УДК 519.614

Вычисление матриц Адамара-Мерсенна

Журнал: Информационные управляющие системы. 2012. № 5.

Балонин Н.А.

д-р техн. наук, профессор, старший научный сотрудник

Сергеев М.Б.

д-р техн. наук, профессор, директор

НИИ Информационно-управляющих систем НИУ ИТМО

Мироновский Л.А.

д-р техн. наук, профессор

Санкт-Петербургский государственный университет аэрокосмического приборостроения

***Аннотация**: В статье приведено определение обобщенных матриц Адамара, порядок которых равен числам Мерсенна. Рассмотрены свойства матриц Адамара-Мерсенна, описан алгоритм их построения, приведены числовые примеры.*

***Ключевые слова**: ортогональные матрицы, матрицы Адамара, матрицы Белевича, числа Мерсенна*

Введение

Матрицы Адамара нашли применение в практике построения помехоустойчивых и защитных кодов, в шифровании и маскировании. К сожалению, матрицы Адамара существуют не для всех порядков n, поэтому актуальной остается задача поиска ортогональных матриц, близких к ним по смыслу. Решению этой проблемы посвящены работы [1–5].

В работах [1, 2] показано, что элементы искомых матриц распадаются на некоторые группы (уровни) одинаковых по абсолютным величинам чисел. Наиболее экономно устроены матрицы Адамара, имеющие одноуровневую структуру – все их элементы равны {1, –1}.

Классический способ построения матриц Адамара порядков $n = 2^k$ основан на использовании итерационной формулы Сильвестра

$$\mathbf{S_{2n}} = \begin{pmatrix} \mathbf{S}_n & \mathbf{S_n} \\ \mathbf{S_n} & -\mathbf{S_n} \end{pmatrix}, \qquad (1)$$

где в качестве начального значения используется число $\mathbf{S_1} = 1$.

Помимо простоты построения, матрицы Адамара отличает экстремальное свойство – максимальный по абсолютной величине элемент такой матрицы (*m*-норма) имеет наименьшее значение на множестве ортонормированных матриц того же порядка. Расширительное толкование матриц Адамара возможно при опоре на отмеченное минимаксное свойство [1, 2], при одновременном ослаблении жесткого ограничения на значения уровней, а именно, допуская для элементов М-матриц два значения $\pm a$ и $\pm b$. Далее без ограничения общности будем считать, что $|a|=1$, $|b|<1$.

Таким образом, задача сводится к отысканию матриц с минимальной *m*-нормой на множестве ортогональных двухуровневых матриц.

Модифицированная формула Сильвестра

Цель данной работы состоит в описании последовательности двухуровневых ортогональных М-матриц, аналогичных последовательности Сильвестра (1), но построенной для чисел Мерсенна $n= 2^k-1$, где k–целое. Так как значения уровней элементов матриц изменились, модифицируем формулу удвоения порядка Сильвестра.

Положение 1. Рассмотрим модифицированную формулу Сильвестра

$$\mathbf{S_{2n}} = \begin{pmatrix} \mathbf{M}_n & \mathbf{M_n} \\ \mathbf{M_n} & \mathbf{M_n^*} \end{pmatrix}, \qquad (2)$$

где матрица $\mathbf{M_n^*}$ образована перестановкой уровней a=1 и $-b$. Полученная по этой формуле матрица $\mathbf{S_{2n}}$ симметрична, но ее порядок четен и на единицу меньше порядка следующей матрицы Мерсенна $\mathbf{M_{2n+1}}$. Для рекурсивного перехода от матрицы к матрице одного лишь удвоения порядка недостаточно, необходимо дополнительное окаймление матрицы $\mathbf{S_{2n}}$ (добавление строки и столбца).

Алгоритм построения матриц Адамара-Мерсенна

Алгоритм основан на свойствах собственных чисел и собственных векторов блочных матриц.

Положение 2. Сформируем матрицу $\mathbf{M_{2n+1}}$ путем следующего окаймления матрицы $\mathbf{S_{2n}}$ вида (2):

$$\mathbf{M_{2n+1}} = \begin{pmatrix} -\lambda & \mathbf{e'} \\ \mathbf{e} & \mathbf{S_{2n}} \end{pmatrix},$$

где $\lambda, \mathbf{e}$ – соответственно собственное число и собственный вектор матрицы $\mathbf{S_{2n}}$. Полученная таким образом матрица будет симметричной и ортогональной при старте итераций с начальной матрицы

$$\mathbf{M}_3 = \begin{pmatrix} a & -b & a \\ -b & a & a \\ a & a & -b \end{pmatrix},$$

собственное значение матрицы удвоенного порядка будет равно $\lambda = -a$. При этом половина компонент собственного вектора состоит из $-b$, остальная половина – из a. Происходит это при следующих значениях образующей пары: $b=a/2$ при $n=3$, в остальных случаях $b = \frac{p \pm \sqrt{4p}}{p-4} a$, $p=n+1$. Справедливость положения следует непосредственно из условия ортогональности.

Указанные значения элементов матриц являются корнями некоторых алгебраических уравнений, называемых далее характеристическими. Примеры характеристических уравнений для уровней, отвечающих условию ортогональности столбцов матрицы Адамара-Мерсенна, приведены в таблице 1.

Таблица 1. Уравнения и значения уровней М-матриц

k	Матрица	Уравнение	Уровни
1	M_1	$b=a$	$b=a$
2	M_3	$2b-a=0$	$b=a/2$
3	M_7	$b^2-4ab+2a^2=0$	$b=(2\pm\sqrt{2})a$
4	M_{15}	$3b^2-8ab+4a^2=0$	$b=2a/3$ и $b=2a$
5	M_{31}	$7b^2-16ab+8a^2=0$	$b=(8\pm2\sqrt{2})a/7$
6	M_{63}	$15b^2-32ab+16a^2=0$	$b=4a/5$, $b=4a/3$
7	M_{127}	$31b^2-64ab+32a^2=0$	$b=(32\pm4\sqrt{2})a/31$
8	M_{255}	$63b^2-128ab+64a^2=0$	$b=8a/9$ и $b=8a/7$

В случае построения из матриц Якобсталя матриц Белевича [5] собственному значению $\lambda=0$, соответствует собственный вектор **e**, состоящий из 1. Строительный блок матрицы Адамара-Мерсенна отличается от них только тем, что $\lambda=-a$, а собственный вектор содержит элементы $-b$ и a. Единственная сложность состоит в том, что с ростом порядка эти параметры не остаются постоянными, но их модули сближаются. Иными словами, значения элементов матриц Адамара-Мерсенна стремятся к {1, −1}, т.е. в пределе они точно такие же, как и матриц Адамара.

Пример 1. Одна итерация модифицированного алгоритма Сильвестра дает

$$\mathbf{M}_3=\begin{pmatrix} a & -b & a \\ -b & a & a \\ a & a & -b \end{pmatrix}, \quad \mathbf{S}_6=\begin{pmatrix} a & -b & a & a & -b & a \\ -b & a & a & -b & a & a \\ a & a & -b & a & a & -b \\ a & -b & a & -b & a & -b \\ -b & a & a & a & -b & -b \\ a & a & -b & -b & -b & a \end{pmatrix}$$

Уровни матрицы Адамара-Мерсенна $\mathbf{M_7}$: $a=1$, $b=\frac{p-\sqrt{4p}}{p-4}\cong0.5858$, при $p=8$. Среди собственных чисел {–1,–2.2426,–2.2426,2.2426,2.2426,2.2426} выберем λ=–1, отвечающее уровню $a=1$ этой матрицы. Соответствующий собственный вектор $\mathbf{e}=(-b,-b,-b,a,a,a)\cong(-0.5858,-0.5858,-0.5858,1,1,1)$. Добавляя кайму, получаем:

$$\mathbf{M}_7 = \begin{pmatrix} a & -b & -b & -b & a & a & a \\ -b & a & -b & a & a & -b & a \\ -b & -b & a & a & -b & a & a \\ -b & a & a & -b & a & a & -b \\ a & a & -b & a & -b & a & -b \\ a & -b & a & a & a & -b & -b \\ a & a & a & -b & -b & -b & a \end{pmatrix}.$$

Портреты матриц более высоких порядков приведены на рис. 1.

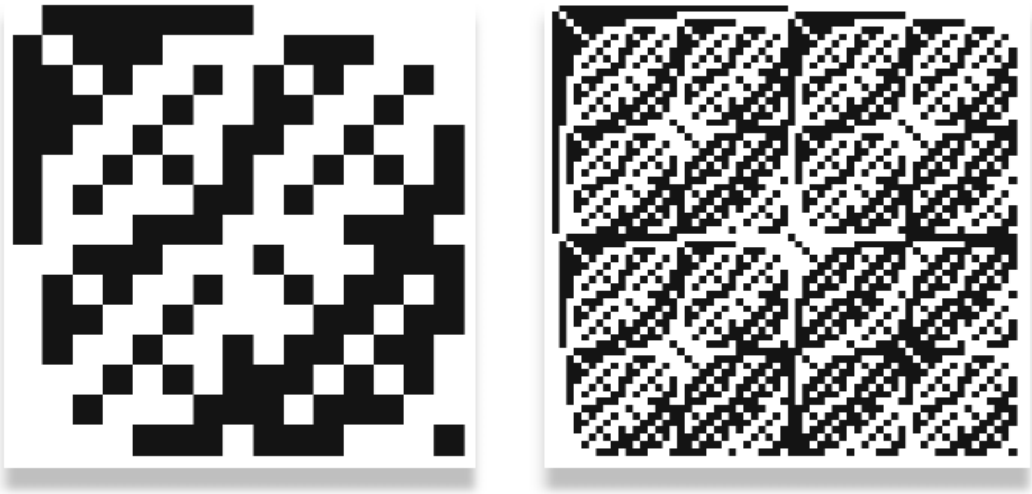

Рисунок 1 – Примеры матриц Адамара-Мерсенна $\mathbf{M}_{15}$, $\mathbf{M}_{63}$. Здесь белое поле – элемент матрицы со значением a= 1, черное поле – элемент со значением $-b$.

Пример 2. Симметричная матрица Адамара восьмого порядка:

$$\mathbf{A} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{pmatrix}$$

Среди собственных чисел {–1,–2.8284,–2.8284,–2.8284,2.8284,2.8284,2.8284} матрицы седьмого порядка, полученной отбрасыванием первой строки и первого столбца, выберем λ=–1, отвечающее уровню a=1 этой матрицы. Соответствующий собственный вектор имеет вид **e**=(1,1,1,1,1,1,1).

Пример 3. Симметричная матрица Белевича [5] шестого порядка имеет следующий вид:

$$\mathbf{C}=\begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & -1 & -1 & 1 \\ 1 & 1 & 0 & 1 & -1 & -1 \\ 1 & -1 & 1 & 0 & 1 & -1 \\ 1 & -1 & -1 & 1 & 0 & 1 \\ 1 & 1 & -1 & -1 & 1 & 0 \end{pmatrix}$$

Среди собственных чисел {0,–2.2361,–2.2361,2.2361,2.2361} матрицы пятого порядка, полученной отбрасыванием первой строки и первого столбца, выберем $\lambda=0$, отвечающее нулевому диагональному элементу этой матрицы. Соответствующий собственный вектор имеет вид $\mathbf{e}=(1,1,1,1,1)$.

Заключение.

В процессе поиска матриц нечетных порядков близких к матрицам Адамара удалось выделить класс двухуровневых матриц, названных матрицами Адамара-Мерсенна. Размер этих матриц равен числам Мерсенна 2^k-1, а их элементы с ростом значений целочисленного аргумента k стремятся к значениям {1, –1} как и у матриц Адамара. В области четных порядков пропуски среди матриц Белевича [5] также восполняются М-матрицами с большим количеством уровней [3]. Практическое применение таких матриц целесообразно в задачах повышения степени помехоустойчивости и защищенности при передаче информации.

Список литературы

1. Балонин Н.А., Сергеев М.Б. М-матрицы // Информационные управляющие системы. 2011. № 1. С.14-21.
2. Балонин Н.А., Мироновский Л.А. Матрицы Адамара нечетного порядка. // Информационно-управляющие системы. 2006, N3. С. 46-50.
3. Балонин Ю. Н., Сергеев М. Б. М-матрица 22-го порядка // Информационно-управляющие системы. 2011. № 5. С. 87–90.
4. Шинтяков Д.В. Алгоритм поиска матриц Адамара нечетного порядка // Сб. докл. Девятой научной сессии ГУАП: Часть II. Технич. науки / ГУАП. 2006. С.207-211.
5. Belevitch, V. (1950), Theorem of 2n-terminal networks with application to conference telephony. Electr. Commun., vol. 26, P. 231–244.

ДЛЯ ОБЛОЖКИ

В наши дни Марен Мерсенн известен более всего как исследователь «чисел Мерсенна», играющих важную роль в теории чисел, криптографии и генераторах псевдослучайных чисел. Однако Мерсенн – один из первых, кто оценил скорость звука. Он описал схему зеркального телескопа, позднее реализованную Ньютоном. Основываясь на его исследованиях, французский математик Жозеф Совёр объяснил феномен обертонов. Мерсенн также издал перевод на французский язык «Механики» Галилея (1634), редактировал издания Евклида, Архимеда и других античных классиков.