Math-Net.Ru

Общероссийский математический портал

Ф. М. Малышев, Четыре бесконечные серии k -конфигураций, *Матем. вопр. криптогр.*, 2013, том 4, выпуск 4, 65–75

DOI: <https://doi.org/10.4213/mvk100>

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: 54.224.187.69

26 апреля 2023 г., 04:27:01

УДК 519.142.1

Четыре бесконечные серии k -конфигураций

Ф. М. Малышев

Математический институт им. В. А. Стеклова РАН, Москва

Получено 22.IV.2013

Предлагаются способы построения k -конфигураций на счетном (в том числе на конечном) множестве X . В случае конечного X это семейство подмножеств в X с такой матрицей инцидентности $L \in GL(|X|, 2)$, что L и L^{-1} имеют ровно по k единиц в строках и столбцах.

Ключевые слова: конфигурации, булевы матрицы, гиперграфы, орграфы

Four infinite series of k -configurations

F. M. Malyshev

Steklov Mathematical Institute of RAS, Moscow

Abstract. We suggest an approach to the construction of k -configurations on the countable (or finite) set X . If X is finite then k -configuration is a family of subsets in X with the incidence matrix $L \in GL(|X|, 2)$ such that L and L^{-1} have exactly k ones in all rows and columns.

Key words: configuration, Boolean matrices, hypergraphs, digraphs

Citation: *Mathematical Aspects of Cryptography*, 2013, vol. 4, no. 4, pp. 65–75 (Russian).

© 2013 Малышев Ф. М.

§ 1. Введение

Первоначально понятие (v, k) -конфигурации возникло в связи с потребностями криптографического синтеза, для построения специальных рассеивающих матриц в XSL -схемах. С общих комбинаторных позиций это понятие, точнее, понятие $(k'_1, k''_1, k'_2, k''_2)$ -конфигурации, введено в предыдущей работе автора [1].

В случае $k'_1 = k''_1 = k'_2 = k''_2 = k$ и не обязательно конечного X имеем дело с k -конфигурациями на счетном (в том числе и на конечном) множестве X мощности $v > k$. Это семейство подмножеств в X мощности $k \in \mathbb{N}$ каждое, причем любой элемент $x \in X$ содержится ровно в k подмножествах из данного семейства. В результате имеем гиперграф на множестве вершин X .

Формулировка дополнительных требований на подмножества из семейства использует операцию сложения подмножеств X . Для $U, V \subseteq X$ полагаем $U + V = (U \cup V) \setminus (U \cap V)$. Множество всех подмножеств X с таким сложением образует абелеву группу, все ненулевые элементы которой имеют порядок 2. Тем самым, ее можно рассматривать и как векторное пространство над полем $GF(2)$. Пустое подмножество является нулем этого пространства. Одноэлементное подмножество $\{x\} \subset X$ будем обозначать просто x (без скобок). Вектор $U \subseteq X$ удобно отождествлять с функцией f , определенной на всем множестве X и принимающей значения в поле $GF(2)$: $f(x) = 1$, если $x \in U$, и $f(x) = 0$, если $x \in X \setminus U$.

Определение 1. Семейство различных непустых подмножеств X_α , $\alpha \in \Lambda$, в счетном множестве X называется k -конфигурацией, если имеется семейство различных непустых подмножеств $\Lambda_x \subset \Lambda$, $x \in X$, при которых выполняются следующие пять условий:

- i) $|X_\alpha| = k$ для всех $\alpha \in \Lambda$;
- ii) $|\{\alpha \in \Lambda : x \in X_\alpha\}| = k$ для всех $x \in X$;
- iii) $|\Lambda_x| = k$ для всех $x \in X$;
- iv) $|\{x \in X : \alpha \in \Lambda_x\}| = k$ для всех $\alpha \in \Lambda$;
- v) $x = \sum_{\alpha \in \Lambda_x} X_\alpha$.

Из условий i) и ii) для числа единиц в матрице инцидентий семейства $\{X_\alpha, \alpha \in \Lambda\}$ имеем $|\Lambda| \cdot k = |X| \cdot k$, поэтому $|\Lambda| = |X|$.

Для множеств из условий ii) и iv) далее используем обозначения $\Omega_x = \{\alpha \in \Lambda : x \in X_\alpha\}$, $x \in X$, и $O_\alpha = \{x \in X : \alpha \in \Lambda_x\}$, $\alpha \in \Lambda$. Как видим, $\alpha \in \Omega_x \Leftrightarrow x \in X_\alpha$ и $x \in O_\alpha \Leftrightarrow \alpha \in \Lambda_x$.

При необходимости указывать мощность $v = |X|$ в k -конфигурации используется также исторически первоначальное обозначение: (v, k) -конфигурация.

Иными словами, (v, k) -конфигурации в случае конечного v соответствуют гиперграф с v вершинами, матрица инцидентности L которого не вырождена над полем $GF(2)$, причем в матрицах L и L^{-1} в строках и столбцах ровно по k единиц. Определение 1 не предусматривает упорядоченность множеств X и Λ , поэтому матрица инцидентности L для (v, k) -конфигурации определена неоднозначно.

Эквивалентным (v, k) -конфигурациям является понятие (v, k) -матриц, рассматриваемых с точностью до независимых перестановок строк и столбцов. Матрица $L \in GL(v, 2)$ является (v, k) -матрицей, если у матриц L и L^{-1} в каждой строке и в каждом столбце ровно по k единиц. Здесь k обязательно нечетно, так как иначе матрица L вырождена.

Объединение k -конфигураций на непересекающихся множествах X_i , $i \in I$, будет k -конфигурацией на множестве $X = \bigcup_{i \in I} X_i$. Такие k -конфигурации называем разложимыми. Иначе, когда такого разбиения не существует, k -конфигурацию называем неразложимой.

В случае конечных $|I|$ и $v_i = |X_i|$, $i \in I$, матрица инцидентности разложимой (v, k) -конфигурации на множестве $X = \bigcup_{i \in I} X_i$ мощности $v = v_1 + \dots + v_{|I|}$ будет разложимой (v, k) -матрицей.

Ясно, что (v, k) -конфигурация $\{X_\alpha, \alpha \in \Lambda\}$ на множестве X с матрицей инцидентности L порождает также (v, k) -конфигурации $\{\Lambda_x, x \in X\}$, $\{\Omega_x, x \in X\}$ на множестве Λ и $\{O_\alpha, \alpha \in \Lambda\}$ на множестве X с матрицами инцидентности, соответственно, L^{-1} , L^t и $L^* = (L^{-1})^t = (L^t)^{-1}$.

Представление о состоянии дел в данном направлении комбинаторики, относящемся к построению конкретных семейств (v, k) -конфигураций, можно составить по работам [1]–[11] из списка литературы. Кроме фигурирующих там авторов, в этом направлении работали также А. М. Зубков, Е. Г. Красулина, В. Н. Сачков.

В работе [1] выявлен локальный характер условий, налагаемых на семейство подмножеств (v, k) -конфигурации, в результате было пересмотрено само определение понятия (v, k) -конфигурации. Главное значение теперь отводится параметру k . Параметр v не так существен для комбинаторной

природы требований, закладываемых в соответствующие определения. Это позволило понятие (v, k) -конфигурации распространить и на бесконечные счетные множества X .

Основным содержанием работы [1] является описание трех семейств 5-конфигураций, обозначенных буквами $\mathcal{A}$, $\mathcal{B}$ и $\mathcal{C}$. В настоящей работе доказаны четыре теоремы, предоставляющие, в частности, способы построения семейств k -конфигураций подобных типов для произвольного нечетного k .

Большинство известных примеров (v, k) -конфигураций с $v < \infty$ получаются факторизацией (∞, k) -конфигураций по их регулярным группам автоморфизмов. Напомним необходимые определения из работы [1].

Определение 2. Биекция $\varphi: X \rightarrow X$ является регулярным автоморфизмом k -конфигурации $\{X_\alpha, \alpha \in \Lambda\}$, если для некоторой биекции $\psi: \Lambda \rightarrow \Lambda$ выполняются условия:

- i) $\varphi(X_\alpha) = X_{\psi(\alpha)}$ для всех $\alpha \in \Lambda$;
- ii) $\psi(\Lambda_x) = \Lambda_{\varphi(x)}$ для всех $x \in X$;
- iii) $\left(\bigcup_{\alpha: x \in X_\alpha} X_\alpha\right) \cap \varphi\left(\bigcup_{\alpha: x \in X_\alpha} X_\alpha\right) = \emptyset$ для всех $x \in X$;
- iv) $\left(\bigcup_{x: \alpha \in \Lambda_x} \Lambda_x\right) \cap \psi\left(\bigcup_{x: \alpha \in \Lambda_x} \Lambda_x\right) = \emptyset$ для всех $\alpha \in \Lambda$.

Биекция ψ в этом определении условием i) задается однозначно.

Пусть G — некоторая группа подстановок на множестве X , все неединичные элементы которой являются регулярными автоморфизмами k -конфигурации $\{X_\alpha, \alpha \in \Lambda\}$. Через H обозначим соответствующую группу подстановок на Λ , порожденную биекциями $\psi: \Lambda \rightarrow \Lambda$, отвечающими биекциям $\varphi: X \rightarrow X$. По условиям v) определения 1 и i) определения 2 гомоморфное соответствие $\theta: \varphi \mapsto \psi$ инъективно, поэтому $H \cong G$. Обозначим через $\tilde{X}$ множество орбит группы G , а через $\tilde{\Lambda}$ — множество орбит группы H . Для $\tilde{\alpha} \in \tilde{\Lambda}$ через $\tilde{X}_{\tilde{\alpha}} \subset \tilde{X}$ обозначим подмножество орбит в $\tilde{X}$, содержащих точки X_β для некоторого $\beta \in \tilde{\alpha}$. Аналогично определяется семейство подмножеств $\{\tilde{\Lambda}_{\tilde{x}}, \tilde{x} \in \tilde{X}\}$ на множестве $\tilde{\Lambda}$. В работе [1] доказано, что семейство $\{\tilde{X}_{\tilde{\alpha}}, \tilde{\alpha} \in \tilde{\Lambda}\}$ тоже является k -конфигурацией. Таким образом, каждая (∞, k) -конфигурация с богатым множеством регулярных автоморфизмов порождает целую серию k -конфигураций.

§ 2. k -конфигурации типа $\mathcal{A}$

Пусть имеются два множества V и Y . Множество Y конечно четной мощности w . Пусть далее каждому $u \in V$ соответствует (w, κ) -конфигурация $\{Y_\alpha^{(u)}, \alpha \in Y\}$ на множестве Y . (Множество Y и значение κ общие для всех $u \in V$.) Пусть, наконец, на множестве вершин V (возможно бесконечном) задан ориентированный граф Γ без петель и без параллельных дуг, в котором в каждую вершину $u \in V$ входит ровно l дуг $(u_1^+, u), \dots, (u_l^+, u)$ и из каждой вершины $u \in V$ выходит ровно l дуг $(u, u_1^-), \dots, (u, u_l^-)$, $l \geq 1$. Положим

$$X = V \times Y, \quad \Lambda = V \times Y, \quad X_{(u, \alpha)} = (\{u\} \times Y_\alpha^{(u)}) \cup \bigcup_{i=1}^l (\{u_i^+\} \times Y), \quad (u, \alpha) \in V \times Y.$$

Теорема 1. Семейство подмножеств $X_{(u, \alpha)}$, $(u, \alpha) \in \Lambda$, является k -конфигурацией на множестве $X = V \times Y$ с параметром $k = lw + \kappa$.

При $w = 2$, $l = \kappa = 1$ в теореме 1 представлены в частности все неразложимые $(v, 3)$ -конфигурации для конечного четного v (см. [10]). Единственной неразложимой $(v, 3)$ -конфигурацией при нечетном v является $(5, 3)$ -конфигурация в виде дополнений к пяти парам элементов из множества мощности 5, образующим полный цикл.

Доказательство теоремы 1. Пусть $\{Y_y^{(u)}, y \in Y\}$, $u \in V$, — семейство подмножеств в Y , отвечающее семейству $\{Y_\alpha^{(u)}, \alpha \in Y\}$. Эти семейства удовлетворяют условиям i)–v) определения 1 для (w, κ) -конфигурации на множестве Y , отвечающей вершине $u \in V$. Положим $\Lambda_{(u, y)} = (\{u\} \times Y_y^{(u)}) \cup \bigcup_{i=1}^l (\{u_i^+\} \times Y)$, $(u, y) \in V \times Y$. Для доказательства теоремы необходимо убедиться в справедливости условий i)–v) определения 1 k -конфигурации, $k = lw + \kappa$, для семейств $\{X_{(u, \alpha)}, (u, \alpha) \in V \times Y\}$ и $\{\Lambda_{(u, y)}, (u, y) \in V \times Y\}$. Прежде всего, непосредственно из определений имеем $|X_{(u, \alpha)}| = lw + \kappa$ для всех $(u, \alpha) \in V \times Y$ и $|\Lambda_{(u, y)}| = lw + \kappa$ для всех $(u, y) \in V \times Y$, так что условия i) и iii) выполняются. Далее,

$$\Omega_{(u, y)} = \{(x, \alpha) \in V \times Y : (u, y) \in X_{(x, \alpha)}\} = (\{u\} \times \Omega_y^{(u)}) \cup \bigcup_{i=1}^l (\{u_i^-\} \times Y), \\ (u, y) \in V \times Y,$$

поэтому $|\Omega_{(u, y)}| = lw + \kappa$. Аналогично,

$$O_{(u, \alpha)} = \{(x, y) \in V \times Y : (u, \alpha) \in \Lambda_{(x, y)}\} = (\{u\} \times O_\alpha^{(u)}) \cup \bigcup_{i=1}^l (\{u_i^-\} \times Y), \\ (u, \alpha) \in V \times Y, \text{ и } |O_{(u, \alpha)}| = lw + \kappa,$$

значит условия ii) и iv) тоже выполняются. Наконец, если $u_{i1}^{++}, \dots, u_{il}^{++}$ — начала дуг с концами в u_i^+ , то

$$\begin{aligned} \sum_{(x, \alpha) \in \Lambda_{(u, y)}} X_{(x, \alpha)} &= \sum_{(x, \alpha) \in \{u\} \times \Upsilon_y^{(u)}} X_{(x, \alpha)} + \sum_{i=1}^l \sum_{(x, \alpha) \in \{u_i^+\} \times \Upsilon} X_{(x, \alpha)} = \\ &= \sum_{\alpha \in \Upsilon_y^{(u)}} X_{(u, \alpha)} + \sum_{i=1}^l \sum_{\alpha \in \Upsilon} X_{(u_i^+, \alpha)} = \sum_{\alpha \in \Upsilon_y^{(u)}} \left[(\{u\} \times Y_\alpha^{(u)}) + \sum_{i=1}^l (\{u_i^+\} \times Y) \right] + \\ &\quad + \sum_{i=1}^l \sum_{\alpha \in \Upsilon} \left[(\{u_i^+\} \times Y_\alpha^{u_i^+}) + \sum_{j=1}^l (\{u_{ij}^{++}\} \times Y) \right] = \\ &= (u, y) + \sum_{i=1}^l (\{u_i^+\} \times Y) + \sum_{i=1}^l (\{u_i^+\} \times Y) + \sum_{i=1}^l \sum_{\alpha \in \Upsilon} \sum_{j=1}^l (\{u_{ij}^{++}\} \times Y) = (u, y). \end{aligned}$$

Здесь использовались нечетность $\kappa = |Y_\alpha^{(u)}| = |\Upsilon_y^{(u)}| = |\Omega_y^{(u)}|$, $u \in V$, и четность $w = |\Upsilon|$. Поэтому условие v) также выполняется. Теорема 1 доказана.

Замечание 1. В теореме 1 (w, κ) -конфигурации на множестве Y , вообще говоря, различные для разных $u \in V$, поэтому далеко не всякий автоморфизм графа Γ без неподвижных точек будет продолжаться до регулярного автоморфизма конструируемой $(lw + \kappa)$ -конфигурации на множестве X . Если же независимо от конкретного $u \in V$ на множестве Y рассматривается одна и та же (w, κ) -конфигурация, то возникает больше возможностей для построения регулярных автоморфизмов соответствующих $(lw + \kappa)$ -конфигураций, позволяющих строить $(v, lw + \kappa)$ -конфигурации при конечном v .

§ 3. k -конфигурации типа $\mathcal{B}$

Обозначим $e_i \in \mathbb{R}^n$ — вектор с единственной ненулевой координатой с номером i , равной 1, а f_i — аналогичный вектор в $GF(2)^n$, $i = 1, \dots, n$.

Теорема 2. Пусть $X = \Lambda = \mathbb{Z}^n \times GF(2)^n$. Тогда семейство подмножеств

$$X_{(z, \beta)} = \{(z, \beta)\} \cup \bigcup_{i=1}^n \{(z + e_i, \beta), (z + e_i, \beta + f_i)\}, \quad (z, \beta) \in \Lambda,$$

будет k -конфигурацией на множестве X с параметром $k = 2n + 1$.

Доказательство. Положим $\Lambda_{(z, \beta)} = X_{(z, \beta)}$, $(z, \beta) \in X$. Выполнение условий i)–iv) определения 1 следует непосредственно из задания подмножеств $X_{(z, \beta)}$ и из равенств

$$\Omega_{(z, \beta)} = O_{(z, \beta)} = \{(z, \beta)\} \cup \bigcup_{i=1}^n \{(z - e_i, \beta), (z - e_i, \beta + f_i)\}.$$

Проверим выполнение условия ν), в котором, напомним, суммируются подмножества X , как это было определено во введении.

$$\begin{aligned}
\sum_{(u,\alpha) \in \Lambda_{(z,\beta)}} X_{(u,\alpha)} &= X_{(z,\beta)} + \sum_{i=1}^n \sum_{(u,\alpha) \in \{(z+e_i,\beta), (z+e_i,\beta+f_i)\}} X_{(u,\alpha)} = \\
&= X_{(z,\beta)} + \sum_{i=1}^n [X_{(z+e_i,\beta)} + X_{(z+e_i,\beta+f_i)}] = \\
&= X_{(z,\beta)} + \sum_{i=1}^n (z+e_i, \beta) + \sum_{i=1}^n (z+e_i, \beta+f_i) = \\
&+ \sum_{i=1}^n \left[(z+e_i, \beta) + \sum_{j=1}^n (z+e_i+e_j, \beta) + \sum_{j=1}^n (z+e_i+e_j, \beta+f_j) + \right. \\
&\left. + (z+e_i, \beta+f_i) + \sum_{j=1}^n (z+e_i+e_j, \beta+f_i) + \sum_{j=1}^n (z+e_i+e_j, \beta+f_i+f_j) \right] = \\
&= (z, \beta) + \sum_{i=1}^n \sum_{j=1}^n \left[(z+e_i+e_j, \beta) + (z+e_i+e_j, \beta+f_j) + \right. \\
&\left. + (z+e_i+e_j, \beta+f_i) + (z+e_i+e_j, \beta+f_i+f_j) \right] = \\
&= (z, \beta) + \sum_{1 \leq i \neq j \leq n} \left[(z+e_i+e_j, \beta) + (z+e_i+e_j, \beta+f_j) + \right. \\
&\left. + (z+e_i+e_j, \beta+f_i) + (z+e_i+e_j, \beta+f_i+f_j) \right] + \\
&+ \sum_{i=1}^n [(z+2e_i, \beta) + (z+2e_i, \beta+f_i) + (z+2e_i, \beta+f_i) + (z+2e_i, \beta)] = (z, \beta).
\end{aligned}$$

В сумме с $i \neq j$ сокращаются пары слагаемых, отвечающих индексам (i, j) и (j, i) . Теорема 2 доказана.

У построенной конфигурации кроме прочих имеются регулярные автоморфизмы, переводящие $(z, \alpha) \in \mathbb{Z}^n \times GF(2)^n$ в $(zL + a, \alpha L)$, где L — подстановочная матрица, а $a \in \mathbb{Z}^n \setminus \{0\}$ — фиксированный ненулевой целочисленный вектор. Факторизуя по таким автоморфизмам, можно получать бесконечные семейства $(\nu, 2n+1)$ -конфигураций с ν , кратными 2^n .

§ 4. k -конфигурации типа $\mathcal{C}$

Предположим, что каждому целому $z \in \mathbb{Z}$ соответствует (w, κ) -конфигурация $\{Y_\alpha^{(z)}, \alpha \in \Upsilon\}$ на конечном множестве Y нечетной мощности w . (Множество Υ и значение κ , как и само множество Y , общие для всех $z \in \mathbb{Z}$.)

Теорема 3. Семейство подмножеств

$$X_{(z,\alpha)} = \left(\{z\} \times (Y \setminus Y_\alpha^{(z)}) \right) \cup (\{z-1\} \times Y), \quad (z, \alpha) \in \mathbb{Z} \times \Upsilon = \Lambda,$$

является k -конфигурацией на множестве $X = \mathbb{Z} \times Y$ с параметром $k = 2w - \kappa$.

Доказательство. Пусть $\{\Upsilon_y^{(z)}, y \in Y\}$ семейство подмножеств Υ , отвечающее (w, κ) -конфигурации $\{Y_\alpha^{(z)}, \alpha \in \Upsilon\}$, $z \in \mathbb{Z}$, и пусть

$$\Omega_y^{(z)} = \{\alpha \in \Upsilon : y \in Y_\alpha^{(z)}\}, \quad y \in Y, \quad O_\alpha^{(z)} = \{y \in Y : \alpha \in \Upsilon_y^{(z)}\}, \quad \alpha \in \Upsilon.$$

Тогда

$$\begin{aligned} \Omega_{(z,y)} &= \{(u, \alpha) \in \Lambda : (z, y) \in X_{(u,\alpha)}\} = \left(\{z\} \times (\Upsilon \setminus \Omega_y^{(z)}) \right) \cup (\{z+1\} \times \Upsilon), \\ &\quad (z, y) \in \mathbb{Z} \times Y. \end{aligned}$$

Положим $\Lambda_{(z,y)} = \left(\{z\} \times (\Upsilon \setminus \Upsilon_y^{(z)}) \right) \cup (\{z+1\} \times \Upsilon)$, $(z, y) \in \mathbb{Z} \times Y$. Тогда

$$\begin{aligned} O_{(z,\alpha)} &= \{(u, y) \in X : (z, \alpha) \in \Lambda_{(u,y)}\} = \left(\{z\} \times (Y \setminus O_\alpha^{(z)}) \right) \cup (\{z-1\} \times Y), \\ &\quad (z, \alpha) \in \mathbb{Z} \times \Upsilon. \end{aligned}$$

Выполнение условий i)–iv) определения 1 для семейства $X_{(z,\alpha)}$, $(z, \alpha) \in \mathbb{Z} \times \Upsilon$, сомнений не вызывает. При проверке выполнения условия v) воспользуемся нечетностью $w = |Y| = |\Upsilon|$ и нечетностью $\kappa = Y_\alpha^{(z)} = \Upsilon_y^{(z)} = \Omega_y^{(z)} = O_\alpha^{(z)}$ для всех $z \in \mathbb{Z}$. С учетом этого имеем

$$\begin{aligned} \sum_{(u,\alpha) \in \Lambda_{(z,y)}} X_{(u,\alpha)} &= \sum_{(u,\alpha) \in \{z\} \times (\Upsilon \setminus \Upsilon_y^{(z)})} X_{(u,\alpha)} + \sum_{(u,\alpha) \in \{z+1\} \times \Upsilon} X_{(u,\alpha)} = \\ &= \sum_{\alpha \in \Upsilon \setminus \Upsilon_y^{(z)}} X_{(z,\alpha)} + \sum_{\alpha \in \Upsilon} X_{(z+1,\alpha)} = \sum_{\alpha \in \Upsilon} X_{(z,\alpha)} + \sum_{\alpha \in \Upsilon_y^{(z)}} X_{(z,\alpha)} + \sum_{\alpha \in \Upsilon} X_{(z+1,\alpha)} = \\ &= \sum_{\alpha \in \Upsilon} \left[\left(\{z\} \times (Y \setminus Y_\alpha^{(z)}) \right) + (\{z-1\} \times Y) \right] + \\ &\quad + \sum_{\alpha \in \Upsilon_y^{(z)}} \left[\left(\{z\} \times (Y \setminus Y_\alpha^{(z)}) \right) + (\{z-1\} \times Y) \right] + \\ &\quad + \sum_{\alpha \in \Upsilon} \left[\left(\{z+1\} \times (Y \setminus Y_\alpha^{(z+1)}) \right) + (\{z\} \times Y) \right] = \\ &= \sum_{\alpha \in \Upsilon} \left[(\{z\} \times Y) + (\{z\} \times Y_\alpha^{(z)}) + (\{z-1\} \times Y) \right] + \end{aligned}$$

$$\begin{aligned}
& + \sum_{\alpha \in \Upsilon_y^{(z)}} \left[(\{z\} \times Y) + (\{z\} \times Y_\alpha^{(z)}) + (\{z-1\} \times Y) \right] + \\
& + \sum_{\alpha \in \Upsilon} \left[(\{z+1\} \times Y) + (\{z+1\} \times Y_\alpha^{(z+1)}) + (\{z\} \times Y) \right] = \\
& = (\{z\} \times Y) + (\{z\} \times Y) + (\{z-1\} \times Y) + (\{z\} \times Y) + (z, y) + (\{z-1\} \times Y) + \\
& + (\{z+1\} \times Y) + (\{z+1\} \times Y) + (\{z\} \times Y) = (z, y).
\end{aligned}$$

Теорема 3 доказана.

Замечание 2. Подбирая (w, κ) -конфигурации $\{Y_\alpha^{(z)}, \alpha \in \Upsilon\}$ на множестве Y специальным образом (например, одинаковыми, независимыми от $z \in \mathbb{Z}$) будем получать возможность строить $(v, 2w - \kappa)$ -конфигурации путем факторизации $(v, 2w - \kappa)$ -конфигураций из доказанной теоремы по их регулярным автоморфизмам.

§ 5. k -конфигурации типа $\mathcal{A}'$

Укажем еще один способ построения k -конфигураций, основанный на тех же соображениях, что и в теореме 1.

Пусть имеются два множества V и Y . Множество Y конечно мощности w . И пусть каждому $u \in V$ соответствует (w, κ) -конфигурация $\{Y_\alpha^{(u)}, \alpha \in \Upsilon\}$ на множестве Y . (Множество Υ и значение κ общие для всех $u \in V$.) Пусть, наконец, на множестве вершин V (возможно бесконечном) задан ориентированный граф Γ без петель и без параллельных дуг, в котором в каждую вершину $u \in V$ входит ровно l дуг $(u_1^+, u), \dots, (u_l^+, u)$ и из каждой вершины $u \in V$ выходит ровно l дуг $(u, u_1^-), \dots, (u, u_l^-)$, $l \geq 1$. Положим

$$\begin{aligned}
X &= V \times Y, \quad \Lambda = V \times \Upsilon, \\
X_{(u, \alpha)} &= (\{u\} \times Y_\alpha^{(u)}) \cup \bigcup_{i=1}^l (\{u_i^+\} \times Y), \quad (u, \alpha) \in V \times \Upsilon.
\end{aligned}$$

Теорема 4. Пусть в графе Γ число ориентированных путей длины 2 из каждой вершины в любую другую вершину четно. Тогда семейство подмножеств $X_{(y, \alpha)}$, $(y, \alpha) \in \Lambda$, является k -конфигурацией на множестве $X = V \times Y$ с параметром $k = lw + \kappa$.

Доказательство. В случае четного w утверждение теоремы 4 совпадает с утверждением уже доказанной теоремы 1. Если w нечетно, то доказательство теоремы 1 можно дословно повторить вплоть до самого конца,

когда необходимо убеждаться, что $\sum_{i=1}^l \sum_{a \in V} \sum_{j=1}^l (\{u_{ij}^{++}\} \times Y) = \sum_{i=1}^l \sum_{j=1}^l (\{u_{ij}^{++}\} \times Y) = 0$. Это следует из условий на граф Γ , согласно которым для каждого элемента $a \in V$ равенство $a = u_{ij}^{++}$ имеет место для четного числа пар индексов (i, j) . Теорема 4 доказана.

По сравнению с теоремой 1 условия на граф Γ в формулировке теоремы 4 являются более жесткими. Так, если множество его вершин V конечно, а A — матрица инцидентности, то $A^2 = 0$ и потому $(A + I_{|V|})^2 = I_{|V|}$. Здесь $I_{|V|}$ — единичная матрица. Полученное равенство означает, что $A + I_{|V|}$ является инволютивной $(|V|, l+1)$ -матрицей, в частности, l обязательно четно.

Несмотря на это замечание, теорема 4 представляет определенный интерес, поскольку по конфигурациям с параметрами $(|V|, l+1)$ и (w, κ) позволяет строить конфигурацию с большими параметрами — $(|V| \cdot w, lw + \kappa)$.

В свете теорем 1–4 представляется сомнительной возможность обобщимого описания (v, k) -конфигураций как в общем случае, так и при конкретном нечетном $k \geq 5$. Подчеркнем, что теоремы 1–4 позволяют строить только массовые достаточно большие серии (v, k) -конфигураций. Противоположный класс составляют уникальные конфигурации, характерные для классической комбинаторики, являющиеся, как правило, особыми решениями экстремальных задач.

Список литературы

1. Малышев, Ф. М. Три семейства 5-конфигураций // Математические вопросы криптографии. — 2013. — Т. 4. Вып. 3. — С. 83–97.
2. Малышев, Ф. М., Тараканов, В. Е. О (v, k) -конфигурациях // Математический сборник. — 2001. — Т. 192. Вып. 9. — С. 85–108.
3. Тришин, А. Е. Примеры (v, k) -матриц // Вестник ИКСИ (серия К), специальный выпуск, посвященный 100-летию академика А. Н. Колмогорова. Академия ФСБ России. — М.: 2003 г. — С. 179–185.
4. Тришин, А. Е. Классификация циркулянтных $(v, 5)$ -матриц // Обзор. прикл. и пром. матем. — 2004. — Т. 11. Вып. 2. — С. 258–259.
5. Фролов, А. А. Описание абелевых $(v, 5)$ -групп матриц // Обзор. прикл. и пром. матем. — 2004. — Т. 11. Вып. 2. — С. 262–263.

6. *Фролов, А. А.* Класс инволютивных неабелевых $(v,5)$ -групп матриц // Обозр. прикл. и пром. матем. — 2005. — Т. 12. Вып. 1.
7. *Тришин, А. Е., Фролов, А. А.* Способ построения (v,k) -матриц при помощи функции след // Обозр. прикл. и пром. матем. — 2006. — С. 362–364.
8. *Фролов, А. А.* Новое семейство инволютивных $(v,5)$ -групп // Обозр. прикл. и пром. матем. — 2007. — Т. 14. Вып. 3. — С. 569–570.
9. *Фролов, А. А.* Классификация неразложимых абелевых $(v,5)$ -групп // Дискретная математика. — 2008. — Т. 20. Вып. 1. — С. 94–108.
10. *Мальшиев, Ф. М., Фролов, А. А.* Классификация $(v,3)$ -конфигураций // Математические заметки. — 2012. — Т. 91. Вып. 5. — С. 741–749.
11. *Мальшиев, Ф. М., Фролов, А. А.* Классификационные теоремы для (v,k) -конфигураций // Труды конференции МаБИТ–2010, секция «Математические проблемы информационной безопасности». — М.: МЦНМО, 2011. — С. 61–65.