольца. В кольце появляются спирали, для которых так же сохраняется константа квадрата. Причем половина из них вращаются по часовой стрелке, остальные против часовой стрелке (см. рис. 2).

Эти дополнительные сверх свойства M матриц можно обнаружить следующим образом. Если к нему приставить справа такую же M матрицу, то при суммировании по всем диагональным направлениям получаем константу квадрата, а их оказывается всего 4 два из них сверху вниз, и 2 снизу вверх.

$$\begin{array}{c} \searrow\ \searrow\ \searrow\ \searrow \\ \left(\begin{array}{cccc||cccc} 13 & 2 & 12 & 7 & 13 & 2 & 12 & 7 \\ 16 & 3 & 9 & 6 & 16 & 3 & 9 & 6 \\ 1 & 14 & 8 & 11 & 1 & 14 & 8 & 11 \\ 4 & 15 & 5 & 10 & 4 & 15 & 5 & 10 \end{array}\right) \\ \nearrow\ \nearrow\ \nearrow\ \nearrow \end{array}$$

Проверим для M матриц 5го порядка.

$$\begin{array}{c} \searrow\ \searrow\ \searrow\ \searrow\ \searrow \\ \left(\begin{array}{ccccc||ccccc} 16 & 5 & 14 & 23 & 7 & 16 & 5 & 14 & 23 & 7 \\ 24 & 8 & 17 & 1 & 15 & 24 & 8 & 17 & 1 & 15 \\ 2 & 11 & 25 & 9 & 18 & 2 & 11 & 25 & 9 & 18 \\ 10 & 19 & 3 & 12 & 21 & 10 & 19 & 3 & 12 & 21 \\ 13 & 22 & 6 & 20 & 4 & 13 & 22 & 6 & 20 & 4 \end{array}\right) \\ \nearrow\ \nearrow\ \nearrow\ \nearrow\ \nearrow \end{array}$$

В этом случае число констант квадратов по диагональным направлениям равно $2\cdot 5=10$, 5 из них сверху вниз и 5 снизу вверх.

Очевидно, что при топологическом преобразовании M матриц в кольцо, эти диагональные направления и дают спирали, вращающиеся как по часовой стрелке, так и против часовой стрелке.

Приложения

Рис.1. Фрагмент M матрицы 48 порядка с константой 870

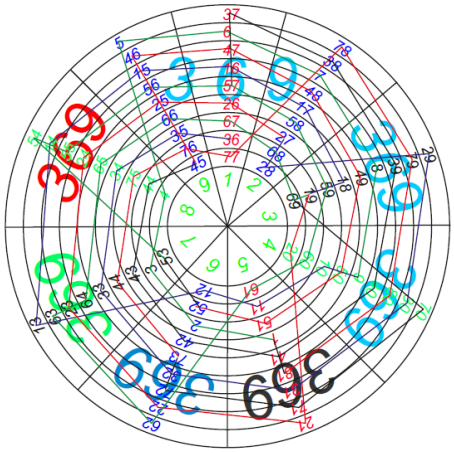

Рис.2. Топологическая структура M матрицы 9-го порядка.

Актуальностью построения M матриц высокого порядка обусловливается ее применением в информационной безопасности, а именно в криптографии.

ЛИТЕРАТУРА

1. Байзаков А.Б., Момбеков А.Д., Айтбаев К.А. О разнообразии констант квадратов в подблоках при декомпозиции матриц // Доклады НАН КР, Бищкек, 2017. №2. – С.19-24.
2. Байзаков А.Б., Момбеков А.Д. О некоторых свойствах квадратных матриц, сохраняющих симметрию // Известия НАН КР, Бишкек, 2018. – С.1-14
3. Байзаков А.Б., Момбеков А.Д. О принципе сохранения симметрий во вложенных М матрицах // II Борубаевкие чтения, Бищкек, 1 март, 2018, с.21.
4. Байзаков А.Б., Момбеков А.Д. О некоторых свойствах квадратных матриц, сохраняющих симметрию // Известия НАН КР, Бишкек, 2018. №3. – С19-30.
5. Baizakov A.B., Mombekov F.D., Sharshenbekov M.M. On the properties of the squared constants in block M matrices // Abstract:s of international conference Matematicial analysis, differential equations. – Issyk-Kul, Kyrgyz Repuplik. 2018. – P.37.
6. Борубаев А.А., Байзаков А.Б. Математические модели построения и выявления свойств магических матриц высокого порядка // Авторское свидетельство №3754 Кыргызпатента об авторском праве. – 28.11.2019.
7. Baizakov A.B., Sharshenbekov M.M., Aitbaev K.A. Magic square: Terms of arithmetic progression – identifiers // Вестник Института математики НАН КР, 2022, №1, – С.77-81.
8. Baizakov A.B., Mombekov A.J., Sharshenbekov M.M. Creation of the database of low-order M-matrices is on important step of the decomposition method // Вестник Института математики НАН КР, 2022. №2. – С.65-68.
9. Байзаков А.Б., Айтбаев К.А., Шаршенбеков М.М. Компьютерное моделирование магических квадратов нечетного порядка методом террас и ее применение в криптографии // Известия НАН КР. – Бишкек, – 2020, №4, – С51-58.
10. Байзаков А.Б., Момбеков А.Дж., Шаршенбиев Б. Сантоку. Логикалык тапшырмалар Бищкек, «Кыргыз Жер», 2020, – 192 б. (с грифом МНО КР)
11. Байзаков А.Б., Айтбаев К.А., Шаршенбеков М.М. Magic square: Terms of arithmetic progression – identifiers // Авторское свидетельство №5075 Кыргызпатента об авторском праве. – 21.12.2022..
12. Кордемский Б.А. Математическая смекалка. – М.: ГИТТЛ, 1959. – 576 с.
13. Гантмахер Ф.Т. Теория матриц. – М.: Наука, 1988. – 552с.

14. Ланкастер П. Теория матриц. -пер. с англ. – М.: Наука, 1978. – 280 с.
15. Колмогоров А.Н., Фомин С.В. Элементы теории функций и функционального анализа. – М.: Наука, 1972. – 544 с.
16. Ю. В. Чебраков. Теория магических матриц. Выпуск ТММ-1. – С. –Петербург, 2008
17. Heinz H. Magic Squares, Magic Stars & Other Patterns. – Last updated Nov 2009. – http: // www.magic-squares.net/