G. A. Bekishev, Hadamard matrices and difference families,
Mat. Zametki, 1990, Volume 47, Issue 3, 11–16

Математические заметки

том 47 выпуск 3 март 1990

МАТРИЦЫ АДАМАРА И РАЗНОСТНЫЕ СЕМЕЙСТВА

Г. А. Бекишев

Квадратная $(-1, +1)$-матрица H называется *матрицей Адамара*, если ее строки, а значит, и столбцы попарно ортогональны. Другими словами, $HH^T = nI$, где n — порядок матрицы H, а I — единичная матрица. Условие $n \equiv 0 \pmod 4$ является необходимым для существования матрицы Адамара n-го порядка при $n > 2$. Будет ли это условие и достаточным — остается нерешенной проблемой.

Пусть $B = (b_1, \ldots, b_k)$ — подмножество (блок) в абелевой группе G конечного порядка v. Обозначим через $\nu_B(f)$ кратность вхождения элемента $f \in G$ в разности $b_i - b_j$ элементов блока B $(i, j = 1, 2, \ldots, k)$. Семейство $B_1, B_2, \ldots, B_m$ блоков в группе G называется (v, k, λ)-*разностным семейством*, если каждый блок B_j имеет мощность k и для любого ненулевого элемента $f \in G$ сумма кратностей вхождения f в разности элементов блоков семейства равна λ: $\nu_{b_1}(f) + \ldots + \nu_{b_m}(f) = \lambda$. Число m блоков (v, k, λ)-разностного семейства должно удовлетворять условию

$$m \cdot k(k-1) = \lambda(v-1). \tag{1}$$

При $m = 1$ (v, k, λ)-разностное семейство называется разностным множеством.

В силу (1) разностное семейство с параметрами v, $k = (v - 1)/2$, $\lambda = (v-3)/2$, где v нечетно, состоит из двух блоков. Как показано в [1], при $v = p^r$, где p — простое нечетное число, в качестве блоков разностного семейства с указанными параметрами могут быть взяты подмножества элементов поля Галуа $F = GF(p^r)$

$$B_1 = \{x \in F : \chi(x) = +1\},$$
$$B_2 = \{x \in F : \chi(x) = -1\},$$

где $\chi(x)$ — характер поля F, т. е. $\chi(0) = 0$, $\chi(x) = +1$, если x — квадрат, и $\chi(x) = -1$, если x — не квадрат.

Примером $(v, (v-1)/2, (v-3)/2)$-разностного семейства при $v \neq p^r$ может служить построенная автором статьи пара блоков

$$B_1 = \{1, 2, 3, 4, 5, 7, 10, 13, 17, 18\},$$
$$B_2 = \{1, 2, 3, 4, 6, 8, 10, 13, 14, 17\}$$

из элементов группы Z_{21} классов вычетов по модулю 21.

В настоящей заметке доказывается следующая

ТЕОРЕМА. *Пусть* $G = \{x_0, x_1, \ldots, x_{v-1}\}$ — *абелева группа нечетного порядка* v, *элементы которой занумерованы так, что*

$$x_j + x_{v-1-j} = 0 \qquad (j = 0, 1, \ldots, (v-1)/2). \tag{2}$$

Пусть B_1, B_2 — $(v, (v-1)/2, (v-3)/2)$-*разностное семейство в* G. *Пусть* e — *вектор из* $+1$ *размерности* v, *а* $S_{B_i} = \| \alpha_{st}^{(i)} \|_0^{v-1}$ — *квадратные* $(-1, +1)$-*матрицы порядка* v, *определенные равенствами*

$$\alpha_{st}^{(i)} = \begin{cases} +1, & x_t \in B_i + x_s, \\ -1, & x_t \notin B_i + x_s \end{cases} \tag{3}$$

$(i = 1, 2;\ s, t = 0, 1, \ldots, v-1)$.

Тогда

$$H = \begin{Vmatrix} +1 & e & e & +1 \\ e^T & S_{B_1} & S_{B_2}^T & e^T \\ e^T & S_{B_2} & -S_{B_1}^T & -e^T \\ +1 & e & -e & -1 \end{Vmatrix} \tag{4}$$

— *матрица Адамара порядка* $n = 2v + 2$.

Эта теорема сводит построение матриц Адамара к построению $(v, (v-1)/2, (v-3)/2)$-разностных семейств в абелевых группах нечетного порядка v.

Доказательству теоремы предпошлем ряд вспомогательных предложений.

Квадратную матрицу $C = \| c_{ik} \|_0^{v-1}$ будем называть *правосимметрической*, если в ней элементы, расположенные симметрично относительно вспомогательной диагонали, равны, т. е.

$$c_{ik} = c_{v-1-k,\, v-1-i} \qquad (i, k = 0, 1, \ldots, v-1). \tag{5}$$

Это равносильно тому, что $C^{T'} = C$, где символ T' обозначает операцию транспонирования матриц вокруг вспомогательной диагонали. Символ T' обладает теми же свойствами, что и операция T транспонирования матриц вокруг главной диагонали. В частности, $(AB)^{T'} = B^{T'} \cdot A^{T'}$. Отсюда легко вытекает, что *произведение правосимметрических матриц* A *и* B *является правосимметрической матрицей тогда и только тогда, когда эти матрицы перестановочны*: $AB = BA$.

Пусть G — группа, о которой говорится в теореме 1. Пусть $B = \langle b_1, b_2, \ldots, b_k \rangle$ — произвольный блок элементов в группе G. Матрица $I_B = \| \beta_{st} \|_0^{v-1}$, определенная равенствами

$$\beta_{st} = \begin{cases} 1, & x_t \in B + x_s, \\ 0, & x_t \notin B + x_s \end{cases} \qquad (s, t = 0, 1, \ldots, v-1) \tag{6}$$

представляет собою *матрицу инциденций орбиты блока* B. Обозначим через $S_B = \| \alpha_{st} \|_0^{v-1}$ матрицу, получающуюся из матрицы

I_B заменой в ней нулей на -1. Очевидно, матрицы I_B и S_B связаны равенством

$$S_B = 2 \cdot I_B - J, \quad J = e^T e. \tag{7}$$

ЛЕММА 1. *Матрица S_B блока $B = \langle b_1, \ldots, b_k \rangle$ — правосимметрическая $(-1, +1)$-матрица порядка v, каждая строка и каждый столбец которой содержит ровно k положительных единиц.*

Доказательство. В силу (7) достаточно доказать, что инцидентная матрица I_B — правосимметрическая, каждая строка и каждый столбец которой содержит точно k единиц. Рассмотрим сначала частный случай, когда блок B состоит из одного элемента: $B = \langle b \rangle$, $b \in G$. В этом случае орбита блока B будет орбитой элемента b и имеет вид

$$b + x_0, \; b + x_1, \ldots, b + x_{v-1},$$

т. е. представляет собою, очевидно, некоторую перестановку элементов группы G. Соответственно этому замечанию, матрица инциденций $I_{\langle b \rangle}$ будет некоторой перестановочной матрицей, т. е. с точностью до перестановки столбцов, единичной матрицей I порядка v. Следовательно, каждая строка и каждый столбец матрицы $I_{\langle b \rangle}$ содержит в точности одну единицу.

Покажем, что матрица $I_{\langle b \rangle}$ — правосимметрическая. Формулы (6) для элементов матрицы $I_{\langle b \rangle}$ в рассматриваемом частном случае примут вид

$$\beta_{st} = \begin{cases} 1, & b + x_s = x_t, \\ 0, & b + x_s \neq x_t. \end{cases} \tag{8}$$

Пусть теперь $\beta_{st} = 1$, т. е. согласно формулам (8) $b + x_s = x_t$. Переписывая это равенство в виде $b - x_t = -x_s$ и замечая, что в силу (2) — $x_t = x_{v-1-t}$, $-x_s = x_{v-1-s}$, получаем $b + x_{v-1-t} = x_{v-1-s}$. Следовательно, $\beta_{v-1-t,\, v-1-s} = 1$. Аналогично покажем, что если $\beta_{st} = 0$, то и $\beta_{v-1-t,\, v-1-s} = 0$. Таким образом, матрица $I_{\langle b \rangle}$ — правосимметрическая.

Пусть $B = \langle b_1, \ldots, b_k \rangle$. Поскольку, очевидно,

$$I_B = I_{\langle b_1 \rangle} + \ldots + I_{\langle b_k \rangle},$$

а сумма правосимметрических матриц является матрицей правосимметрической, то мы заключаем, что матрица I_B правосимметрическая, в каждой строке и каждом столбце которой содержится ровно k единиц. Это завершает доказательство леммы.

ЛЕММА 2. *Пусть A и B — произвольные блоки в группе G, не обязательно равномощные. Тогда*

$$S_A \cdot S_B^T = S_B^T \cdot S_A. \tag{9}$$

В частности, матрица S_B — нормальная: $S_B \cdot S_B^T = S_B^T \cdot S_B$.

Доказательство. Пусть l и k — мощности блоков A и B. Учитывая равенство (7), получаем

$$S_A \cdot S_B^T = (2I_A - J)(2I_B - J)^T = 4I_A I_B^T + (v - 2k - 2l)J, \quad (10)$$

$$S_B^T \cdot S_A = (2I_B - J)^T (2I_A - J) = 4I_B^T \cdot I_A + (v - 2k - 2l)J. \quad (11)$$

Таким образом, достаточно доказать, что

$$I_A \cdot I_B^T = I_B^T \cdot I_A. \quad (12)$$

Поскольку, как было показано при доказательстве леммы 1, матрицы I_A и I_B^T — правосимметрические, то равенство (12) будет иметь место тогда и только тогда, когда матрица $I_A I_B^T = \| u_{st} \|_0^{v-1}$ сама является правосимметрической. Итак, покажем, что $u_{st} = u_{v-1-t,\ v-1-s}$ для всех $s,\ t = 0, 1, \ldots, v-1$. Очевидно,

$$u_{st} = |\,(A + x_s) \cap (B + x_t)\,|;$$

$$u_{v-1-t,\ v-1-s} = |\,(A + x_{v-1-t}) \cap (B + x_{v-1-s})\,|.$$

Заметим, далее, что если X и Y — два произвольных блока в группе G, $f \in G$ — произвольный элемент, то

$$|\,X \cap Y\,| = |\,(X + f) \cap (Y + f)\,|. \quad (13)$$

Полагая здесь $X = A$, $Y = B$, $f = -x_s - x_t$, получаем с учетом свойства (2) нумерации элементов группы G

$$u_{st} = |\,(A + x_s) \cap (B + x_t)\,| = |\,(A + x_s + f) \cap (B + x_t + f)\,| = |\,(A - x_t) \cap (B - x_s)\,| = |\,(A + x_{v-1-t}) \cap (B + x_{v-1-s})\,| = u_{v-1-t,\ v-1-s}.$$

ЛЕММА 3. *Для произвольного блока $B = \langle b_1, \ldots, b_k \rangle$ в группе G матрица $S_B S_B^T = \| \tau_{st} \|_0^{v-1}$ — дважды симметрическая. Ее элементы равны*

$$\tau_{st} = v - 4k + 4\nu_B (x_t - x_s) \qquad (s,\ t = 0, 1, \ldots, v-1). \quad (14)$$

Доказательство. Полагая в (10) $A = B$, получаем

$$S_B S_B^T = 4I_B \cdot I_B^T + (v - 4k)J. \quad (15)$$

Покажем, что элементы матрицы $I_B I_B^T = \| \gamma_{st} \|_0^{v-1}$ определяются по формулам

$$\gamma_{st} = \nu_B (x_t - x_s) \qquad (s,\ t = 0, 1, \ldots, v-1). \quad (16)$$

Для доказательства заметим, что при любом $f \in G$ число общих элементов в блоках B и $B + f$ равно кратности вхождения f в разности элементов блока B: $|\,B \cap (B + f)\,| = \nu_B (f)$. Поэтому, принимая вновь во внимание формулу (13), находим

$$\gamma_{st} = |\,(B + x_s) \cap (B + x_t)\,| = |\,(B + x_s - x_s) \cap (B + x_t - x_s)\,| = |\,B \cap (B + x_t - x_s)\,| = \nu_B (x_t - x_s).$$

Формулы (14) легко теперь следуют из формул (15) и (16).

ЛЕММА 4. *Пусть* $B_1, \ldots, B_m$ — (v, k, λ)-*разностное семейство в группе* G. *Тогда*

$$Q = \| q_{st} \|_0^{v-1} = \sum_{i=1}^{m} S_{B_i} S_{B_i}^T = (4mk - 4\lambda) I + (mv - 4mk + 4\lambda) J. \quad (17)$$

Доказательство. В силу определения разностного семейства с параметрами v, k, λ

$$\sum_{i=1}^{m} \nu_{B_i}(x_t - x_s) = \begin{cases} mk, & t = s, \\ \lambda, & t \neq s. \end{cases}$$

Принимая во внимание эти формулы и формулы (14), получаем

$$q_{st} = m(v - 4k) + 4 \sum_{i=1}^{m} \nu_{B_i}(x_t - x_s) = \begin{cases} mv, & s = t, \\ mv - 4km + 4\lambda, & s \neq t \end{cases}$$
$$(s, t = 0, 1, \ldots, v - 1),$$

что эквивалентно формуле (17).

Доказательство теоремы. Пусть выполняются условия теоремы. Поскольку в рассматриваемом случае число блоков $m = 2$, $k = (v - 1)/2$, $\lambda = (v - 3)/2$, то формула (17) примет вид

$$Q = S_{B_1} S_{B_1}^T + S_{B_2} S_{B_2}^T = (2v + 2) I - 2J. \quad (18)$$

Рассмотрим клеточную матрицу H порядка $n = 2v + 2$, определенную равенством (4). Покажем, что H является нормализованной матрицей Адамара.

В силу леммы 1 каждая строка и каждый столбец матрицы S_{B_i} $(i = 1, 2)$ содержит $(v - 1)/2$ положительных единиц и $(v + 1)/2$ отрицательных. Поэтому каждая строка матрицы H, кроме первой, содержит $v + 1$ элементов, равных $+1$ и столько же элементов, равных -1. Отсюда следует, что 1-я строка ортогональна ко всем остальным строкам матрицы H.

Далее, так как в силу леммы 1 $S_{B_i} e^T = S_{B_i}^T e^T = -e^T$ $(i = 1, 2)$, то

$$e^T + S_{B_1} e^T - S_{B_2}^T e^T - e^T = 0,$$
$$e^T + S_{B_2} e^T + S_{B_1}^T e^T + e^T = 0.$$

Эти формулы показывают, что последняя строка в матрице H ортогональна к остальным ее строкам.

Наконец, в силу леммы 2 и формулы (18)

$$e^T e + S_{B_1} S_{B_1}^T - S_{B_2}^T S_{B_1} - e^T e = 0,$$
$$e^T e + S_{B_1} S_{B_1}^T + S_{B_2}^T S_{B_2} + e^T e = (2v + 2) I,$$
$$e^T e + S_{B_2} S_{B_2}^T + S_{B_1}^T S_{B_1} + e^T e = (2v + 2) I.$$

Из этих равенств следует, что внутренние строки в матрице H попарно ортогональны. Теорема доказана.

Новосибирский институт
народного хозяйства

Поступило
23.06.87

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

[1] Wilson R. M. Cyclotomy and difference families in elementary abelian groups // J. Numer. Theory. 1972. V. 4. P. 17—47.