УДК 004.421

АЛГОРИТМ И ПРОГРАММА ПОИСКА И ИССЛЕДОВАНИЯ М-МАТРИЦ

Ю.Н. Балонин, М.Б. Сергеев

Рассматриваются алгоритм и программный комплекс поиска и исследования матриц ортогональных базисов – минимаксных матриц (**M**-матриц). Приведена схема алгоритма, даны комментарии к блокам расчета, пояснен интерфейс программного комплекса MMatrix, разработанного с участием авторов статьи. Результатом работы универсального алгоритма являются матрицы Адамара, матрицы Белевича (**C**-матрицы, conference matrices) и матрицы, дополняющие указанные и близкие к ним по свойствам четных и нечетных порядков, в частности, матрица 22-го порядка, для которого **C**-матрицы не существует. Приведены примеры портретов найденных альтернативных матриц 255-го и 257-го порядков, отвечающих последовательностям чисел Мерсенна и Ферма. Пояснен новый путь получения матриц Адамара, отличный от ранее известных переборных процедур и процедур, опирающихся на вычисление символов Лагранжа, имеющий теоретическое и прикладное значения.

Ключевые слова: ортогональные матрицы, **M**-матрицы, матрицы Адамара, матрицы Мерсенна, матрицы Ферма, численные методы, алгоритм вычислений.

Введение

Для применения в процедурах построения помехоустойчивых и защитных кодов, в маскировании информации необходимы оригинальные ортогональные базисы [1, 2], поиск которых возможен в исследовательской программной среде. В настоящей работе описывается программный комплекс MMatrix, разработанный с участием авторов специально для этой цели и зарегистрированный под названием «Программа поиска **M**-матриц» [3]. Научная концепция построения матриц ортогональных базисов, обладающих экстремальными минимаксными свойствами, рассмотрена в работах [4–7].

В классе ортогональных матриц особое место занимают матрицы спектрального преобразования Фурье, определенные над полем вещественных или комплексных чисел. Деление весьма условно, поскольку, так же как и в случае жордановых матриц собственных значений и собственных векторов, существуют комплексная и вещественная формы, связанные между собой. При переходе к вещественной форме столбцы, порожденные значениями четных и нечетных базисных функций и разнесенные в комплексной форме по отдельным составляющим, размещаются в одной матрице рядом. В итоге утрачивается одно из свойств комплексных матриц: значения синусов и косинусов кратных частот трактуются теперь уже не как вещественная и мнимая составляющие, вместе образующие катеты прямоугольного треугольника с гипотенузой единичной длины, а как самостоятельные значения. Иными словами, модуль каждого элемента в вещественной форме зависит от периода дискретизации и не равен, в общем случае, единице. Тем не менее, частные формы вещественных ортогональных матриц с единичными нормами элементов возможны. Согласно гипотезе Адамара, порядок этих матриц кратен 4.

С появлением вычислительных средств преимущества, которые предполагают вычисления со столь просто устроенными матрицами, обеспечили серьезный интерес к исследованию матриц Адамара – именно так они были названы. К последовательности матриц порядков 2, 4, 8, 16, 32 и т.п., порождаемых процедурой удвоения порядка от 1, предложенной еще Сильвестром, Адамар добавил еще две стартовые матрицы пропущенных порядков 12 и 20. Процесс нахождения таких матриц плохо поддается формализации, компьютерный поиск отчасти подтвердил гипотезу Адамара, но порядок матрицы, подлежащий проверке, не превышает пока тысячи. Дальнейший прогресс в этом направлении возможен при включении в область исследований матриц с элементами нескольких значений, в том числе и пропущенных нечетных порядков включительно.

Минимаксные ортогональные матрицы (М-матрицы)

В работе [7] введено определение уровней матрицы, которым соответствуют значения ее элементов. Введение уровней позволяет, во-первых, классифицировать матрицы, во-вторых – представлять их графические портреты.

Определение 1. Матрица Адамара – квадратная двухуровневая матрица $\mathbf{H}_n$ порядка n, кратного 4, состоящая из элементов из множества {1, –1}, столбцы которой ортогональны:

$$\mathbf{H}_n^T\mathbf{H}_n = n\,\mathbf{I}\,,$$

где **I** – единичная матрица.

Определение 2. Матрица Белевича (**C**-matrix, conference-matrix) – квадратная трехуровневая матрица $\mathbf{C}_n$ порядка n, кратного 2, с нулевой диагональю и остальными элементами из множества {1, –1}, обладающая свойством

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

На классе ортогональных матриц заданной размерности и та, и другая матрицы (после ортонормирования) экстремальны по весьма простому критерию − они минимальны по значению максимума среди абсолютных значений их элементов. В этом смысле их можно называть минимаксными ортогональными матрицами или частными случаями таких матриц для четных порядков.

Определение 3. **M**-матрица или обобщенная матрица Адамара в строгом смысле – это матрица, максимум абсолютных значений элементов (m-норма) которой минимален на классе ортогональных матриц (после ортонормирования строк или векторов) заданного четного или нечетного порядков n.

Определение 4. **M**-матрица или обобщенная матрица Адамара в менее строгом смысле – это матрица, максимум абсолютных значений элементов (m-норма) которой локально-минимален на классе ортогональных матриц (после ортонормирования строк или векторов) заданного четного или нечетного порядков n.

Важными частными случаями **M**-матриц являются бинарные (адамаровы) матрицы, тринарные (**C**-матрицы), а также матрицы, содержащие, в общем случае, более трех уровней.

Алгоритм поиска M-матриц

Алгоритм поиска **M**-матриц ориентирован на достижение глобального (или локального, при снижении требований) минимума максимума абсолютных значений ортогональной матрицы, т.е. минимальной m-нормы.

В качестве начального приближения используется кососимметрическая теплицева матрица **A** оператора гильбертова преобразования с единичной диагональю, внедиагональные элементы вычисляются как функция разности индексов $a_{ij} = M/(i-j)$, где M – масштабный множитель. Перед использованием столбцы матрицы **A** нормируются. Ниже описаны этапы итерации процесса поиска **M**-матриц, представленной на схеме на рис. 1.

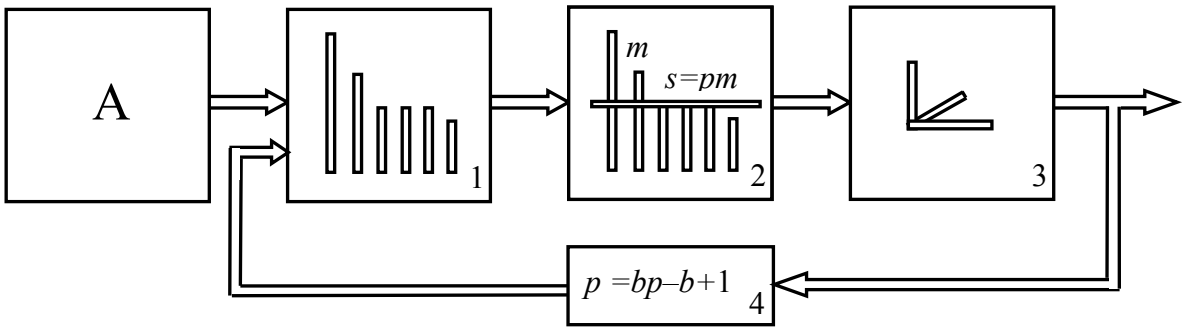


Рис. 1. Схема реализации алгоритма поиска **M**-матриц: 1 – перестановка столбцов; 2 – ограничение норм; 3 – ортогонализация Грамма-Шмидта; 4 – уменьшение величины сжатия p

Блок 1. Перестановка столбцов итерируемой матрицы так, чтобы первым стал столбец с максимальным по абсолютной величине элементом, вторым и последующими – тот, который менее всего уступает по этому показателю предыдущему столбцу.

Блок 2. Ограничение норм элементов матрицы насыщением: абсолютные значения всех элементов должны быть понижены до границы насыщения, $s = pm$, $p < 1$, m – текущее значение максимального по абсолютной величине элемента матрицы (m-норма).

Блок 3. Ортогонализация сжатой матрицы по методу Грама–Шмидта. Перестановка столбцов создает эффективное зацепление за максимально измененный в желаемом смысле вектор, ортогонализация не меняет его направление, не восстанавливает, как это может быть в противном случае.

Блок 4. Уменьшение величины сжатия пересчетом порога $p = bp - b + 1$, $b < 1$ (обычно 0,995). Переход к блоку 1 для совершения следующей итерации.

Практика показала, что количество требуемых итераций – около тысячи. Полезно осуществить несколько запусков, варьируя стартовое значение для p, пока финальная m-норма не перестанет меняться.

Выбор начального приближения при реализации предложенного алгоритма определен следующим. Ортогональная единичная матрица **I** не годится в качестве начального условия, поскольку ортогонализация всего лишь восстановит ее. Случайные матрицы создают ненужные проблемы для воспроизведения эксперимента. Стартовые симметричные матрицы тоже мало подходят: эволюция к оптимуму связана с прохождением неоптимальных локальных стадий, навязывание симметричной структуры, желаемой для итоговой матрицы, существенно снижает вариативность поиска в начале.

Линейный оператор гильбертова преобразования, связанный с матрицей **A,** представляет собой фазовращатель, дифференцирующий тригонометрические функции (сигналы). Он тесно связан с оператором Фурье, используемым также в теории комплексных матриц Адамара. Годятся и иные модификаторы единичной матрицы, необходимая для поиска модификация вектор-столбцов **A** управляется всего одним параметром M . Финальная ортогональная матрица формируется на выходе блока 3.

Таким образом, на каждом цикле итерируемая матрица ортогонализуется и нормируется. Далее матрица сжимается по m-норме, например, применением функции насыщения для абсолютных значений элементов вектор-столбцов. Ограничение абсолютных значений приводит к потере ортогональности векторов, восстанавливаемой на следующей итерации.

Этот процесс иллюстрируется рис. 1. Последовательные сжатия и ортогонализации (растяжение) образуют пульсации, в процессе которых ортогональный базис поворачивается, стремясь занять наиболее компактное положение, при котором проекции базисных векторов, т.е. максимум абсолютных значений элементов столбцов, будут принимать минимальное значение.

Амплитуда пульсаций регулируется коэффициентом насыщения p, это значение, согласно заложенной итерационной формуле, стремится к единице. Работа алгоритма зависит всего лишь от двух параметров: коэффициента раствора вектор-столбцов $M < 1$ матрицы Гильберта **A** и начального значения p, имеющего в программном комплексе обозначение P ($P < 1$). Оба этих параметра, M и P, вынесены в отдельные окна интерфейса программного комплекса для варьирования при принятии решения о продолжении циклов итераций или рестарте с новой матрицей **A.** Образуется эффективная двухпараметрическая процедура поиска **M**-матриц, которая способна находить при смене параметров M и P не только абсолютные, но и локальные оптимумы по заданному критерию m.

Интерфейс программного комплекса MMatrix

Интерфейс программного комплекса MMatrix представлен на рис. 2. Верхний ряд составляют кнопки генерации начальных стартовых матриц на основе известных заранее аналитических форм в виде матриц Гильберта (Hilbert) и, в дополнение к ней, Адамара (Hadamard), Белевича (Belevitch), Мерсенна (Mersenne) [4], Ферма (Fermat) [6] и других.

В окнах ниже фиксируется графический портрет матрицы, где интенсивность серого цвета пикселя свидетельствует об уровне ее элемента (слева), и выводится профиль уровней элементов найденных матриц – гистограмма (справа).

Имеются окна для задания общего количества итераций, промежуточных точек вывода, значений шага процедуры сжатия элементов, начального значения коэффициента сжатия P и других. Программно реализуется генерация некоторых рекомендуемых значений параметров двухпараметрической процедуры оптимизации для успешного поиска оптимальных и регулярных локально-оптимальных структур.

На панель интерфейса выведены кнопки процедур перестановки, сортировки, инверсии значений элементов уровней. Встроенный матричный калькулятор позволяет вычислить произведение Кронекера с целью поиска матриц высокого порядка на основе матриц более низких порядков.

Имеется окно ввода ранее найденной матрицы для продолжения итераций с нею. Интерфейс предусматривает введение символьных обозначений уровней, что позволяет применить процедуры поиска уравнений их связи. Программный комплекс обеспечивает возможность фиксировать найденные результаты в текстовом файле и в виде изображений матриц.

На рис. 3 приведены две **M**-матрицы матричных фракталов Эйлера (Мерсенна) 255-го и Ферма 257-го порядков, найденные с использованием описываемого программного комплекса MMatrix. Это левая (рис. 3, а) и правая (рис. 3, б) ветви основной последовательности матриц порядков, равных степени двойки.

Заключение

Достоинство реализованного в программном комплексе MMatrix итерационного алгоритма состоит в том, что результатом его работы может являться и локальный оптимум, который интересен сам по себе – именно так обнаруживаются малоуровневые субоптимальные регулярные структуры.

Рассматриваемый алгоритм обладает уникальными качествами, поскольку, хотя основа его построена на работе с вещественными числами, результатом вычислений являются целочисленные решения системы квадратичных уравнений, следующих из условия ортогональности матрицы. В результате его работы единообразно находятся, например, и **M**-матрицы 12-го и 20-го порядков, исторически полу-

ченные Адамаром совершенно иным способом, и матрицы Белевича порядков 6, 10, 14, 18 и т.д., имеющие тоже вполне самостоятельную историю их получения.

Известно, что проблема Адамара открыта, т.е. общего алгоритма поиска этих матриц нет. В таких обстоятельствах независимый путь получения матриц Адамара, отличный от переборных процедур, имеет большое прикладное значение. В теории матриц Белевича есть порядки, для которых матриц такого вида не существует. Это немедленно поднимает вопрос об альтернативных решениях, которые могут быть получены и исследованы при помощи такого комплекса. Так, например, было получено минимаксное решение для 22-го порядка [5]. Вес матриц Адамара и Белевича в теории информации внушителен, что поднимает интерес к их замещениям, если матрицы отсутствуют.

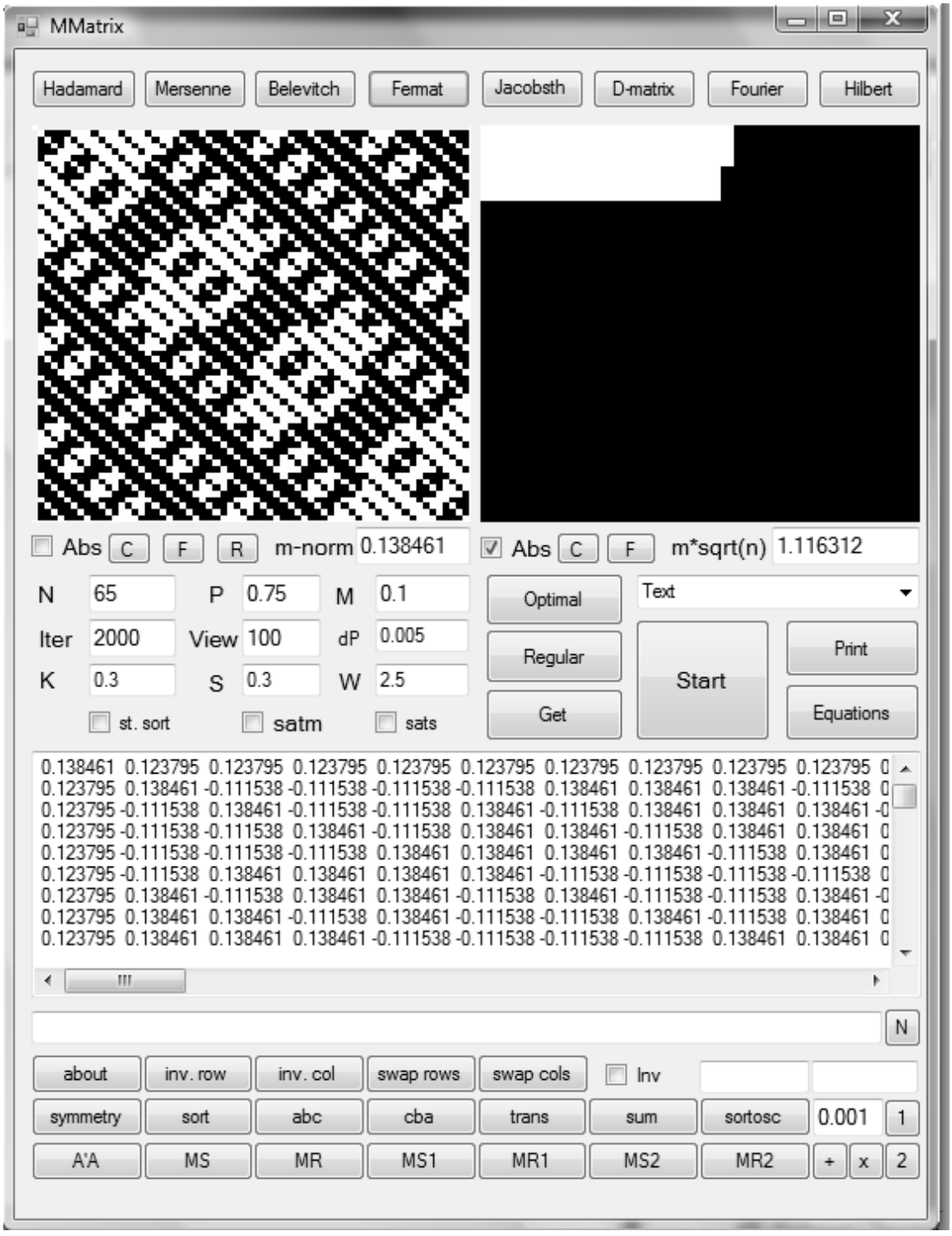
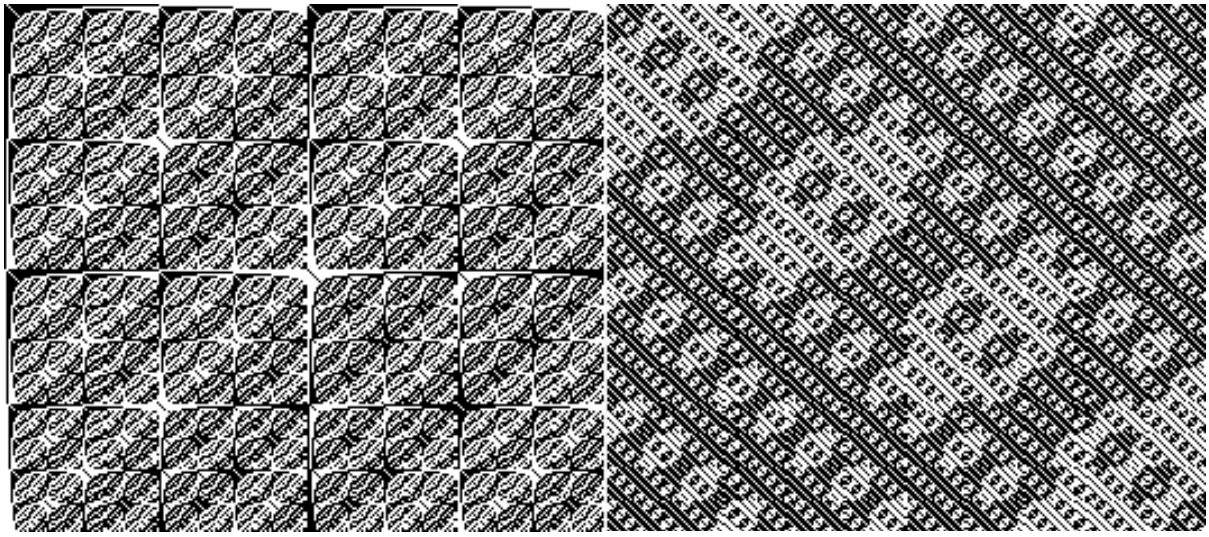


Рис. 2. Интерфейс программного комплекса MMatrix



а б

Рис. 3. Примеры портретов найденных матриц Мерсенна (размер 255×255 пикселей) (а) и Ферма (размер 257×257 пикселей) (б) 255-го и 257-го порядков соответственно

Литература

1. Аршинов М.Н., Садовский Л.Е. Коды и математика – М.: Наука, 1983. – 144 с.
2. Блэйхут Р. Быстрые алгоритмы цифровой обработки сигналов. – М.: Мир, 1989. – 448 с.
3. Сергеев М.Б., Балонин Н.А., Балонин Ю.Н. Программа поиска М-матриц. Свидетельство о государственной регистрации программы для ЭВМ № 2012614356 от 16 мая 2012 г.
4. Балонин Н.А., Сергеев М.Б., Мироновский Л.А. Вычисление матриц Адамара–Мерсенна // Информационно-управляющие системы. – 2012. – № 5. – С. 92–94.
5. Балонин Ю.Н., Сергеев М.Б. М-матрица 22-го порядка // Информационно-управляющие системы. – 2011. – № 5. – С. 87–90.
6. Балонин Н.А., Сергеев М.Б., Мироновский Л.А. Вычисление матриц Адамара–Ферма // Информационно-управляющие системы. – 2012. – № 6 (61). – С. 90–93.
7. Балонин Н.А., Сергеев М.Б. О двух способах построения матриц Адамара–Эйлера // Информационно-управляющие системы. – 2013. – № 1 (62). – С. 7–10.

Балонин Юрий Николаевич – Санкт-Петербургский государственный университет аэрокосмического приборостроения (ГУАП), программист, tomaball@mail.ru

Сергеев Михаил Борисович – Санкт-Петербургский государственный университет аэрокосмического приборостроения (ГУАП), доктор технических наук, профессор, зав. кафедрой; НИИ информационно-управляющих систем НИУ ИТМО, директор, mbse@mail.ru