Math-Net.Ru

Общероссийский математический портал

Ф. М. Малышев, Три семейства 5-конфигураций, *Матем. вопр. криптогр.*, 2013, том 4, выпуск 3, 83–97

DOI: <https://doi.org/10.4213/mvk93>

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: 3.85.5.30

26 апреля 2023 г., 08:38:11

Три семейства 5-конфигураций

Ф. М. Малышев

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

Получено 11.IV.2012

В работе рассматриваются три типа конфигураций, которые включают в себя большую долю известных $(v; 5)$ -конфигураций, построенных разными способами. Вводится понятие регулярных автоморфизмов конфигураций более общей природы. Определяется их факторизация по группам регулярных автоморфизмов.

Ключевые слова: конфигурации, булевы матрицы, гиперграфы, орграфы

Three series of 5-configurations

F. M. Malyshev

Steklov Mathematical Institute of RAS, Moscow

Abstract. The paper examines three types of configurations which include many known $(v; 5)$ configurations constructed by different methods. For configurations of more general structure the concept of regular automorphisms are introduced and their factorization by the groups of regular automorphisms is defined.

Key words: configurations, Boolean matrices, hypergraphs, orgraphs

Citation: *Mathematical Aspects of Cryptography*, 2013, vol. 4, no. 3, pp. 83–97 (Russian).

§ 1. Введение

Тематика настоящей работы сосредоточена вокруг довольно специфических конструкций, так называемых $(v; k)$ -конфигураций. В общем случае под $(v; k)$ -конфигурацией понимается гиперграф на v вершинах, 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. В случае четного k сумма всех строк матрицы L была бы нулевой, поэтому $(v; k)$ -конфигурации возможны только при нечетных k , $1 \leq k < v$.

Часто используется эквивалентное $(v; k)$ -конфигурации понятие $(v; k)$ -матрицы. Это рассматриваемая с точностью до перестановки строк и столбцов такая матрица $L \in GL(v, 2)$, что в строках и в столбцах матриц L и L^{-1} ровно по k единиц. Для различных v и k матрицы с таким свойством используются, в частности, в шифр-алгоритмах AES, ARIA, SEED, SMS-4, а также в некоторых других. Коммутацию в SP-сети можно рассматривать как умножение на перестановочную матрицу, которая является $(v; 1)$ -матрицей.

Коль скоро в понятие $(v; k)$ -конфигурации заложены признаки, присущие (v, k, λ) -конфигурациям [1], то естественно, что в изучении и построении $(v; k)$ -конфигураций важную роль играют такие комбинаторные конструкции, относящиеся к блок-схемам, как матрицы Адамара, конечные проективные плоскости, совершенные разностные множества. При построении $(v; k)$ -конфигураций используются также теоретико-числовые конструкции, конечно-порожденные группы, графы с различными свойствами симметрии, в том числе графы ребер однородных многогранников. По этой тематике имеется достаточно развитая, но далекая от завершения теория. Построением $(v; k)$ -конфигураций в разное время занимались А. М. Зубков, Е. Г. Красулина, Ф. М. Малышев, В. Н. Сачков, В. Е. Тараканов, А. Е. Тришин, А. А. Фролов (см. [2–10]).

К настоящему времени получена (см. [9]) исчерпывающая классификация $(v; 3)$ -конфигураций, приведенная ниже в конце § 2. На фоне накопившегося богатства конкретных примеров $(v; k)$ -конфигураций, построенных разными способами, полученная классификация обосновывает своевременность постановки следующих трех вопросов. Прежде всего, это выявление комбинаторно эквивалентных $(v; k)$ -конфигураций среди имеющегося семейства построенных. Кроме того, необходимо пересмотреть само определение понятия $(v; k)$ -конфигурации, в котором определяющее значение должно отводиться параметру k , параметр v не так существен для вскрытия комбинаторной природы требований, закладываемых в соответствующие определения. Наконец, необходимо формировать начальную базу для классифи-

кации в будущем $(v; 5)$ -конфигураций. Настоящая статья относится к двум последним из этих вопросов.

Кроме введения статья содержит два параграфа. В следующем параграфе дается определение k -конфигурации на счетном множестве. Особенность вводимого определения заключается в его локальном характере. Последний параграф посвящен трем конкретным бесконечным сериям 5-конфигураций, обозначаемых соответственно буквами A , B и C . Данные серии интересны главным образом тем, что включают в себя в качестве комбинаторно эквивалентных значительную часть известных $(v; 5)$ -конфигураций, которые изначально были построены путем привлечения совершенно различных математических конструкций.

§ 2. Понятие k -конфигурации на счетном множестве

Абстрактные конфигурации в самом общем их понимании (см. [11, стр. 1076]) состоят из g подмножеств некоторого множества X , объявляемых прямыми, и p выделенных элементов X , объявляемых точками. При этом предполагается, что каждая точка принадлежит (инцидентна) ровно γ прямым, а каждая прямая содержит ровно π точек (инцидентна π точкам). Общее количество инцидентов равно

$$p\gamma = g\pi. \quad (1)$$

Такая конструкция называется конфигурацией с параметрами p, γ, g, π , а при $p = g$ — конфигурацией с параметрами p, γ . Если X — аффинное или проективное пространство с выделенными в нем p точками и g прямыми, то говорят о геометрической конфигурации. В различных ситуациях на конфигурации могут накладываться дополнительные условия. Например (см. [1]), в определении (v, k, λ) -конфигурации требуется: 1) $p = g = v$; 2) $\gamma = \pi = k$; 3) пересечение любой пары выделенных подмножеств инцидентно ровно λ точкам.

По аналогии с вышеприведенной системой условий введем понятие $(k'_1, k''_1, k'_2, k''_2)$ -конфигурации на счетном (в том числе и на конечном) множестве X . Это семейство подмножеств множества X мощности k'_1 каждое, причем каждый элемент X содержится ровно в k''_1 подмножествах. Для формулировки дополнительных условий будем отождествлять подмножества X с элементами $|X|$ -мерного линейного пространства над полем $GF(2)$: подмножеству $U \subseteq X$ сопоставим вектор, у которого множество номеров единичных координат совпадает с U . Для двух подмножеств $U, V \subset X$ полагаем $U + V = (U \cup V) \setminus (U \cap V)$. Пустое подмножество является нулем этого пространства. Одноэлементное подмножество $\{x\} \subset X$ в случаях, когда

оно рассматривается как элемент линейного пространства, иногда будем обозначать буквой x без скобок.

Определение 1. Семейство различных непустых подмножеств X_α , $\alpha \in \Lambda$, счетного множества X называется $(k'_1, k''_1, k'_2, k''_2)$ -конфигурацией, если соответствующий гиперграф связан и имеется семейство различных непустых подмножеств $\Lambda_x \subset \Lambda$, $x \in X$, для которых выполняются следующие пять условий:

- i) $|X_\alpha| = k'_1$ для всех $\alpha \in \Lambda$,
- ii) $|\{\alpha \in \Lambda: x \in X_\alpha\}| = k''_1$ для всех $x \in X$,
- iii) $|\Lambda_x| = k'_2$ для всех $x \in X$,
- iv) $|\{x \in X: \alpha \in \Lambda_x\}| = k''_2$ для всех $\alpha \in \Lambda$,
- v) $x = \sum_{\alpha \in \Lambda_x} X_\alpha$.

При необходимости указывать мощность $v = |X|$ в обозначении $(k'_1, k''_1, k'_2, k''_2)$ -конфигурации будем использовать также расширенное обозначение: $(v; k'_1, k''_1, k'_2, k''_2)$ -конфигурация.

В условиях определения 1 в случае конечного множества X по аналогии с равенством (1) имеем: $k''_1|X| = k'_1|\Lambda|$, $k''_2|\Lambda| = k'_2|X|$. Если $|X| = |\Lambda| = v$, то $k''_1 = k'_1 = k_1$, $k''_2 = k'_2 = k_2$, и, согласно условию v) определения 1, произведение матрицы инцидентности L семейства $\{X_\alpha, \alpha \in \Lambda\}$ и матрицы инцидентности L' семейства $\{\Lambda_x, x \in X\}$ будет единичной матрицей, поэтому $L' = L^{-1}$. Тем самым, при $|\Lambda| = |X| < \infty$ семейство $\{\Lambda_x, x \in X\}$ в определении 1 однозначно задается семейством $\{X_\alpha, \alpha \in \Lambda\}$. Из условий i), ii) следует, что у матрицы L в строках и в столбцах ровно по k_1 единиц. Аналогично, по условиям iii), iv) у матрицы L^{-1} в строках и в столбцах ровно по k_2 единиц. В результате получаем так называемые $(v; k_1, k_2)$ -матрицы. Первым обратил внимание на важность этого понятия А. Е. Тришин. При $k_1 = k_2 = k$ получаем как раз понятие $(v; k)$ -матрицы.

Далее $(k'_1, k''_1, k'_2, k''_2)$ -конфигурацию при $k''_1 = k'_1 = k_1$, $k''_2 = k'_2 = k_2$ называем (k_1, k_2) -конфигурацией, а при $k_1 = k_2 = k$ — k -конфигурацией. В следующем параграфе 5-конфигурации рассматриваются прежде всего для бесконечных множеств X . Каждая из предлагаемых там конфигураций обладает богатой группой автоморфизмов, за счет чего по ней строится бесконечная серия 5-конфигураций на конечных множествах X .

Определение 2. Биекция $\varphi: X \rightarrow X$ является регулярным автоморфизмом $(k'_1, k''_1, k'_2, k''_2)$ -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) $(\bigcup_{\alpha: x \in X_\alpha} X_\alpha) \cap \varphi(\bigcup_{\alpha: x \in X_\alpha} X_\alpha) = \emptyset$ для всех $x \in X$,
- iv) $(\bigcup_{x: \alpha \in \Lambda_x} \Lambda_x) \cap \psi(\bigcup_{x: \alpha \in \Lambda_x} \Lambda_x) = \emptyset$ для всех $\alpha \in \Lambda$.

Биекция ψ в этом определении условием i) задается однозначно.

Предложение 1. Если $|X| = |\Lambda| < \infty$, то в определении 2 условие ii) следует из условия i).

Доказательство. Из условия v) определения 1 имеем: $\sum_{\beta \in \Lambda_{\varphi(x)}} X_\beta = \varphi(x) = \varphi(\sum_{\alpha \in \Lambda_x} X_\alpha) = \sum_{\alpha \in \Lambda_x} \varphi(X_\alpha) = \sum_{\alpha \in \Lambda_x} X_{\psi(\alpha)} = \sum_{\psi^{-1}(\beta) \in \Lambda_x} X_\beta = \sum_{\beta \in \psi(\Lambda_x)} X_\beta$. Сравнивая крайние выражения в полученной цепочке равенств и помня, что $L' = L^{-1}$, получаем $\psi(\Lambda_x) = \Lambda_{\varphi(x)}$. Предложение 1 доказано.

Пусть G — группа подстановок на множестве X , состоящая (за исключением тождественной биекции $e \in G$) из регулярных автоморфизмов $(k'_1, k''_1, k'_2, k''_2)$ -конфигурации $\{X_\alpha, \alpha \in \Lambda\}$. Через H обозначим соответствующую группу подстановок на Λ . Она порождена биекциями $\psi: \Lambda \rightarrow \Lambda$, отвечающими биекциям $\varphi \in G$. Гомоморфное соответствие $\theta: \varphi \mapsto \psi$ инъективно, поэтому $H \cong G$. Действительно, если ψ — тождественная биекция, то для всех $x \in X$

$$\varphi(x) = \varphi\left(\sum_{\alpha \in \Lambda_x} X_\alpha\right) = \sum_{\alpha \in \Lambda_x} \varphi(X_\alpha) = \sum_{\alpha \in \Lambda_x} X_{\psi(\alpha)} = \sum_{\alpha \in \Lambda_x} X_\alpha = x,$$

откуда и следует изоморфность гомоморфизма $\theta: G \rightarrow H$.

Обозначим через $\tilde{X}$ множество орбит группы G , а через $\tilde{\Lambda}$ — множество орбит группы H . (Элементы множеств $\tilde{X}$ и $\tilde{\Lambda}$ обозначаем буквами, снабженными волной.) Для $\tilde{\alpha} \in \tilde{\Lambda}$ через $\tilde{X}_{\tilde{\alpha}} \subset \tilde{X}$ обозначим подмножество всех орбит, содержащих точки X_α для некоторого $\alpha \in \tilde{\alpha}$. Такое задание подмножества $\tilde{X}_{\tilde{\alpha}}$ корректно: оно не зависит от конкретного $\alpha \in \tilde{\alpha}$, поскольку $X_{\psi(\alpha)} = \varphi(X_\alpha)$. Аналогично определяется семейство подмножеств $\{\tilde{\Lambda}_{\tilde{x}}, \tilde{x} \in \tilde{X}\}$ множества $\tilde{\Lambda}$.

Орбиту G , содержащую точку $x \in X$, обозначаем через $[x] \in \tilde{X}$. Аналогично орбиту H , содержащую элемент $\alpha \in \Lambda$, обозначаем через $[\alpha] \in \tilde{\Lambda}$. Тогда $\tilde{X}_{\tilde{\alpha}} = \{[x]: x \in X_\alpha\}$ при любом $\alpha \in \tilde{\alpha} = [\alpha]$ и $\tilde{\Lambda}_{\tilde{x}} = \{[\alpha]: \alpha \in \Lambda_x\}$ при любом $x \in \tilde{x} = [x]$. (Отметим, что орбиты, обозначаемые символами $\tilde{x}$ и $[x]$, не обязаны совпадать.)

Предложение 2. Пусть G — группа регулярных автоморфизмов $(k'_1, k''_1, k'_2, k''_2)$ -конфигурации $\{X_\alpha, \alpha \in \Lambda\}$ на множестве X , $\tilde{X}$ — множество орбит группы G на X и $\tilde{\Lambda}$ — множество орбит группы $H = \theta(G)$ на Λ . Тогда семейство подмножеств $\{\tilde{X}_{\tilde{\alpha}}, \tilde{\alpha} \in \tilde{\Lambda}\}$ множества $\tilde{X}$ также является $(k'_1, k''_1, k'_2, k''_2)$ -конфигурацией.

Доказательство. Заметим прежде всего что $|\tilde{X}_{\tilde{\alpha}}| = k'_1$ при всех $\tilde{\alpha} \in \tilde{\Lambda}$. Действительно, по определению $|\tilde{X}_{\tilde{\alpha}}| \leq k'_1 = |X_\alpha|$. Если $|\tilde{X}_{\tilde{\alpha}}| < k'_1$, то в X_α , $\alpha \in \tilde{\alpha}$, существует пара точек $x, \varphi(x)$, $\varphi \in G \setminus \{e\}$, из одной орбиты. Тогда $X_\alpha \cap \varphi(X_\alpha) \neq \emptyset$, что противоречит условию iii) определения 2.

Проверим, что множества $\tilde{X}_{\tilde{\alpha}}$ различны для различных $\tilde{\alpha} \in \tilde{\Lambda}$. Действительно, пусть $|\tilde{X}_{[\alpha']}| = |\tilde{X}_{[\alpha'']}|$, где $\alpha', \alpha'' \in \Lambda$, $\alpha' \neq \alpha''$. Для любой точки $x' \in X_{\alpha'}$ имеем $[x'] \cap X_{\alpha''} = \{x''\}$ (по условию iii) определения 2 других точек из $X_{\alpha''}$ в этом пересечении, кроме x'' , нет). Если $[\alpha'] \neq [\alpha'']$, то найдутся две такие различные точки $x', y' \in X_{\alpha'}$, что $[x'] \cap X_{\alpha''} = \{x''\}$, $x'' = \varphi(x')$, $\varphi \in G$, и $[y'] \cap X_{\alpha''} = \{y''\}$, $y'' = \varphi_1(y')$, $\varphi_1 \in G \setminus \{\varphi\}$. Иначе имели бы $X_{\alpha''} = \varphi(X_{\alpha'}) = X_{\psi(\alpha')}$, $\psi = \theta(\varphi) \in H$, $\alpha'' = \psi(\alpha')$ и $[\alpha'] = [\alpha'']$. Обозначим $\Omega_x = \{\alpha \in \Lambda: x \in X_\alpha\}$, $x \in X$. Тогда $|\Omega_x| = k'_1$ для всех $x \in X$ по условию ii) определения 1. Рассмотрим семейство $\{\varphi(X_\alpha) = X_{\psi(\alpha)}, \alpha \in \Omega_{x'}\}$ и отвечающее ему множество $\{\psi(\alpha), \alpha \in \Omega_{x'}\} = \Omega_{x''} = \{\alpha \in \Lambda: x'' \in X_\alpha\}$. Коль скоро $\alpha'' \in \Omega_{x''}$, то $\alpha'' = \psi(\alpha_0)$, $\alpha_0 \in \Omega_{x'}$, причем $\alpha_0 \neq \alpha'$. После этого заключаем, что $X_{\alpha'} \cap \varphi_1^{-1}(\varphi(X_{\alpha_0})) \neq \emptyset$, так как в пересечении содержится точка y' . Это противоречит условию iii) определения 2, поскольку $\varphi_1^{-1}\varphi \in G \setminus \{e\}$ и $\alpha', \alpha_0 \in \Omega_{x'}$.

Проверим, что $\tilde{\Omega}_{\tilde{x}} = \{\tilde{\alpha} \in \tilde{\Lambda}: \tilde{x} \in \tilde{X}_{\tilde{\alpha}}\}$ состоит ровно из k'_1 элементов для всех $\tilde{x} \in \tilde{X}$, т. е. что $|\tilde{\Omega}_{\tilde{x}}| = k'_1$. Прежде всего, $|\tilde{\Omega}_{[x]}| \leq |\Omega_x| = k'_1$. В самом деле, если $[x] \in \tilde{X}_{\tilde{\alpha}}$, то для некоторого $\alpha \in \tilde{\alpha}$ имеем $[x] \cap X_\alpha = \{\varphi(x)\}$, где $\varphi \in G$. Тогда $x \in \varphi^{-1}(X_\alpha) = X_{\psi^{-1}(\alpha)}$, $\psi = \theta(\varphi)$, то есть $\tilde{X}_{\tilde{\alpha}} = \{[y]: y \in X_{\psi^{-1}(\alpha)}, \psi^{-1}(\alpha) \in \Omega_x\}$. Отсюда и следует неравенство $|\tilde{\Omega}_{[x]}| \leq |\Omega_x|$. Осталось проверить, что если $\alpha', \alpha'' \in \Omega_x$, $\alpha' \neq \alpha''$, то $[\alpha'] \neq [\alpha'']$. Действительно, иначе имели бы $\alpha'' = \psi(\alpha')$, $\psi = \theta(\varphi) \in H$, $\varphi \neq e$, и $X_{\alpha'} \cap X_{\alpha''} = X_{\alpha'} \cap X_{\psi(\alpha')} = X_{\alpha'} \cap \varphi(X_{\alpha'}) \neq \emptyset$ содержит x , что противоречит условию iii) определения 2. Таким образом, для различных $\alpha', \alpha'' \in \Omega_x$ имеем $[\alpha'] \neq [\alpha'']$, $\tilde{X}_{[\alpha']} \neq \tilde{X}_{[\alpha'']}$ и $|\tilde{\Omega}_{[x]}| = |\Omega_x| = k'_1$.

Совершенно аналогично вышеприведенным рассуждениям проверяется, что $|\tilde{\Lambda}_{\tilde{x}}| = k'_2$ для всех $\tilde{x} \in \tilde{X}$, $\tilde{\Lambda}_{[x]} \neq \tilde{\Lambda}_{[y]}$ при $[x] \neq [y]$ и что $|\tilde{\Omega}_{\tilde{\alpha}}| = k''_2$ для всех $\tilde{\alpha} \in \tilde{\Lambda}$. Считаем $\Omega_\alpha = \{x \in X: \alpha \in \Lambda_x\}$, $\alpha \in \Lambda$, и $\tilde{\Omega}_{\tilde{\alpha}} = \{\tilde{x} \in \tilde{X}: \tilde{\alpha} \in \tilde{\Lambda}_{\tilde{x}}\}$, $\tilde{\alpha} \in \tilde{\Lambda}$.

Для доказательства предложения 2 остается проверить условие v) определения 1 для семейств подмножеств $\{\tilde{X}_{\tilde{\alpha}}, \tilde{\alpha} \in \tilde{\Lambda}\}$ и $\{\tilde{\Lambda}_{\tilde{x}}, \tilde{x} \in \tilde{X}\}$. Оно заключается в равенстве $[x] = \sum_{\tilde{\alpha} \in \tilde{\Lambda}_{[x]}} \tilde{X}_{\tilde{\alpha}}$. Это равенство при каждом фиксированном $x \in X$ непосредственно следует из своего прототипа: $x = \sum_{\alpha \in \Lambda_x} X_{\alpha}$. Чтобы в этом убедиться, можно расположить множество элементов X в двумерной таблице, в строках которой записаны элементы орбит группы G . По условию iii) определения 2 мощность каждой орбиты совпадает с порядком группы $|G|$. Столбцы таблицы нумеруются элементами G . В первом столбце под единственным элементом $e \in G$ располагаются представители орбит — по одному из орбиты. Если в начале строки (под e) стоит $x \in X$, то на ее пересечении со столбцом с номером $\varphi \in G$ стоит $\varphi(x)$. В отдельном столбце справа от таблицы для X располагаем элементы $\tilde{X}$, равные орбитам на соответствующих строках. Отображение $\pi: X \rightarrow \tilde{X}$, $y \mapsto [y]$, элементу таблицы $y \in X$ ставит в соответствие элемент последнего столбца, располагающийся в одной строке с y . Как уже доказано, соответствие $\alpha \mapsto [\alpha]$ задает биекцию $\Lambda_x \rightarrow \tilde{\Lambda}_{[x]}$, причем $\tilde{X}_{[\alpha]}$ является совокупностью орбит, содержащих элементы X_{α} . Подмножества X_{α} , $\alpha \in \Lambda$, если пересекаются с какой-то орбитой G , то только по единственному элементу — в X_{α} нет пар элементов из одной орбиты. В результате между системами множеств X_{α} и $\tilde{X}_{[\alpha]} = \pi(X_{\alpha})$, $\alpha \in \Lambda_x$, имеется биекция. Сюръективное отображение $\pi: \bigcup_{\alpha \in \Lambda_x} X_{\alpha} \rightarrow \bigcup_{\tilde{\alpha} \in \tilde{\Lambda}_{[x]}} \tilde{X}_{\tilde{\alpha}}$, $\pi: y \mapsto [y]$, биекцией, вообще говоря, не является. Ограничения $\pi|_{X_{\alpha}}: X_{\alpha} \rightarrow \tilde{X}_{[\alpha]}$ биективны при каждом $\alpha \in \Lambda_x$. Приведенные замечания позволяют выписать равенство

$$|\{\tilde{\alpha} \in \tilde{\Lambda}_{[x]}: \tilde{y} \in \tilde{X}_{\tilde{\alpha}}\}| = \sum_{y \in \pi^{-1}(\tilde{y})} |\{\alpha \in \Lambda_x: y \in X_{\alpha}\}|, \quad (2)$$

справедливое для всех $x \in X$ и $\tilde{y} \in \bigcup_{\tilde{\alpha} \in \tilde{\Lambda}_{[x]}} \tilde{X}_{\tilde{\alpha}}$, в том числе и для $\tilde{y} = [x]$. Условие v) определения 1 для семейства $\{\tilde{X}_{\tilde{\alpha}}, \tilde{\alpha} \in \tilde{\Lambda}\}$ выполняется, поэтому в правой части равенства (2) все слагаемые являются четными, кроме случая $y = x$, возникающего при $\tilde{y} = [x]$. Таким образом, левая часть в (2) всегда четная, кроме случая $\tilde{y} = [x]$, когда она является нечетной из-за единственного слагаемого в правой части с $y = x$. Этим доказано выполнение условия v) определения 1 для семейства подмножеств $\{\tilde{X}_{\tilde{\alpha}}, \tilde{\alpha} \in \tilde{\Lambda}\}$ в множестве $\tilde{X}$.

Предложение 2 полностью доказано.

В свете предложения 2 среди $(k'_1, k''_1, k'_2, k''_2)$ -конфигураций естественно выделить классы так называемых массовых конфигураций, содержащихся среди серий конфигураций, близких друг другу по различным признакам.

Подобные серии возникают, в частности, в результате факторизаций даже одной конфигурации на бесконечном множестве, если она обладает достаточно богатым набором регулярных автоморфизмов. При факторизации подобной конфигурации по различным группам регулярных автоморфизмов можно получать такие конфигурации на конечных множествах различной мощности, которые локально устроены одинаковым образом.

Противоположный класс составляют уникальные конфигурации, характерные для классической комбинаторики. Они возникают в результате редких стечений обстоятельств, связанных с конечными целочисленными величинами. В других разделах математики подобные объекты называют еще исключительными. На первых этапах классификационных исследований такие конфигурации приходится игнорировать, хотя именно они, обладая неповторимой внутренней красотой, чаще всего стимулируют к дальнейшему поиску новых конфигураций.

В качестве примера рассмотрим 3-конфигурацию на рисунке 1, являющуюся замкнутой цепью из звеньев в виде пар треугольников.

Рис. 1

Рис. 2

Рис. 3

Подмножествами X_α на рисунке 1 являются вершины помеченных треугольников.

Левая часть рисунка 1, если ее неограниченно продолжать вверх и вниз, будет представлять 3-конфигурацию на множестве целых чисел $\mathbb{Z}$ в виде семейства 3-подмножеств $\{2i, 2i+1, 2i+2\}$, $\{2i, 2i+1, 2i+3\}$, $i \in \mathbb{Z}$. Биекции $\varphi_r: \mathbb{Z} \rightarrow \mathbb{Z}$, $r \in \mathbb{Z}$, $\varphi_r(z) = z + 2r$, $z \in \mathbb{Z}$, при $|r| \geq 3$ удовлетворяют условиям

определения 2, являются регулярными автоморфизмами такой конфигурации. Факторизуя ее по группам $G = \langle \varphi_{v/2} \rangle$, будем получать $(v; 3)$ -конфигурации для четных $v \geq 6$. Полагая $G = \langle \varphi_2 \rangle$, несмотря на определенные нарушения требований iii) и iv) в определении 2, в результате факторизации получим и оставшуюся, как бы вырожденную в этой серии, $(4; 3)$ -конфигурацию (см. рис. 2).

Завершает классификацию $(v; 3)$ -конфигураций триангуляция листа Мёбиуса на рисунке 3. Там выделенные жирным ребра составляют край листа Мёбиуса. Это единственная $(v; 3)$ -конфигурация при нечетном v , именно при $v = 5$. В классе 3-конфигураций данную конфигурацию приходится причислять к исключительным. В то же время 3-конфигурация на рисунке 3 естественно вписывается в $(v; 3, k)$ -конфигурации, представленные на рисунках 4 и 5 для четных и нечетных v соответственно. На рисунке 4 (при четном v) имеем боковую поверхность антипризмы, а на рисунке 5 (при нечетном v) — триангуляцию листа Мёбиуса. Нетрудно убедиться, что матрица инцидентий L этих конфигураций не вырождена только для v , не делящихся на 3, когда $v \equiv \pm 1 \pmod{3}$. Число единиц k в строках и в столбцах у матрицы L^{-1} равно ближайшему к $\frac{2v}{3}$ целому числу, которое будем обозначать $\left\lfloor \frac{2v}{3} \right\rfloor$.

Рис. 4

Рис. 5

Рис. 6

Обратим внимание, что эти две серии конфигураций (на рис. 4 и 5) локально устроены одинаково. Если $v = 3k - 1$ (соответственно $v = 3k + 1$), то независимо от четности v множества Λ_x устроены так, как показано ниже на рисунке 7 (соответственно на рис. 8) крестиками. При конечном v приведенные на рисунках 7 и 8 полосы замыкаются либо в боковую поверхность антипризмы (при четном v), либо в лист Мёбиуса (при нечетном v).

Ориентируясь в этих сериях на $(v; 3)$ -конфигурации, из уравнения $\left\lfloor \frac{2v}{3} \right\rfloor = k = 3$ получаем два решения: $v = 4$ и $v = 5$. При $v = 5$ имеем как раз $(5; 3)$ -конфигурацию на рисунке 3, а при $v = 4$ — $(4; 3)$ -конфигурацию —

Рис. 7

Рис. 8

вырожденную антипризму на рисунке 6 (ср. с рис. 2). Основания на рисунке 6 выделены жирными ребрами, они являются двуугольниками. В результате $(v; 3)$ -конфигурации состоят как бы из двух серий: одной бесконечной для четных v (рис. 1 и рис. 2), и другой, состоящей из двух конфигураций — $(4; 3)$ -конфигурации и $(5; 3)$ -конфигурации — представляемых триангуляциями замкнутых полос; при этом $(4; 3)$ -конфигурация входит в обе серии.

Другой круг вопросов, которые не рассматриваются в настоящей работе, но которые в будущем потребуют внимания, связан с включением конкретной $(v_0; k'_1, k''_1, k'_2, k''_2)$ -конфигурации, полученной из каких-либо соображений, в серию ей подобных $(v; k'_1, k''_1, k'_2, k''_2)$ -конфигураций для достаточно широкого множества значений v . В идеале на пути обобщения факторизации конфигураций по группам регулярных автоморфизмов, хотелось бы построить в каком-либо виде аналог топологической теории односвязных накрывающих пространств. Например, $(v; 3, \llbracket 2v/3 \rrbracket)$ -конфигурации на рисунках 4 и 5 можно представлять в виде факторов $(\infty; 3, \infty)$ -конфигураций, представленных на рисунках 7 и 8 в виде семейств троек вершин треугольников, на которые разбивается часть плоскости между параллельными прямыми. Для этих конфигураций автоморфизмами семейств треугольников $\{X_\alpha, \alpha \in \Lambda\}$ являются параллельные сдвиги вдоль полос на целое число позиций и скользящие симметрии (сдвиги на полуцелое число позиций с последующей симметрией относительно средней линии на полосе).

В этих конфигурациях $k_2 = k'_2 = k''_2 = |\Omega_\alpha| = |\Lambda_x| = \infty$ для всех точек $x \in X$ и для всех нумерующих тройки $\alpha \in \Lambda$, $|X| = |\Lambda| = \infty$. Конфигурации на рисунках 7 и 8 различаются видом множеств $\Lambda_x, x \in X$, элементы которых помечены крестиками. Для остальных точек $y \in X$ множества Λ_y получаются из указанных либо параллельным сдвигом, либо скользящей симметрией. Условие v) в определении 1 предполагает здесь распространение понятия суммы $\sum_{\theta \in \Xi} Y_\theta$ подмножеств Y_θ из X , введенного

в начале параграфа, на случай бесконечного числа слагаемых $|\Xi| = \infty$ в тех ситуациях, когда для каждого $x \in X$ число $n_x = |\{\theta \in \Xi : Y_\theta x\}|$ конечно. Тогда $x \in \sum_{\theta \in \Xi} Y_\theta \Leftrightarrow n_x \equiv 1 \pmod{2}$.

Для получения $(v; 3, \llbracket 2v/3 \rrbracket)$ -конфигурации при $v \equiv -1 \pmod{3}$ нужно факторизовать конфигурацию на рисунке 7, а при $v \equiv 1 \pmod{3}$ — конфигурацию на рисунке 8.

§ 3. Конструкции бесконечных серий 5-конфигураций

3.1. Определение 5-конфигураций серии $\mathcal{A}$

Пусть Y — множество из $|Y| \geq 3$ элементов, и пусть на множестве вершин Y задан ориентированный граф Γ без петель и без параллельных дуг, в котором в каждую вершину y входит ровно две дуги: (u_1, y) , (u_2, y) — и из каждой вершины y выходит ровно две дуги: (y, v_1) , (y, v_2) . Конфигурацию $\{X_\alpha, \alpha \in \Lambda\}$ зададим на множестве $X = Y \times \{0, 1\}$. Элемент $(y, \varepsilon) \in Y \times \{0, 1\}$ обозначаем через $y^{(\varepsilon)}$. Тогда $X = \bigcup_{y \in Y} \{y^{(0)}, y^{(1)}\}$. Положим $\Lambda = X$ и

$$X_{y^{(i)}} = \{y^{(i)}, u_1^{(0)}, u_1^{(1)}, u_2^{(0)}, u_2^{(1)}\}, \quad y \in Y, \quad i = 0, 1. \quad (3)$$

Предложение 3. Семейство (3) является 5-конфигурацией на множестве X .

Доказательство. Прежде всего, $|X_{y^{(i)}}| = 5$, так как y, u_1, u_2 — три различных элемента в Y , поскольку в графе Γ нет петель и параллельных дуг. Далее, при любом $y \in Y$ конкретный элемент $y^{(i)} \in X$ может входить в 5-подмножество вида (3) либо в качестве первого элемента — один раз, либо в качестве одного из четырех других элементов. В последнем случае $y^{(i)} \in X_{v_j^{(l)}}$, $j = 1, 2$, $l = 0, 1$, причем все четыре возможности для пар $(j, l) \in \{1, 2\} \times \{0, 1\}$ реализуются. Других подмножеств X_x , $x \in X$, содержащих $y^{(i)}$, нет, так как нет других дуг, кроме (y, v_1) , (y, v_2) , выходящих из y , как нет и других дуг, кроме (u_1, y) , (u_2, y) , входящих в вершину y . Этим доказано условие ii) определения 1: $|\Omega_x| = 5$, $x \in X$. Напомним, что у нас $\Lambda = X$ и потому $\Omega_x = \{y \in X : X_y \ni x\}$.

Необходимо еще убедиться, что среди пяти подмножеств $X_{y^{(i)}}$, $X_{v_1^{(0)}}$, $X_{v_1^{(1)}}$, $X_{v_2^{(0)}}$, $X_{v_2^{(1)}}$ нет одинаковых. Для конфигураций дуг, входящих в вершины y, v_1, v_2 , имеют место 20 разных случаев, представленных на рисунках 9, 10, 11, отвечающих соответственно трем возможным значениям $|\{v_1, v_2\} \cap \{u_1, u_2\}|$, а именно 2, 1, 0. Во всех случаях подмножество $X_{y^{(i)}}$

характеризуется тем, что $|X_{y^{(i)}} \cap \{y^{(0)}, y^{(1)}\}| = 1$, а $|X_{v_j^{(l)}} \cap \{y^{(0)}, y^{(1)}\}|$ четно для всех $(j, l) \in \{1, 2\} \times \{0, 1\}$. Далее, $|X_{v_1^{(l)}} \cap \{v_1^{(0)}, v_1^{(1)}\}| = 1$, $l = 1, 2$, а $|X_{v_2^{(l)}} \cap \{v_1^{(0)}, v_1^{(1)}\}|$ четно. Наконец, $X_{v_j^{(0)}} \cap \{v_j^{(0)}, v_j^{(1)}\} \neq X_{v_j^{(1)}} \cap \{v_j^{(0)}, v_j^{(1)}\}$, $j = 1, 2$.

Рис. 9

Рис. 10

Полагая $\Lambda_{y^{(i)}} = X_{y^{(i)}}$, $y^{(i)} \in X$, освобождаемся от необходимости проверять условия iii) и iv) в определении 1, как и от проверки различия подмножеств Λ_x , $x \in X$. Наконец, условие v) в определении 1, заключающееся в равенстве $y^{(i)} = X_{y^{(i)}} + X_{u_1^{(0)}} + X_{u_1^{(1)}} + X_{u_2^{(0)}} + X_{u_2^{(1)}}$, следует из того, что $X_{u_j^{(0)}} + X_{u_j^{(1)}} = \{u_j^{(0)}, u_j^{(1)}\}$, $j = 1, 2$.

Предложение 3 доказано.

Рис. 11

3.2. Определение 5-конфигураций серии В

Пусть Y — множество вершин квадратов, на которые разбивается плоскость двумя перпендикулярными друг другу семействами равноотстоящих параллельных прямых. Конфигурацию $\{X_\alpha, \alpha \in \Lambda\}$ будем задавать на множестве $X = Y \times \{00, 01, 10, 11\}$. Элемент $(y, ij) \in Y \times \{00, 01, 10, 11\}$ обозначаем через $y^{(ij)}$. Тогда $X = \bigcup_{y \in Y} \{y^{(00)}, y^{(01)}, y^{(10)}, y^{(11)}\}$.

На множестве Y задается ориентированный граф Γ с дугами в виде сторон квадратов, горизонтальные дуги направлены направо, а вертикальные — вверх. Как и при определении конфигураций серии А, здесь тоже в каждую вершину y входит ровно две дуги: горизонтальная (u_1, y) и вертикальная (u_2, y) . Из каждой вершины y также выходит ровно две дуги: горизонтальная (y, v_1) и вертикальная (y, v_2) . Полагаем $\Lambda = X$ и

$$X_{y^{(ij)}} = \{y^{(ij)}, v_1^{(0j)}, v_1^{(1j)}, v_2^{(i0)}, v_2^{(i1)}\}, \quad y \in Y, \quad i = 0, 1, \quad j = 0, 1. \quad (4)$$

Предложение 4. Семейство (4) задает 5-конфигурацию на множестве X .

Доказательство. Равенство $|X_{y^{(ij)}}| = 5$ здесь очевидно. Далее, $\Omega_{y^{(ij)}} = \{\alpha \in \Lambda: y^{(ij)} \in X_\alpha\} = \{y^{(ij)}, u_1^{(0j)}, u_1^{(1j)}, u_2^{(i0)}, u_2^{(i1)}\}$, поэтому $|\Omega_x| = 5$ для всех $x \in X$. Наконец, $y^{(ij)} = X_{y^{(ij)}} + X_{v_1^{(0j)}} + X_{v_1^{(1j)}} + X_{v_2^{(i0)}} + X_{v_2^{(i1)}}$, поэтому

можно считать $\Lambda_{y^{(ij)}} = X_{y^{(ij)}}$. В результате условия iii) и iv) тоже выполняются. Предложение 4 доказано.

Построенная конфигурация имеет много регулярных автоморфизмов (параллельных сдвигов плоскости), факторизуя по которым получаем бесконечное семейство располагающихся на двумерных торах $(v; 5)$ -конфигураций, где v — любое целое число, кратное 4 и не меньшее 12.

§ 3.1. Определение 5-конфигураций серии C

Здесь конфигурацию $\{X_\alpha, \alpha \in \Lambda\}$ будем задавать на множестве $X = Y \times \{0, 1, 2\} = \bigcup_{y \in Y} \{y^{(0)}, y^{(1)}, y^{(2)}\}$, где $y^{(\varepsilon)} = (y, \varepsilon) \in Y \times \{0, 1, 2\}$, а Y — множество целочисленных точек на прямой. Снова полагаем $\Lambda = X$. Обозначим еще $y - 1 = u$, $y + 1 = v$, $y \in Y$. В этих обозначениях считаем

$$X_{y^{(i)}} = \{u^{(0)}, u^{(1)}, u^{(2)}, y^{(j)}, y^{(l)}\}, \quad \{j, l\} = \{0, 1, 2\} \setminus \{i\}, \quad y \in Y, \quad i = 0, 1, 2. \quad (5)$$

Предложение 5. Семейство (5) задает 5-конфигурацию на множестве X .

Доказательство. В силу равенства $y^{(i)} = X_{y^{(j)}} + X_{y^{(l)}} + X_{v^{(0)}} + X_{v^{(1)}} + X_{v^{(2)}}$, где $\{i, j, l\} = \{0, 1, 2\}$, следует положить $\Lambda_{y^{(i)}} = \{y^{(j)}, y^{(l)}, v^{(0)}, v^{(1)}, v^{(2)}\}$. Заметим, что $\Lambda_{y^{(i)}} = \Omega_{y^{(i)}} = \{\alpha \in \Lambda : y^{(i)} \in X_\alpha\}$. После этого предложение 5 следует из взаимной симметрии между подмножествами $X_{y^{(i)}}$ и $\Lambda_{y^{(i)}}$.

У построенной конфигурации регулярными автоморфизмами являются, в частности, сдвиги вдоль прямой, факторизация по которым порождает бесконечное семейство $(v, 5)$ -конфигураций, где v — любое целое число, кратное 3 и не меньшее 9.

Автор признателен А. М. Зубкову за внимание к работе и полезные критические замечания.

Список литературы

1. Холл М. Комбинаторика. — М. : Мир, 1970.
2. Малышев Ф. М., Тараканов В. Е. О (v, k) -конфигурациях // Матем. сборник. — 2001. — Т. 192. № 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. — М. : Академия ФСБ России, 2003. — С. 179–185.

4. *Тришин А. Е.* Классификация циркулянтных $(v, 5)$ -матриц // *Обозр. прикл. промышл. матем.* — 2004. — Т. 11. Вып. 2. — С. 258–259.
5. *Фролов А. А.* Описание абелевых $(v, 5)$ -групп // *Обозр. прикл. и промышл. матем.* — 2004. — Т. 11. Вып. 2. — С. 262–263.
6. *Фролов А. А.* Класс инволютивных неабелевых $(v, 5)$ -групп // *Обозр. прикл. промышл. матем.* — 2005. — Т. 12. Вып. 1. — С. 197–199.
7. *Фролов А. А.* Новое семейство инволютивных $(v, 5)$ -групп // *Обозр. прикл. промышл. матем.* — 2007, — Т. 14. Вып. 3. — С. 569–570.
8. *Фролов А. А.* Классификация неразложимых абелевых $(v, 5)$ -групп // *Дискретная математика.* — 2008. — Т. 20. № 1. — С. 94–108.
9. *Малышев Ф. М., Фролов А. А.* Классификация $(v, 3)$ -конфигураций // *Матем. заметки.* — 2012. — Т. 91. Вып. 5. — С. 741–749.
10. *Малышев Ф. М., Фролов А. А.* Классификационные теоремы для (v, k) -конфигураций // *Труды конференции МаБИТ - 2010, секция «Матем. проблемы инф. безопасности».* — М.: МЦНМО, 2011. — С. 61–65.
11. *Математическая энциклопедия.* Т. 2. — М.: 1979.