Математическая физика, анализ, геометрия
2001, т. 8, № 1, с. 58–81

Вписанный в куб правильный симплекс, полуциркулянтные матрицы Адамара и гауссовы суммы

А.И. Медяник

Физико-технический институт низких температур им. Б.И. Веркина НАН Украины
Пр. Ленина, 47, г. Харьков, 61164, Украина

E-mail:medianik@ilt.kharkov.ua

Статья поступила в редакцию 1 марта 2000 года

Представлена Ю.А. Аминовым

С помощью метода тригонометрических сумм доказывается, что если число $2n-1$ простое или равно произведению двух простых чисел-близнецов, то существует полуциркулянтная матрица Адамара порядка $4n$ и в $(4n-1)$-мерный куб можно вписать правильний симплекс той же размерности. Изучаются также групповые свойства пар полиномов, порождающих матрицы Адамара полуциркулянтного типа, и устанавливаются эффективно проверяемые необходимые условия существования для данного полинома (из некоторого группового кольца над целыми числами) другого полинома, образующего с ним такую пару, которые используются для практического построения с помощью компьютера матриц Адамара всех порядков $4n \leq 80$.

Настоящая статья является продолжением исследований, начатых автором в [1], с применением нового средства — тригонометрических полиномов, в частности, сумм Гаусса, что позволяет не только получить более простые доказательства установленных ранее теорем о бесконечных сериях матриц Адамара полуциркулянтного типа, но и расширить их список (см. теоремы 1 и 2). Кроме того, для нужд практического нахождения (с помощью компьютеров) полуциркулянтных матриц Адамара высших порядков в ней изучаются групповые свойства пар полиномов, порождающих их (теорема 3). Эти свойства вместе с полученными для разностных множеств порождающих полиномов необходимыми условиями (лемма 3) настолько эффективны, что с помощью созданной автором универсальной программы (на ПЭВМ с

© А.И. Медяник, 2001

процессором 486-го типа) удается найти порождающие полиномы для полуциркулянтных матриц Адамара всех порядков $4n \le 80$ (см. табл. 2 и 3). Причем при $4n \le 68$ эта программа позволяет найти все различные (неэквивалентные в смысле теоремы 3) матрицы Адамара, общее число которых приводится в разд. 7.

1. Для удобства изложения напомним основную лемму из [1]:

Основная лемма. *Пусть C — циклическая группа порядка $2n-1$ с порождающим элементом u ($u^{2n-1} = u^0 = 1$), и $s_n = 1 + \sum\limits_{r=1}^{2n-2} u^r$. Если существуют такие полиномы $t_1 = \sum\limits_{r=1}^{n} u^{i_r}$ и $t_2 = \sum\limits_{r=1}^{n} u^{j_r}$, где $\{i_r\}$ и $\{j_r\}$ — наборы различных натуральных чисел, меньших $2n$, что для них и сопряженных им полиномов $\overline{t}_1 = \sum\limits_{r=1}^{n} u^{2n-1-i_r}$ и $\overline{t}_2 = \sum\limits_{r=1}^{n} u^{2n-1-j_r}$ в групповом кольце $R(C)$ над целыми числами выполняется соотношение*

$$t_1\overline{t}_1 + t_2\overline{t}_2 = n(1+s_n), \tag{1}$$

то существует матрица Адамара порядка $4n$ полуциркулянтного типа.

Поясним, что матрица Адамара (нормализованная), существование которой утверждается этой леммой, имеет вид

$$H = \begin{pmatrix} A & B \\ B & -A \end{pmatrix}, \quad A = \begin{pmatrix} 1 & e \\ e' & \overline{A} \end{pmatrix}, \quad B = \begin{pmatrix} 1 & e \\ e' & \overline{B} \end{pmatrix},$$

где подматрицы A и B имеют порядок $2n$ и содержат в себе циркулянты $\overline{A}$ и $\overline{B}$ (соответственно правый и левый) порядка $2n-1$, причем e и e' в них — строки и столбцы из $+1$. Сами циркулянты строятся с помощью наборов натуральных чисел i_r и j_r следующим образом: в первой строке циркулянта A (правого) сначала на местах с номерами i_r, $r = 1, \ldots, n$, расставляется число -1, а на остальных — число $+1$, после чего из первой строки $\overline{A}$ циклической перестановкой вправо, т.е. сдвигом на одну позицию вправо всех элементов, кроме последнего, который переходит на первую позицию, последовательно получаются остальные строки $\overline{A}$; аналогично с помощью чисел j_r строится циркулянт B (левый), только циклические перестановки элементов его первой строки производятся влево; первый элемент строки при этом переходит на последнюю позицию.

Заметим, что строки матрицы H', которая получается из H удалением первого столбца, состоящего из $+1$, являются координатами вершин правильного гиперсимплекса в E^{4n-1}, вписанного в $(4n-1)$-мерный куб с ребром 2, центр которого находится в начале координат, а каждое ребро параллельно

одной из осей координат. Поэтому нахождение полуциркулянтной матрицы Адамара того или иного порядка $4n$ означает одновременно и возможность построения правильного симплекса, вписанного в куб той же размерности.

2. Полагая теперь $n > 1$, рассмотрим соотношение (1) в поле комплексных чисел, положив $u = e^{\frac{2\pi i}{2n-1}}$. Тогда полином s_n, равный сумме всех корней степени $2n-1$ из 1, обратится в нуль, а полиномы t_j и $\overline{t}_j$, $j = 1, 2$, станут комплексно сопряженными. И значит, равенство (1) примет вид

$$|t_1|^2 + |t_2|^2 = n. \tag{2}$$

Не следует, однако, думать, что если (2) выполняется, то для соответствующих полиномов кольца $R(C)$ выполняется (1). Например, для $n = 8$ и $t_1 = 1+u^3+u^5+u^7+u^8+u^{10}+u^{12}+u^{14}$, $t_2 = 1+u^2+u^3+u^5+u^6+u^7+u^8+u^{14}$ имеем

$$t_1\overline{t}_1 + t_2\overline{t}_2 - 8 = (1 + u^5 + u^{10})(8 + 7u + 9u^2 + 9u^3 + 7u^4).$$

Если положить $u = e^{\frac{2\pi i}{15}}$, то первый сомножитель в правой части обратится в нуль, так как s_8 делится на него. Это означает, что для t_1 и t_2 в поле комплексных чисел выполняется (2), тогда как в $R(C)$ соотношение (1) места не имеет.

Лемма 1. *Для того чтобы в групповом кольце $R(C)$ для полиномов $t_1 = \sum\limits_{r=1}^{n} u^{i_r}$ и $t_2 = \sum\limits_{r=1}^{n} u^{j_r}$ выполнялось соотношение (1), необходимо и достаточно, чтобы (2) имело место для всех $u = e^{\frac{2\pi mi}{2n-1}}$, $m = 1, 2, \ldots, 2n-2$. Точнее, достаточно, чтобы для каждого делителя $d > 1$ числа $2n-1$ равенство (2) имело место хотя бы для одного первообразного корня степени d из единицы.*

Доказательство. Необходимость по существу обоснована выше. Докажем достаточность, обозначив через φ_j полином, корнями которого являются все первообразные корни из единицы степени делителя $d_j > 1$, $j = 1, 2, \ldots, k$. Так как по предположению $|t_1|^2 + |t_2|^2 = n$ для любого первообразного корня из единицы степени d_j, то в групповом кольце $R(C)$ имеем

$$t_1\overline{t}_1 + t_2\overline{t}_2 - n = t(u)\prod_{j=1}^{k}\varphi_j, \tag{3}$$

где $t(u)$ — некоторый неизвестный полином. Поскольку $d_j > 1$, то произведение всех φ_j — полиномов деления круга — равно $(u^{2n-1}-1)/(u-1) = s_n$,

степень которого равна $2n-2$. Такую же степень в $R(C)$ имеет и левая часть (3), значит $t(u)$ — постоянная. И так как свободный член левой части (3) равен n, а свободный член s_n равен 1, то $t = n$. Таким образом, соотношение (3) эквивалентно равенству (1), что и требовалось доказать. Последнее утверждение леммы следует из того, что каждый полином деления круга φ_j является неприводимым над полем рациональных чисел, в частности, если d_j — простое число, то $\varphi_j = 1 + u + u^2 + ... + u^{d_j - 1}$ [2, с. 64]. Лемма доказана.

Заметим, что в рассмотренном выше примере $1+u^5+u^{10} = (1+u+u^2)(1-u+u^3-u^4+u^5-u^7+u^8)$, где первый сомножитель является третим полиномом деления круга, корнями которого служат первообразные корни третьей степени из 1, а второй — полином деления круга, корнями которого являются первообразные корни из 1 степени 15. Что касается второго сомножителя в этом примере, то он, очевидно, не есть пятый полином деления круга. И значит, одно из условий леммы 1 для него не выполняется.

3. Пусть теперь $2n - 1 = p$, где p — простое число. Рассмотрим тригонометрическую гауссову сумму (см. [3], с. 124–I25):

$$\tau = \sum_{m=1}^{p-1} \left(\frac{m}{p}\right) = e^{\frac{2\pi m i}{2n-1}},$$

где $\left(\frac{m}{p}\right)$ — символ Лежандра, который равен 1, если m — квадратичный вычет по модулю p, и -1, если m — квадратичный невычет. Добавим, что если $m \equiv 0 (\mathrm{mod}\, p)$, то $\left(\frac{m}{p}\right) = 0$. Гаусс доказал, что $\tau = \varepsilon\sqrt{p}$, причем $\varepsilon = 1$ для $p \equiv 1 (\mathrm{mod}\, 4)$ и $\varepsilon = i$ для $p \equiv -1 (\mathrm{mod}\, 4)$. Используя это, докажем следующую теорему.

Теорема 1. *Если $2n-1$ — простое число, то существует матрица Адамара порядка $4n$ полуциркулянтного типа и в $(4n-1)$-мерный куб можно вписать правильный симплекс той же размерности.*

Доказательство. Положим $p = 2n - 1$ и построим полиномы

$$t_1 = 1 + \sum_{r=1}^{n-1} u^{i_r}, \quad t_2 = 1 + \sum_{r=1}^{n-1} u^{j_r}, \quad u = e^{\frac{2\pi i}{p}},$$

где i_r и j_r — соответственно квадратичные вычеты и невычеты по модулю p. По свойству гауссовой суммы $t_1 - t_2 = \tau = \varepsilon\sqrt{p}$. Кроме того, очевидно, $t_1 + t_2 = 1$. Отсюда находим $t_1 = (1 + \varepsilon\sqrt{p})/2, t_2 = (1 - \varepsilon\sqrt{p})/2$. И значит, $|t_1|^2 + |t_2|^2 = \frac{1}{4}\left(|1 + \varepsilon\sqrt{p}|^2 + |1 - \varepsilon\sqrt{p}|^2\right)$. Непосредственно проверяется, что

и при $\varepsilon = 1$, и при $\varepsilon = i$ $|t_1|^2 + |t_2|^2 = n$. Следовательно, для полиномов t_1 и t_2 выполняются условия леммы 1 и, значит, основной леммы, откуда и вытекает утверждение теоремы 1.

Заметим, что утверждение доказанной теоремы совпадает с утверждениями теорем 1 и 2 из [1], в которых случаи $p \equiv 1(\mathrm{mod}\,4)$ и $p \equiv -1(\mathrm{mod}\,4)$ рассматривались отдельно друг от друга.

4. Как известно, гауссова сумма обобщается на случай натурального ведущего модуля, когда число $2n-1$ — составное, но свободное от квадратов, т.е. равно произведению различных простых чисел: $2n-1 = \prod\limits_{j=1}^{k} p_j$ (см. [3], с. 239). При этом вместо символа Лежандра используется символ Якоби $\left(\frac{m}{2n-1}\right) = \prod\limits_{j=1}^{k}\left(\frac{m}{p_j}\right)$. Тогда для обобщенной гауссовой суммы $\tau = \sum\limits_{m=0}^{2n-2}\left(\frac{m}{2n-1}\right)e^{\frac{2\pi mi}{2n-1}}$ по теореме XI [3, с. 497] $\tau = \varepsilon\sqrt{2n-1}$, причем ε — то же самое, что и в сумме Гаусса.

Полагая $u = e^{\frac{2\pi i}{2n-1}}$, найдем частичные суммы τ_1 и τ_2 , соответствующие по аналогии с символом Лежандра последовательностям чисел m, для которых символ Якоби равен 1 или -1, т.е.

$$\tau_1 = \sum_{r=1}^{N_1} u^{i_r}, \quad \tau_2 = \sum_{r=1}^{N_2} u^{j_r}, \tag{4}$$

где числа N_1 и N_2 подлежат определению.

Во-первых, символ Якоби отличен от нуля только для чисел, взаимно простых с модулем $2n-1$. Их количество равно функции Эйлера φ (см. [3, с. 59]):

$$\varphi(2n-1) = (2n-1)\prod_{j=1}^{k}\left(1-\frac{1}{p_j}\right) = \prod_{j=1}^{k}(p_j-1)\,.$$

Во-вторых, по свойству III [3, с. 138], требование $\left(\dfrac{m}{2n-1}\right) = 1$ определяет в группе классов вычетов по модулю $2n-1$, взаимно простых с модулем, подгруппу индекса 2 (так как по предположению число $2n-1$ свободно от квадратов). А значит, τ_1 и τ_2 содержат одинаковое число слагаемых $N_1 = N_2 = \dfrac{1}{2}\prod\limits_{j=1}^{k}(p_j-1)$.

По свойству обобщенной гауссовой суммы

$$\tau_1 - \tau_2 = \tau = \varepsilon\sqrt{2n-1}. \tag{5}$$

Запишем теперь условие равенства нулю суммы всех корней из 1 степени $2n-1$ в виде

$$1+\tau_1+\tau_2-\sum_{s=1}^{k-1}(-1)^s\sum_{j_1\neq j_2\neq\ldots\neq j_s}\sum_{m=1}^{M_{j_1\ldots j_s}}u^{p_{j_1}p_{j_2}\ldots p_{j_s}m}=0,$$

где $M_{j_1\ldots j_s}=\dfrac{2n-1}{\prod\limits_{r=1}^{s}p_{j_r}}-1$. Отсюда, учитывая, что для любого делителя d_j числа $2n-1$ $\sum\limits_{m=1}^{\frac{2n-1}{d_j}-1}u^{d_jm}=-1$, получаем

$$\tau_1+\tau_2=-1-\sum_{s=1}^{k-1}(-1)^sC_k^s=(-1)^k. \tag{6}$$

Из уравнений (5) и (6) находим

$$\tau_1=\frac{(-1)^k+\varepsilon\sqrt{2n-1}}{2},\quad \tau_2=\frac{(-1)^k-\varepsilon\sqrt{2n-1}}{2}. \tag{7}$$

Легко проверяется, что при любом значении $\varepsilon=1$ или $\varepsilon=i$ $|\tau_1|^2+|\tau_2|^2=n$, т.е. для полиномов τ_1 и τ_2 выполняется условие (2). Однако поскольку число слагаемых в них равно $\dfrac{1}{2}\prod\limits_{j=1}^{k}(p_j-1)$, что заведомо меньше $n=\dfrac{1}{2}\left(1+\prod\limits_{j=1}^{k}p_j\right)$, то этого еще недостаточно для существования полуциркулянтной матрицы Адамара порядка $4n$.

Теорема 2. *Если $2n-1=p(p+2)$, причем p и $p+2$ оба являются простыми числами, то существует матрица Адамара порядка $4n$ полуциркулянтного типа и в $(4n-1)$-мерный куб можно вписать правильный симплекс той же размерности.*

Доказательство. По условию теоремы $n=\frac{p(p+2)+1}{2}=\frac{(p+1)^2}{2}$, $N_1=N_2=\frac{p^2-1}{2}$. Построим полиномы t_1 и t_2 с помощью (4), положив $u=e^{\frac{2\pi i}{2n-1}}$:

$$t_1=\tau_1+\sum_{m=1}^{p+1}u^{pm},\quad t_2=\tau_2+\sum_{m=1}^{p+1}u^{pm}. \tag{8}$$

При этом число слагаемых в t_1 и t_2 станет равным n (так как $\frac{p^2-1}{2} + (p+1) = n$). Далее, поскольку $\sum\limits_{m=1}^{p+1} u^{pm} = -1$, то, учитывая, что в рассматриваемом случае $k = 2$ и $2n-1 \equiv -1 (\mathrm{mod}\, 4)$, с помощью (7) находим $t_1 = \frac{-1+i\sqrt{2n-1}}{2}, t_2 = \frac{-1-i\sqrt{2n-1}}{2}$. Для первообразных корней степени $2n-1$ из единицы имеем $|t_1|^2 + |t_2|^2 = n$, т.е. условие (2) леммы 1 для них выполняется. Докажем теперь, что оно выполняется и для первообразных корней из 1 степеней p и $p+2$.

В качестве первообразного корня степени p из 1 можно взять $\overline{u} = u^{p+2}$. Так как для любого m $\overline{u}^{pm} = 1$, то $\sum\limits_{m=1}^{p+1} \overline{u}^{pm} = p+1$. А значит, $t_1(\overline{u}) = \tau_1(\overline{u}) + p + 1$, $t_2(\overline{u}) = \tau_2(\overline{u}) + p + 1$. Кроме того, для любого натурального $r < p$ и любого натурального $s < p+2$ $\overline{u}^{r+ps} = \overline{u}^r$, причем среди чисел $r+ps$ только одно кратно p+2 (т.е. не взаимно просто с $2n-1$), а остальные имеют отличный от нуля символ Лежандра $\left(\frac{r+ps}{p+2}\right)$. И поскольку для каждого r и любого целого b сравнение $px \equiv b - r$ имеет одно и только одно решение $x \bmod (p+2)$ [3, с. 49–50], то числа $r, r+p, r+2p, \ldots, r+(p+1)p$ принадлежат различным классам вычетов по модулю $p+2$, т.е. среди них имеется точно $\frac{p+1}{2}$ чисел, символ Лежандра для которых по простому модулю $p+2$ равен 1, и столько же чисел, для которых он равен -1. А так как $\left(\frac{r+ps}{p}\right) = \left(\frac{r}{p}\right)$, то символ Якоби для первых $\frac{p+1}{2}$ чисел равен $\left(\frac{r}{p}\right)$, а для вторых — отличается только знаком. Это означает, что $\left(\frac{p+1}{2}\right)$ из членов $\overline{u}^r, \overline{u}^{r+p}, \ldots, \overline{u}^{r+(p+1)p}$ входят в $\tau_1(\overline{u})$, и столько же — в $\tau_2(\overline{u})$, т.е. $\tau_1(\overline{u}) = \tau_2(\overline{u}) = \frac{p+1}{2}\sum\limits_{r=1}^{p-1} \overline{u}^r = -\frac{p+1}{2}$. Таким образом,

$$|t_1(\overline{u})|^2 + |t_2(\overline{u})|^2 = |-\frac{p+1}{2} + p + 1|^2 + |-\frac{p+1}{2} + p + 1|^2 = n.$$

Аналогично рассматривается и случай первообразного корня из 1 степени $p+2$ $\overline{u} = u^p$, для которого получается

$$\prod_{m=1}^{p+1} \overline{u}^{pm} = -1, \quad \tau_1(\overline{u}) = \tau_2(\overline{u}) = \frac{p-1}{2}\sum_{r=1}^{p+1} \overline{u}^r = -\frac{p-1}{2}.$$

И значит,

$$|t_1(\overline{u})|^2 + |t_2(\overline{u})|^2 = |-\frac{p-1}{2} - 1|^2 + |-\frac{p-1}{2} - 1|^2 = n.$$

Тем самым для полиномов t_1 и t_2, задаваемых формулами (8), выполняются все условия леммы 1. Следовательно, по основной лемме эти полиномы порождают полуциркулянтную матрицу Адамара порядка $4n = 2(p+1)^2$. Теорема доказана.

5. Теоремы 1 и 2 дают бесконечные серии матриц Адамара полуциркулянтного типа для случаев, когда число $2n-1$ является простым или равно произведению двух простых чисел-близнецов. Для нахождения полуциркулянтных матриц Адамара произвольного порядка необходимо изучить свойства полиномов t_1 и t_2, удовлетворяющих условиям леммы 1, в частности соотношению (2).

Полагая $z = e^{i\nu}$, где $\nu = \dfrac{2\pi m}{2n-1}$, а m – натуральное число, меньшее $2n-1$, представим полиномы t_1 и t_2 в виде

$$t_1 = \sum_{k=0}^{2n-2} x_k z^k, \quad t_2 = \sum_{k=0}^{2n-2} \overline{x}_k z^k, \tag{9}$$

считая, что каждое $x_k(\overline{x_k})$ равно 0 или 1, причем $\sum\limits_{k=0}^{2n-2} x_k = \sum\limits_{k=0}^{2n-2} \overline{x}_k = n$. Тогда соотношение (2) примет вид

$$\left|\sum_{k=0}^{2n-2} x_k z^k\right|^2 + \left|\sum_{k=0}^{2n-2} \overline{x}_k z^k\right|^2 = n, \tag{10}$$

Так как $|e^{i\nu}| = 1$, то при умножении t_1 и t_2 на z и, вообще, на z^s равенство в (10) не нарушится. Это означает, что каждое решение (10) порождает другие его решения, которые получаются из него циклической перестановкой на s позиций коэффициентов x_k и $\overline{x}_k$ (поскольку $z^{2n-1} = 1$). Поэтому, не ограничивая общности, можно считать, что $x_0 = \overline{x}_0 = 1$. Но так как среди x_k имеется n коэффициентов, равных 1, то возможны, вообще говоря, n различных представлений полинома t_1 с $x_0 = 1$. Чтобы это представление определялось однозначно, следует подбирать s так, чтобы $ns \equiv -\sum\limits_{k=0}^{2n-2} \operatorname{sign}(x_k) k \bmod (2n-1)$. Тогда, так как числа n и $2n-1$ взаимно простые, по заданной сумме число $s < 2n-1$ находится однозначно. При этом, очевидно, при переходе от полинома t_1 к полиному $z^s t_1$ (с учетом, что $z^{2n-1} = 1$) получим полином вида (9), у которого сумма коэффициентов x_k равна или кратна числу $2n-1$.

Особенность указанных циклических преобразований полиномов t_1 и t_2 заключается в том, что они могут проводиться независимо друг от друга и при этом равенство (10) сохраняется. Однако имеются и совместные (не независимые) преобразования их коэффициентов, в результате которых равенство в (10) не нарушается и которые представляют особый интерес в силу их нетривиальности.

Для их рассмотрения изучим сначала свойства полинома t вида $t = \sum\limits_{k=0}^{2n-2} x_k z^k$, где $z = e^{i\nu}$, $\nu = \frac{2\pi m}{2n-1}, m \in \{1, 2, \ldots, 2n-2\}$ и $\sum\limits_{k=0}^{2n-2} x_k = n$, причем x_k равно 1 или 0, а значит, и $\sum\limits_{k=0}^{2n-2} x_k^2 = n$.

Лемма 2. *Для полинома t справедливо соотношение*

$$|t|^2 = n + 2\sum_{k=1}^{n-1}\left(\sum_{j=0}^{2n-2} x_j x_{|j+k|}\right)\cos k\nu, \tag{11}$$

где $|j+k|$ — наименьший (неотрицательный) вычет числа $j+k$ по модулю $2n-1$.

Доказательство. Согласно утверждению задачи 39 [4, с. 92, 294], для квадрата модуля полинома от $z = e^{i\nu}$ с комплексными коэффициентами x_k справедливо равенство

$$\left|\sum_{k=0}^{2n-2} x_k z^k\right|^2 = \sum_{k=0}^{2n-2} |x_k|^2 + \sum_{k=1}^{2n-2} (\lambda_k \cos k\nu + \mu_k \sin k\nu),$$

где $\lambda_k + i\mu_k = 2\sum\limits_{j=0}^{2n-2-k} x_j \overline{x}_{j+k}$. Но так как в нашем случае x_k вещественны, то $\mu_k = 0$ для всех k. Кроме того, по предположению $\sum\limits_{k=0}^{2n-2} |x_k|^2 = \sum\limits_{k=0}^{2n-2} x_k^2 = n$. И значит,

$$\left|\sum_{k=0}^{2n-2} x_k z^k\right|^2 = n + 2\sum_{k=1}^{2n-2}\left(\sum_{j=0}^{2n-2-k} x_j x_{j+k}\right)\cos k\nu.$$

Замечая, что для любого $k < n$ справедливо тождество

$$\sum_{j=0}^{2n-2-k} x_j x_{j+k} + \sum_{j=0}^{k-1} x_j x_{j+2n-1-k} \equiv \sum_{j=0}^{2n-2} x_j x_{|j+k|}$$

после попарного объединения слагаемых (с учетом того, что при $\nu = \dfrac{2\pi m}{2n-1}$ $\cos(2n-1-k)\nu = \cos k\nu$) и получаем утверждение леммы 2.

Из соотношения (11) видно, что $|t|^2$ зависит только от величин $d_k = \sum\limits_{j=0}^{2n-2} x_j x_{|j+k|}$, $k = 1, 2, \ldots, n-1$, которые совпадают с числом пар отличных от нуля коэффициентов x_j, равных, по предположению, 1, положительная разность порядковых номеров которых равна k или $2n-1-k$. Поэтому будем называть множество таких пар для всех k, $1 \le k \le n-1$, разностным множеством полинома t.

Оказывается, что для решения вопроса о существовании полуциркулянтных матриц Адамара имеет значение обратная задача: найти по заданному разностному множеству $\{d_k\}$ сам полином t. Для этого надо решить следующую систему уравнений:

$$\sum_{i=0}^{2n-2} x_i = n, \quad \sum_{i=0}^{2n-2} x_i^2 = n,$$
$$\sum_{i=0}^{2n-2} x_i x_{|i+k|} = d_k, \quad k = 1, 2, \ldots, n-1. \tag{12}$$

Так как из первых двух уравнений следует, что $\sum\limits_{k=1}^{n-1} d_k = \frac{n(n-1)}{2}$, то, считая это тривиальное условие выполненным, достаточно найти решение следующей системы уравнений второй степени:

$$\sum_{i=0}^{2n-2} x_i^2 = n\,,$$
$$\sum_{i=0}^{2n-2} x_i x_{|i+k|} = d_k, \quad k = 1, 2, \ldots, n-1. \tag{13}$$

Прежде всего заметим, что матрица $D_k = ||c_{ij}||$ квадратичной формы $\sum\limits_{i=0}^{2n-2} 2x_i x_{|i+k|}$ представляет собой правый циркулянт, поскольку $c_{ij} = 1$ только для $j = |i+k|$ или $j = |i-k|$ и равно нулю для остальных i и j. Так что в каждой строке и в каждом столбце симметричной матрицы D_k имеются лишь два отличных от нуля элемента, равных 1. В частности, в нулевой строке ($i = 0$) — это элементы c_{0k} и $c_{0(2n-1-k)}$, в первой ($i = 1$) — $c_{1(k+1)}$ и c_{10} при $k = 1$ или $c_{1(2n-k)}$ при $k > 1$. Собственные значения и собственные векторы циркулянтов известны [5, с. 273]. Именно, если z_1 — один из корней уравнения $z^{2n-1} = 1$, то собственное значение D_k равно $\lambda = \sum\limits_{j=0}^{2n-2} c_{0j} z_1^j$,

а соответствующий ему собственный вектор — $t = \{1, z_1, z_1^2, \ldots, z_1^{2n-2}\}$. Тем самым все матрицы D_k, $k = 1, 2, \ldots, n-1$, имеют одни и те же собственные векторы, соответствующие различным корням из 1 степени $2n-1$. В силу симметричности D_k, все собственные векторы можно выбрать вещественными, а именно, корню $z = 1$ отвечает собственный вектор $\{1, 1, \ldots, 1\}$, корню $z = \cos\frac{2\pi}{2n-1} + i\sin\frac{2\pi}{2n-1}$ и сопряженному ему корню $z = \cos\frac{2\pi}{2n-1} - i\sin\frac{2\pi}{2n-1}$ — соответственно $\{1, \cos\frac{2\pi}{2n-1}, \ldots, \cos\frac{2(2n-2)\pi}{2n-1}\}$ и $\{0, \sin\frac{2\pi}{2n-1}, \ldots, \sin\frac{2(2n-2)\pi}{2n-1}\}$ и аналогичные собственные векторы для комплексно сопряженных корней $\cos\frac{2\pi m}{2n-1} \pm i\sin\frac{2\pi m}{2n-1}$, $m = 2, 3, \ldots, n-1$. Найдем квадраты длин этих векторов

$$1 + \sum_{m=1}^{2n-2} \cos^2\frac{2\pi m}{2n-1} = 1 + 2\sum_{m=1}^{n-1} \cos^2\frac{2\pi m}{2n-1} = n + \sum_{m=1}^{n-1} \cos\frac{4\pi m}{2n-1} = \frac{2n-1}{2},$$

$$\sum_{m=1}^{2n-2} \sin^2\frac{2\pi m}{2n-1} = 2n - 2 - \sum_{m=1}^{2n-2} \cos^2\frac{2\pi m}{2n-1} = \frac{2n-1}{2}.$$

После нормировки получим следующую систему собственных векторов t_0, t_m, t_{2n-1-m}, $m = 1, 2, \ldots, n-1$:

$$t_0 = \left(\frac{1}{\sqrt{2n-1}}, \frac{1}{\sqrt{2n-1}}, \ldots, \frac{1}{\sqrt{2n-1}}\right),$$

$$t_m = \left(\sqrt{\frac{2}{2n-1}}, \sqrt{\frac{2}{2n-1}}\cos\frac{2\pi m}{2n-1}, \ldots, \sqrt{\frac{2}{2n-1}}\cos\frac{2\pi m(2n-2)}{2n-1}\right),$$

$$t_{2n-1-m} = \left(0, \sqrt{\frac{2}{2n-1}}\sin\frac{2\pi m}{2n-1}, \ldots, \sqrt{\frac{2}{2n-1}}\sin\frac{2\pi m(2n-2)}{2n-1}\right).$$

Рассмотрим матрицу $T = (t_0, t_1, \ldots, t_{2n-2})$, столбцами которой являются t_k, $k = 0, 1, \ldots, 2n-2$. Матрица T — ортогональная. Заменим в системе (13) переменные $x(x_0, x_1, \ldots, x_{2n-2})$ на $y(y_0, y_1, \ldots, y_{2n-2})$ по формуле $x = Ty$. Тогда, согласно [5, с. 63], все матрицы D_k преобразуются к диагональному виду

$$(x, D_k x) = \sum_{i,j=0}^{2n-2} c_{ij} x_i x_j = \sum_{m=0}^{2n-2} \lambda_m y_m^2,$$

где λ_m — собственные значения D_k, которые просто находятся

$$\lambda_m = \sum_{j=0}^{2n-2} c_{0j}\left(\cos\frac{2\pi m}{2n-1} + i\sin\frac{2\pi m}{2n-1}\right)^j = \left(\cos\frac{2\pi m}{2n-1} + i\sin\frac{2\pi m}{2n-1}\right)^k$$

$$+\left(\cos\frac{2\pi m}{2n-1}+i\sin\frac{2\pi m}{2n-1}\right)^{2n-1-k}=2\cos\frac{2\pi km}{2n-1}.$$

При этом исходная система (13) с учетом того, что $\cos\frac{2\pi kj}{2n-1}$ и $\cos\frac{2\pi k(2n-1-j)}{2n-1}$ равны, приводится к такому виду:

$$y_0^2+\sum_{j=1}^{n-1}(y_j^2+y_{2n-1-j}^2)=n,$$

$$y_0^2+\sum_{j=1}^{n-1}(y_j^2+y_{2n-1-j}^2)\cos\frac{2\pi kj}{2n-1}=d_k,\quad k=1,2,\dots,n-1, \tag{14}$$

т.е. получаем n линейных уравнений относительно n неизвестных $y_0^2, y_1^2+y_{2n-2}^2,\dots,y_{n-1}^2+y_n^2$. Решение этой системы имеет вид

$$y_0^2=\frac{n^2}{2n-1},\quad y_j^2+y_{2n-1-j}^2=\frac{2}{2n-1}\left(n+2\sum_{k=1}^{n-1}d_k\cos\frac{2\pi kj}{2n-1}\right). \tag{15}$$

Действительно,

$$\sum_{i=0}^{2n-2}y_i^2=\frac{n^2}{2n-1}+\frac{2}{2n-1}\sum_{j=1}^{n-1}\left(n+2\sum_{k=1}^{n-1}d_k\cos\frac{2\pi kj}{2n-1}\right)$$

$$=\frac{n(3n-2)}{2n-1}+\frac{4}{2n-1}\sum_{k=1}^{n-1}d_k\sum_{j=1}^{n-1}\cos\frac{2\pi kj}{2n-1}=\frac{n(3n-2)}{2n-1}-\frac{2}{2n-1}\sum_{k=1}^{n-1}d_k=n,$$

так как по предположению $\sum\limits_{k=1}^{n-1}d_k=\frac{n(n-1)}{2}$. Далее,

$$y_0^2+\sum_{j=1}^{n-1}(y_j^2+y_{2n-1-j}^2)\cos\frac{2\pi kj}{2n-1}$$

$$=\frac{n^2}{2n-1}-\frac{n}{2n-1}+\frac{4}{2n-1}\sum_{m=1}^{n-1}d_m\sum_{j=1}^{n-1}\cos\frac{2\pi mj}{2n-1}\cos\frac{2\pi kj}{2n-1}$$

$$=\frac{n(n-1)}{2n-1}+\frac{2}{2n-1}\sum_{m=1}^{n-1}d_m\sum_{j=1}^{n-1}\left(\cos\frac{2\pi(m-k)j}{2n-1}+\cos\frac{2\pi(m+k)j}{2n-1}\right)$$

$$=\frac{n(n-1)}{2n-1}+\frac{2d_k}{2n-1}(n-1-1/2)-\frac{2}{2n-1}\sum_{m\neq k}d_m=d_k.$$

Указанное решение (15) является единственным решением системы (14), поскольку ее ранг равен n. Если бы он был меньше n, то малым изменением d_k, $k = 1, 2, \ldots, n-1$, при котором их сумма сохраняется, можно было бы добиться, чтобы ранг расширенной матрицы стал большим ранга основной, что невозможно. Учитывая, что $x = Ty$, получаем следующее решение исходной системы (13):

$$x_0 = \frac{1}{\sqrt{2n-1}}\left[y_0 + \sqrt{2}\sum_{j=1}^{n-1} y_j,\right] \; ; \quad m = 1, 2, \ldots, n-1\,,$$

$$x_m = \frac{1}{\sqrt{2n-1}}\left[y_0 + \sqrt{2}\sum_{j=1}^{n-1}\left(y_j \cos\frac{2\pi mj}{2n-1} + y_{2n-1-j}\sin\frac{2\pi mj}{2n-1}\right)\right],$$

$$x_{2n-1-m} = \frac{1}{\sqrt{2n-1}}\left[y_0 + \sqrt{2}\sum_{j=1}^{n-1}\left(y_j \cos\frac{2\pi mj}{2n-1} - y_{2n-1-j}\sin\frac{2\pi mj}{2n-1}\right)\right]. \tag{16}$$

Нетрудно проверить, что это решение будет также и решением первоначальной "смешанной" системы (12) при $y_0 = \dfrac{n}{\sqrt{2n-1}}$.

Непосредственным следствием (16) является такое соотношение:

$$\sum_{j=1}^{n-1} y_j^2 = \frac{1}{2}x_0^2 + \sum_{m=1}^{n-1} x_m x_{2n-1-m} - \frac{n}{2(2n-1)}. \tag{17}$$

Давая y_j и y_{2n-1-j}, $j = 1, 2, \ldots, n-1$, произвольные значения, удовлетворяющие условиям (15), что заведомо возможно, если для любого j заданные числа d_k удовлетворяют неравенству

$$n + 2\sum_{k=1}^{n-1} d_k \cos\frac{2\pi jk}{2n-1} \geq 0, \tag{18}$$

получим вместе с $y_0 = \dfrac{n}{\sqrt{2n-1}}$ из (16) решение системы (12), которое, как видим, определяется неоднозначно и, вообще говоря, не будет целочисленным.

Лемма 3. *Если полиномы t_1 и t_2 вида (9) удовлетворяют условию (10) при любом $m = 1, 2, \ldots, 2n-2$, то для чисел d_k и $\overline{d_k}$ их разностных множеств для любого $k = 1, 2, \ldots, n-1$ выполняется равенство $d_k + \overline{d_k} = n$.*

И наоборот, если для любого k сумма чисел d_k и $\overline{d_k}$ равна n, то для соответствующих полиномов t_1 и t_2 при любом m выполняется соотношение (10). Для того чтобы существовала пара таких полиномов, необходимо, чтобы для каждого $j = 1, 2, \ldots, n-1$ элементы d_k разностного множества полинома t_1 удовлетворяли неравенству

$$\sum_{k=1}^{n-1} d_k \cos \frac{2\pi jk}{2n-1} \le 0. \tag{19}$$

Доказательство. По определению $d_k = \sum\limits_{j=0}^{2n-2} x_j x_{|j+k|}$ и аналогично задается $\overline{d_k}$. Поэтому согласно лемме 2 для полиномов t_1 и t_2 имеем

$$|t_1|^2 + |t_2|^2 = 2n + 2\sum_{k=1}^{n-1} (d_k + \overline{d_k}) \cos \frac{2\pi mk}{2n-1}\,. \tag{20}$$

Так как по предположению $|t_1|^2 + |t_2|^2 = n$ (это и есть условие (10), только иначе записанное), то

$$n + 2\sum_{k=1}^{n-1} (d_k + \overline{d_k}) \cos \frac{2\pi mk}{2n-1} = 0.$$

Преобразуем это равенство, используя тригонометрическое тождество (см. [4, с. 88]):

$$\frac{1}{2} + \sum_{k=1}^{n-1} \cos \frac{2\pi mk}{2n-1} = \frac{\sin(\frac{2n-1}{2}\frac{2\pi m}{2n-1})}{2\sin\frac{\pi m}{2n-1}} = 0, \tag{21}$$

для чего умножим последнее на $2n$ и вычтем из нашего равенства. В результате получим соотношение

$$\sum_{k=1}^{n-1} \left(d_k + \overline{d_k} - n\right) \cos \frac{2\pi mk}{2n-1} = 0.$$

По условию леммы это равенство справедливо при любом $m = 1, 2, \ldots, 2n-2$. Но так как числам m и $2n-1-m$ соответствуют, очевидно, равносильные уравнения, то достаточно рассмотреть первые $n-1$ уравнений с $m < n$. Определитель получаемой системы отличен от нуля, потому что его матрица является главным минором основной матрицы системы (14). Добавляя к первому столбцу этой матрицы сумму остальных столбцов, умноженную на два, все элементы этого столбца, кроме первого, можно в силу (21) обратить в

нуль. Так как наша система однородная, то отсюда следует, что для любого $k = 1, 2, \ldots, n-1 \quad d_k + \overline{d_k} - n = 0$, откуда и следует первое утверждение леммы.

Справедливость обратного утверждения следует из (20). Для доказательства необходимого условия (19) заметим, что для t_1 и t_2 и любого $j = 1, 2, \ldots, n-1$ согласно (18) должны выполняться неравенства:

$$|t_1|^2 = n + 2\sum_{k=1}^{n-1} d_k \cos\frac{2\pi jk}{2n-1} \geq 0,$$

$$|t_2|^2 = n + 2\sum_{k=1}^{n-1} \overline{d_k} \cos\frac{2\pi jk}{2n-1} \geq 0.$$

Но так как $|t_1|^2 + |t_2|^2 = n$, то для того, чтобы эти два неравенства выполнялись одновременно, для каждого j должно также выполняться и неравенство $\sum\limits_{k=1}^{n-1} d_k \cos\frac{2\pi jk}{2n-1} \leq 0$. Добавим, что числа $\overline{d_k}$ при этом удовлетворяют аналогичному неравенству. Лемма 3 доказана полностью.

6. В предыдущем разделе были указаны тривиальные (циклические) перестановки коэффициентов полиномов t_1 и t_2, при которых равенство в соотношении (10) сохраняется. Существование нетривиальных их перестановок, при которых также сохраняется равенство (10), вытекает из следующей теоремы.

Теорема 3. *Если полиномы t_1 и t_2 вида (9) удовлетворяют условиям леммы 1, т.е. порождают матрицу Адамара полуциркулянтного типа, то полиномы t_1' и t_2' вида*

$$t_1' = \sum_{k=0}^{2n-2} x_{|ks|} z^k, \quad t_2' = \sum_{k=0}^{2n-2} x_{|ks|} z^k,$$

где знак модуля имеет тот же смысл, что и в лемме 2, а $s < 2n-1$ — любое натуральное число, взаимно простое с $2n-1$, также порождают матрицу Адамара полуциркулянтного типа.

Доказательство. Рассмотрим сначала случай, когда число m, входящее в аргумент z, точнее в $\nu = \frac{2\pi m}{2n-1}$, взаимно просто с $2n-1$, т.е. случай первообразных корней степени $2n-1$ из 1.

Пусть $t_1 = \sum\limits_{k=0}^{2n-2} x_k z^k$, причем $\nu = \frac{2\pi m_1}{2n-1}$, $(m_1, 2n-1) = 1$. И пусть $m_2 < 2n-1$ — другое натуральное число, взаимно простое с $2n-1$. Тогда существует

такое натуральное $r < 2n-1$, что $m_2 = |rm_1|$. Положим $t_1' = \sum\limits_{k=0}^{2n-2} x_k (z^r)^k = \sum\limits_{k=0}^{2n-2} x_k z^{|rk|}$.

Так как $(r, 2n-1) = 1$, то числа $|rk|$ при изменении k пробегают те же значения, что и само k, но в другом порядке. Переставим слагаемые в t_1' так, чтобы показатели степени возрастали от 0 до $2n-2$. Тогда получим $t_1' = \sum\limits_{m=0}^{2n-2} x_{|ms|} z^m$, где натуральное $s < 2n-1$ определяется из соотношения $|rs| = 1$. Действительно, при $m = |kr|$ имеем $||kr|s| = |krs| = |k|rs|| = k$ (остаток от деления произведения нескольких чисел на $2n-1$ не зависит от замены любого из них соответствующим остатком). При этом числа d_k, $k = 1, 2, \ldots, n-1$, заменяются, очевидно, числами $d_{|ks|'}$, где $|ks|' = min(|ks|, 2n-1-|ks|)$, которые пробегают те же значения, что и d_k, но в другом порядке, так как если $k_1 + k_2 = 2n-1$, то $|sk_1| + |sk_2| = 2n-1$, ибо класс вычетов суммы двух натуральных чисел совпадает с суммой классов вычетов слагаемых.

Аналогично для $t_2 = \sum\limits_{m=0}^{2n-2} \overline{x}_k z^m$ получим $t_2' = \sum\limits_{m=0}^{2n-2} \overline{x}_{|ms|} z^m$, причем числа $\overline{d}_k$ заменяются при этом числами $\overline{d}_{|ks|'}$. И так как $d_{|ks|'} + \overline{d}_{|ks|'} = n$ по лемме 3 для t_1' и t_2' выполняются условия (10), причем, поскольку в качестве m_2 можно взять любое натуральное число, взаимно простое с $2n-1$, то соотношение (10) справедливо для полиномов t_1' и t_2' при любом $s < 2n-1$, не имеющем с $2n-1$ общих делителей.

Перейдем теперь к первообразным корням степени $p = \frac{2n-1}{q}$, где $q > 1$ — любой делитель числа $2n-1$, если оно не простое. Для таких корней из 1 $\nu = \frac{2\pi m_q}{2n-1}$, причем наибольший общий делитель чисел m_q и $2n-1$ равен в точности q, а сами числа m_q связаны с числом m_1, соответствующим выбранному первообразному корню степени $2n-1$ из 1, соотношениями $m_q = |hqm_1|$, где h — натуральное число, взаимно простое с p, так как $(m_q, 2n-1) = q$. Поставим в соответствие каждому h натуральное число $c < p$ такое, что $ch \equiv 1 (\mathrm{mod}\, p)$. Для любого h

$$t_1(z^{hq}) = \sum_{k=0}^{2n-2} x_k z^{|hqk|} = \sum_{m=0}^{p-1} \left(\sum_{j=0}^{q-1} x_{|mc+pj|} \right) z^{qm}.$$

На самом деле, если $k = |mc + pj|$, то $|hqk| = |hq(mc+pj)| = |hqmc| = |qm(1+pj')| = qm$. Аналогично для полинома t_1' получаем

$$t_1'(z^{\overline{h}q}) = \sum_{k=0}^{2n-2} x_{|ks|} z^{|\overline{h}qk|} = \sum_{m=0}^{p-1} \left(\sum_{j=0}^{q-1} x_{|ms\overline{c}+pj|} \right) z^{qm}.$$

Действительно, если $|ks| = |ms\overline{c} + pj|$, то учитывая, что по предположению $|rs| = 1$, имеем $|\overline{h}qk| = |\overline{h}qrsk| = |\overline{h}qr|ks|| = |\overline{h}qr(ms\overline{c} + pj)| = |\overline{h}qrsm\overline{c}| = |qm\overline{h}\overline{c}| = |qm(1 + pj')| = qm$. Легко заметить, что для данного s $t'_1(z^{\overline{h}q}) = t_1(z^{\overline{h}q})$, если $c \equiv s\overline{c} (\mathrm{mod}\, p)$. Точно так же доказывается, что при том же условии $t'_2(z^{\overline{h}q}) = t_2(z^{hq})$. Поэтому, если полиномы t_1 и t_2 удовлетворяют условиям леммы 1 и, в частности, равносильному (2) условию (10) при любом $m = 1, 2, \ldots, 2n-2$, то всем этим условиям удовлетворяют и полиномы t'_1 и t'_2. А значит, они порождают матрицу Адамара полуциркулянтного типа, что и требовалось доказать.

Как известно, первообразные корни из 1 степени $2n - 1$, как и все корни из единицы, образуют группу. Поэтому свойства решений уравнений (2), когда по одному решению строятся другие его решения, естественно называть групповыми свойствами полиномов, порождающих полуциркулянтные матрицы Адамара. Вместе с необходимыми условиями (19) они позволяют значительно сократить перебор при построении матриц Адамара с помощью компьютерных программ. Это весьма важно, поскольку нахождение полинома t_2 с целочисленными коэффициентами при заданном полиноме t_1 из уравнения $|t_2|^2 = n - |t_1|^2$ — очень трудоемкая задача, учитывая замечание, сделанное в разделе 5 по поводу условий (18). Возвращаясь к теореме 3, заметим, что при $s = 2n - 2$ полином $t'_1 = x_0 + \sum\limits_{k=1}^{2n-2} x_k z^{2n-1-k}$, значит, является комплексно сопряженным полиному t_1 и имеет одинаковое с ним разностное множество. Такое же разностное множество имеют, очевидно, все циклические производные полинома t_1. Поэтому из всех таких n-членов (полином t_1 содержит ровно n ненулевых одночленов) можно рассматривать только один, например, предшествующий всем остальным в лексикографическом смысле. Теорема 3 позволяет распределить оставшиеся n-члены по классам эквивалентности, соответствующим различным делителям числа $2n - 1$. В результате, общее количество подлежащих перебору полиномов можно сократить дополнительно примерно в $\frac{1}{2}\varphi(2n - 1)$ раз, где $\varphi(2n - 1)$ — функция Эйлера, равная числу натуральных чисел, меньших $2n - 1$ и взаимно простых с ним. Из таблицы 1 видно, сколько различных полиномов t_1 надо рассматривать для каждого из $n \leq 20$. Их количество равно суммарному числу классов эквивалентности, отвечающих каждому из делителей целочисленной функции Эйлера (см. две средние графы табл. 1). В последней графе этой таблицы приводится общее число различных (в лексикографическом смысле) n-членов, которые пришлось бы перебирать без учета теоремы 3.

Таблица 1. Распределение полиномов (n-членов), предшествующих всем своим циклическим производным и сопряженным себе, по классам эквивалентности

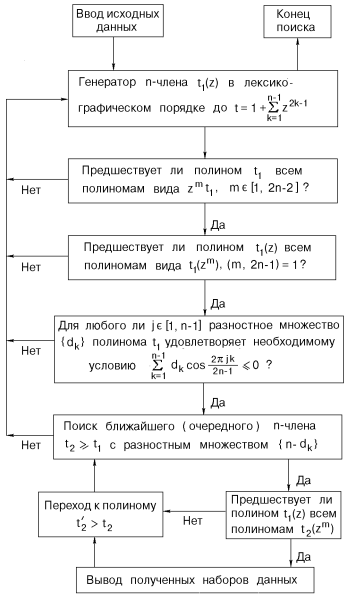
n	φ	Число классов эквивалентности, каждый из которых состоит из числа полиномов, равного указанному в скобках делителю функции Эйлера $\varphi(2n-1)$	Общее число n-членов
2	2	1(1)	1
3	4	1(2)	2
4	6	1(1), 1(3)	4
5	6	1(1), 3(3)	10
6	10	1(1), 5(5)	26
7	12	2(2), 12(6)	76
8	8	2(1), 13(2), 51(4)	232
9	16	1(2), 1(4), 93(8)	750
10	18	1(1), 3(3), 276(9)	2494
11	12	2(1), 4(2), 78(3), 1380(6)	8524
12	22	1(1), 2693(11)	29624
13	20	4(2), 4(5), 10444(10)	104468
14	18	2(1), 61(3), 41347(9)	372308
15	28	2(2), 95638(14)	1338936
16	30	1(1), 3(3), 25(5), 323367(15)	4850640
17	20	2(1), 4(2), 4862(5), 1766095(10)	17685270
18	24	2(1), 2(2), 46(3), 71(4), 4123(6), 5400782(12)	64834550
19	36	2(2), 78(6), 13269066(18)	238843660
20	24	16(2), 28(3), 110(4), 46958(6), 73616290(12)	883677784

7. В соответствии с леммой 1 для построения матрицы Адамара полуциркулянтного типа надо найти два полинома t_1 и t_2, удовлетворяющих условию (2) или в развернутом виде (10), коэффициенты x_k первого из которых должны удовлетворять необходимому условию (19). Если полином t_1 задан, то для его чисел d_k автоматически выполняется неравенство (18). Если для него выполняется и неравенство (19), причем для $j = 1, 2, \ldots, n-1$, то согласно лемме 3 для t_2 выполняется неравенство (18) с заменой всех d_k на $\overline{d}_k = n - d_k$ и, значит, его коэффициенты $\overline{x}_k$ можно найти по формулам, аналогичным (16), полагая в них $y_0 = \dfrac{n}{\sqrt{2n-1}}$ и подбирая y_j и y_{2n-1-j} таким образом, чтобы они удовлетворяли (15). Однако хотя такое решение существует всегда, сами коэффициенты $\overline{x}_k$ могут получиться при этом отличными от 0 и 1, причем не целыми, как правило, и даже отрицательными. В частности, при $\overline{x}_0 = 1$ и

$\sum_{j=1}^{n-1} y_j^2 < \frac{1}{2} - \frac{n}{2(2n-1)}$ среди $\overline{x}_k$ заведомо будут отрицательные, что следует из соотношения (17). Нас же интересуют только такие полиномы t_2, которые в качестве коэффициентов имеют числа 0 и 1, причем число последних равно n. Поэтому их приходится искать подбором, перебирая один за одним полиномы t_1, скажем, в лексикографическом порядке. Эта задача является технически сложной и весьма трудоемкой, особенно при больших значениях n. Групповые свойства полиномов t_1 и t_2 (теорема 3) и необходимые условия (19) позволяют существенно сократить этот неизбежный перебор.

Рассмотрим в связи с этим блок-схему алгоритма поиска полуциркулянтных матриц Адамара порядка $4n$ (табл. 2). Так как n из $2n-1$ коэффициентов x_k равны 1, то среди них найдутся два соседние. Поэтому, умножая t_1 на подходящую степень z, можно добиться, чтобы $x_0 = x_1 = 1$ ($|t_1|$ при этом не изменяется). Это означает, что достаточно рассматривать полиномы t_1 в лексикографическом порядке от $1 + \sum_{k=1}^{n-1} z^k$ до $1 + \sum_{k=1}^{n-1} z^{2k-1}$ (см. второй блок алгоритма). Заметим, что при $n \geq 3$ общее их количество равно $1 + \sum_{m=3}^{n-1} C_{2m-5}^{m-3}$. Третий блок позволяет исключить из перебора циклические производные полинома t_1, благодаря чему их общее число сокращается до $\frac{1}{2}\left(\frac{C_{2n-1}^{n}}{2n-1} + C_{n-1}^{[\frac{n}{2}]}\right)$. После чего (четвертый блок) исключаются из перебора полиномы, эквивалентные t_1 в смысле теоремы 3, а также их циклические производные, если t_1 предшествует всем им в лексикографическом порядке. Далее (пятый блок) проверяется, выполняется ли для разностного множества полинома необходимое условие (19). И наконец, для каждого оставшегося в результате проведенного отсеивания полинома t_1 подбирается полином t_2 (один или несколько) такой, чтобы вместе они порождали матрицу Адамара полуциркулянтного типа. В отношении затрат машинного времени — это наиболее трудоемкий блок. Например, при $n = 16$ для выполнения всех предусмотренных в этом блоке программы процедур требуется в 70 раз больше времени, чем на все остальные ее блоки. Если такого полинома t_2 для очередного t_1 не существует, то программа переходит к рассмотрению следующего в лексикографическом смысле полинома t_1, пока не исчерпает их полностью. Наша программа с указанной в табл. 2 блок-схемой рассчитана на нахождение всех различных (неэквивалентных) пар полиномов t_1 и t_2, порождающих полуциркулянтные матрицы Адамара, что, вообще говоря, не обязательно.

Таблица 2. Блок-схема алгоритма поиска полиномов $t_1(z)$ и $t_2(z)$ $(z^{(2n-1)} = 1)$, удовлетворяющих равенству $|t_1(z)|^2 + |t_2(z)|^2 = n$



Достаточно для каждого n найти лишь одно решение, например, первое в лексикографическом смысле (см. табл. 3 для $n \leq 20$).

Таблица 3. Полуциркулянтные матрицы Адамара порядка $4n \le 80$

$4n$	Показатели степеней членов полиномов t_1 и t_2 $(t_1 \le t_2)$, порождающих полуциркулянтную матрицу Адамара, и разностное множество полинома t_1	$4n$
4	0 0 0 1 2 4 7 8 10 12 13 16 17 18 22 23 25 26 29 32 34 36 20: 12 12 10 10 10 9 9 11 9 9 10 11 10 10 9 9 9 9 12 (73663402/351918)	80
8	0 1 0 1 0 1 2 4 5 8 10 12 14 15 18 20 21 23 26 27 30 31 32 2: 1 19: 11 11 10 10 10 8 10 9 10 8 8 9 10 11 9 9 10 8 (1/1) (13269146/77403)	76
12	0 1 2 0 1 3 0 1 2 3 6 9 11 12 14 15 19 20 21 24 25 27 29 31 3: 2 1 18: 10 10 10 10 9 7 11 9 8 7 9 8 9 10 9 9 8 (1/1) (5405026/46250)	72
16	0 1 2 4 0 1 2 4 0 1 2 4 7 8 10 12 15 16 19 21 23 25 26 28 29 4: 2 2 2 17: 11 9 9 8 9 8 8 7 8 10 8 8 9 7 8 9 (2/1) (1770963/20284)	68
20	0 1 2 3 5 0 1 3 5 6 0 1 2 3 6 9 10 11 14 15 17 20 22 24 25 27 5: 3 3 2 2 16: 9 9 8 10 7 9 7 7 7 7 8 9 8 7 8 (4/2) (323396/4696)	64
24	0 1 2 3 5 6 0 1 3 5 7 8 0 1 2 3 4 5 6 7 9 13 14 16 19 23 24 6: 4 3 3 2 3 15: 9 8 8 7 8 7 8 6 7 9 7 7 7 7 (6/3) (95640/1895)	60
28	0 1 2 3 4 7 9 0 1 2 4 5 8 10 0 1 2 3 4 5 6 7 10 12 15 16 20 22 7: 4 4 3 3 3 4 14: 8 8 7 7 8 7 6 6 6 8 6 8 6 (14/3) (41410/1198)	56
32	0 1 2 3 4 5 9 11 0 1 3 5 6 8 11 12 0 1 2 3 4 5 6 8 10 13 14 18 19 8: 5 5 3 4 3 4 4 13: 8 7 6 7 7 6 5 7 6 6 6 7 (66/15) (10452/378)	52
36	0 1 2 3 4 5 8 10 13 0 1 2 4 6 7 10 11 13 0 1 2 3 4 5 6 8 12 14 17 19 9: 5 5 5 4 5 3 4 5 12: 6 8 6 6 6 6 5 5 6 5 7 (95/11) (2694/135)	48
40	0 1 2 3 4 5 7 9 13 14 0 1 3 4 6 7 10 12 14 15 0 1 2 3 4 5 6 10 12 15 17 10: 6 6 4 5 5 5 5 4 5 11: 6 7 5 5 6 5 5 4 6 6 (280/28) (1464/107)	44

Поскольку при $n = 1$ и $s_1 = 1$ полиномы $t_1 = t_2 = 1$ удовлетворяют условию (2), то формально можно считать, что при $n = 1$ также имеется матрица Адамара полуциркулянтного типа, что отражено и в табл. 3. При этом показатели членов, входящих в полиномы t_1 и t_2, представлены соответственно в первой и второй строке (нуль соответствует свободному члену). В третьей строке после двоеточия располагается разностное множество полинома t_1 , причем число d_k, $k = 1, 2, \ldots, n-1$, занимает k-е место (разностное множество полинома t_2 получается вычитанием из числа n, стоящего до двоеточия, чисел, расположенных после него). Там же в скобках указано число различных (неэквивалентных) полиномов t_1 — общее количество (числитель) и удовлетворяющих необходимому условию (знаменатель). Отношение этих чисел говорит о высокой эффективности условия (19). Тем не менее, с ростом n и она становится недостаточной для процессора 486-го типа. Поэтому при нахождении всех решений пришлось ограничиться $n \leq 17$ (для $n = 17$ весь процесс счета занимает 45 суток).

Приведенные в табл. 3 данные свидетельствуют об универсальности нашего метода, позволяющего находить матрицы Адамара любого порядка. Впрочем, как и для известного метода Уильямсона [6, с. 299–304], универсальность этого метода пока что гипотетическая. Но поскольку неудачных попыток не было, причем для всех n — четных и нечетных, и так как, кроме того, с увеличением n число различных неэквивалентных решений быстро растет (если при $n \leq 10$ оно равно: 1 (при $n \leq 5$), 2 (при $n = 6$), 4 (при $n = 7$) и 8 (при $8 \leq n \leq 10$), то при последующих значениях n (до 17 включительно) оно равно: $11-22$, $12-28$, $13-44$, $14-98$, $15-138$, $16-202$, $17-288$), то можно надеяться, что наш метод окажется действительно универсальным. Однако, чтобы его можно было эффективно применять при больших значениях n, требуется усилить необходимое условие (19), для чего надо найти условия, при которых решение системы (12), задаваемое формулами (16), является целочисленным, точнее, когда каждое из x_m, $m = 1, 2, \ldots, 2n-2$, равно 0 или 1. И такие условия можно найти, исходя из того, что при выполнении соотношений $\sum\limits_{m=0}^{2n-2} x_m = n$ и $\sum\limits_{m=0}^{2n-2} x_m^2 = n$ условие целочисленности x_m можно заменить двойными неравенствами $0 \leq x_m \leq 1$, $m = 1, 2, \ldots, 2n-2$ (т.к. тогда из равенства $\sum\limits_{m=0}^{2n-2} (x_m^2 - x_m) = 0$ следует, что каждое x_m равно 0 или 1. Поэтому имеет место следующая теорема.

Теорема 4. *Для того, чтобы система уравнений второй степени (13)* $c \sum\limits_{k=1}^{n-1} d_k = \dfrac{n(n-1)}{2}$ *имела целочисленное решение в числах* 0 *и* 1, *необходимо и достаточно, чтобы имела решение следующая система линейных*

(двойных) неравенств ($m = 1, 2, \ldots, n-1$):

$$\frac{-n}{\sqrt{2(2n-1)}} \le \sum_{i=1}^{n-1} y_i \le \frac{n-1}{\sqrt{2(2n-1)}},$$

$$\frac{-n}{\sqrt{2(2n-1)}} \le \sum_{j=1}^{n-1} \left(y_j \cos\frac{2\pi mj}{2n-1} + y_{2n-1-j} \sin\frac{2\pi mj}{2n-1} \right) \le \frac{n-1}{\sqrt{2(2n-1)}},$$

$$\frac{-n}{\sqrt{2(2n-1)}} \le \sum_{j=1}^{n-1} \left(y_j \cos\frac{2\pi mj}{2n-1} - y_{2n-1-j} \sin\frac{2\pi mj}{2n-1} \right) \le \frac{n-1}{\sqrt{2(2n-1)}}$$

при выполнении следующих условий ($j = 1, 2, \ldots, n-1$):

$$y_j^2 + y_{2n-1-j}^2 = \frac{2}{2n-1} \left(n + 2 \sum_{k=1}^{n-1} d_k \cos\frac{2\pi jk}{2n-1} \right).$$

Но эта теорема представляет скорее теоретический интерес, поскольку ее последние условия — квадратичные и, значит, для решения получаемой системы линейных неравенств (см. [7, с. 162–165]) одного симплекс-метода будет недостаточно.

8. Необходимо добавить, что одним из путей построения полуциркулянтных матриц Адамара для больших n является поиск специальных классов полиномов t_1 и t_2. Например, когда они являются симметричными ($x_k = x_{2n-1-k}$ для всех $k = 1, 2, \ldots, n-1$) или кососимметричными ($x_k \ne x_{2n-1-k}$ для всех значений k). И хотя такие пары полиномов для многих значений n действительно существуют, для некоторых n их нет вообще, даже если один из полиномов произвольный, а другой симметричный или кососимметричный (к таким значениям, в частности, относятся $n = 13$ и $n = 14$). Поэтому такой упрощенный подход к поиску матриц Адамара не всегда результативен.

Автор искренне признателен всем сотрудникам вычислительного центра ФТИНТ НАН Украины за оказанное внимание и помощь и выражает особую благодарность программистам В.И. Хатунцеву и А.А. Моторной, системным программистам С.А. Головко и В.И. Белану, оператору Л.Н. Промоскаль.

Список литературы

[1] *А.И. Медяник*, Вписанный в куб правильный симплекс и матрица Адамара полуциркулянтного типа. — *Мат. физ., анализ, геом.* (1997), т. 4, № 4, с. 458–471.

[2] *Е. Артін*, Теорія Галуа. Радянська школа, Київ (1963).

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

[4] *Г. Полиа, Г. Сеге*, Задачи и теоремы из анализа. Ч. II. Наука, Москва (1978).

[5] *Р. Белльман*, Введение в теорию матриц. Наука, Москва (1969).

[6] *М. Холл*, Комбинаторика. Мир, Москва (1970).

[7] *Д. Гейл*, Теория линейных экономических систем. Изд-во иностр. лит., Москва (1963).

Regular simplex inscribed into a cube, half-circulant Hadamard matrices and Gaussian sums

A.I. Medianik

It is proved with help of trigonometric sums method that if a number $2n-1$ is prime or equal to product of two prime twin numbers then a half-circulant Hadamard matrix of order $4n$ exists and into a $(4n-1)$-cube one can inscribe a regular simplex of the same dimensions. Group properties of polinomial pairs which give Hadamard matrices of half-circulant type is investigated as well, and it's installed effective necessary existence conditions for a given polinomial (from a group ring over whole numbers) another polinomial which forms with it such the pair what makes use for practical construction of Hadamard matrices of all orders $4n \leq 80$ with help of PC.

Вписаний в куб правильний симплекс, напівциркулянтні матриці Адамара і гаусові суми

А.Г. Медяник

За допомогою методу тригонометричних сум доводиться, що коли число $2n-1$ просте або є добутком двох простих чисел-близнюків, то існує напівциркулянтна матриця Адамара порядка $4n$ і в $4n-1$-вимірний куб можна вписати правильний симплекс тієї самої вимірності. Вивчаються також групові властивості пар поліномів, що породжують матриці Адамара напівциркулянтного типу, та встановлюються ефективні необхідні умови існування для даного полінома (з деякого групового кільця над цілими числами) другого полінома, який утворює з ним таку пару, що використовується для практичного знаходження за допомогою комп'ютера матриць Адамара усіх порядків $4n \leq 80$.