УДК 512.643.8

М-МАТРИЦА 22-ГО ПОРЯДКА

Ю. Н. Балонин,
инженер
М. Б. Сергеев,
доктор техн. наук, профессор
Санкт-Петербургский государственный университет аэрокосмического приборостроения

Публикуется отсутствующая в ряде С-матриц шестиуровневая ортогональная матрица 22-го порядка с минимальным по норме максимальным элементом. Рассматриваются ее свойства, приводится анализ системы алгебраических уравнений для значений ее элементов, указываются метод нахождения матрицы и дополнительные неоптимальные решения, близкие по структуре к матрицам Белевича.

Ключевые слова *— минимаксные матрицы, матрицы Адамара, матрицы Белевича.*

В работах [1, 2] описан класс минимаксных М-матриц, являющихся ортогональными матрицами с минимальным по норме максимальным элементом. Важными представителями этого класса являются матрицы Адамара и Белевича.

Напомним, матрица Адамара — квадратная матрица $\mathbf{A}$ размерности n, кратной 4, состоящая из чисел ±1, столбцы которой ортогональны:

$$\mathbf{A}^{\mathrm{T}}\mathbf{A} = n\mathbf{I},$$

где $\mathbf{I}$ — единичная матрица. Величина максимального элемента (m-норма) ортонормированной матрицы определяется как $m = 1/\sqrt{n}$. Матрица одноуровневая.

Матрица Белевича (конференц-матрица, или С-матрица) — квадратная матрица размерности, кратной 2, с нулевой диагональю и остальными элементами, равными ±1, обладающая свойством

$$\mathbf{C}^{\mathrm{T}}\mathbf{C} = (n-1)\mathbf{I}.$$

Норма матрицы $m = 1/\sqrt{(n-1)}$. Матрица двухуровневая.

В работе [1] сформулирован универсальный алгоритм поиска М-матриц, результативность которого зависит от порядка n матрицы, а также опубликованы матрицы порядков 3, 5, 7, 9, 11, пропущенные в последовательности матриц Адамара и Белевича. М-матрицы 13-го порядка (M_{13}) и старше предположительно являются хаотическими, что не исключает существования так называемых регулярных квазиоптимальных уровневых матриц и матриц особых порядков.

Ввиду сложности поиска матриц Адамара высоких порядков в научной литературе осуществляется сетевой мониторинг и существует традиция публиковать вновь открытые матрицы [3]. Определенный вес этому придает практическая сфера приложения матриц Адамара к построению помехоустойчивых и защищенных кодов. Согласно данным [3], к 2004 г. были опубликованы все матрицы Адамара до 428-го порядка включительно (найдена Kharaghani и Tayfeh-Rezaie), первая следующая неизвестная матрица имеет порядок 668.

М-матрицы нечетных порядков и матрицы пропущенных четных порядков изучены значительно хуже. Отмеченные пропуски связаны с классическими проблемами теории чисел. Впервые это обстоятельство в 1950 г. обнаружил Витольд Белевич [4]. Он ввел математическое понятие конференц-матриц (С-матриц), называемых так по причине их изначального возникновения в задачах объединения в единую систему идеальных трансформаторов. Оказывается, что из-за расщепления сигнала между абонентами необходимым условием отсутствия диссипации (потерь энергии) является существование определенных им квадратных матриц. Возникнув в инженерных задачах, матрицы быстро нашли применение в областях, которые представляют интерес для математики. Нахождение конференции матриц не тривиальная задача, поскольку они существуют не для всех значений n. Порядки, для которых они существуют, всегда представимы в виде $2k + 2$ (где k — целое), но это само по себе не является достаточным условием [5]. Так, С-матрицы существуют для n = 2, 6, 10, 14, 18, 26, 30, 38 и 42, но не существуют для n = 22 или n = 34.

Белевичем были получены С-матрицы для n до 38, он также отметил, что для $n = 66$ имеется несколько вариантов таких матриц.

Пропуски 22 и 34 хорошо известны в теории чисел. Заинтересовавшись теоремой Ферма, математик из Петербурга Л. Эйлер потратил 7 лет на разбор задачи, связанной с представлением чисел суммой квадратов. Сформулированная им теорема, несомненно, принадлежит к числу высших достижений математики XVII–XVIII вв. В виде суммы двух квадратов представимы все числа, в разложение которых на простые множители все простые вида $4k + 3$ входят в четных степенях (недопустимы множители 3, 7, 11 и т. п.). Особенность матрицы 22-го порядка состоит в том, что множителями $n - 1 = 21$ являются числа 3 и 7. То же самое касается порядка 34: множителями $n - 1 = 33$ являются числа 3 и 11.

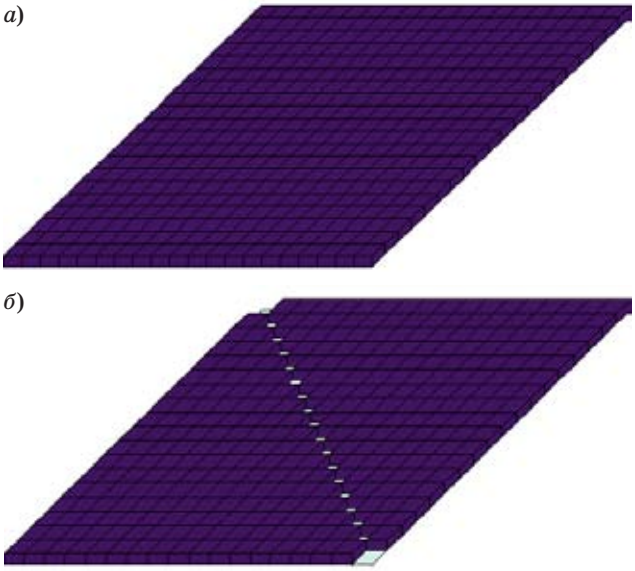
Проблемы теории чисел относятся к труднейшим, на их доказательства уходят, как у Эйлера, годы, а то и десятки лет. Совпадения исключений Белевича с указанными Эйлером случаями неразложимости чисел связывают между собой довольно разные объекты — числа и матрицы. Если матрица Белевича не существует, возникает закономерный вопрос: что же замещает ее? Решение в классе М-матриц, обобщающих матрицы Адамара и Белевича, имеет значение как для теории матриц, так и для теории чисел, поскольку объекты соотносимы. Именно поэтому вопрос поиска М-матриц 22-го, 34-го и подобных порядков приобретает особое звучание. Они восполняют пропуски в указанном выше ряде С-матриц. Поиск матриц более высоких порядков сложен ввиду ограничения универсального алгоритма. С ростом размерности задачи наиболее частым итогом является хаотическая матрица [1].

Цель настоящей работы состоит в публикации найденной шестиуровневой нехаотической матрицы M_{22}.

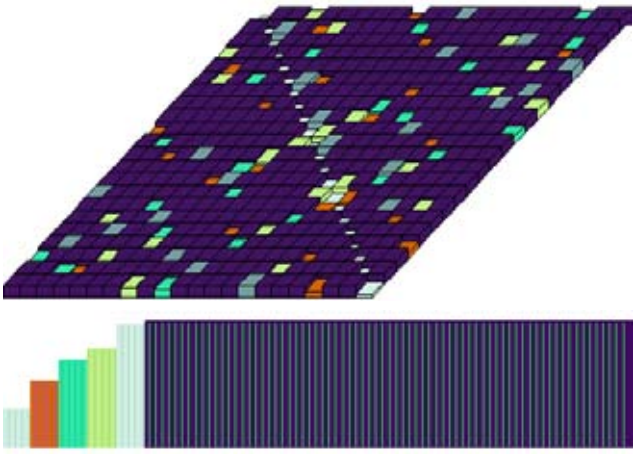
Структуры матриц Адамара и Белевича приведены на рис. 1, показаны абсолютные значения элементов.

Уровневая структура найденной с использованием алгоритма из работы [1] минимаксной ортогональной матрицы M_{22} приведена на рис. 2, показаны абсолютные значения элементов уровней.

Найденная матрица M_{22} имеет 6 уровней, обозначенных снизу вверх как a, b, c, d, e, f. Значения элементов уровней следующие: a=0.307566, b=0.529895, c=0.692434, d=0.784526, e=0.980202, f=1. В математике особое значение имеют симметричные структуры. Заметим, что приведенная матрица близка к симметричной, однако симметрию модулей ее элементов нарушает только слой элементов e. Это указывает на возможность поиска иного решения, но пока найденная матрица минимальна по m-норме.



■ ***Рис. 1.*** *Структуры матриц Адамара* (*а*) *и Белевича* (*б*)



■ ***Рис. 2.*** *Структура матрицы M_{22} с пятью нижними уровнями по 22 элемента*

Элементы уровней матрицы обладают известной еще Эйлеру особенностью латинских квадратов: 22 элемента каждого из уровней, отличного от верхнего (f), расположены в строках и столбцах ее без пересечений: нет двух элементов с одинаковым значением у них индекса строки или столбца.

Регулярная М-матрица, таким образом, представляет собой недостроенный латинский квадрат. После эквивалентных преобразований перестановкой строк и столбцов любой ее уровень можно рассматривать как диагональный, что является характерной чертой матриц Белевича с нулевой диагональю.

Существует также некоторое подобие M_{22} ранее найденным [1] матрицам M_3 и M_7 (порядки,

равные множителям 21). К особенностям решения стоит отнести корреляцию числа слоев M_{11} и M_{22} — их 6. Однако матрица порядка 22, найденная из M_{11} по правилу Сильвестра [1], не сводима к указанной, поскольку ее уровни имеют не по 22, а по 44 элемента. Найденная матрица M_{22} имеет заметно меньшую m-норму [6].

Элементы матриц Адамара, Белевича и М-матриц малых порядков отвечают целочисленным решениям системы диофантовых квадратичных уравнений. С ростом размерности задачи в решения приходится включать иррациональность — обобщение понятия целочисленности создателем теории алгебраических чисел Эрнстом Кумером позволило ему в свое время указать на ошибки попыток доказательств теоремы Ферма математиками Французской академии О. Коши и Г. Ламе [7].

Условие ортогональности столбцов приводит к системе аналитических уравнений:

$$a+c-f=0;$$
$$2af+2bf-cd+cf-df+2ef-3f^2=0;$$
$$2af+bd+bf-2cf+df-2ef+f^2=0;$$
$$ae-af-2bf-2cf-2df-ef+5f^2=0;$$
$$2af-bc+bf+cf+2df+2ef-5f^2=0.$$

Из $a+c=f$, $f=1$ находим $c=1-a$. Выражая $2e=4a++b+bd+d-1$, получаем

$$a(4a-3)+(a-5)(b+bd+d)+4bd+7=0,$$
$$a(5+d)+bd+3b-d-3=0,\ a(5+b)+bd+3d+b-5=0.$$

Это квадратное уравнение и два линейных уравнения, из которых находим выражения для $a=3+(d+b-2)/(d-b)$ и $d=0{,}5(b^2-2b-15\pm(b^4+8b^3+38b^2++184b+345)^{1/2})/(b+3)$. Подставляя в линейное уравнение и решая его, получим в итоге значения уровней матрицы:

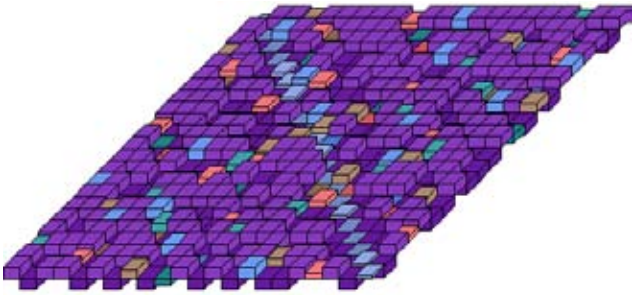
$$a=0.307566,\ b=0.529895,\ d=0.784526,$$

а также неоптимальные (в смысле m-нормы) решения $a=3.05985$, $b=-2.79873$, $d=5.28235$ и $a=3.20158$, $b=4.31117$, $d=-3.98317$, помимо комплексных корней. Параметры c, e находим из уравнений связи. Неоптимальные варианты интересны тем, что итерации с ними устойчивы и позволяют находить новые квазиоптимальные уровневые матрицы.

Заметим, что из всех уравнений только одно квадратное уравнение противоречит условию a=0, b=1, c=1, d=1, e=1, f=1 — получению матрицы Белевича.

Дополнительное исследование позволяет найти в окрестности указанного решения с нормой $m=0.2269$ две квазиоптимальные шестиуровневые матрицы иной структуры с нормой $m=0.2271$, у которых нижний уровень стремится к 0. В обоих случаях значение a=0 аналитически недостижимо. В лучшем случае (наилучшее приближение к матрице Белевича) имеем $a=0.0053$, при этом $b=0.4022$, $c=0.7965$, $d=0.893$, $e=0.8982$, $f=1$. Более того, за понижение нижнего уровня приходится платить увеличением m-нормы. Именно это обстоятельство и выделяет указанную матрицу M_{22}. Она ближе к матрице Адамара с ее менее выраженной диагональю, поскольку иная структура при $n=22$ становится недостижимой, и анализ это подтверждает. Матрицы, близкие к матрице Белевича, — неоптимальны, наблюдается компромиссное решение.

Отметим, что подъем нижней диагонали порождает расщепление верхнего уровня с образованием четырех промежуточных ступеней — побочных диагоналей, поскольку перестановками матрица диагонализируется относительно любого слоя элементов a, b, c, d, e. Расщепление или бифуркация — характерная черта математических объектов детерминированного хаоса [1]. Итерации решения нелинейного (квадратического) уравнения, входящего в условие ортогональности, с понижением нормы максимального элемента порождают уровни-аттракторы.



a	f	f	d	f	f	f	f	f	b	f	f	e	f	f	f	f	f	f	c	f	f
f	-a	e	f	b	-d	f	f	f	-f	-c	-f	-f	-f	-f	f	f	-f	f	f	-f	-f
f	-f	-a	-f	f	-f	-f	f	f	f	-f	-b	f	f	f	-f	d	-e	-f	f	-c	f
d	f	-f	-a	-f	-c	f	-f	-f	-f	f	-f	-f	e	f	-f	f	-f	f	f	b	f
f	b	f	-f	a	-f	f	-f	-f	f	f	-f	f	-f	-f	c	f	f	-f	-d	-f	e
f	-d	-f	-c	-f	a	e	b	-f	f	-f	f	f	-f	-f	f	-f	-f	f	f	f	f
f	f	-f	f	f	-f	a	-f	-f	-f	-f	f	f	b	f	f	-f	c	-d	f	-e	-f
f	f	f	-f	-f	b	-f	-a	f	-f	-f	-f	-c	f	-f	f	-f	f	-f	e	f	d
f	f	f	-f	-f	-f	-f	f	-a	e	f	d	-b	f	c	f	-f	-f	f	-f	-f	-f
b	-f	f	-f	f	f	-f	-f	-f	-a	d	f	-f	-f	f	e	f	-f	-f	f	f	-c
f	-c	-f	f	f	-f	-f	f	d	a	-e	-f	-f	f	f	-f	b	f	-f	f	f	f
f	-f	-b	-f	e	f	f	-f	d	f	f	a	-f	f	-f	-f	-f	f	c	f	-f	-f
f	f	-f	f	-f	-f	-f	c	b	f	f	f	-a	-f	-f	-f	e	d	-f	f	f	-f
f	-f	f	-f	-f	-f	b	-e	f	-f	-f	f	f	-a	d	-f	c	f	f	-f	f	-f
e	f	-f	-f	f	f	-f	f	-c	-f	-f	f	-f	-d	-a	-b	f	f	f	-f	-f	f
f	f	-f	-f	c	f	f	f	f	-f	f	-f	f	-f	b	-a	-f	-f	-e	-f	d	-f
f	f	d	f	f	e	-f	-f	-f	f	-f	-f	f	c	-f	-f	a	-f	f	-b	f	-f
f	-f	f	e	f	-f	c	f	-f	-f	b	f	-d	f	-f	-f	-f	-a	-f	-f	f	f
f	-e	-f	f	-f	f	-d	-f	f	-f	f	c	f	f	-f	f	f	-f	-a	-f	-f	b
c	f	f	f	-d	f	f	-f	e	f	-f	f	-f	-f	f	-f	-b	-f	-f	-a	-f	f
f	-f	-c	b	-f	f	f	f	-f	f	-e	-f	-f	f	f	d	f	f	-f	-f	a	-f
f	-f	f	f	-f	f	-f	d	-f	-c	f	-f	f	-f	e	-f	-f	f	b	f	-f	a

■ ***Рис. 3.*** *Объемный и плоский портреты матрицы M_{22}*

В заключение отметим, что самостоятельно найти матрицу M_{22} крайне сложно. Отклонения на тысячные доли от найденных авторами статьи начальных значений сжатия и амплитуды элементов стартовой матрицы Гильберта, регламентирующих схождение алгоритма [1], приводят к хаотическим матрицам. Это при том, что сами по себе начальные значения порождены комбинаторной задачей с 2^{11} исходами, так как *m*-нормы сортируемых столбцов матрицы Гильберта, согласно используемому алгоритму, симметричны относительно центральной оси. Столбцы стартовой матрицы Гильберта должны быть переставлены в последовательности

q=[1 22 21 22 03 19 4 5 18 17 6 16 7 8 15 9 14 13 10 11 12].

Приведенный вектор перестановки q представляет собой 22-элементный ключ решения, которое крайне маловероятно получить случайно, что и определяет публикуемую матрицу (рис. 3) как базовую в практических приложениях, связанных с задачей построения защищенных кодов в системах передачи информации.

Литература

1. **Балонин Н. А., Сергеев М. Б.** М-матрицы // Информационно-управляющие системы. 2011. № 1. С. 14–21.
2. **Балонин Н. А., Мироновский Л. А.** Матрицы Адамара нечетного порядка // Информационно-управляющие системы. 2006. № 3. С. 46–50.
3. **Мониторинг** матриц Адамара. http://mathworld.wolfram.com/HadamardMatrix.html (дата обращения: 28.08.2011).
4. **Belevitch V.** Theorem of 2n-terminal networks with application to conference telephony // Electr. Commun. 1950. Vol. 26. P. 231–244.
5. **Van Lint J. H., Seidel J. J.** Equilateral point sets in elliptic geometry // Indagationes Mathematicae. 1966. Vol. 28. P. 335–348.
6. **Мониторинг** М-матриц. http://mathscinet.ru (дата обращения: 28.08.2011).
7. **Сингх С.** Великая теорема Ферма / пер. с англ. Ю. А. Данилова/ МЦНМО. — М., 2000. — 288 с.