УДК 519.614

Вычисление матриц Адамара-Ферма

Журнал: Информационные управляющие системы. 2012. № 6.

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 отвечает числовой последовательности Ферма. Рассмотрены свойства матриц Адамара-Ферма, описан алгоритм их построения, приведены числовые примеры.*

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

Введение

В теории и практике построения помехоустойчивых и защитных кодов, в шифровании и маскировании нашли применение матрицы Адамара – ортогональные матрицы с элементами ±1. К сожалению, такие матрицы существуют лишь для n=2 и для n, кратных четырем. В связи с этим возникает задача поиска ортогональных матриц других порядков, близких к матрицам Адамара по некоторым свойствам [1–5]. Один из подходов состоит в том, чтобы попытаться найти ортогональные матрицы, у которых элементы близки по абсолютной величине, принимая два или три различных значения (будем называть такие матрицы двухуровневыми и трехуровневыми).

В теории чисел существуют хорошо известные последовательности чисел Мерсенна и Ферма. Последовательность Мерсенна задается формулой $n=2^k-1$ и начинается с чисел 1, 3, 5, 15, 31, …, она принадлежит подмножеству чисел вида $4k-1$. Последовательность Ферма задается формулой $n = 2^{2^k} + 1$ и начинается с чисел 3, 5, 17, 257, 65537, 4294967297, 18446744073709551617, …, она принадлежит подмножеству чисел вида $4k+1$.

В работе авторов [1] предложен итерационный способ построения последовательности двухуровневых ортогональных матриц (они названы матрицами Адамара-Мерсенна), порядки которых равны числам Мерсенна. В его основе лежит аналогия с классическим способом построения матриц Адамара порядков $n = 2^k$ с помощью 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 $\mathbf{S}_1 = 1$.

В настоящей заметке предлагается итерационная процедура построения последовательности трехуровневых ортогональных матриц, порядки которых равны числам Ферма, а также числам вида $n=2^k+1$, где k – четное (за исключением $k=1$): 3, 5, 17, 65, 257, 1025, … . .

Матрицы, порождаемые этой процедурой (будем называть их матрицами Адамара-Ферма и обозначать $\mathbf{F}_n$), обладают следующими свойствами:

(i) они симметричны, ортогональны с тремя значениями элементов a=1, $-b$ ($b<a$), $b<s<a$;

(ii) все элементы первой строки и столбца (и только они), равны s (кроме начального элемента, которой равен a).

Особо оговорим случай-исключение, матрицу $\mathbf{F}_3$ (k – нечетное число), когда значения $b=s=2a$ (превышают на старте значение a). Таким образом, задача сводится к отысканию матриц с минимальной m-нормой на множестве ортогональных трехуровневых матриц порядков, равным числам последовательности Ферма.

Модифицированная формула Сильвестра

Пусть имеется матрица Адамара-Ферма $\mathbf{F}_n$ порядка n. Обозначим через $\mathbf{S}_{n-1}$ симметричную матрицу, получаемую из матрицы $\mathbf{F}_n$ удалением ее первых строки и столбца. Модифицируем формулу удвоения порядка Сильвестра, заменив ее учетверением порядка по следующему принципу.

Положение 1. Рассмотрим модифицированную формулу Сильвестра

$$\mathbf{S}_{4n-4} = \begin{pmatrix} \mathbf{S}^*_{n-1} & \mathbf{S}_{n-1} & \mathbf{S}_{n-1} & \mathbf{S}_{n-1} \\ \mathbf{S}_{n-1} & \mathbf{S}^*_{n-1} & \mathbf{S}_{n-1} & \mathbf{S}_{n-1} \\ \mathbf{S}_{n-1} & \mathbf{S}_{n-1} & \mathbf{S}^*_{n-1} & \mathbf{S}_{n-1} \\ \mathbf{S}_{n-1} & \mathbf{S}_{n-1} & \mathbf{S}_{n-1} & \mathbf{S}^*_{n-1} \end{pmatrix}, \qquad (2)$$

где матрица $\mathbf{S}^*_{n-1}$ образована заменой значений уровней a на $-b$ и наоборот.

Полученная по формуле (2) матрица $\mathbf{S}_{4n-4}$ симметрична, но ее порядок четен и на единицу меньше порядка следующей матрицы Адамара-Ферма $\mathbf{F}_{4n-3}$. Для завершения рекурсивного перехода необходимо дополнительное окаймление матрицы (добавление строки и столбца). Важнейшим требованием является ортогональность матрицы, получаемой в результате окаймления.

Алгоритм построения матриц Адамара-Ферма

Для нахождения ортогонализирующего окаймления применим прием, описанный в работе [1]. Он основан на свойствах собственных чисел и собственных векторов блочных матриц.

Положение 2. Сформируем матрицу $\mathbf{F}_{4n-3}$ путем следующего окаймления матрицы $\mathbf{S}_{4n-4}$ (2):

$$\mathbf{F_{4n-3}} = \begin{pmatrix} -\lambda & \mathbf{e}' \\ \mathbf{e} & \mathbf{S_{4}}_{n-4} \end{pmatrix},$$

где λ, $\mathbf{e}$ – собственное число и собственный вектор матрицы $\mathbf{S}_{4n-4}$.

Полученная таким образом матрица будет симметричной и ортогональной, если начинать итерационный процесс с матрицы

$$\mathbf{F}_5 = \begin{pmatrix} a & s & s & s & s \\ s & a & -b & -b & -b \\ s & -b & a & -b & -b \\ s & -b & -b & a & -b \\ s & -b & -b & -b & a \end{pmatrix}, \qquad (3)$$

Матрицу $\mathbf{S}_4$ получаем удалением ее первой строки и первого столбца («каймы»). Здесь $a=-\lambda$ – собственное число матрицы $\mathbf{S}_4$, взятое с обратным знаком, s – элементы соответствующего собственного вектора, причем $b<s<a$.

При $n=5$ имеем $b=s=2a/3$, в остальных случаях $b=\frac{n-q}{q}a$, $s=\frac{\sqrt{np-2\sqrt{p}}}{2q}a$, $q=\frac{p+\sqrt{p}}{2}$, $p=n-1$. Справедливость положения 2 следует непосредственно из условия ортогональности.

Вырожденный случай-исключение $\mathbf{F}_3$ получается из $\mathbf{F}_5$ усечением той же структуры: но только вдвое (вследствие чего $b=s=2a$)

$$\mathbf{F}_3=\begin{pmatrix} a & s & s \\ s & a & -b \\ s & -b & a \end{pmatrix}.$$

Структура матрицы $\mathbf{F}_5$ и построенная по ней итерационно матрицы $\mathbf{F}_{17}$ показаны на рис. 1, промежуточный уровень второй матрицы отвечает элементам отмеченного собственного вектора. Здесь белое поле – элемент матрицы вида $a=1$, черное поле – элемент вида $-b$, серое поле – элемент каймы $b<s<a$.

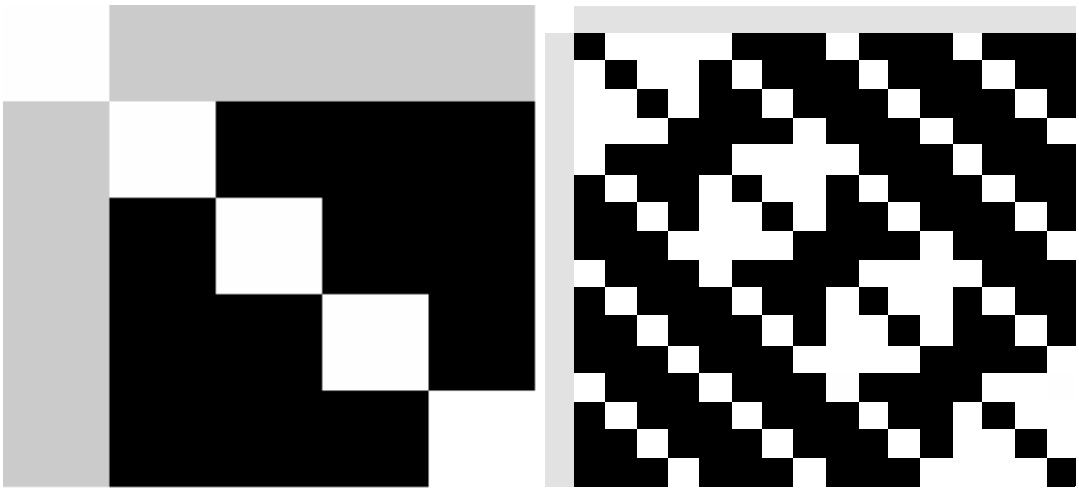

Рисунок 1 – Портреты матриц Адамара-Ферма $\mathbf{F}_5$, $\mathbf{F}_{17}$.

Полузависимые значения уровней матриц являются корнями следующих алгебраических уравнений, называемых далее характеристическими

$$qb-(n-q)a=0,\ q^2s^2-\frac{np-2\sqrt{p}}{4}a^2=0.$$

Уровни матриц Адамара-Мерсенна и Адамара-Ферма приведены на рис. 2, промежуточный уровень второй матрицы отвечает элементам собственного вектора симметричного вложения $\mathbf{S}_{16}$.

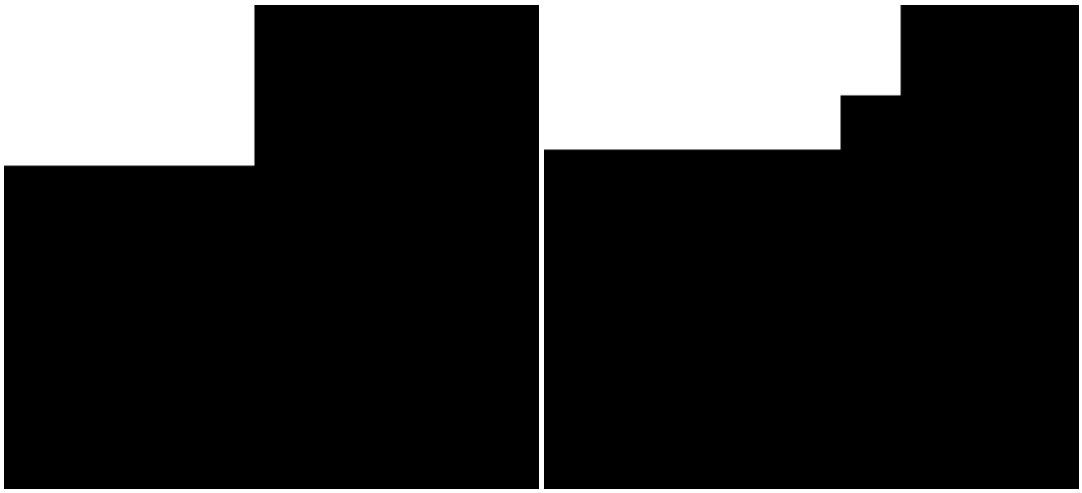

Рисунок 2 – Примеры уровней матриц Адамара-Мерсенна $\mathbf{M}_{15}$ и Ферма $\mathbf{F}_{17}$.

Примеры характеристических уравнений для уровней, отвечающих условию ортогональности столбцов матрицы Адамара-Ферма, приведены в таблице 1.

Таблица 1. Уравнения и значения уровней М-матриц

k	Матрица	Уравнения	Уровни
1	$\mathbf{F}_3$	$b=2a,\ s=2a$	$b=s=2a$
2	$\mathbf{F}_5$	$3b=2a,\ 3s=2a$	$b=s=2a/3$
4	$\mathbf{F}_{17}$	$10b=7a$, $10^2s^2=66a^2$	$b=7a/10$, $s=\sqrt{66}a/10$
6	$\mathbf{F}_{65}$	$36b=29a$, $36^2s^2=1036a^2$	$b=29a/36$, $s=\sqrt{1036}a/36$
8	$\mathbf{F}_{257}$	$136b=121a$, $136^2s^2=16440a^2$	$b=121a/136$, $s=\sqrt{16440}a/136$

При построении матриц Адамара-Мерсенна [1], собственному значению $\lambda=-a$ соответствует собственный вектор $\mathbf{e}$, составленный из обоих элементов внутреннего блока (у матриц Адамара элементы собственного вектора равны 1). Строительный блок матрицы Адамара-Ферма отличается от них только тем, что собственный вектор содержит некоторые новые элементы $b<s<a$. При этом с ростом порядка уровни матриц не остаются постоянными, но их значения сближаются. Иными словами, элементы матриц Адамара-Ферма с ростом n стремятся к $\{1, -1\}$, т.е. в пределе они точно такие же, как и матриц Адамара.

Пример. Для матрицы Адамара-Ферма (3) первая итерация модифицированного алгоритма Сильвестра дает

$$\mathbf{S}_4 = \begin{pmatrix} a & -b & -b & -b \\ -b & a & -u & -b \\ -b & -b & a & -b \\ -b & -b & -b & a \end{pmatrix}, \quad \mathbf{S}_4^* = \begin{pmatrix} -b & a & a & a \\ a & -b & a & a \\ a & a & -b & a \\ a & a & a & -b \end{pmatrix}.$$

На их основе строим расширенный блок следующей матрицы:

$$\mathbf{S}_{16} = \begin{pmatrix} -b & a & a & a & a & -b & -b & -b & a & -b & -b & -b & a & -b & -b & -b \\ a & -b & a & a & -b & a & -b & -b & -b & a & -b & -b & -b & a & -b & -b \\ a & a & -b & a & -b & -b & a & -b & -b & -b & a & -b & -b & -b & a & -b \\ a & a & a & -b & -b & -b & -b & a & -b & -b & -b & a & -b & -b & -b & a \\ a & -b & -b & -b & -b & a & a & a & a & -b & -b & -b & a & -b & -b & -b \\ -b & a & -b & -b & a & -b & a & a & -b & a & -b & -b & -b & a & -b & -b \\ -b & -b & a & -b & a & a & -b & a & -b & -b & a & -b & -b & -b & a & -b \\ -b & -b & -b & a & a & a & a & -b & -b & -b & -b & a & -b & -b & -b & a \\ a & -b & -b & -b & a & -b & -b & -b & -b & a & a & a & a & -b & -b & -b \\ -b & a & -b & -b & -b & a & -b & -b & a & -b & a & a & -b & a & -b & -b \\ -b & -b & a & -b & -b & -b & a & -b & a & a & -b & a & -b & -b & a & -b \\ -b & -b & -b & a & -b & -b & -b & a & a & a & a & -b & -b & -b & -b & a \\ a & -b & -b & -b & a & -b & -b & -b & a & -b & -b & -b & -b & a & a & a \\ -b & a & -b & -b & -b & a & -b & -b & -b & a & -b & -b & a & -b & a & a \\ -b & -b & a & -b & -b & -b & a & -b & -b & -b & a & -b & a & a & -b & a \\ -b & -b & -b & a & -b & -b & -b & a & -b & -b & -b & a & a & a & a & -b \end{pmatrix}$$

Среди собственных чисел $\mathbf{S}_{16}$, рассчитанной с учетом a=1 и b=0.7, выберем λ=–1, отвечающее уровню a=1 этой матрицы. Соответствующий собственный вектор будет содержать 16 одинаковых элементов. Их значения получаем из условия ортогональности $s \cong 0.8124$.

После расчета матрицы $\mathbf{F}_{17,}$ через две итерации получим матрицу $\mathbf{F}_{257,}$ отвечающему следующему числу Ферма, ее структура показана на рис. 3. Интересно отметить, что все эти матрицы содержат на портретах стилизованную букву Ф.

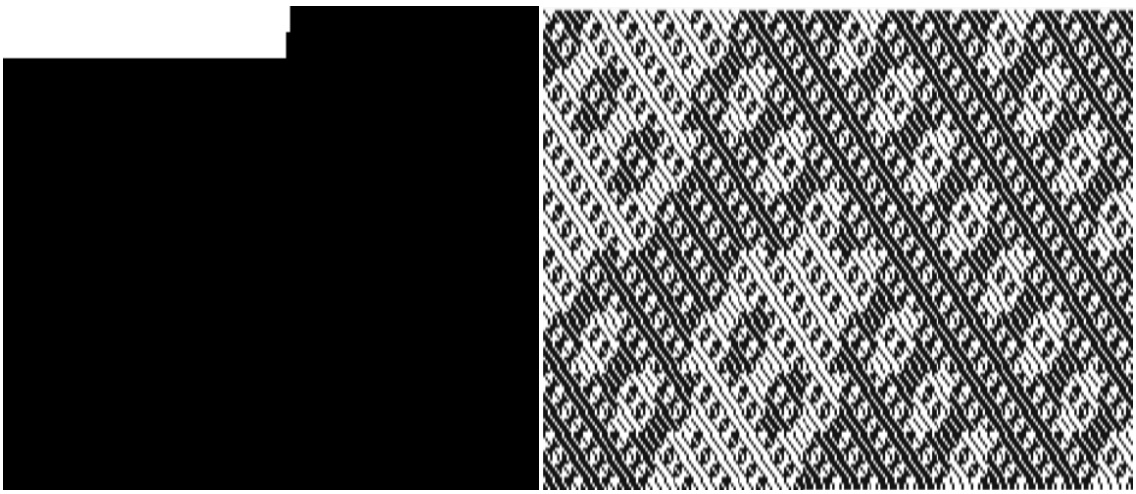

Рисунок 3 – График уровней элементов и портрет матрицы Адамара-Ферм $\mathbf{F}_{257}$.

Заключение.

В процессе поиска ортогональных матриц нечетных порядков, близких по своим свойствам к матрицам Адамара, удалось выделить класс трехуровневых матриц, названных матрицами Адамара-Ферма. Разработан итерационный алгоритм построения матриц Адамара-Ферма порядка 2^k+1 при k=1 и при всех четных k. Элементы этих матриц с ростом k стремятся к значениям $\{1, -1\}$, как и у матриц Адамара.

С учетом ранее полученных итерационных процедур построения матриц Адамара, Белевича и Адамара-Мерсенна теперь порядки начальных матриц охватывают все целые числа начала числовой оси. Известные в теории пропуски среди матриц Белевича [5] также восполняются матрицами, близким к матрицам Адамара-Мерсенна или Адамара-Ферма, что подтверждает их значимость.

Полученные матрицы могут найти применение в задачах повышения степени помехоустойчивости и защищенности при передаче информации.

Список литературы

1. Балонин Н.А., Сергеев М.Б., Мироновский Л.А. Вычисление матриц Адамара-Мерсенна // Информационные управляющие системы. 2012. № 5. С. 92-94.
2. Балонин Н.А., Сергеев М.Б. М-матрицы // Информационные управляющие системы. 2011. № 1. С. 14-21.
3. Балонин Н.А., Мироновский Л.А. Матрицы Адамара нечетного порядка. // Информационно-управляющие системы. 2006, N3. С. 46-50.
4. Балонин Ю. Н., Сергеев М. Б. М-матрица 22-го порядка // Информационно-управляющие системы. 2011. № 5. С. 87–90.
5. Шинтяков Д.В. Алгоритм поиска матриц Адамара нечетного порядка // Сб. докл. Девятой научной сессии ГУАП: Часть II. Технич. науки / ГУАП. 2006. С.207-211.
6. Belevitch, V. (1950), Theorem of 2n-terminal networks with application to conference telephony. Electr. Commun., vol. 26, P. 231–244.

ИЛЛЮСТРАЦИЯ

Современник и друг математика Марена Мерсенна, Пьер Ферма, был руководителем образованного им блестящего научного семинара, который посещали такие крупные ученые, как Декарт, Паскаль и др. Он широко известен благодаря так называемой теореме Ферма, трехсотлетние поиски доказательства которой создали целые отрасли математики, возросшие на еще более древней почве задач античности, идущих от великого Диофанта.