Math-Net.Ru

Общероссийский математический портал

Ф. М. Малышев, В. Е. Тараканов, О (v, k) -конфигурациях, *Матем. сб.*, 2001, том 192, номер 9, 85–108

DOI: <https://doi.org/10.4213/sm595>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 18.207.199.55

26 апреля 2023 г., 14:04:57

УДК 519.142

Ф. М. Малышев, В. Е. Тараканов

О (v, k) -конфигурациях

В работе вводятся и изучаются новые комбинаторные объекты – (v, k) -конфигурации. Они возникают путем ослабления условий, определяющих хорошо известные комбинаторные объекты – (v, k, λ) -конфигурации. Доказывается ряд результатов о существовании (v, k) -конфигураций. Указываются способы их построения, основанные, в частности, на теоретико-групповых конструкциях и квадратичных вычетах по простому модулю. Приводится обширный список примеров (v, k) -конфигураций, включающий ряд бесконечных серий.

Библиография: 7 названий.

§ 1. Введение

Рассматриваемые в работе (v, k) -конфигурации являются естественным обобщением интенсивно изучаемых в комбинаторной математике (v, k, λ) -конфигураций и представляют интерес для современной теории кодирования.

Напомним (см., например, [1]), что совокупность $X_0, \dots, X_{v-1}$ подмножеств множества X , $|X| = v$, называется (v, k, λ) -конфигурацией, если $|X_i| = k$, $i = 0, 1, \dots, v-1$, и

$$|X_i \cap X_j| = \lambda, \quad 0 \leq i < j \leq v-1. \quad (1)$$

Предполагается, что $0 < \lambda < k < v-1$. Из (1) следует (см. [1; гл. 10]), что

$$|\{i = \overline{0, v-1} : x \in X_i\}| = k \quad \forall x \in X. \quad (2)$$

Таким образом, $(0, 1)$ -матрица инцидентности

$$L = \|l_{ix}\|, \quad i = \overline{0, v-1}, \quad x \in X, \quad l_{ix} = \begin{cases} 1, & \text{если } x \in X_i, \\ 0, & \text{если } x \notin X_i, \end{cases}$$

рассматриваемого семейства имеет ровно по k единиц в каждой строке и в каждом столбце.

Из условия (2) условие (1), вообще говоря, не следует.

ОПРЕДЕЛЕНИЕ 1. (v, k) -конфигурацией называется семейство k -подмножеств $X_0, \dots, X_{v-1}$ множества X , $0 < k < v = |X|$, удовлетворяющее условию (2), для которого существует другое семейство k -подмножеств $Y_0, Y_1, \dots, Y_{v-1}$ в X , тоже удовлетворяющее (2), такое, что при всех $i, j = \overline{0, v-1}$

$$|X_i \cap Y_j| \pmod{2} = \delta_{ij} = \begin{cases} 1 & \text{при } i = j, \\ 0 & \text{при } i \neq j. \end{cases} \quad (3)$$

Работа выполнена при частичной поддержке Программы поддержки ведущих научных школ (грант № 00-15-96136).

Если в этом определении вместо (3) имеет место условие

$$|X_i \cap Y_j| \pmod{2} = \bar{\delta}_{ij} = \begin{cases} 0 & \text{при } i = j, \\ 1 & \text{при } i \neq j, \end{cases} \quad (3')$$

то семейство $\{X_i : i = \overline{0, v-1}\}$ называется $(v, k)'$ -конфигурацией.

Очевидно, (v, k, λ) -конфигурация при нечетном k и четном λ является (v, k) -конфигурацией, а при четном k и нечетном λ — $(v, k)'$ -конфигурацией. В этих случаях $Y_j = X_j, j = \overline{0, v-1}$.

Множество X в дальнейшем обычно отождествляется с множеством чисел $\{0, 1, \dots, v-1\}$, которыми нумеруются строки и столбцы матриц инцидентности (v, k) -конфигураций.

Рассматривая элементы матрицы инцидентности (v, k) - или $(v, k)'$ -конфигурации как элементы поля $\text{GF}(2)$, получаем эквивалентные и более удобные для нас понятия (v, k) -матрицы и $(v, k)'$ -матрицы.

ОПРЕДЕЛЕНИЕ 2. Квадратную матрицу L порядка v над полем $\text{GF}(2)$ с k единицами в каждой строке и в каждом столбце называем (v, k) -матрицей, если существует другая матрица L^- с такими же свойствами, для которой

$$L \cdot L^- = I. \quad (4)$$

Если

$$L \cdot L^- = I + J, \quad (4')$$

то L называем $(v, k)'$ -матрицей.

Здесь $I = I_v$ — единичная матрица; $J = J_v$ — матрица из одних единиц.

Матрицу L в этом определении можно рассматривать как матрицу инцидентности для семейства k -подмножеств $X_0, \dots, X_{v-1}$ v -множества X , а L^- — как транспонированную к матрице инцидентности M для другого семейства $Y_0, \dots, Y_{v-1}$ k -подмножеств X : $L^- = M^T$. Таким образом, введенные в определениях 1 и 2 понятия эквивалентны и взаимозаменяемы.

В работе описаны различные способы построения (v, k) -конфигураций, в частности, использующие свойства (v, k) -групп, связанных с совершенными разностными множествами. Изучаются условия существования (v, k) -матриц в общем случае и более детально для $k \leq 9$. Приводится ряд примеров (v, k) -матриц, в том числе порождаемых регулярными и симметрическими графами. В последнем, пятом параграфе приводится сводка основных результатов в виде таблицы (v, k) -конфигураций со ссылками на основной текст работы.

В вопросах существования различных комбинаторных конфигураций ценными являются как общие результаты, так и отдельные нетривиальные примеры. При изложении мы старались, по возможности, придерживаться тех конкретных представлений, в которых эти примеры впервые были получены, чтобы они не выглядели тривиальными частными случаями обнаруженных позднее более общих конструкций.

Авторы признательны А. М. Зубкову и В. Н. Сачкову за полезные обсуждения и советы в ходе выполнения этой работы. Мы благодарны также Д. А. Кондрашову и А. Е. Тришину за проделанные по нашей просьбе вычисления на ЭВМ.

§ 2. Примеры (v, k) -матриц

ПРЕДЛОЖЕНИЕ 1. а) (v, k) -конфигурации возможны только при нечетных k ;

б) $(v, k)'$ -конфигурации возможны только для v и k разной четности;

в) если v нечетно, то L является (v, k) -матрицей тогда и только тогда, когда $L + J$ является $(v, v - k)'$ -матрицей;

г) если v четно, то L является (v, k) -матрицей $((v, k)'$ -матрицей) тогда и только тогда, когда $L + J$ является $(v, v - k)$ -матрицей (соответственно $(v, v - k)'$ -матрицей);

д) пусть L есть $(v, k)'$ -матрица, тогда матрица L^- условием $(4')$ однозначно определяется по L :

$$L^- = \begin{cases} (L + J)^{-1} + J & \text{при нечетном } v, \\ L^-(I + J) & \text{при четном } v, \end{cases}$$

причем $L^- \cdot L = I + J$, т.е. L^- – тоже $(v, k)'$ -матрица с $(L^-)^- = L$;

е) если L является $(v, k)'$ -матрицей $((v, k)$ -матрицей), то и транспонированная к ней матрица L^T является $(v, k)'$ -матрицей (соответственно (v, k) -матрицей).

Прежде чем доказывать это предложение, заметим, что $L + J$ – матрица инцидентности для семейства $\overline{X}_i = X \setminus X_i, i = \overline{0, v-1}$, а $(L^- + J)^T$ – для семейства $\overline{Y}_i = X \setminus Y_i, i = \overline{0, v-1}$. Аналог п. д) для (v, k) -матриц мы не приводим ввиду его очевидности. Как следствие п. д) получаем однозначную восстанавливаемость в определении 1 семейства $\{Y_i : i = \overline{0, v-1}\}$ по семейству $\{X_i : i = \overline{0, v-1}\}$ как для (v, k) -, так и для $(v, k)'$ -конфигурации. Обратим также внимание на взаимозаменимость этих семейств в определении 1.

ДОКАЗАТЕЛЬСТВО ПРЕДЛОЖЕНИЯ 1 проведем отдельно по каждому пункту, используя, кроме условий (4) и $(4')$, следующие замечания:

- (i) если k четно, то $JL = LJ = JL^- = L^-J = 0$ и матрицы L, L^- вырождены;
- (ii) если k нечетно, то $JL = LJ = JL^- = L^-J = J$;
- (iii) если v четно, то $J^2 = 0, (I + J)^2 = I$ и матрица $I + J$ невырождена;
- (iv) если v нечетно, то $J^2 = J$.

Приступим теперь к доказательству предложения.

а) Из (4) следует невырожденность L , что в случае четного k противоречит (i).

б) Если v четно, то из условий $(4')$ и (iii) следует невырожденность L , в силу чего согласно (i) k нечетно.

Если v нечетно, то из условий $(4')$ и (iv) имеем

$$(L + J)(L^- + J) = LL^- + LJ + JL^- + J^2 = I + J + 2kJ + J = I.$$

Тем самым, матрица $\overline{L} = L + J$ невырождена с $\overline{k} = v - k$ единицами в строках и столбцах. Согласно (i) $\overline{k}$ нечетно и, значит, $k = v - \overline{k}$ четно.

в) При нечетном v из (iv) и (4) имеем

$$(L + J)(L^- + J) = LL^- + JL^- + LJ + J^2 = I + 2kJ + J = I + J.$$

Обратно, пусть $L_1 \cdot L_1^- = I + J$, где $L_1 = I + J$, а в строках и столбцах матрицы L_1^- , как и у L_1 , по $\bar{k} = v - k$ нулей. Тогда

$$L \cdot (L_1^- + J) = (L_1 + J)(L_1^- + J) = L_1 \cdot L_1^- + L_1 J + J L_1^- + J^2 = I + J + 2\bar{k}J + J = I.$$

г) Здесь v четно. Для (v, k) -матрицы L из (4) и (iii) имеем $(L + J)(L^- + J) = LL^- = I$. Обратно, если $L + J - (v, k)$ -матрица, то по доказанному $L = (L + J) + J$ — тоже (v, k) -матрица.

Для $(v, k)'$ -матрицы L из (4') и (iii) имеем $(L + J)(L^- + J) = LL^- = I + J$. В обратном убеждаемся аналогично предыдущему.

д) Если v нечетно, то согласно б) k четно. Из (4') и (iv) имеем

$$(L + J)(L^- + J) = I,$$

а $L^- = L + J$. Далее, учитывая (i), получаем

$$\begin{aligned} L^- L &= [(L + J)^{-1} + J] \cdot L = (L + J)^{-1} L = (L + J)^{-1} (L + J + J) \\ &= I + (L + J)^{-1} J = I + (L^- + J) J = I + J. \end{aligned}$$

Если v четно, то k нечетно. Из условий (4') и (iii) имеем $L^- = L^{-1}(I + J)$, $L^{-1} = L^-(I + J)$ и, привлекая еще условие (ii),

$$L^- L = L^{-1}(I + J)L = L^{-1}(L + J) = I + L^{-1}J = I + L^-(I + J)J = I + L^-J = I + J.$$

е) Транспонируя обе части равенства (4') (или (4)) и применяя утверждение д), получаем требуемое.

Согласно п. в) при нечетном v существует взаимно однозначное соответствие между (v, k) -матрицами и $(v, v - k)'$ -матрицами. В частности, (v, k) -конфигурация при нечетном v существует в том и только том случае, когда существует $(v, v - k)'$ -конфигурация. Однако как при исследовании условий существования, так и при построении (v, k) -конфигураций понятие $(v, k)'$ -матриц с нечетным v оказывается полезным (см. предложения 6, 13, 17 и примеры из п. 3.5).

$(v, k)'$ -конфигурации с четным v далее в настоящей работе не рассматриваются. Отметим только, что они не могут быть построены непосредственно по (v, k, λ) -конфигурациям (см. п. б) предложения 1), но все же существуют; например, если $L - (2k, k)$ -матрица, то $L + J$ будет $(2k, k)'$ -матрицей с $(L + J)^- = L^- = L^{-1}$, и наоборот, если $L - (2k, k)'$ -матрица, то $L + J - (2k, k)$ -матрица с $(L + J)^{-1} = L^-$. Согласно п. г) предложения 1 здесь как L , так и $L + J$ являются одновременно $(2k, k)$ - и $(2k, k)'$ -матрицами. Существование (v, k) -матриц с четным v ниже доказывается для любого нечетного $k < v$ (см. предложение 7).

Обратимся теперь к способам построения (v, k) -матриц. Прежде всего, $(v, 1)$ -матрицы — это в точности подстановочные матрицы. Уже они с помощью приводимых ниже предложений и предложения 1 п. г) позволяют получать нетривиальные примеры (v, k) -матриц с $k > 1$ (см. таблицу 1 в §5). Так, при четном v все $(v, v - 1)$ -матрицы получаются инвертированием подстановочных матриц.

ПРЕДЛОЖЕНИЕ 2. Если $L - (v, k)$ -матрица, а P и $Q - подстановочные или, иначе, $(v, 1)$ -матрицы, то $PLQ - тоже (v, k) -матрица.$$

ПРЕДЛОЖЕНИЕ 3. Пусть L_i – (v_i, k) -матрицы, $i = 1, 2$. Тогда

$$L = \begin{pmatrix} L_1 & 0 \\ 0 & L_2 \end{pmatrix}$$

будет $(v_1 + v_2, k)$ -матрицей.

Матрицу, приводимую перестановками строк и столбцов к указанному в предложении 3 виду, называем *разложимой*. Естественно, больший интерес представляют как раз неразложимые (v, k) -матрицы. Назовем также (v, k) -конфигурацию *неразложимой*, если гиперграф на X , задаваемый подмножествами X_i , $i = \overline{0, v-1}$, связан. Нетрудно убедиться, что на каждой связной компоненте мощности w рассматриваемого гиперграфа индуцируется задание (w, k) -конфигурации, а неразложимость (v, k) -конфигурации равносильна неразложимости ее матрицы инцидентности.

ОПРЕДЕЛЕНИЕ 3. (v, k) -конфигурацию $(X_i : i \in X)$ называем *инволютивной*, если $i \in X_i$ для всех $i \in X$, а включение $i \in X_j$ равносильно включению $j \in X_i$ для всех $i, j \in X$.

Матрица инцидентности L инволютивной (v, k) -конфигурации будет инволютивной: $L^{-1} = L$, причем вдоль ее главной диагонали располагаются только единицы.

Следующие два примера инволютивных (v, k) -матриц получены А. М. Зубковым и Е. Г. Красулиной.

ПРИМЕР 1. Матрица

$$L = \begin{pmatrix} D_1 & J_{2r} & 0 & \dots & 0 & 0 \\ 0 & D_2 & J_{2r} & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & D_{n-1} & J_{2r} \\ J_{2r} & 0 & 0 & \dots & 0 & D_n \end{pmatrix} = L^{-1},$$

где D_i , $i = \overline{1, n}$, – симметричные подстановочные матрицы порядка $2r$, будет инволютивной (v, k) -матрицей с $v = 2rn$, $k = 2r + 1$. Для проверки условия $L^2 = I$ можно воспользоваться замечаниями из доказательства предложения 1.

ПРИМЕР 2. Если B – (v, k) -матрица, то

$$L = \begin{pmatrix} 0 & B \\ B^{-1} & 0 \end{pmatrix} = L^{-1}$$

будет инволютивной $(2v, k)$ -матрицей.

В примере 1 в качестве D_i , $i = \overline{1, n}$, могут выступать произвольные инволютивные $(2r, k_1)$ -матрицы. Тогда L будет инволютивной $(2rn, 2r + k_1)$ -матрицей.

ПРЕДЛОЖЕНИЕ 4. Пусть $(X'_i : i \in X')$ – инволютивная (v', k') -конфигурация, а $(X''_i : i \in X'')$ – инволютивная (v'', k'') -конфигурация. Тогда семейство

$$(X_{(i,j)} = (X'_i, j) \cup (i, X''_j) : (i, j) \in X' \times X'')$$

будет инволютивной $(v'v'', k' + k'' - 1)$ -конфигурацией на множестве $X = X' \times X''$. Она неразложима, если и только если обе исходные конфигурации неразложимы.

ДОКАЗАТЕЛЬСТВО. Положим $Y_{(i,j)} = (Y'_i, j) \cup (i, Y''_j)$. Тогда

$$X_{(i,j)} \cap Y_{(i,j)} = (X'_i \cap Y'_i, j) \cup (i, X''_j \cap Y''_j)$$

как объединение двух множеств нечетной мощности с одноэлементным пересечением будет иметь нечетную мощность. Далее,

$$X_{(i_1,j)} \cap Y_{(i_2,j)} = (X'_{i_1} \cap Y'_{i_2}, j)$$

имеет четную мощность при $i_1 \neq i_2$, а $|X_{(i,j_1)} \cap Y_{(i,j_2)}|$ четно при $j_1 \neq j_2$. Наконец, при $i_1 \neq i_2$ и $j_1 \neq j_2$ имеем

$$X_{(i_1,j_1)} \cap Y_{(i_2,j_2)} = ((i_2, Y''_{j_2}) \cap (X'_{i_1}, j_1)) \cup ((i_1, X''_{j_1}) \cap (Y'_{i_2}, j_2)).$$

Левая и правая компоненты этого объединения по условию инволютивности или одновременно пусты, или равны соответственно $\{(i_2, j_1)\}$ и $\{(i_1, j_2)\}$. В любом случае число элементов в левой части четно.

Другие примеры инволютивных (v, k) -матриц будут приведены ниже (см. предложения 7 и 15).

ПРЕДЛОЖЕНИЕ 5. Пусть $L_i - (v_i, k_i)$ -матрицы, $i = 1, 2$. Тогда их тензорное произведение будет $(v_1 v_2, k_1 k_2)$ -матрицей, неразложимой при неразложимых сомножителях и разложимой, если хотя бы одна из матриц L_i , $i = 1, 2$, разложима.

ДОКАЗАТЕЛЬСТВО. $(L_1 \otimes L_2)^{-1} = L_1^{-1} \otimes L_2^{-1}$.

СЛЕДСТВИЕ 1. Если v_2 четно, то $L_1 \otimes (L_2 + J) - (v_1 v_2, k_1(v_2 - k_2))$ -матрица.

ПРЕДЛОЖЕНИЕ 6. Пусть $L_0 - (v_0, k_0)$ -матрица, v_0 нечетно, $L_i - (v_{12}, k_i)$ -матрицы, $i = 1, 2$. Предположим, что

$$L_1 \wedge L_2 = L_1^{-1} \wedge L_2^{-1} = 0, \quad (5)$$

где $\wedge$ - операция поэлементной конъюнкции. Тогда

$$L = L_1 \otimes J_{v_0} + L_2 \otimes (L_0 + J_{v_0})$$

является (v, k) -матрицей с $v = v_{12} \cdot v_0$, $k = k_1 v_0 + k_2(v_0 - k_0)$. При этом матрица L неразложима, если и только если связан гиперграф, заданный строками матрицы $L_1 + L_2$.

ДОКАЗАТЕЛЬСТВО. Согласно (5) одинаково расположенные элементы матриц L_1 и L_2 не могут одновременно принимать значение 1, и таким же свойством обладают матрицы L_1^{-1} и L_2^{-1} . Поэтому число единиц как в строках, так и столбцах матрицы L равно $k_1 v_0 + k_2(v_0 - k_0) = k$. Положим

$$L^- = L_1^{-1} \otimes J_{v_0} + L_2^{-1} \otimes (L_0^{-1} + J_{v_0}).$$

У матрицы L^- в строках и столбцах также по k единиц. Покажем, что $L^- = L^{-1}$. Для этого представим матрицы L и L^- в блочном виде - по v_{12} блоков размера

$v_0 \times v_0$ в полосах и колонках. Далее обозначаем: $J_{v_0} = J$, $I_{v_0} = I$. Очевидно, $J^2 = J$. У матрицы $L \cdot L^{-1}$ в каждой из клеток по главной диагонали будет блок

$$J^2 + (J + L_0)(J + L_0^{-1}) = J^2 + J^2 + L_0 J + J L_0^{-1} + I = I.$$

Содержимое всякой клетки вне главной диагонали у $L \cdot L^{-1}$ представляется как сумма четного числа блоков $J^2 = J$, четного числа блоков $(J + L_0) \cdot (J + L_0^{-1}) = J + I$ и, возможно, некоторого числа блоков $(J + L_0)J = J^2 + J = 0$ и блоков $J(J + L_0^{-1}) = 0$; таким образом, каждая клетка — нулевая. Итак, $L^{-1} = L^{-1}$. Утверждение, касающееся неразложимости L , очевидно.

ПРЕДЛОЖЕНИЕ 7. Пусть B — квадратная $(0, 1)$ -матрица порядка w с нулями по главной диагонали и с $\frac{1}{2}(k-1)$ единицами в строках и столбцах, k нечетное; D — диагональная $(0, 1)$ -матрица порядка w . Тогда

$$L = \begin{pmatrix} I_w + B + D & B + D \\ B + D & I_w + B + D \end{pmatrix}$$

является $(2w, k)$ -матрицей.

ДОКАЗАТЕЛЬСТВО. $L^2 = I_{2w}$.

СЛЕДСТВИЕ 2. Для любого четного v и любого нечетного k , $1 < k < v$, существуют неразложимые (v, k) -матрицы.

ДОКАЗАТЕЛЬСТВО. Достаточно в предложении 7 положить $D = 0$, а в качестве B взять циклическую матрицу с единицами в нулевой строке на местах $1, 2, \dots, \frac{1}{2}(k-1)$.

Напомним, что матрица $B = \|b_{ij}\|$, $i, j = \overline{0, w-1}$, является циклической, если $b_{i,j} = b_{(i+1) \pmod w, (j+1) \pmod w}$ для всех $i, j = \overline{0, w-1}$.

ОПРЕДЕЛЕНИЕ 4. Семейство ν -подмножеств $Z_z \subset Z$, $z \in Z$, в λ -множестве Z называем симметрическим, если $z \in Z_z \forall z \in Z$; $z \in Z_u \Leftrightarrow u \in Z_z \forall z, u \in Z$.

Условия этого определения равносильны требованию, чтобы матрица инцидентности семейства была симметрической с единицами на главной диагонали.

ПРЕДЛОЖЕНИЕ 8. Если $Z_z \subset Z$, $z \in Z$, — симметрическое семейство ν -подмножеств в λ -множестве Z , $\lambda \geq \nu > 1$, а $(X_i : i \in X)$ — (v, k) -конфигурация с четным v , то система подмножеств

$$\mathcal{X}_{(z,i)} = (Z_z \setminus \{z\}, X) \cup (z, X_i), \quad (z, i) \in Z \times X,$$

определяет $(\lambda v, (\nu-1)v + k)$ -конфигурацию на $Z \times X$. При этом ее матрица неразложима, если и только если гиперграф семейства $\{Z_z : z \in Z\}$ связан.

ДОКАЗАТЕЛЬСТВО. Достаточно положить

$$\mathcal{Y}_{(z,i)} = (Z_z \setminus \{z\}, X) \cup (z, Y_i), \quad (z, i) \in Z \times X.$$

§ 3. (v, k) -группы

В этом параграфе будет рассматриваться один специальный класс (v, k) -конфигураций – конфигурации на конечных группах, для которых все подмножества из семейства получаются из одного всевозможными левыми сдвигами.

3.1. Перенос общих конструкций (v, k) -конфигураций на конечные группы. Пусть G – конечная группа, $|G| = v$, и в ней выбрано подмножество $H \subset G$ с $|H| = k$. У матрицы инцидентности $L = L(G, H)$ семейства $\{gH : g \in G\}$ в строках и столбцах по k единиц. Транспонированная матрица L^T является матрицей инцидентности семейства $\{gH^{-1} : g \in G\}$, где $H^{-1} = \{h^{-1} : h \in H\}$.

ПРЕДЛОЖЕНИЕ 9. Если $L = L(G, H)$ является (v, k) -матрицей, то $L^{-1} = M^T$, где $M = L(G, S)$ для некоторого $S \subset G$, $|S| = k$.

ДОКАЗАТЕЛЬСТВО. Если строки и столбцы рассматриваемых матриц пронумеровать элементами G и положить $L^{-1} = \|l_{g', g''}^-\|$, $g', g'' \in G$, то $S = \{g \in G : l_{g, e}^- = 1\}$.

Условие $L \cdot M^T = I$ равносильно требованиям

$$\begin{aligned} |H \cap S| & \text{ нечетно,} \\ |H \cap gS| & \text{ четно } \forall g \in G \setminus \{e\}. \end{aligned} \quad (6)$$

Подмножество S при этом однозначно определяется по H . Не ограничивая общности, в рассматриваемой ситуации можно считать, что единица группы e принадлежит $H \cap S$, так как всегда можно перейти к паре $H' = h^{-1}H$, $S' = h^{-1}S$, где $h \in H \cap S$. Далее условие $e \in H \cap S$, как правило, будет предполагаться выполненным.

ОПРЕДЕЛЕНИЕ 5. Пара (G, H) , где G – конечная группа, а $H \subset G$ – ее непустое подмножество, называется (v, k) -группой, если $|G| = v$, $|H| = k$ и существует подмножество $S \subset G$, $|S| = k$, удовлетворяющее условиям (6).

Подмножества S и H являются взаимозаменяемыми и, как уже было сказано, однозначно восстанавливаются одно по другому. Ниже при необходимости указывать для (v, k) -группы (G, H) вместе с H и множество S будет использоваться также обозначение (G, H, S) .

Очевидно, что вместе с (v, k) -группой (G, H, S) имеем еще (v, k) -группы:

$$\begin{aligned} (G, S, H); \quad (G, H^{-1}, S^{-1}); \quad (G, S^{-1}, H^{-1}); \\ (G, \varphi(H), \varphi(S)) \quad \forall \varphi \in \text{Aut } G; \\ (G, gH, gS) \quad \text{и} \quad (G, Hg, Sg) \quad \forall g \in G. \end{aligned}$$

Это замечание можно рассматривать как аналог предложения 2 для (v, k) -групп.

ПРЕДЛОЖЕНИЕ 10. Пусть имеется (v, k) -группа (G, H, S) и $e \in H \cap S$. Тогда подгруппы, порожденные элементами из H и из S , совпадают: $\langle H \rangle = \langle S \rangle$, а разбиения гиперграфов $(G, \{gH : g \in G\})$ и $(G, \{gS : g \in G\})$ на связные компоненты совпадают с разбиением на левые смежные классы по подгруппе $\langle H \rangle$.

ДОКАЗАТЕЛЬСТВО. Пусть G_0 – связная компонента гиперграфа $(G, \{gH : g \in G\})$, содержащая e , и $g_1, g_2 \in G_0$. Тогда H и g_2H связаны, а значит, и g_1H с $g_1(g_2H)$ связаны. Но H и g_1H тоже связаны, поэтому в силу транзитивности H и $(g_1g_2)H$ связаны. Таким образом, G_0 – подгруппа, содержащая $\langle H \rangle$. Далее, для каждого $g \in G$ подмножество gH целиком содержится в смежном классе по $\langle H \rangle$ – в $g\langle H \rangle$, поэтому $G_0 \subset \langle H \rangle$ и, значит, $G_0 = \langle H \rangle$.

Пусть $L_0 = L(G_0, H)$. Тогда матрица $L = L(G, H)$ представляется блочно-диагональной матрицей с одинаковыми блоками по диагонали, совпадающими с L_0 . Число блоков равно $[G : G_0] = |G/G_0|$. Строки и столбцы каждого блока нумеруются элементами какого-либо одного смежного класса по G_0 .

Все предыдущие рассуждения можно повторить для гиперграфа $(G, \{gS : g \in G\})$ и получить блочно-диагональное представление матрицы инцидентности $M = L(G, S)$. Число блоков будет равно $[G : \langle S \rangle]$, и каждый блок совпадает с матрицей $M_0 = L(\langle S \rangle, S)$. Здесь $\langle S \rangle$ совпадает со связной компонентой гиперграфа $(G, \{gS : g \in G\})$. Утверждения доказываемого предложения теперь следуют из соотношения $M^\tau = L^{-1}$.

По доказанному при $e \in H \cap S$ неразложимость (v, k) -матрицы $L = L(G, H)$, отвечающей (v, k) -группе (G, H) , равносильна условию $G = \langle H \rangle$. В этом случае (v, k) -группу (G, H) тоже будем называть *неразложимой*.

ОПРЕДЕЛЕНИЕ 6. Назовем (v, k) -группу (G, H, S) *инволютивной*, если $S = H^{-1}$ и $e \in H \cap S$.

Инволютивность (v, k) -группы (G, H) равносильна инволютивности (v, k) -конфигурации $(gH : g \in G)$, а последнее, как ранее было замечено, равносильно тому, что (v, k) -матрица $L = L(G, H)$ является инволютивной и на ее главной диагонали стоят единицы.

Аналогами предложений 4–6 и 8 для (v, k) -групп являются приводимые ниже предложения 11–13 и 14 соответственно.

ПРЕДЛОЖЕНИЕ 11. Пусть (G_i, H_i, S_i) , $i = 1, 2$, – инволютивные (v_i, k_i) -группы. Тогда $(G_1 \times G_2, (H_1, e_2) \cup (e_1, H_2), (S_1, e_2) \cup (e_1, S_2))$ будет инволютивной $(v_1v_2, k_1 + k_2 - 1)$ -группой, которая неразложима, если и только если обе исходные (v_i, k_i) -группы неразложимы.

ПРЕДЛОЖЕНИЕ 12. Если (G_i, H_i, S_i) – (v_i, k_i) -группы, $i = 1, 2$, то $(G_1 \times G_2, H_1 \times H_2, S_1 \times S_2)$ – (v_1v_2, k_1k_2) -группа; она инволютивна, если инволютивны (G_i, H_i, S_i) , $i = 1, 2$. Кроме того, она неразложима тогда и только тогда, когда (G_i, H_i, S_i) , $i = 1, 2$, неразложимы.

В предложении 6 по (v_{12}, k_i) -матрицам L_i , $i = 1, 2$, и (v', k') -матрице L' с нечетным v' строилась (v, k) -матрица $L = L_1 \otimes J_{v'} + L_2 \otimes L'$ с $v = v_{12} \cdot v'$ и $k = k_1v' + k_2k'$. Перенос этого предложения на (v, k) -группы использует аналогичное понятие (v, k) -группы $(G, H, S)'$, $v = |G|$, $k = |H| = |S|$, $H, S \subset G$, которое мы определим только для нечетных v . Если G – конечная группа нечетного порядка v и H, S – k -подмножества в ней, для которых

$$\begin{aligned} |H \cap S| & \text{ чётно,} \\ |H \cap gS| & \text{ нечётно } \forall g \in G \setminus \{e\}, \end{aligned} \quad (6')$$

то семейство k -подмножеств $\{gH : g \in G\}$ образует $(v, k)'$ -конфигурацию (см. (3')) с другим семейством k -подмножеств $\{gS : g \in G\}$, а матрица инцидентности семейства $\{gH : g \in G\}$ будет $(v, k)'$ -матрицей.

ОПРЕДЕЛЕНИЕ 7. Группу G нечетного порядка v с k -подмножествами H, S , удовлетворяющими (6'), называем $(v, k)'$ -группой.

Пусть имеется $(v, k)'$ -группа $(G, H', S')'$. Рассмотрим множества $H = G \setminus H'$, $S = G \setminus S'$. Нетрудно заметить, что тогда $|H \cap S|$ нечетно, а $|H \cap gS|$ четно при всех $g \in G \setminus \{e\}$. Таким образом, (G, H, S) есть $(v, v-k)$ -группа. Аналогично, при наличии $(v, v-k)$ -группы, переходя к дополнениям, получаем $(v, k)'$ -группу при нечетном v и (v, k) -группу при четном v . Тем самым, $(v, k)'$ -группа (v нечетно) существует тогда и только тогда, когда существует $(v, v-k)$ -группа. В частности, k должно быть четным, поскольку $(v, v-k)$ -группы существуют только при нечетном $v-k$. Таким образом, здесь имеем полную аналогию с (v, k) - и $(v, k)'$ -матрицами.

ПРЕДЛОЖЕНИЕ 13. Пусть $(G, H', S')' - (v', k')'$ -группа, v' нечетно; $\mathfrak{G} \supset G$ — нормальное расширение G , $|\mathfrak{G}/G| = v_{12}$, $\pi: \mathfrak{G} \rightarrow \mathfrak{G}/G$ — канонический гомоморфизм. Пусть, далее, $(\mathfrak{G}/G, H_i, S_i) - (v_{12}, k_i)$ -группы, $i = 1, 2$, такие, что $H_1 \cap H_2 = \emptyset$, $S_1 \cap S_2 = \emptyset$, а $\{z_g \in \pi^{-1}(g) : g \in H_2 \cup S_2\}$ — система представителей, удовлетворяющая условию

$$z_{h_1} z_{s_1}^{-1} = z_{h_2} z_{s_2}^{-1} \quad \text{при} \quad h_1 s_1^{-1} = h_2 s_2^{-1}, \quad h_1, h_2 \in H_2, \quad s_1, s_2 \in S_2. \quad (7)$$

Тогда существует (v, k) -группа $(\mathfrak{G}, \mathfrak{H}, \mathfrak{S})$ с $v = v_{12} \cdot v'$, $k = k_1 \cdot v' + k_2 \cdot k'$,

$$\mathfrak{H} = \bigcup_{h \in H_1} \pi^{-1}(h) \cup \bigcup_{h \in H_2} (z_h \cdot H'), \quad \mathfrak{S} = \bigcup_{s \in S_1} \pi^{-1}(s) \cup \bigcup_{s \in S_2} (z_s \cdot S').$$

При этом соответствующая (v, k) -матрица неразложима тогда и только тогда, когда гиперграф $(\mathfrak{G}/G, \{g(H_1 \cup H_2) : g \in \mathfrak{G}/G\})$ связан.

ДОКАЗАТЕЛЬСТВО сводится к непосредственной проверке условий (6) для группы $\mathfrak{G}$ с учетом тех же условий для группы $\mathfrak{G}/G$, а также условий (6') для группы G и условий (7). Последние обеспечивают выполнение соотношений

$$\left| \left(\bigcup_{h \in H_2} (z_h H') \right) \cap \left(q \cdot \bigcup_{s \in S_2} (z_s S') \right) \right| \text{ четно } \quad \forall q \in \mathfrak{G} \setminus G. \quad (8)$$

Новое (по сравнению с предложением 6) условие (7) заведомо выполняется при $k_2 = 1$, а также если расширение $\mathfrak{G} \supset G$ расщепимо, т.е. если $\mathfrak{G}$ представляется полупрямым произведением $\mathfrak{G} = \overline{\mathfrak{G}} \ltimes G$ и $z_g \in \overline{\mathfrak{G}} \quad \forall g \in H_2 \cup S_2$. Условие (7) в формулировке предложения 13 может быть также заменено более слабым условием (8).

ОПРЕДЕЛЕНИЕ 8. Если G — группа с единицей e , $e \in O \subset G$ и $O^{-1} = O$, то подмножество O называем *симметрическим*.

Подмножество $O \subset G$ симметрическое тогда и только тогда, когда семейство $\{gO : g \in G\}$ симметрическое.

ПРЕДЛОЖЕНИЕ 14. Пусть (G, H, S) – (v, k) -группа, v четно, $\mathfrak{G} \triangleright G$ – нормальное расширение, $|\mathfrak{G}/G| = \lambda$, а $O \subset \mathfrak{G}/G$ – симметрическое подмножество, $|O| = \nu > 1$. Тогда имеем $(\lambda\nu, (\nu - 1)v + k)$ -группу $(\mathfrak{G}, \mathfrak{H}, \mathfrak{S})$ с

$$\mathfrak{H} = \bigcup_{g \in O \setminus \{eG\}} \pi^{-1}(g) \cup H \quad \text{и} \quad \mathfrak{S} = \bigcup_{g \in O \setminus \{eG\}} \pi^{-1}(g) \cup S.$$

При этом соответствующая матрица инцидентности неразложима, если и только если гиперграф семейства $\{gO : g \in \mathfrak{G}/G\}$ связан.

3.2. Универсальный способ построения (v, k) -групп с заданным нечетным k . Пусть имеется (v, k) -группа (G, H, S) , $e \in H \cap S$, $|H \cap S| = k_0 \leq k$,

$$H = \{h_1, \dots, h_k\}, \quad S = \{s_1, \dots, s_k\}, \quad h_i = s_i, \quad i = \overline{1, k_0}.$$

Для $g \in G \setminus \{e\}$ положим

$$\mathfrak{N}(g) = \{(i, j) \in (\overline{1, k})^2 : h_i = gs_j\} \subset (\overline{1, k})^2 \setminus \{(l, l) : l = \overline{1, k_0}\}. \quad (9)$$

Два разных элемента $(i', j'), (i'', j'') \in (\overline{1, k})^2$ назовем *противоречивыми*, если $i' = i''$ (и тогда $j' \neq j''$) или $j' = j''$ (и тогда $i' \neq i''$). В подмножестве $\mathfrak{N}(g)$ противоречивые пары исключены – если $(i', j'), (i'', j'') \in \mathfrak{N}(g)$, то $i' \neq i''$ и $j' \neq j''$. Согласно (6) мощность $\mathfrak{N}(g)$ четная. Далее, ясно, что

$$\begin{aligned} \bigcup_{g \in G \setminus \{e\}} \mathfrak{N}(g) &= (\overline{1, k})^2 \setminus \{(l, l) : l = \overline{1, k_0}\}, \\ \mathfrak{N}(g_1) \cap \mathfrak{N}(g_2) &= \emptyset \quad \text{при} \quad g_1 \neq g_2. \end{aligned} \quad (10)$$

Сделанных замечаний достаточно, чтобы предложить способ построения всех (v, k) -групп с заданным нечетным k . Для этого заранее задаемся нечетным $k_0 < k$ и (в качестве (10)) разбиением

$$(\overline{1, k})^2 \setminus \{(l, l) : l = \overline{1, k_0}\} = \bigcup_{\alpha \in A} \mathfrak{N}_\alpha \quad (11)$$

на непересекающиеся подмножества $\mathfrak{N}_\alpha$, $\alpha \in A$, четной мощности и без противоречивых пар в каждом из этих подмножеств. Далее исходим из абстрактной системы образующих (9):

$$h_1, \dots, h_k, s_1, \dots, s_k,$$

на которую, кроме соотношений

$$h_1 = s_1 = e, \quad h_i = s_i, \quad i = \overline{2, k_0}, \quad (12)$$

налагаем соотношения

$$h_{i'} \cdot s_{j'}^{-1} = h_{i''} \cdot s_{j''}^{-1}, \quad (i', j'), (i'', j'') \in \mathfrak{N}_\alpha, \quad \alpha \in A. \quad (13)$$

Последние соотношения привлекаются потому, что на роль подмножеств $\mathfrak{N}(g)$, $g \in G \setminus \{e\}$, для (v, k) -группы (G, H, S) , которую мы хотим построить, претендуют как раз подмножества $\mathfrak{N}_\alpha$, $\alpha \in A$ (см. (9)).

К соотношениям (12), (13) добавляем любые другие соотношения, но так, чтобы в результате получилась конечная группа G , в которой элементы $h_1, \dots, h_k$ различны и элементы $s_1, \dots, s_k$ различны (из-за дополнительных соотношений совпадения среди них возможны). Если дополнительно

$$|\{h_{k_0+1}, \dots, h_k\} \cap \{s_{k_0+1}, \dots, s_k\}| = \Delta$$

четно, то получим (v, k) -группу (G, H, S) . В самом деле, тогда $|H \cap S| = k_0 + \Delta$ нечетно, а для $g \in G \setminus \{e\}$ мощность $H \cap gS$ ввиду соотношений (13) будет складываться из мощностей нескольких подмножеств $\mathfrak{N}_\alpha$, $\alpha \in A$, которые четны. Тем самым, условия (6) выполнены.

Ясно, что любая наперед заданная (v, k) -группа может быть получена на этом пути в результате подбора k_0 , разбиения (11) и дополнительных (к (12) и (13)) соотношений.

Как видим, за счет дополнительных соотношений возможно (и это допускается) увеличение k_0 на четное число Δ , а $\mathfrak{N}(g)$, $g \in G \setminus \{e\}$, может быть объединением нескольких подмножеств $\mathfrak{N}_\alpha$, $\alpha \in A$. Поэтому без ограничения общности изначально можно полагать: $k_0 = 1$; $|\mathfrak{N}_\alpha| = 2 \ \forall \alpha \in A$, и тогда все равно полный перебор допустимых разбиений (11) и наборов дополнительных соотношений предоставит все возможные (v, k) -группы G с заданным значением k . Но следует оговориться, что для каких-то разбиений (11) (v, k) -групп может и не существовать.

Описанный здесь способ построения (v, k) -групп будет продемонстрирован в следующих двух пунктах.

3.3. Описание $(v, 3)$ -групп. Пусть $\mathbb{Z}_v = \{0, 1, \dots, v-1\}$ – группа вычетов по модулю v .

ПРЕДЛОЖЕНИЕ 15. *С точностью до изоморфизмов и сдвигов, переводящих выделенные подмножества друг в друга, неразложимые $(v, 3)$ -группы (G, H, S) , $e \in H \cap S$, исчерпываются следующим списком:*

- 1) $(\mathbb{Z}_{2n}, \{0, 1, n+1\}, \{0, n-1, 2n-1\})$, $n \geq 2$;
- 2) $(\mathbb{Z}_{2n} \times \mathbb{Z}_2, \{(0, 0), (1, 0), (1, 1)\}, \{(0, 0), (2n-1, 0), (2n-1, 1)\})$, $n \geq 1$;
- 3) $(\mathbb{Z}_5, \{0, 1, 4\}, \{0, 2, 3\})$.

ДОКАЗАТЕЛЬСТВО. Имеем $|H| = |S| = 3$, а $|H \cap S| = 1$ или 3. Рассмотрим соответствующие случаи – $H = S$ и $H \cap S = \{e\}$ – отдельно.

а) Пусть $H = S = \{h_0 = e, h_1, h_2\}$. Вначале предположим, что если $(i, j) \in \mathfrak{N}(g)$, то и $(j, i) \in \mathfrak{N}(g)$ для всех $0 \leq i \neq j \leq 2$. Тогда $h_1^2 = h_2^2 = e$, $h_1 h_2 = h_2 h_1$ и имеем случай 2) с $v = 4$. Если же такое предположение не выполняется, то для некоторых различных $i, j, l = \overline{0, 2}$ и $g \in G \setminus \{e\}$ имеем $h_j = gh_l$, $h_i = gh_j = g^2 h_l$, в силу чего $G = \langle g \rangle$, $v = 4$, $H = \{g^{-1}, e, g\}$ или $\{e, g, g^2\}$. Это, соответственно, случай 1) с $v = 4$.

б) Пусть теперь $H = \{h_0 = e, h_1, h_2\}$, $S = \{s_0 = e, s_1, s_2\}$, где e, h_1, h_2, s_1, s_2 – пять различных элементов. В этом случае в (11) имеем разбиение на четыре непротиворечивые пары. С точностью до симметрий вида $H \leftrightarrow S$, $s_1 \leftrightarrow s_2$, $h_1 \leftrightarrow h_2$ возможны только следующие три разбиения:

- A) $(1, 1), (2, 2); (1, 2), (2, 1); (1, 0), (0, 1); (2, 0), (0, 2);$
- B) $(1, 1), (0, 2); (2, 1), (1, 0); (2, 2), (0, 1); (1, 2), (2, 0);$
- C) $(1, 1), (2, 2); (2, 1), (0, 2); (1, 2), (2, 0); (1, 0), (0, 1),$

которые рассмотрим отдельно. Напомним, что непротиворечивая пара $(i, j), (l, t)$ из одного подмножества в разбиении (11) приводит к соотношению $h_i s_j^{-1} = h_l s_t^{-1}$. В каждом из случаев А), В), С) будем иметь четыре (по числу пар в разбиении (11)) таких соотношения.

А) Из соотношений

$$h_1 s_1^{-1} = h_2 s_2^{-1}; \quad h_1 s_2^{-1} = h_2 s_1^{-1}; \quad h_1 = s_1^{-1}, \quad h_2 = s_2^{-1}$$

имеем $h_1^2 = h_2^2, h_1 h_2 = h_2 h_1$. Положим $h = h_1, c = h_1^{-1} h_2$. Тогда $c^2 = e, H = \{e, h, hc\}, S = \{e, h^{-1}, h^{-1}c\}$. Возможны два случая: $c \in \langle h \rangle = G$ и $c \notin \langle h \rangle, G = \langle h \rangle \times \langle c \rangle$. В первом из них $c = h^{v/2}$ и получаем случай 1) с $v \geq 6$, а во втором — имеем случай 2) с $v \geq 8$ или 1) с $v \geq 6$ в случае нечетного $v/2$.

В) Из соотношений

$$h_1 s_1^{-1} = s_2^{-1}; \quad h_2 s_1^{-1} = h_1; \quad h_2 s_2^{-1} = s_1^{-1}; \quad h_1 s_2^{-1} = h_2$$

имеем $s_1 = h_1^{-1} h_2, s_2 = h_2^{-1} h_1, h_1^2 = h_2 h_1^{-1} h_2, h_2^2 = h_1 h_2^{-1} h_1$. Из двух последних равенств получаем $h_1^2 h_2 = h_2 h_1^{-1} h_2^2 = h_2 h_1^{-1} h_1 h_2^{-1} h_1 = h_1$, или $h_1 h_2 = e$. Полагая $h_1 = h$, имеем $H = \{e, h, h^{-1}\}, S = \{e, h^2, h^{-2}\}, h^5 = e$, что отвечает случаю 3).

С) Из соотношений

$$h_1 s_1^{-1} = h_2 s_2^{-1}; \quad h_2 s_1^{-1} = s_2^{-1}; \quad h_1 s_2^{-1} = h_2; \quad h_1 = s_1^{-1}$$

имеем: $s_2 = h_2^{-1} h_1, s_1 = h_1^{-1}, h_1 h_2 h_1 = h_2, h_1^2 = h_2 h_1^{-1} h_2 = (h_1 h_2 h_1) h_1^{-1} h_2$. Из последнего следует $h_1 = h_2^2$, а затем из предыдущего $h_2^4 = e$. В результате имеем противоречащее исходному предположению равенство $H = S = \{e, h_2, h_2^2\}$.

Обратим внимание, что $(v, 3)$ -группы семейств 1) и 2) предложения 15 являются инволютивными и все $(v, 3)$ -группы оказались коммутативными. Соответствующие $(v, 3)$ -матрицы получаются по схеме предложения 7, за исключением матрицы для $(5, 3)$ -группы — единственной $(v, 3)$ -группы нечетного порядка.

Заметим еще, что для всех $(v, 3)$ -групп $(G, H, S), e \in H \cap S$, имеется автоморфизм группы G , меняющий H и S местами. В общем случае это неверно. Прежде чем в этом убедиться, приведем пример циклической $(v, 5)$ -группы.

ПРИМЕР 3. $(\mathbb{Z}_{10}, \{0, 1, 4, 5, 7\}, \{0, 2, 4, 7, 8\})$ — $(10, 5)$ -группа.

Условия (6) в этом примере проверяются непосредственно.

Все автоморфизмы φ группы $\mathbb{Z}_{10}$ исчерпываются умножениями на 1, 3, 7, 9 и для каждого из них $\varphi(\{0, 1, 4, 5, 7\}) \neq \{0, 2, 4, 7, 8\}$. Из-за этого в аналогичной предложению 15 классификации для $(v, 5)$ -групп наряду с примером 3 следовало бы указывать $(v, 5)$ -группу $(\mathbb{Z}_{10}, \{0, 2, 4, 7, 8\}, \{0, 1, 4, 5, 7\})$.

Из предложения 15 вытекает

СЛЕДСТВИЕ 3. *Существуют инволютивные неразложимые (v, k) -группы с параметрами $k = 2r + 1, v = 2^r \cdot w_1 \cdots w_r$, где $r, w_i, i = \overline{1, r}$, — произвольные целые, не меньшие 2.*

Доказательство следует из предложения 11 и случаев 1) и 2) предложения 15.

3.4. Пример некоммутативной $(v, 5)$ -группы. Пусть $H = S = \{h_1 = e, h_2, h_3, h_4, h_5\}$, $\sigma \in S_5$, $\sigma = (1)(2, 5)(3, 4)$. В качестве разбиения (11) рассматриваем

$$\bigcup_{i=2}^5 \{(1, i), (\sigma(i), 1)\} \cup \bigcup_{2 \leq i \neq j \leq 5} \{(i, j), (\sigma(i), \sigma(j))\} = (\overline{1, 5})^2 \setminus \{(l, l) : l = \overline{1, 5}\}.$$

Такое разбиение предоставляет соотношения

$$\begin{aligned} h_1 h_2^{-1} &= h_5 h_1^{-1}; & h_1 h_3^{-1} &= h_4 h_1^{-1}; \\ h_2 h_3^{-1} &= h_5 h_4^{-1}; & h_2 h_4^{-1} &= h_5 h_3^{-1}; \\ h_3 h_4^{-1} &= h_4 h_3^{-1}; & h_5 h_2^{-1} &= h_2 h_5^{-1}. \end{aligned}$$

Отсюда, полагая $h_2 = h$, $h_3 = t$ и помня, что $h_1 = e$, имеем

$$H = S = \{e, h, t, t^{-1}, h^{-1}\}, \quad h^2 = t^2, \quad h^4 = e.$$

Эти соотношения выполняются для $h, t \in S_7$,

$$h = (1, 2, 3, 4)(5, 6)(7), \quad t = (4, 3, 2, 1)(5)(6, 7),$$

причем ограничение $G = \langle h, t \rangle \subset S_7$ на подмножество $\{5, 6, 7\}$ совпадает с S_3 и, значит, G некоммутативна. Здесь $v = |G| = 12$, поэтому имеем некоммутативную неразложимую инволютивную $(12, 5)$ -группу с симметричной матрицей инцидентности.

3.5. Циклические (v, k) -конфигурации. Существенным частным случаем (v, k, λ) -конфигураций $(X_i \subset X : i = \overline{0, v-1})$ являются конфигурации, у которых группа автоморфизмов содержит циклическую группу $\mathbb{Z}_v$ порядка v , регулярно действующую на множестве X . Ему соответствует важный частный случай (v, k) -групп, отвечающих циклическим группам; в этом случае конфигурации и матрицы инцидентности L называем *циклическими*.

В соответствии с нашими определениями *циклическая (v, k) -матрица* или (v, k) -*циркулянт* – это невырожденная над $\text{GF}(2)$ циклическая $(0, 1)$ -матрица L порядка v с k единицами в строке, для которой матрица L^{-1} обладает тем же свойством. Строки и столбцы здесь нумеруем элементами из $\mathbb{Z}_v$. Матрица L полностью определяется своей начальной строкой, последующие получаются из предыдущих циклическим сдвигом вправо на единицу. Совокупность номеров единичных элементов в начальной строке L является k -подмножеством $H \subset \mathbb{Z}_v$ (см. определение 5), для которого имеется другое k -подмножество $S \subset \mathbb{Z}_v$, удовлетворяющее условиям (6). Конкретно, S – совокупность номеров единичных элементов в начальном столбце матрицы L^{-1} .

Условия (6) и (6') иногда, особенно в циклическом случае, удобно представлять в другом, эквивалентном виде. Для этого обозначим через $A * B$ мультимножество, состоящее из всех элементов ab , $a \in A$, $b \in B$, в котором число n_g появлений каждого элемента $g \in G$ равно числу решений уравнения $xy = g$, $x \in A$, $y \in B$. Набор $\{n_g, g \in G\}$ можно рассматривать как целочисленную меру на G , $\sum_{g \in G} n_g = |A| \cdot |B|$.

ПРЕДЛОЖЕНИЕ 16. Для k -подмножества $H \subset G$ существует k -подмножество $S \subset G$, удовлетворяющее условиям (6) (соответственно (6')), тогда и только тогда, когда существует k -подмножество $\hat{S} \subset G$, для которого в мультимножестве $H * \hat{S}$ все элементы $g \in G$, за исключением одного, имеют четную (соответственно нечетную) кратность.

ДОКАЗАТЕЛЬСТВО. Достаточно положить $\hat{S} = S^{-1} \cdot q, q \in G$.

Обратим внимание, что если S однозначно определяется по H условиями (6) (или (6')), то в качестве $\hat{S}$ можно выбрать любое из v возможных подмножеств. Но если фиксировать элемент $q \in G$, на котором четность n_q отлична от четности прочих $n_g, g \in G \setminus \{q\}$, то и $\hat{S}$ будет однозначно восстанавливаться по H .

По предложению 10 неразложимость циклической (v, k) -матрицы L , задаваемой подмножеством $H = \{r_1 = 0, r_2, \dots, r_k\}$, равносильна условию:

$$\text{Н.О.Д. } \{r_2, r_3, \dots, r_k, v\} = 1.$$

Благодаря простоте своего задания (v, k) -циркулянты являются удобным средством для предварительных построений (v, k) -матриц с различными свойствами и проверки гипотез.

Обратимся к примерам циклических (v, k) -групп и (v, k) -циркулянтов. Любая конечная группа с любым своим одноэлементным подмножеством является $(v, 1)$ -группой; аналогично, $\mathbb{Z}_v$ с любым своим элементом будет циклической $(v, 1)$ -группой.

Предложения 1, 3, 6, 7, 11–13 позволяют расширять круг примеров циклических (v, k) -матриц путем специального подбора параметров в их формулировках. Например: в предложении 6 матрицы L_1, L_0 сами должны быть циклическими, а $L_2 = I_{v_{12}}$; в предложениях 11, 12 исходные группы должны быть циклическими со взаимно простыми порядками.

Доказательство следствия 2 содержит пример неразложимой циклической (v, k) -матрицы при любых четном v и нечетном $k, 0 < k < v$.

Все циклические $(v, 3)$ -группы исчерпываются типами 1) и 3) из предложения 15, откуда следует, в частности, что при $k = 3$ либо v четно, либо $v = 5$.

В примере 3 содержится циклическая $(10, 5)$ -группа.

Приведем еще

ПРИМЕР 4. $(\mathbb{Z}_9, \{0, 1, 3, 4, 6\}, \{0, 1, 3, 4, 6\})$ – циклическая $(9, 5)$ -группа.

Далее приводятся несколько бесконечных серий циклических (v, k) -групп.

ПРИМЕР 5. Пусть v – четное, k – нечетное, $0 < k < v, w = v/2, l = \frac{1}{2}(k - 1), R' = \{r_1, \dots, r_l\}$, где $0 \leq r_1 < \dots < r_l \leq w - 1, r \in \mathbb{Z}_v \setminus (R' \cup (R' + w)), H = R' \cup (R' + w) \cup \{r\}$. Тогда $(\mathbb{Z}_v, H, -H + 2r)$ будет (v, k) -группой. Условия (6) проверяются с помощью предложения 16 с $\hat{S} = H - 2r$, но проще с помощью предложения 7 убедиться, что $(\mathbb{Z}_v, H - r, -H + r)$ является (v, k) -группой.

ПРИМЕР 6. Пусть $k \equiv 1 \pmod{4}$, $v = \lambda m$, $m = \frac{1}{2}(k+1)$, $\lambda \geq 2$. Тогда можно построить неразложимую циклическую (v, k) -группу $(\mathbb{Z}_v, H)$,

$$H = \left\{ 0, \frac{v}{m}, 2\frac{v}{m}, \dots, (m-1)\frac{v}{m}, r, \frac{v}{m} + r, 2\frac{v}{m} + r, \dots, (m-2)\frac{v}{m} + r \right\},$$

где $r \in \mathbb{Z}_v$ и r взаимно просто с λ . Условия (6) снова проверяются с привлечением предложения 16 при

$$\widehat{S} = \left\{ 0, -r, \frac{v}{m}, (m-1)\frac{v}{m} - r, 2\frac{v}{m}, (m-2)\frac{v}{m} - r, \dots, (m-2)\frac{v}{m}, 2\frac{v}{m} - r, (m-1)\frac{v}{m} \right\}.$$

Этот же пример получается из предложения 13 при $k_1 = k_2 = 1$, $v_{12} = \lambda$, $v' = m$, $k' = m - 1$.

ПРИМЕР 7. Пусть $k \equiv 1 \pmod{6}$, $m = \frac{1}{3}(2k+1)$, $(\mathbb{Z}_m, H', S')' - (m, \frac{1}{2}(m-1))'$ -группа, C – ненулевой класс смежности в $\mathbb{Z}_{\lambda m}/\mathbb{Z}_m \cong \mathbb{Z}_\lambda$. Тогда $(\mathbb{Z}_{\lambda m}, C \cup H', C \cup S')$ – неразложимая циклическая $(\lambda m, k)$ -группа при любом $\lambda \geq 2$. Условия (6) опять же проверяются с помощью предложения 16 при $\widehat{S} = (-C) \cup (-S')$. Из предложения 13 данный пример получается при $k_1 = k_2 = 1$, $v_{12} = \lambda$, $v' = m$, $k' = \frac{1}{2}(m-1)$.

ПРИМЕР 8. В обозначениях предыдущего примера при $k = 13$ имеем $m = 9$, а в примере 4 приведена циклическая $(9, 4)'$ -группа, поэтому при всех $\lambda \geq 2$ существуют неразложимые циклические $(9\lambda, 13)$ -группы.

Примерами $(v, k)'$ -групп при нечетном v или $(v, v-k)$ -групп, используемых в предложении 13, были циклические группы. Кроме приведенных выше, широкий круг примеров $(v, k)'$ -групп дают, естественно, совершенные разностные множества с параметрами (v, k, λ) при нечетном v и $k \not\equiv \lambda \pmod{2}$ (см. [2]).

Целую серию подобных примеров доставляют еще множество R всех (ненулевых) квадратичных вычетов и множество N всех квадратичных невычетов в кольце классов вычетов $\mathbb{Z}_p$ по простому модулю p .

ПРЕДЛОЖЕНИЕ 17. а) Если $p \equiv 3 \pmod{8}$ простое, то $(\mathbb{Z}_p, R, R)$ является $(p, \frac{1}{2}(p-1))'$ -группой, а $(\mathbb{Z}_p, N \cup \{0\}, N \cup \{0\})' - (p, \frac{1}{2}(p+1))'$ -группой.

б) Если $p \equiv 5 \pmod{8}$ простое, то $(\mathbb{Z}_p, R, N)$ является $(p, \frac{1}{2}(p-1))'$ -группой, а $(\mathbb{Z}_p, N \cup \{0\}, R \cup \{0\}) - (p, \frac{1}{2}(p+1))'$ -группой.

в) Матрицы инцидентности указанных в пп. а) и б) конфигураций неразложимы.

ДОКАЗАТЕЛЬСТВО. Утверждение а) следует из того, что множество R есть совершенное разностное множество с параметрами $(p, \frac{1}{2}(p-1), \frac{1}{4}(p-3))$ (см. [2]).

Докажем б). Для проверки условий (6') воспользуемся предложением 16. У нас $H = R$, $S = N$. Далее, $p \equiv 1 \pmod{4}$, поэтому $(-1) \in R$, $\widehat{S} = N^{-1} = -N = N$. Рассмотрим $R * N$. Нам достаточно проверить, что в $R * N$ ненулевые элементы имеют нечетную кратность. (Кратность нуля нулевая, так как (-1) – квадратичный вычет.) Кратности ненулевых элементов одинаковы. В самом деле, если $g = r_1 + n_1 = r_2 + n_2$ – два различных представления, то $\alpha g = \alpha r_1 + \alpha n_1 = \alpha r_2 + \alpha n_2$ – тоже два различных представления, в которых при $\alpha \in N$ слагаемые αr_i и αn_i

должны быть переставлены местами. Теперь, поскольку $|R| = |N| = \frac{1}{2}(p-1)$, получаем, что $n_g = \left(\frac{1}{2}(p-1)\right)^2 : (p-1) = \frac{1}{4}(p-1)$ нечетно для $g \neq 0$.

Утверждение о неразложимости соответствующих матриц инцидентности очевидно.

По приведенным выше примерам циклических (v, k) -групп с помощью предложений 11, 12, 14 и, главным образом, предложения 13 можно строить много других (v, k) -групп, в том числе и новые циклические (v, k) -группы.

Завершающим в настоящем параграфе является

ПРИМЕР 9. Если

а) $k \equiv 5 \pmod{12}$ и $p = \frac{1}{3}(2k-1)$ простое

или

б) $k \equiv 7 \pmod{12}$ и $p = \frac{1}{3}(2k+1)$ простое,

то для любого $\lambda \geq 2$ существует неразложимая циклическая $(\lambda p, k)$ -матрица.

Для доказательства нужно воспользоваться предложением 13 с $k_1 = k_2 = 1$, $v_{12} = \lambda$ и с (v', k') -группой из предложения 17. В случае б) вместо предложения 13 можно воспользоваться примером 7.

Множество простых p , удовлетворяющих условиям примера 9 как в случае а), так и в случае б), бесконечно по теореме Дирихле о числе простых чисел в арифметической прогрессии [3].

Примеры 6, 7, 9 были получены раньше предложения 13, которое возникло как их обобщение.

§ 4. Условия существования (v, k) -матриц

Наиболее принципиальным здесь является вопрос о существовании для данных v и k , $1 < k < v$, неразложимых (v, k) -матриц. Он полностью решен в случае четного v : согласно следствию 2 при любом четном v и любом нечетном k , $1 < k < v$, неразложимые (v, k) -матрицы существуют. Для нечетного v вопрос о существовании неразложимых (v, k) -матриц в общем виде остается открытым. В то же время, в примерах 6, 7, 9 приведен ряд бесконечных серий таких матриц и, в частности, показано, что неразложимые (v, k) -матрицы с данным нечетным $k > 1$ и бесконечным множеством нечетных значений v существуют для всех $k \equiv 1, 5, 9 \pmod{12}$, а также для бесконечного множества значений $k \equiv 7 \pmod{12}$. Ниже в предложении 19 это утверждение распространяется на все нечетные $k > 3$.

Рассмотрим вначале общую задачу о существовании (v, k) -матриц.

ПРЕДЛОЖЕНИЕ 18. Если v нечетно и существует (v, k) -матрица, то

$$v \geq k + \frac{1 + \sqrt{4k-3}}{2}.$$

ДОКАЗАТЕЛЬСТВО. Пусть $L - (k+c, k)$ -матрица, c четно. У матриц $L_1 = L + J$ и $L_2 = L^{-1} + J$ в строках и столбцах по c единиц, поэтому в столбце матрицы $L_1 \cdot L_2$ не более c^2 единиц. Далее, очевидно, $L_1 L_2 = I + J$, поэтому $c^2 \geq k + c - 1$, или

$$k + c \geq k + \frac{1 + \sqrt{4k-3}}{2}.$$

ПРЕДЛОЖЕНИЕ 19. а) Для каждого $k \equiv 1 \pmod{4}$ существуют $(\frac{3}{2}(k+1), k)$ -матрица и (v, k) -матрицы с $v \geq \frac{5}{2}(k+1)$.

б) Для каждого $k \equiv 3 \pmod{4}$, $k \neq 11$, существуют $(\frac{3}{2}(k+1) + 3, k)$ -матрица и (v, k) -матрицы с $v \geq \frac{5}{2}(k+1) + 3$.

в) Для $k = 11$ существуют $(33, 11)$ -матрица и $(v, 11)$ -матрицы с $v \geq 45$.

г) Для каждого нечетного $k > 3$ имеется бесконечное множество нечетных v , при которых существует неразложимая (v, k) -матрица.

ДОКАЗАТЕЛЬСТВО. а) Пусть $k \equiv 1 \pmod{4}$. Существование $(\frac{3}{2}(k+1), k)$ -матрицы следует из предложения 6 при $k_0 = k_1 = k_2 = 1$, $v_{12} = 3$, $v_0 = \frac{1}{2}(k+1)$. В случае $v \geq \frac{5}{2}(k+1)$ можно применить предложения 2 и 7.

б) $k \equiv 3 \pmod{4}$, $k \neq 11$. Существование $(\frac{3}{2}(k+1) + 3, k)$ -матрицы для $k > 3$ также следует из предложения 6, но при $k_1 = k_2 = 1$, $k_0 = v_{12} = 3$, $v_0 = \frac{1}{2}(k+3)$. При этом потребуются $(v_0, 3)$ -матрицы для нечетного $v_0 \geq 5$, $v_0 \neq 7$. Последние существуют согласно предложениям 2, 7, 15 п. 3). Эти же результаты обеспечивают построение $(v, 3)$ -матриц при $v \geq 9$.

в) Пусть $k = 11$. Снова воспользуемся предложением 6. Возьмем $v_0 = 3$, $v_{12} = 11$, $k_0 = k_2 = 1$, $k_1 = 3$. Пусть A — $(5, 3)$ -матрица, C — $(6, 3)$ -матрица из предложения 7 с нулями по главной диагонали ($D = I_3$). Полагаем

$$L_1 = \begin{pmatrix} A & 0 \\ 0 & C \end{pmatrix}, \quad L_2 = \begin{pmatrix} 0 & I_5 & 0 \\ I_5 & 0 & 0 \\ 0 & 0 & I_1 \end{pmatrix}. \quad (14)$$

Тогда $L_1 \wedge L_2 = L_1^{-1} \wedge L_2^{-1} = 0$. Применяя предложение 6, получаем $(33, 11)$ -матрицу. Существование $(v, 11)$ -матриц при $v \geq 45$ следует из предложений 2 и 7.

г) Будем использовать все то же предложение 6. Если $k \equiv 1 \pmod{4}$, то, полагая в нем $k_0 = k_1 = k_2 = 1$, $v_0 = \frac{1}{2}(k+1)$, v_{12} — любым, получаем требуемое. Матрицы L_1, L_2 можно взять циклическими, но так, чтобы единицы первой строки были на соседних местах.

Пусть $k \equiv 3 \pmod{4}$, $k = 4l + 3$, $l > 0$. В этом случае полагаем $k_1 = k_2 = 1$, $k_0 = 3$, $v_0 = \frac{1}{2}(k+3) = 2l + 3$. Если $l \neq 2$, то существует $(v_0, 3)$ -матрица (см. доказательство п. б)) и при аналогичных L_1, L_2 из предложения 6 получаем требуемое семейство (v, k) -матриц.

Пусть, наконец, $k = 11$ ($l = 2$). Тогда полагаем $k_1 = v_0 = 3$, $k_2 = k_0 = 1$, а в качестве L_1, L_2 берем матрицы вида (14), где C — матрица четного порядка $2w \geq 6$ из предложения 7, полученная при $D = I_w$ и циклической матрице B , единицы в которой располагаются рядом с главной диагональю. (Обратим внимание, что изолированная единица у матрицы L_2 в (14) здесь заменяется на I_{2w-5} — вектор из единиц, располагающийся вдоль главной диагонали.) Теперь остается применить предложение 6.

Минимальные значения v , для которых предложением 19 гарантируется наличие (v, k) -матриц, существенно выше нижней оценки из предложения 18. Для промежуточных значений v большое число примеров (v, k) -матриц предоставляется изложенными выше в § 2 и 3 конструкциями, а также известными (v, k, λ) -конфигурациями (см. [1], [2], [4]–[6]), в частности проективными плоскостями, матрицами Адамара, совершенными разностными множествами.

Грубая, на первый взгляд, оценка предложения 18 в некоторых случаях оказывается точной. Так, проективная плоскость порядка n отвечает $(n^2 + n + 1, n + 1, 1)$ -конфигурации, а дополнения к ее прямым составляют $(n^2 + n + 1, n^2, n + 1)$ -конфигурацию, которая при нечетном n предоставляет (v, k) -матрицу с $v = n^2 + n + 1$, $k = n^2$, когда, как нетрудно видеть, $v - 2 < k + (1 + \sqrt{4k - 3})/2$. Точность оценки из предложения 18 подтверждается также имеющимися примерами для $k = 1, 3, 5, 9$. Для $k = 7$, однако, $(11, 7)$ -матрица пока не построена, но $(13, 7)$ -матрица уже существует (см. предложение 17 п. б)).

Особо прокомментируем п. г) предложения 19, утверждающий, что при любом нечетном $k > 3$ существует бесконечное множество нечетных v , для которых имеются неразложимые (v, k) -матрицы (при четных $v > k$, как утверждается в следствии 2, таковые имеются всегда). При $k = 1$ все $(v, 1)$ -матрицы разложимы. При $k = 3$ неразложимая циклическая $(v, 3)$ -матрица с нечетным v построена только для $v = 5$, а при нечетном $v > 5$ нет даже неразложимых $(v, 3)$ -групп (предложение 15). Нам неизвестны примеры неразложимых $(v, 3)$ -матриц с нечетным v , отличным от 5. Для $v = 7$, как утверждается ниже в предложении 20, $(7, 3)$ -матриц нет. Нетрудно убедиться еще, что $(v, 3)$ -матрица L , удовлетворяющая условию $L^{-1} = L^T$, является прямой суммой $(4, 3)$ -матриц, т.е. в этом классе $(v, 3)$ -матриц неразложимыми могут быть только матрицы с $v = 4$.

ПРЕДЛОЖЕНИЕ 20. *Значение $v = 7$ является единственным среди $v > 3$, для которого не существует $(v, 3)$ -матрицы.*

ДОКАЗАТЕЛЬСТВО. Как мы уже отмечали при доказательстве предложения 19, $(v, 3)$ -матрицы при $v > 3$, $v \neq 7$, существуют. Докажем от противного, что не существует $(7, 3)$ -матриц. В ходе доказательства строки $(7, 3)$ -матрицы, т.е. $(0, 1)$ -векторы $\alpha = (\alpha_1, \dots, \alpha_7)$, отождествляются с множествами $X(\alpha) = \{i = \overline{1, 7} : \alpha_i = 1\}$. Будут рассматриваться только векторы с тремя ненулевыми координатами (векторы веса 3).

Пусть L — $(7, 3)$ -матрица. Строки матрицы L и строки матрицы $(L^{-1})^T$ ортогональны (т.е. имеют “четное пересечение”) тогда и только тогда, когда они имеют разные номера. В частности, для любых двух различных строк в L существует пять ортогональных им обоим строк в $(L^{-1})^T$. Покажем, что любые две различные строки α и β в L имеют одну общую единицу или, иначе,

$$|X(\alpha) \cap X(\beta)| = 1.$$

Для пары векторов X_i, X_j веса 3 с пустым пересечением существует ровно шесть ортогональных им обоим векторов веса 3, причем у всех координата с номером из $\overline{1, 7} \setminus (X_i \cup X_j)$ равна 1. Следовательно, если бы в L были две строки без общих единиц, то в одном из столбцов $(L^{-1})^T$ было бы не меньше пяти единиц вместо требуемых трех. Поэтому любые две строки α и β в L имеют хотя бы одну общую единицу:

$$|X(\alpha) \cap X(\beta)| \geq 1.$$

Пусть $|X_i \cap X_j| = 2$. Не ограничивая общности, считаем $i = 1, j = 2$ и

$$\begin{aligned} X_1 &= (1 \ 1 \ 1 \ 0 \ 0 \ 0 \ 0), \\ X_2 &= (1 \ 1 \ 0 \ 1 \ 0 \ 0 \ 0). \end{aligned}$$

Паре X_1, X_2 ортогональны снова только шесть векторов веса 3:

$$\begin{aligned} Y_3 &= (0 \ 0 \ 0 \ 0 \ 1 \ 1 \ 1), \\ Y_4 &= (0 \ 1 \ 1 \ 1 \ 0 \ 0 \ 0), \\ Y_5 &= (1 \ 0 \ 1 \ 1 \ 0 \ 0 \ 0), \\ Y_6 &= (1 \ 1 \ 0 \ 0 \ 1 \ 0 \ 0), \\ Y_7 &= (1 \ 1 \ 0 \ 0 \ 0 \ 1 \ 0), \\ Y_8 &= (1 \ 1 \ 0 \ 0 \ 0 \ 0 \ 1) \end{aligned}$$

— шесть претендентов на пять последних строк в матрице $(L^{-1})^\tau$. Замечаем, что Y_3 не имеет общих единиц с Y_4 и Y_5 , поэтому он не может быть строкой $(L^{-1})^\tau$ (ввиду симметрии между L и L^{-1}). Но остальные дают 4 единицы в столбце. Таким образом, $|X_i \cap X_j| = 2$ тоже исключено.

Значит, $|X_i \cap X_j| = 1, 1 \leq i \neq j \leq 7$. Все такие матрицы L (с тремя единицами в строках и столбцах) перестановками строк и столбцов приводятся к виду

$$\begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{pmatrix},$$

в чем легко убедиться построчным достраиванием. Однако эта матрица вырождена, т.е. не является $(7, 3)$ -матрицей.

ПРЕДЛОЖЕНИЕ 21. Для $k = 5, 7, 9$ и всех нечетных v таких, что

$$v \geq k + \frac{1 + \sqrt{4k - 3}}{2},$$

существуют (v, k) -матрицы, за возможным исключением $k = 7, v = 11$.

При доказательстве этого предложения будут использованы следующие циклические (v, k) -группы, полученные А. Е. Трипиным с помощью вычислений на ЭВМ:

$$\begin{aligned} (\mathbb{Z}_{13}, \{0, 1, 2, 3, 4\}, \{2, 5, 7, 10, 12\}) & \quad - (13, 5)\text{-группа;} \\ (\mathbb{Z}_{17}, \{0, 2, 3, 4, 5, 6, 7\}, \{2, 3, 5, 6, 7, 13, 15\}) & \quad - (17, 7)\text{-группа;} \\ (\mathbb{Z}_{19}, \{0, 2, 3, 4, 5, 6, 7\}, \{6, 8, 12, 13, 15, 16, 18\}) & \quad - (19, 7)\text{-группа;} \\ (\mathbb{Z}_{17}, \{0, 1, 2, 4, 5, 6, 7, 8, 9\}, \{0, 1, 3, 4, 5, 8, 11, 12, 13\}) & \quad - (17, 9)\text{-группа;} \\ (\mathbb{Z}_{21}, \{0, 2, 3, 4, 5, 6, 7, 8, 9\}, \{4, 6, 9, 10, 12, 13, 15, 16, 17\}) & \quad - (21, 9)\text{-группа.} \end{aligned}$$

Им же проверено, что нет циклических $(11, 7)$ -матриц и нет неразложимых $(9, 3)$ -и $(11, 3)$ -матриц.

ДОКАЗАТЕЛЬСТВО ПРЕДЛОЖЕНИЯ 21. В силу предложений 3 и 7 для $k = 5$ достаточно предъявить $(9, 5)$ -, $(11, 5)$ - и $(13, 5)$ -матрицы. Последняя содержится в списке перед доказательством, $(9, 5)$ -матрицу получаем по предложению 6 с $k_0 = k_1 = k_2 = 1$, $v_{12} = v_0 = 3$, а $(11, 5)$ -матрица получается из предложения 17 п. а).

Для $k = 7$ достаточно предъявить $(13, 7)$ -, $(15, 7)$ -, $(17, 7)$ - и $(19, 7)$ -матрицы. Две последних содержатся в списке перед доказательством; $(13, 7)$ -матрица строится по способу предложения 17 п. б); $(15, 7)$ -матрица получается по предложению 6 с $k_1 = k_2 = 1$, $v_{12} = k_0 = 3$, $v_0 = 5$.

Для $k = 9$ достаточно предъявить $(13, 9)$ -, $(15, 9)$ -, $(17, 9)$ -, $(19, 9)$ - и $(21, 9)$ -матрицы. $(17, 9)$ - и $(21, 9)$ -матрицы содержатся в списке перед доказательством. Далее, прямые проективной плоскости порядка 3 образуют $(13, 4, 1)$ -конфигурацию, а дополнения к прямым – $(13, 9, 4)$ -конфигурацию и, тем самым, $(13, 9)$ -конфигурацию; $(15, 9)$ -матрица получается по предложению 6 при $k_0 = k_1 = k_2 = 1$, $v_0 = 5$, $v_{12} = 3$. Наконец, $(19, 9)$ -матрица получается по предложению 17 п. а).

К сожалению, в предложении 21 остается вопрос о существовании $(11, 7)$ -матрицы, который, надо полагать, со временем будет разрешен. Было бы интересно получить аналогичное предложение (пусть снова только при $k = 3, 5, 7, 9$) и о существовании при заданных v и k , $1 < k < v$, неразложимых (v, k) -матриц. Пока же для этих значений k можно только повторить результаты примеров 6, 9 и предложений 15, 17: неразложимые (v, k) -матрицы существуют

для $v = 5$	при $k = 3$,
для $v = 11$ и $v = 3\lambda$	при $k = 5$,
для $v = 13$ и $v = 5\lambda$	при $k = 7$,
для $v = 13, 19, 37$ и $v = 5\lambda$	при $k = 9$.

Здесь $\lambda \geq 2$ – произвольное; $(13, 9)$ - и $(37, 9)$ -матрицы являются соответственно матрицами инцидентности $(13, 9, 4)$ - и $(37, 9, 2)$ -конфигураций (см. [2]), поэтому неразложимы.

§ 5. Сводка основных примеров (v, k) -конфигураций и способов их построения

В помещенной ниже таблице 1 во второй колонке собраны значения пар (v, k) , для которых построены (v, k) -конфигурации. В следующей колонке указаны примеры (v, k) -матриц или дается отсылка к тексту статьи (при необходимости там указываются ограничения на значения v и k при их параметрическом задании).

При отборе примеров преследовалась цель продемонстрировать в достаточном объеме набор основных средств и способов построения (v, k) -конфигураций, известных на настоящий момент. Случаи четных и нечетных v при этом оказались принципиально различными. При четном v предложение 7 и следствие 2 позволяют строить в больших количествах неразложимые (v, k) -матрицы при любых нечетных k , $1 < k < v$. При нечетном v , как показывают предложения 18–21 и комментарии к ним, ситуация совершенно иная.

Наиболее действенной для построения (v, k) -матриц оказалась конструкция предложения 6, которая по известным (v_{12}, k_i) -матрицам L_i , $i = \overline{1, 2}$, и

(v_0, k_0) -матрице L_0 с нечетным v_0 предоставляет $(v_{12}v_0, k_1v_0 + k_2(v_0 - k_0))$ -матрицу

$$L = L_1 \otimes J_{v_0} + L_2 \otimes (J_{v_0} + L_0).$$

Рис. 1

В таблице 1 представлены также примеры (v, k) -конфигураций, построенные на основе регулярных и симметрических графов [7]. Если в последней колонке указывается название графа Γ , то подразумевается, что X совпадает с множеством его вершин, а сразу после названия графа следует инвариантное описание подмножеств семейства $\{X_i : i \in X\}$, при этом через $\Gamma(i)$ обозначаем совокупность вершин, смежных с i . Говорим еще, что вершина i отстоит от j на l ребер, если имеется путь длины l , соединяющий i и j , но нет более короткого пути, соединяющего их.

Упоминание в таблице (v, k, λ) -конфигурации подразумевает ссылку на монографию [2], названия графов см. в монографии [7]. Обозначение $[v, k]$ в таблице подразумевает произвольную (v, k) -матрицу. Черта сверху указывает на инвертирование всех элементов матрицы. Через $\dagger$ и $\times$ обозначены операции получения (v, k) -матриц, указанные в предложениях 3 и 4 соответственно.

В таблице конкретной паре (v, k) под одним номером может отвечать несколько описаний (v, k) -конфигураций. Кроме того, одна и та же пара (v, k) может оказаться под разными номерами в таблице. В связи с этим встает не рассматриваемый в работе, но очень важный вопрос об эквивалентности соответствующих (v, k) -матриц: получают ли они одна из другой независимыми перестановками строк и столбцов. На языке (v, k) -конфигураций эквивалентность означает совпадение соответствующих семейств k -подмножеств после перестановки элементов основного v -множества X .

ТАБЛИЦА 1

№	(v, k)	Решения и комментарии (всюду k нечетно, $0 < k < v$)
1	$(v, 1)$	Подстановочные матрицы
2	$(5, 3)$	Предложение 15 или предложение 17 п. б)
3	$(7, 3)$	Не существует; предложение 20
4	$(2l + 1, 3)$	Неизвестно ни одного $l \geq 4$ с неразложимой $(2l + 1, 3)$ -конфигурацией (см. предложение 19 п. г) для $k > 3$)
5	$(8, 5)$	$\overline{[4, 3]} \dot{+} [4, 3]$
6	$(9, 5)$	а) Пример 4; б) предложение 6; в) предложение 13
7	$(10, 5)$	а) Пример 3; б) предложение 7
8	$(12, 5)$	а) Γ – икосаэдр, $X_i = \Gamma(i)$; б) п. 3.4 – некоммутативная $(12, 5)$ -группа; в) предложение 8; г) предложение 14
9	$(16, 5)$	$[4, 3] \times [4, 3]$ (предложение 4)
10	$(11, 7)$	Существование неизвестно (предложение 21)
11	$(12, 7)$	а) $\overline{[6, 5]} \dot{+} [6, 5]$; б) $\overline{[12, 5]}$
12	$(15, 7)$	Предложение 6
13	$(16, 7)$	$\overline{[4, 3]} \otimes [4, 3]$
14	$(24, 7)$	$[4, 3] \times [6, 5]$ (предложение 4)
15	$(12, 9)$	$\overline{[4, 3]} \dot{+} [4, 3] \dot{+} [4, 3]$
16	$(13, 9)$	$(13, 9, 4)$ -конфигурация (дополнения к прямым проективной плоскости порядка 3)
17	$(14, 9)$	$\overline{[6, 5]} \dot{+} [8, 5]$
18	$(15, 9)$	а) Предложение 6; б) предложение 13
19	$(16, 9)$	а) $[4, 3] \otimes [4, 3]$; б) $\overline{[8, 7]} \dot{+} [8, 7]$
20	$(20, 9)$	а) Γ – додекаэдр, X_i – множество вершин, отстоящих от i на одно или на два ребра; б) $(5, 3) \otimes (4, 3)$; в) $\overline{[20, 11]}$
21	$(24, 9)$	а) $\overline{[4, 3]} \otimes [6, 5]$; б) $[4, 3] \otimes [6, 3]$
22	$(30, 9)$	а) Γ – граф Леви (рис. 1), $X_i \ni i$ кроме самой i содержит вершины, отстоящие от нее на четыре ребра; б) $[5, 3] \otimes [6, 3]$; в) предложение 6; г) предложение 13
23	$(36, 9)$	а) $[6, 5] \times [6, 5]$ (предложение 4); б) $[6, 3] \otimes [6, 3]$
24	$(37, 9)$	$(37, 9, 2)$ -конфигурация
25	$(v, 11)$	$v = 33$ и $v \geq 45$ (предложение 19)

ТАБЛИЦА 1 (ПРОДОЛЖЕНИЕ)

26	$(9\lambda, 13)$	а) Пример 8; б) предложение 6; в) предложение 13
27	$(2w, k)$	Предложение 7, примеры 1, 2
28	$(2w + 1, k)$	$2w + 1 < k + \frac{1 + \sqrt{4k-3}}{2}$, не существует (предложение 18)
29	$(2^k, k)$	$\Gamma - k$ -мерный куб, $X_i = \Gamma(i)$ (разбивается на две $(2^{k-1}, k)$ -конфигурации)
30	$(2^{k-1}, k)$	$\Gamma - (k - 1)$ -мерный куб, $X_i = \Gamma(i) \cup \{i\}$
31	$(2^r w_1 \cdots w_r, 2r + 1)$	$w_i > 1, i = \overline{1, r}$, следствие предложения 15
32	$(2w, 2w - 1)$	$\overline{[2w, 1]}$
33	$(\lambda \frac{k+1}{2}, k)$	$k \equiv 1 \pmod{4}$; а) пример 6; б) предложение 6; в) предложение 13
34	$(p, \frac{p-1}{2})$	$p \equiv 3 \pmod{8}$ простое; предложение 17 п. а) или $(p, \frac{p-1}{2}, \frac{p-3}{4})$ -конфигурация
35	$(p, \frac{p+1}{2})$	$p \equiv 5 \pmod{8}$ простое; предложение 17 п. б)
36	$(\lambda p, \frac{3p+1}{2})$	$p \equiv 3 \pmod{8}$ простое; а) пример 9 а); б) предложение 6; в) предложение 13
37	$(\lambda p, \frac{3p-1}{2})$	$p \equiv 5 \pmod{8}$ простое; а) пример 9 б); б) предложение 6; в) предложение 13
38	$(v, 4l + 1)$	$v = 3(2l + 1)$ и $v \geq 5(2l + 1)$; предложение 19
39	$(v, 4l + 3)$	$l \neq 2, v = 3(2l + 3)$ и $v \geq 10l + 13$; предложение 19

Список литературы

1. Сачков В. Н. Комбинаторные методы дискретной математики. М.: Наука, 1977.
2. Холл М. Комбинаторика. М.: Мир, 1970.
3. Карацуба А. А. Основы аналитической теории чисел. М.: Наука, 1975.
4. Камерон П., ван Линт Дж. Теория графов, теория кодирования и блок-схемы. М.: Наука, 1980.
5. Картеси Ф. Введение в конечные геометрии. М.: Наука, 1980.
6. Тараканов В. Е. Комбинаторные задачи и $(0, 1)$ -матрицы. М.: Наука, 1985.
7. Харари Ф. Теория графов. М.: Мир, 1973.

Академия криптографии РФ, Москва;
Математический институт им. В. А. Стеклова РАН

Поступила в редакцию
18.12.2000