Математическая физика, анализ, геометрия
1997, т. 4, № 4, с. 458–471

Вписанный в куб правильный симплекс и матрица Адамара полуциркулянтного типа

А.И. Медяник

Физико-технический институт низких температур им. Б.И. Веркина НАН Украины, Украина, 310164, г. Харьков, пр. Ленина, 47
E-mail: medianik@ilt.kharkov.ua

Статья поступила в редакцию 9 ноября 1995 года

Найдено достаточное условие для того, чтобы существовала матрица Адамара порядка $4n$ полуциркулянтного типа (n – произвольное натуральное число), включающая в себя два различных циркулянта порядка $2n \quad 1$ – правый и левый (отсюда название). Из этого условия получается другой, отличный от известного метода Уильямсона метод построения матриц Адамара, геометрический по своей сути. Доказано также, что существует матрица Адамара порядка $2(p+1)$, где p – нечетное простое число полуциркулянтного типа, откуда следует, что в $2(p+1)$-мерный куб можно вписать правильный симплекс той же размерности.

1. Матрицей Адамара порядка m называется $(m \quad m)$-матрица H (элементами которой являются $+1$ и $\quad 1$) такая, что $HH = mI$, где H – транспонированная матрица, а I – единичная матрица порядка m [1, с. 283]. Это равенство означает, что любые две строки H ортогональны. По теореме Ж. Адамара (1893 г.) определитель такой матрицы по абсолютной величине равен ее наибольшему возможному значению $m^{m/2}$ (отсюда название). Если H – матрица Адамара порядка $m > 2$, то m кратно четырем [1, с. 284]. Однако является ли это условие достаточным для существования матрицы Адамара данного порядка $m > 2$, неясно до сих пор.

С 1933 года известно, что вопрос о существовании матрицы Адамара порядка $m = 4n$, где n – любое натуральное число, равносилен вопросу о возможности вписать в $(4n \quad 1)$-мерный куб правильный симплекс той же размерности так, чтобы каждая его вершина совпадала с одной из вершин куба, что позволяет использовать геометрические подходы к построению матриц Адамара [2]. Можно и наоборот: для решения указанной геометрической задачи использовать методы, разработанные для матриц Адамара. Некоторые

из уже известных методов построения матриц Адамара дают бесконечные серии, перечень которых можно найти в [1, с. 287]. Из того же перечня видно, что некоторые из порядков вида $4p$, где p – нечетное простое число, ни в одну из имеющихся серий не входят, например, $92 = 4 \quad 23$, $116 = 4 \quad 29$, $172 = 4 \quad 43$ (см. раздел V перечня). Таковым является и указанный в [3, с. 118] наименьший порядок $428 = 4 \quad 107$, для которого существование матрицы Адамара не доказано. Наиболее эффективным в этих случаях является разработанный в 1944 году метод Уильямсона [4] (см. также [1, с. 299–304]), для которого матрицы Адамара имеет вид

$$H = \begin{pmatrix} A & B & C & D \\ B & A & D & C \\ C & D & A & B \\ D & C & B & A \end{pmatrix},$$

где A, B, C и D – симметрические матрицы нечетного порядка n, переставочные друг с другом и такие, что $A^2 + B^2 + C^2 + D^2 = 4nI_n$, так что $HH \quad = (A^2 + B^2 + C^2 + D^2) \quad I_4 = 4nI_{4n}$ (знаком умножения обозначено прямое, кронекеровское произведение матриц). Кстати, успешности метода Уильямсона для всех нечетных n было бы достаточно для полного решения проблемы существования матриц Адамара. Это следует из того, что прямое произведение матриц Адамара также является матрицей Адамара порядка, равного произведению порядков исходных матриц [1, с. 304].

2. В настоящей статье предлагается и обосновывается другой метод построения матриц Адамара порядка $4n$, где n – произвольное натуральное число, отличительной особенностью которого является следующий вид матрицы Адамара:

$$H = \begin{pmatrix} A & B \\ B & A \end{pmatrix}, \tag{1}$$

где $A(B)$ – матрица порядка $2n$, содержащая подматрицу порядка $2n \quad 1$, которая является правым (соответственно левым) циркулянтом. Условия существования такой полуциркулянтной матрицы Адамара (в терминах группового кольца многочленов) устанавливаются основной леммой (п. 3). В силу отмеченной выше эквивалентности новый метод дает также положительное решение вопроса о существовании вписанного в $(4n \quad 1)$-мерный куб правильного симплекса той же размерности, если, конечно, существует полуциркулянтного типа матрица Адамара порядка $4n$. Последнее, в частности, имеет место, если число $2n \quad 1$ простое, что утверждается теоремами 1 и 2 (п. 4). Выясняется также, что сам метод, аналитический по форме, имеет геометрическую сущность (п. 5).

3. Прежде чем определить матрицы A и B, введем необходимые понятия и обозначения. Считая, что индексы i, j пробегают целочисленные значения от 0 до $2n-1$, а индексы k, m – от 1 до $2n-1$, введем такую матрицу порядка $2n$:

$$U=(u_{ij})=\{e_{00},e_{k\,k-1}\}, \tag{2}$$

где в фигурных скобках перечислены все ненулевые элементы U, причем местоположение элемента определяется индексами при e, а сама эта буква означает его равенство $+1$. Знак модуля в (2) и далее понимается как положительный вычет по $\bmod(2n-1)$, причем если $k-1=0$, то $k-1=2n-1$. Таким образом, согласно (2) $u_{ij}=1$ при $i=j=0$ или $i=k$, $j=k-1$; все остальные элементы U равны нулю, т.е. в каждой строке и в каждом столбце матрицы U имеется только один отличный от нуля элемент, равный $+1$.

Заметим, что часть матрицы U без нулевых строки и столбца представляет собой циркулянт в том смысле, что при переходе от каждой строки этой матрицы порядка $2n-1$, начиная с первой, к следующей каждый ее элемент, кроме последнего, смещается на одну позицию вправо, а последний – переходит на первую позицию; иначе говоря, все строки указанной матрицы получаются посредством последовательной (правой) циклической перестановки элементов его первой строки. Поэтому будем называть его правым циркулянтом.

Для транспонированной матрицы имеем: $U^{\prime}=(u_{ji})=\{e_{00},e_{m\,m+1}\}$, или, что то же самое, $U^{\prime}=\{e_{00},e_{m-1\,m}\}$; и значит, $UU^{\prime}=I$, т.е. $U^{\prime}=U^{-1}$. Далее, $U^2=\{e_{00},e_{k\,k-2}\}$, $U^3=U^2\,U=\{e_{00},e_{k\,k-3}\}$ и, вообще, $U^m=U^{m-1}\,U=\{e_{00},e_{k\,k-m}\}$. Отсюда следует $U^{2n-1}=I$. Поэтому можно считать $U^{2n-1-m}=U^{-m}$, причем $U^{-m}=\{e_{00},e_{k\,k-(2n-1-m)}\}=\{e_{00},e_{k\,k+m}\}$, а это равносильно $U^{-m}=\{e_{00},e_{k-m\,k}\}$. Сравнивая представления U^{-m} и U^m, видим, что $(U^m)^{\prime}=U^{-m}$. Очевидно, как часть матрицы U без нулевых строки и столбца, так и соответствующие подматрицы для всех ее степеней U^m являются правыми циркулянтами.

Введем теперь матрицу порядка $2n$ другого типа

$$V=(v_{ij})=\{e_{00},e_{1-k\,k}\}, \tag{3}$$

все отличные от нуля элементы которой, за исключение v_{00}, располагаются на малой диагонали, параллельной побочной диагонали матрицы. Значит, матрица V является симметрической, поэтому $V^2=I$. Из (2) и (3) следует, что $UV=\{e_{00},e_{2-k\,k}\}$, $U^2V=\{e_{00},e_{3-k\,k}\}$ и $U^mV=\{e_{00},e_{m+1-k\,k}\}$; причем все матрицы U^mV – симметрические, а значит, $(U^mV)^2=I$. Из последнего соотношения получаем

$$U^mV=VU^{-m}. \tag{4}$$

В силу отмеченных свойств, по аналогии с матрицей U^m, часть матрицы $U^m V$, которая остается после удаления нулевых строки и столбца, также является циркулянтом, но только не правым, а левым: при переходе от каждой строки этой матрицы порядка $2n-1$, начиная с первой, к следующей каждый ее элемент, кроме первого, смещается на одну позицию влево, а первый переходит на последнюю позицию.

И наконец, введем еще одну матрицу порядка $2n$, кососимметрическую

$$W = (w_{ij}) = \begin{matrix} & e_{0k}, & \\ -e_{k0} & & \end{matrix}, \tag{5}$$

у которой, за исключением w_{00}, в нулевой строке стоят $+1$, а в нулевом столбце -1. Так как все элементы матрицы W при $i-1$, $j-1$ равны нулю, то

$$U^m W = W U^m = VW = WV = W\,. \tag{6}$$

Наряду с этим непосредственно проверяется, что $W^2 = \begin{matrix} & -(2n-1)e_{00}, & \\ -e_{km} & & \end{matrix}$, т.е. все элементы матрицы W^2, кроме стоящих в нулевых строке и столбце, равны -1, а элемент на их пересечении равен $-(2n-1)$. Согласно [5, с. 233], матрица W^2 представима в виде

$$W^2 = -\sum_m U^m\,. \tag{7}$$

Здесь и далее пределы суммирования для m и k не указываются, так как они принимают одни и те же значения от 1 до $2n-1$.

Определим теперь наши матрицы A и B в (1) равенствами

$$A = W + \sum_k a_k U^k, \quad B = W + \sum_m b_m U^m V\,, \tag{8}$$

где каждое из a_k и b_m равно $+1$ или -1, причем $\sum_k a_k = \sum_m b_m = 1$. Заметим, что последнее возможно в силу нечетности $2n-1$. Так как матрицы U^k и $U^m V$ без нулевых строки и столбца являются циркулянтами, соответственно правым и левым, то таким же свойством обладают и матрицы A, B. Поэтому матрицу H вида (1) с данными A и B будем называть полуциркулянтной. Из представлений (8) следует, что каждый элемент матрицы H равен $+1$ или -1, причем так как $\sum_k a_k = \sum_m b_m = 1$, то $h_{00} = h_{02n} = 1$, и, значит, все элементы нулевой строки H равны $+1$. В нулевом ее столбце все элементы, кроме h_{00} и h_{2n0}, равны -1.

Как установлено выше, транспонированной для U^m является матрица U^{-m}. Поэтому, учитывая симметричность матрицы $U^m V$, имеем

$$A = W + \sum_k a_k U^{-k}, \quad B = W + \sum_m b_m U^m V\,. \tag{9}$$

По определению прямого кронекеровского произведения матриц (см., например, [1, с. 288]), матрица (1) представима в виде

$$H = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad A + \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad B,$$

а транспонированная – в виде

$$H = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad A + \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad B,$$

По свойству прямого произведения $(A_1 \quad B_1) \quad (A_2 \quad B_2) = A_1A_2 \quad B_1B_2$, где A_1, A_2, B_1 и B_2 – матрицы одного и того же порядка. Поэтому

$$HH = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad (AA + BB) + \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad (AB \quad BA), \qquad (*)$$

Используя представления (8) и (9), с помощью равенств (6) и (5) последовательно получаем

$$AB \quad BA = \left(W + \sum_k a_k U^k\right) \left(W + \sum_m b_m U^m V\right)$$

$$\left(W + \sum_m b_m U^m V\right) \left(W + \sum_k a_k U^{\ k}\right)$$

$$= 2W \left(\sum_m b_m \quad \sum_k a_k\right) + \sum_k a_k U^k \quad \sum_m b_m U^m V \quad \sum_m b_m U^m V \quad \sum_k a_k U^{\ k}$$

$$= \sum_{k,m} \left(a_k b_m U^{k+m} V \quad b_m a_k U^{m+k} V\right).$$

А значит, второе слагаемое в (*) равно нулю. Аналогично преобразуя другое выражение из (*), имеем

$$AA + BB = 2W^2 + \sum_k a_k U^k \quad \sum_k a_k U^{\ k} + \left(\sum_m b_m U^m V\right)^2$$

$$= 2W^2 + \sum_k a_k U^k \quad \sum_k a_k U^{\ k} + \sum_m b_m U^m \quad \sum_m b_m U^{\ m}.$$

Так как H является матрицей Адамара, если $HH = 4nI_{4n} = 4nI_2 \quad I_{2n}$, то с учетом равенства (*) получим, что матрица H вида (1) с A и B, задающимися равенствами (8), будет матрицей Адамара при выполнении условия

$$2W^2 + \sum_k a_k U^k \quad \sum_k a_k U^{\ k} + \sum_m b_m U^m \quad \sum_m b_m U^{\ m} = 4nI_{2n}. \qquad (10)$$

С целью упрощения последнего равенства положим $S = \sum_k U^k$ и обозначим через T_1 (T_2) сумму тех членов $\sum_k a_k U^k$ (соответственно $\sum_m b_m U^m$), для которых $a_k = +1$ ($b_m = +1$). Так как по предположению каждое a_k и b_m равно $+1$ или -1 и $\sum_k a_k = \sum_m b_m = 1$, то число положительных коэффициентов a_k равно числу положительных коэффициентов b_m и равно n. Используя вышесказанное и равенство (7), соотношение (10) приводим к виду

$$2S + (2T_1 - S)(2\bar{T}_1 - S) + (2T_2 - S)(2\bar{T}_2 - S) = 4nI_{2n}\,,$$

где $\bar{T}_1$ и $\bar{T}_2$ – сопряженные к T_1 и T_2 выражения, получающиеся из них заменой U^k на U^{-k} и U^m на U^{-m}, соответственно. Очевидно, для любого m $U^m S = SU^m = S$. Поэтому $S^2 = (2n-1)S, T_1 S = ST_1 = nS, T_2 S = ST_2 = nS$. Теперь (10) легко приводится к виду

$$T_1\bar{T}_1 + T_2\bar{T}_2 = n(S + I_{2n})\,. \tag{11}$$

Заметим, что если в (11) матрицу U заменить любой ее степенью, то равенство не нарушится. Это соображение полезно для практического построения матриц Адамара полуциркулянтного типа. Имеются и другие групповые свойства, которые представляют практический интерес и могут стать предметом отдельного исследования.

Поскольку в (11) фигурирует только матрица U и ее степени, причем $U^{2n-1} = I$, то это равенство можно рассматривать как соотношение между элементами группового кольца $R(C)$ над целыми числами, где C – циклическая группа с элементами u, $u^2, \ldots, u^{2n-2}$, $u^{2n-1} = 1$. Считая, что элемент u соответствует матрице U, равенство (11) после замены U на u в T_1, T_2 и S и связанной с этим замены обозначений последних на t_1, t_2 и s для $R(C)$ принимает вид

$$t_1\bar{t}_1 + t_2\bar{t}_2 = n(1 + s)\,. \tag{12}$$

Очевидно, что если верно (12), то верно и (11), а вместе с ним и соотношение (10) с W^2, выражающимся через степени U (7). Таким образом, нами доказано следующее утверждение.

Основная лемма. *Пусть C – циклическая группа порядка $2n-1$ (n – натуральное число) с порождающим элементом u и $s = 1 + \sum_{r=1}^{2n-2} u^r$. Если существуют такие полиномы $t_1 = \sum_{r=1}^{n} u^{i_r}$, $t_2 = \sum_{r=1}^{n} u^{j_r}$, где i_r, j_r – наборы из n различных чисел последовательности $1, 2, \ldots, 2n-1$, что для них и сопряженных им полиномов $\bar{t}_1$, $\bar{t}_2$ со степенями, показатели которых дополняют i_r и j_r до $2n-1$, выполняется соотношение (12), то существует матрица Адамара порядка $4n$ полуциркулянтного типа.*

Матрица Адамара, существование которой утверждается основной леммой, имеет вид (1), где A и B определяются равенствами (8) и (5). При этом

слагаемые с коэффициентами $a_k = 1$ и $b_m = 1$ входят в них только для тех k и m, для которых u^k и u^m входят в t_1 и t_2, соответственно. Для остальных значений k и m $a_k = a_m =$ 1. Как уже отмечалось, все элементы нулевой строки такой матрицы равны $+1$, а все элементы нулевого столбца, за исключением h_{00} и h_{2n0}, равны 1. Поэтому, умножив все, кроме двух, строки матрицы, на 1, можем привести ее к нормальному виду

$$\tilde{H} = \begin{pmatrix} \tilde{A} & \tilde{B} \\ \tilde{B} & \tilde{A} \end{pmatrix}, \quad \tilde{A} = \begin{pmatrix} 1 & e \\ e & \bar{A} \end{pmatrix}, \quad \tilde{B} = \begin{pmatrix} 1 & e \\ e & \bar{B} \end{pmatrix}, \qquad (13)$$

где e и e – строка и столбец из $2n$ 1 единиц, а e и e – из 1, матрицы $\bar{A}$ и $\bar{B}$ имеют порядок $2n$ 1 и являются правым и левым циркулянтом, соответственно, причем в каждую их строку 1 входит n раз, а $+1$ – n 1 раз (при умножении строк матрицы H на 1 элементы $+1$ и 1 меняются местами).

Если в нормализованной матрице Адамара $\tilde{H}$ отбросить нулевой столбец, то строки оставшейся матрицы можно рассматривать в качестве координат вершин правильного гиперсимплекса, вписанного в $(4n$ 1)-мерный куб с центром в начале координат. При этом все координаты каждой вершины равны по абсолютной величине единице. Действительно, так как строки $\tilde{H}$ попарно ортогональны, то квадрат расстояния d_{ij} между вершинами (x_i) и (y_i) нашего гиперсимплекса равен

$$d_{ij}^2 = \sum_{i=1}^{4n\ \ 1} (x_i \quad y_i)^2 = \sum_{i=1}^{4n\ \ 1} (x_i^2 \quad y_i^2)^2 \quad 2 \sum_{i=1}^{4n\ \ 1} x_i y_i = 2(4n \quad 1) \quad 2(\ \ 1) = 8n\,,$$

т.е. один и тот же для любых двух вершин.

4. В отличие от метода Уильямсона, который не дает бесконечных серий, для матриц Адамара полуциркулянтного типа имеет место следующая теорема.

Теорема 1. *Если* p 1(mod 4) – *простое число, то существует матрица Адамара порядка* $2(p+1)$ *полуциркулянтного типа, а в* $2(p+1)$*-мерный куб можно вписать правильный симплекс той же размерности.*

Доказательство. Прежде всего заметим, что поскольку p – нечетное простое число, то $2(p+1)$ есть число вида $4n$, где $n = \frac{p+1}{2}$, т.е. $p = 2n$ 1. Положим

$$t_1 = 1 + \sum_{r=1}^{n\ \ 1} u^{i_r}, \quad t_2 = 1 + \sum_{r=1}^{n\ \ 1} u^{j_r}, \qquad (\ \ )$$

где i_r – квадратичные вычеты по mod p, а j_r – квадратичные невычеты. Так как по условию $p \quad 1 \bmod 4$, то распределение квадратичных вычетов (и невычетов) по mod p является симметричным относительно $p/2$ [6, с. 157]. Это означает, что $\bar{t}_1 = t_1$ и $\bar{t}_2 = t_2$, т.е. $t_1\bar{t}_1 + t_2\bar{t}_2 = t_1^2 + t_2^2$. Используя это, преобразуем левую часть (12) с помощью $s = 1 + \sum_{r=1}^{2n} {}^{2} u^r$ следующим образом:

$$t_1\bar{t}_1 + t_2\bar{t}_2 = t_1^2 + \left(1 + \sum_{r=1}^{n} {}^{1} u^{j_r}\right)^2 = t_1^2 + \left(s \quad \sum_{r=1}^{n} {}^{1} u^{i_r}\right)^2$$

$$= t_1^2 + s + \left(\sum_{r=1}^{n} {}^{1} u^{i_r}\right)^2 1 + s + 2\sum_{r=1}^{n} {}^{1} u^{i_r} + \left(\sum_{r=1}^{n} {}^{1} u^{i_r}\right)^2 . \qquad (14)$$

Поскольку i_r – квадратичный вычет, то $i_r \quad x^2 (\mathrm{mod}\ p)$ для некоторого x, причем таких значений по mod p имеется два. Рассмотрим сравнение $x_1^2 + x_2^2 \quad l (\mathrm{mod}\ p)$, $l = 1, 2, \ldots, p \quad 1$. Для любого значения l это сравнение имеет $p \quad 1$ решений [6, с. 169]. Причем, если x_1, x_2 – его решение, то решениями также являются пары x_1, $\quad x_2$; $\quad x_1$, x_2; $\quad x_1$, $\quad x_2$ по mod p. Далее, если l не является квадратичным вычетом, то ни x_1, ни x_2 не равны нулю, и поэтому все эти четыре решения различны. А значит, число решений сравнения $q_1 + q_2 = j_r$, где q_1 и q_2 – квадратичные вычеты, соответствующие x_1 и x_2, равно $\frac{p \quad 1}{4}$. Тем самым каждый член u^{j_r} с показателем, не являющимся квадратичным вычетом, входит в (14) с коэффициентом $2 \quad \frac{p \quad 1}{4} = n \quad 1$. Если же l – квадратичный вычет, то наряду с решением 0, x_2 (или x_1, 0) есть по mod p еще только одно производное решение 0, $\quad x_2$ (или $\quad x_1$, 0). Поэтому число решений сравнения $q_1 + q_2 \quad i_r$ равно $\frac{p \quad 1 \quad 2 \; 2}{4} = \frac{p \quad 5}{4}$. И значит, каждый член u^{i_r} с показателем, являющимся квадратичным вычетом, входит в (14) с коэффициентом $2 + 2 \quad \frac{p \quad 5}{4} = \frac{p \quad 1}{2} = n \quad 1$. Свободный член в (14) равен $1 + 2\left(2 \quad \frac{n \quad 1}{2}\right) = 2n \quad 1$. Следовательно, $t_1\bar{t}_1 + t_2\bar{t}_2 = 2n \quad 1 + s + (n \quad 1)\sum_{i=1}^{n} {}^{1}(u^{i_r} + u^{j_r}) = n(1 + s)$, т.е. справедливо равенство (12). А значит, по основной лемме существует матрица Адамара порядка $4n = 2(p + 1)$ полуциркулянтного типа, что и требовалось доказать.

Известная теорема Пэли утверждает, что если $p^r \quad 1 (\mathrm{mod}\ 4)$, где p – простое число, а r – любое натуральное, то существует матрица Адамара порядка $2(p^r + 1)$ (см. [1, с. 292]). Эта матрица имеет вид

$$H = S \quad \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} + I \quad \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix},$$

где S – некоторая симметрическая матрица порядка $p^r + 1$ с нулями на главной диагонали, которая строится с помощью квадратичных вычетов (и невы-

четов) в конечных полях Галуа $GF(p^r)$. При $r = 1$ матрица принимает вид

$$S = \begin{pmatrix} 0 & e \\ e & Q \end{pmatrix},$$

где $Q = (q_{ij})$, $i, j = 0, 1, \ldots, p \quad 1$, причем $q_{ij} = 1$, если $i \quad j$ — квадратичный вычет по mod p; $q_{ij} = \quad 1$, если $i \quad j$ — квадратичный невычет, и $q_{ij} = 0$ при $i = j$. Перестановкой строк и столбцов матрицу Пэли можно преобразовать к виду

$$H = \begin{pmatrix} S+I & S & I \\ S & I & S & I \end{pmatrix}.$$

Отсюда видно, что такая матрица полуциркулянтной в нашем смысле не является, а значит, доказанная теорема дает матрицу Адамара порядка $2(p+1)$, отличную от построенной Пэли в 1933 году.

Так как $p = 2n \quad 1$ сравнимо с $1(\mathrm{mod}\ 4)$, то число n – нечетное, и, значит, теоремой 1 утверждается существование бесконечной серии полуциркулянтных матриц Адамара порядка $4n$ с нечетным n. Оказывается, при n четном также имеется бесконечная серия матриц Адамара полуциркулянтного типа, что следует из нашей основной леммы, доказанной для произвольного натурального n.

Теорема 2. *Если* $p \qquad 1(\mathrm{mod}\ 4)$ – *простое число, то существует матрица Адамара полуциркулянтного типа порядка* $2(p+1)$, *а в* $2(p+1)$*-мерный куб можно вписать правильный симплекс той же размерности.*

Доказательство. Как и в предыдущей теореме, $p = 2n \quad 1$, но теперь число n является четным. Так же, как и ранее, определим полиномы t_1 и t_2 равенствами (**). Поскольку $p \qquad 1(\mathrm{mod}\ 4)$, то распределение квадратичных вычетов (и невычетов) по mod p является кососимметрическим относительно $p/2$ [6, с. 157], а значит, если j_r — квадратичный невычет, то $p \quad j_r$ – квадратичный вычет, и поэтому $t_2 = \bar{t}_1$. Теперь имеем

$$t_1\bar{t}_1 + t_2\bar{t}_2 = 2\left(1 + \sum_{r=1}^{n\ \ 1} u^{i_r}\right)\left(1 + \sum_{r=1}^{n\ \ 1} u^{p\ \ i_r}\right) = 2\left[s + \sum_{r=1}^{n\ \ 1} u^{i_r} \quad \sum_{r=1}^{n\ \ 1} u^{p\ \ i_r}\right]. \quad (15)$$

Как видим, сравнение $x_1^2 + x_2^2 \qquad l(\mathrm{mod}\ p)$, которое рассматривалось в доказательстве теоремы 1, надо заменить другим: $x_1^2 \quad x_2^2 \qquad l$, но и оно для любого $l = 1, 2, \ldots, p \quad 1$ имеет тоже $p \quad 1$ решений [6, с. 169]; поскольку, если $p \qquad 1(\mathrm{mod}\ 4)$, то x_2^2 и $p \quad x_2^2$ одновременно являются квадратичными вычетами и, значит, эти два сравнения фактически ничем не отличаются. Если $l = i_r$, то наряду с решением x_1, 0 сравнение $x_1^2 \quad x_2^2 \qquad i_r(\mathrm{mod}\ p)$ имеет

еще одно решение $x_1,\ 0 \pmod p$, а если $l = j_r$, то его решениями являются и $0,\ x_2$ и $0,\ x_2 \pmod p$. Следовательно, коэффициент как при u^{i_r}, так и при u^{j_r} в (15) в квадратных скобках равен $\frac{p\ \ 1\ \ 2}{4} = \frac{n\ \ 2}{2}$, а свободный член равен $n\ \ 1$. После упрощений (15) получаем

$$t_1\bar{t}_1 + t_2\bar{t}_2 = 2\left[s + n\ \ \ 1 + \frac{n\ \ 2}{2}(s\ \ \ 1)\right] = n(1+s)\,,$$

т.е. и в рассматриваемом случае имеет место соотношение (12). А значит, для любого нечетного простого числа p существует матрица Адамара порядка $2(p+1)$ полуциркулянтного типа, что и требовалось доказать.

5. Выясним теперь геометрический смысл основной леммы. Рассмотрим циркулянты $\bar{A}$ и $\bar{B}$, входящие в нормализованную матрицу Адамара $\tilde{H}$ (13) и $(2n\ \ 1)$-мерный куб с центром в начале координат, для каждой вершины которого все координаты равны по абсолютной величине единице (ребро куба равно 2). Строки циркулянтов $\bar{A}$ и $\bar{B}$ представляют собой координаты вершин этого куба в $E^{2n\ \ 1}$. Все вершины, имеющие своими координатами строки из $\bar{A}$, являются вершинами некоторого $(2n\ \ 2)$-мерного симплекса, а вершины, имеющие своими координатами строки из $\bar{B}$, являются вершинами другого симплекса той же размерности. Добавим к каждому их них одну вершину, все координаты которой равны $+1$. Получим $(2n\ \ 1)$-мерные симплексы S_1 и S_2 с общей вершиной. Непосредственно проверяется, что эти симплексы обладают следующими свойствами:

1) вершины оснований симплексов S_1 и S_2 лежат на гиперсфере радиуса $\sqrt{4n}$ с центром в их общей вершине;

2) расстояние между i-й вершиной S_1 и j-й вершиной S_2 равно расстоянию между j-й вершиной S_1 и i-й вершиной S_2;

3) сумма квадратов длин соответствующих ребер S_1 и S_2 равна $8n$.

Заметим, что эти условия в несколько ином контексте были найдены автором ранее [7].

Лемма 1. *Если в $(2n\ \ 1)$-мерный куб с ребром 2 можно вписать $(2n\ \ 1)$-мерные симплексы S_1 и S_2 такие, что для них выполняются условия 1)–3), то в $(4n\ \ 1)$-мерный куб можно вписать правильный симплекс той же размерности.*

Доказательство. Выберем систему координат в $E^{2n\ \ 1}$ так, чтобы ее начало совпадало с центром нашего куба, а оси координат были параллельны его ребрам. Обозначим через A и B матрицы, i-я строка которых представляет собой координаты i-й вершины основания симплекса S_1 и S_2, соответственно. Построим из них следующую матрицу H порядка $4n\ \ 1$

(обозначения те же, что и в (13)):

$$H = \begin{pmatrix} A & e & B \\ e & 1 & e \\ B & e & A \end{pmatrix}$$

и рассмотрим симплекс S, вершинами которого являются точка 1, 1,... 1 и все точки, координаты которых совпадают со строками матрицы H . Докажем, что этот симплекс правильный.

В силу условия 1) число 1 в каждой строке матрицы H встречается $2n$ раз, а число $+1$ — $2n$ 1 раз, т.е. любая вершина с такими координатами удалена от вершины 1, 1,...,1 на расстояние $\overline{4 \quad 2n} = \overline{8n}$. По условию 3) то же значение имеет и расстояние между любыми двумя вершинами, координаты которых являются двумя строками матрицы H из ее первых или последних $2n$ 1 строк. Так как в каждой строке матриц A и B число 1 встречается n раз, а $+1$ — n 1 раз, то вершина $\underbrace{+1, +1, \ldots, +1}_{n \ 1 \text{ раз}}, \underbrace{1, \ 1, \ldots, \ 1}_{n \text{ раз}}$ симплекса S тоже удалена от всех остальных его вершин на расстояние $\overline{8n}$.

Рассмотрим, наконец, случай, когда координатами одной вершины симплекса S является i-я строка из первых $2n$ 1 строк матрицы H , а другой – j-я строка из $2n$ 1 ее последних строк. Пусть $x_{i_1}, x_{i_2}, \ldots, x_{i_{4n \ 1}}$ – координаты первой вершины, а $x_{j_1}, x_{j_2}, \ldots, x_{j_{4n \ 1}}$ – второй. Тогда квадрат расстояния между ними равен

$$d^2 = \sum_{r=1}^{2n \ 1} (x_{i_r} \quad x_{j_r})^2 + \sum_{r=2n+1}^{4n \ 1} (x_{i_r} \quad x_{j_r})^2 + (x_{i_{2n}} \quad x_{j_{2n}})^2 .$$

С другой стороны, по условию 2) доказываемой леммы

$$\sum_{r=1}^{2n \ 1} (x_{i_r} \quad x_{j_r})^2 = \sum_{r=2n+1}^{4n \ 1} (x_{i_r} + x_{j_r})^2 .$$

Но так как $x_{i_r}^2 = x_{j_r}^2 = 1$ для всех r, то

$$\sum_{r=1}^{2n \ 1} x_{i_r} x_{j_r} + \sum_{r=2n+1}^{4n \ 1} x_{i_r} x_{j_r} = 0 .$$

А значит, $d^2 = 4(2n \quad 1) + 4 = 8n$ (при этом учтено, что $x_{i_{2n}} = 1$, а $x_{j_{2n}} = 1$). Тем самым все ребра симплекса S равны между собою, и значит, он правильный, что и требовалось доказать.

Добавив к матрице H слева столбец из $+1$, получим нормализованную матрицу Адамара $\tilde{H}$ порядка $4n$, однако, вообще говоря, не полуциркулянтного типа. Чтобы сделать ее таковой, основания симплексов S_1 и S_2 должны еще иметь группу самосовмещений, которая включает в себя некоторую циклическую подгруппу порядка $2n-1$, переставляющую их вершины по правому или левому циклу. Найдем ее.

Рассмотрим для этого в E^{2n-1} прямоугольную систему координат $x_1, x_2, \ldots, x_{2n-1}$. Пусть P – правильный симплекс, все вершины P_i которого находятся на положительных полуосях данной системы координат на одном и том же расстоянии от начала координат. Группа симметрий этого симплекса порождается транспозициями $R_i = (i, i+1)$, $i = 1, 2, \ldots, 2n-2$, которые соответствуют отражениям симплекса в гиперплоскостях, перпендикулярных ребрам P_iP_{i+1} и проходящих через их середину [8, с. 96–100, 177]. Так как $2n-2$ – четное число, то движения

$$R = \prod_{i=1}^{2n-2} R_i = (1, 2n-1, 2n-2, \ldots, 2)R^+ = \prod_{i=2n-2}^{1} R_i = (1, 2, 3, \ldots, 2n-1)$$

являются, очевидно, вращениями. Вращение $R^+(R)$ имеет порядок $2n-1$ и переставляет вершины P_i симплекса и, значит, оси координат x_i по правому (левому) циклу. Таким образом, чтобы нормализованная матрица $\tilde{H}$ была полуциркулянтной, необходимо к условиям 1)–3) леммы 1 добавить еще одно:

4) Основания симплексов S_1 и S_2 обладают группой самосовмещений, включающей в себя вращение $R^+(R)$. Далее имеет место следующее утверждение.

Лемма 2. *Если для симплексов S_1 и S_2 выполняются условия 1), 3) и 4), причем соответствующими вершинами оснований симплексов S_1 и S_2 служат те, которые являются образами их первых вершин при вращениях $(R^+)^{i-1}$ и $(R)^{i-1}$, соответственно ($i = 1, 2, \ldots, 2n-1$), то для них выполняется и условие 2).*

Доказательство. Пусть c^1_k, c^2_k, $k = 1, 2, \ldots, 2n-1$ – координаты первой вершины основания симплекса S_1 и S_2, соответственно. Тогда координатами их i-х вершин будут $c^1_{k\ 1+i}$ и $c^2_{k+1\ i}$. Обозначим $d_{i,j}$ – расстояние между i-й вершиной основания S_1 и j вершиной основания S_2 ($j > i$). Тогда

$$d^2_{i,j} = \sum_{k=1}^{2n-1} \left(c^1_{k\ 1+i} - c^2_{k+1\ j}\right)^2 = 2(2n-1) - 2\sum_{k=1}^{2n-1} c^1_{k\ 1+i}\, c^2_{k+1\ j}\,.$$

Найдем теперь квадрат расстояния между j-й вершиной S_1 и i-й S_2:

$$d^2_{j,i} = \sum_{k=1}^{2n-1} \left(c^1_{k\ 1+j} - c^2_{k+1\ i}\right)^2 = 2(2n-1) - 2\sum_{k=1}^{2n-1} c^1_{k\ 1+j}\, c^2_{k+1\ i}$$

$$= \quad 2(2n \quad 1) \quad 2\sum_{r=1}^{2n \quad 1} c^1_{r \quad 1+i}\, c^2_{r+1 \quad j} \ ,$$

где $r = \ k+j \quad i$, т.е. $r = k+j \quad i$ при $k+j \quad i \quad 2n \quad 1$ и $k+j \quad i(2n \quad 1)$ в противном случае. Как видим, $d_{j,i} = d_{i,j}$, что и требовалось доказать.

Условия 1), 3) и 4) получены нами из условий основной леммы. Докажем теперь, что верно и обратное. Действительно, пусть c^1_k и c^2_k – как и выше, координаты первых вершин оснований симплексов S_1 и S_2. По условию 1) среди c^1_k, c^2_k координата $\quad 1$ встречается n раз, а $+1$ — по $n \quad 1$ раз. Обозначим через $N^1_r(N^2_r)$, $r = 1, 2, \ldots, 2n \quad 2$ число упорядоченных пар элементов последовательности $c^1_k(c^2_k)$, равных $\quad 1$, для которых разность их порядковых номеров равна r по mod $(2n \quad 1)$. Очевидно, $N^j_{2n \quad 1 \quad r} = N^j_r$, $j = 1, 2$. Выразим через $N^j_{i \quad 1}$ квадрат расстояния d_j между первой и i-й вершинами $(i > 1)$ основания S_j, учитывая при этом, что $N^1_{i \quad 1}$ отрицательных координат первой и i-й вершины S_1 равны между собой (аналогично для S_2):

$$d^2_1 = 2(n \quad N^1_{i \quad 1})(1 \quad (\quad 1))^2 = 8(n \quad N^1_{i \quad 1}) \ ,$$

$$d^2_2 = 2(n \quad N^2_{i \quad 1})(1 \quad (\quad 1))^2 = 8(n \quad N^2_{i \quad 1}) \ .$$

Так как по условию 3) $d^2_1 + d^2_2 = 8n$, то подставляя сюда найденные для d_1 и d_2 значения, получим $N^1_{i \quad 1} + N^2_{i \quad 1} = n$. Следовательно, для любого $r = 1, 2, \ldots, 2n \quad 2$ по условию 4) справедливо соотношение $N^1_r + N^2_r = n$.

Пусть $i_1, i_2, \ldots, i_n$ – порядковые номера координат c^1_k, равных $\quad 1$, $j_1, j_2, \ldots, j_n$ – порядковые номера координат c^2_k, равных $\quad 1$. Положим

$$t_1 = \sum_{r=1}^{n} u^{ir}, \quad t_2 = \sum_{r=1}^{n} u^{jr} \ .$$

Заметим, что если в t_1 входят u^k и u^m, то в $\bar{t}_1$ входят $u^{\quad k}$ и $u^{\quad m}$ и, значит, в произведение $t_1\bar{t}_1$ входят: 1 (дважды) $u^{k \quad m}$ и $u^{m \quad k}$, где знак модуля означает то же, что и раньше. Таким образом, по определению чисел N^1_r имеем $t_1\bar{t}_1 = n + \sum_{r=1}^{2n \quad 1} N^1_r u^r$. Аналогично, $t_2\bar{t}_2 = n + \sum_{r=1}^{2n \quad 1} N^2_r u^r$. А так как по доказанному $N^1_r + N^2_r = n$, то $t_1\bar{t}_1 + t_2\bar{t}_2 = 2n + n\sum_{r=1}^{2n \quad 1} u^r = n(1+s)$, т.е. для полиномов t_1 и t_2 выполняется условие (12) основной леммы.

Из доказанного следует, что выполнения геометрических по сути условий 1), 3 и 4) достаточно для существования матрицы Адамара полуциркулянтного типа порядка $4n$ (n – натуральное число).

Список литературы

[1] *М. Холл*, Комбинаторика. Мир, Москва (1970), 424 с.

[2] *А.И. Медяник*, О построении матриц Адамара. — Математическая физика, анализ, геометрия (1995), т. 2, № 1, с. 87–93.

[3] *Дж. Конвей, Н. Слоэн*, Упаковки шаров, решетки и группы. Т. 1. Мир, Москва (1990), 413 с.

[4] *J. Williamson*, Hadamar's determinant theorem and sum of four squares. — Duke Math. J. (1944), v. 11, p. 65–81.

[5] *П. Ланкастер*, Теория матриц. Наука, Москва (1982), 270 с.

[6] *Г. Хассе*, Лекции по теории чисел. Изд-во иностр. лит., Москва (1953), 527 с.

[7] *А.И. Медяник*, Правильный симплекс, вписанный в куб. — Укр. геометр. сб. (1973), вып. 13, с. 109–112.

[8] *Г.С.М. Коксетер, У.О.Дж. Мозер*, Порождающие элементы и определяющие соотношения дискретных групп. Наука, Москва (1980), 240 с.

Regular simplex inscribed into a cube and Hadamard matrix of half-circulant type

A.I. Medianik

It's discovered a sufficient condition for existence of the Hadamard matrix of order $4n$ (n – natural number) of half-circulant type, which contains two different circulants of order $2n \quad 1$: right and left one (from here the term). A new method of the Hadamard matrices construction, which is geometrical in point of fact and different from the well-known Williamson method, is received. It's proved as well, that there is the Hadamard matrix of order $2(p+1)$ of half-circulant type, where p is odd prime number, whence it follows, that into $2(p+1)$-dimensional cube one can to inscribe a regular simplex of the same dimension.

Вписаний в куб правильний симплекс та матриця Адамара напівциркулянтного типу

А.Г. Медяник

Знайдено достатню умову для того, щоб існувала матриця Адамара порядку $4n$ напівциркулянтного типу (n – довільне натуральне число), яка включає в себе два різних циркулянта порядку $2n \quad 1$ — правий та лівий (звідси назва). З цієї умови випливає інший, відмінний від відомого методу Уіл'ямсона метод побудови матриць Адамара, геометричний по своїй суті. Доведено також, що існує матриця Адамара порядку $2(p+1)$, де p – непарне просте число напівциркулянтного типу, звідки випливає, що в $2(p+1)$-вимірний куб можна вписати правильний симплекс тієї ж вимірності.