Math-Net.Ru

Общероссийский математический портал

Ф. М. Малышев, А. А. Фролов, Классификация $(v, 3)$ -конфигураций, *Матем. заметки*, 2012, том 91, выпуск 5, 741–749

DOI: <https://doi.org/10.4213/mzm9362>

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: 54.224.135.184

26 апреля 2023 г., 09:52:58

Классификация $(v, 3)$ -конфигураций

Ф. М. Малышев, А. А. Фролов

Под $(v, 3)$ -конфигурацией понимается невырожденная матрица размера v над полем $\text{GF}(2)$, рассматриваемая с точностью до перестановки строк и столбцов, у которых в строках и столбцах ровно по три единицы, причем у обратной матрицы в строках и столбцах тоже ровно по три единицы. Доказывается, что при каждом четном $v \geq 4$ имеется только одна неразложимая $(v, 3)$ -конфигурация, при нечетном v их нет, за исключением единственной $(5, 3)$ -конфигурации.

Библиография: 3 названия.

Понятие (v, k) -конфигурации для произвольного нечетного k и целого $v > k$ дается в работе [1] путем ослабления условий, определяющих хорошо известные объекты – (v, k, λ) -конфигурации. Первоначальным поводом введения (v, k) -конфигураций явились конкретные практические приложения, связанные с современной теорией кодирования.

В работе [1] приводятся всевозможные свойства (v, k) -конфигураций, даются условия существования и конкретные конструкции их построения, в том числе с помощью: (v, k, λ) -конфигураций, конечных проективных плоскостей, матриц Адамара, циркулянтных матриц, совершенных разностных множеств, конечных групп, конечных графов с различными свойствами симметрии. В заключении работы [1], как и в монографии [2] приводится таблица из 17 серий и 22 конкретных (v, k) -конфигураций.

В общем случае в соответствии с аннотацией под (v, k) -конфигурацией, $0 < k < v$, можно понимать матрицу $L \in \text{GL}(v, 2)$ такую, что у L и у L^{-1} во всех строках и во всех столбцах ровно по k единиц. Чаше (v, k) -конфигурации будем называть (v, k) -матрицами.

При наличии (v_1, k) -матрицы L_1 и (v_2, k) -матрицы L_2 имеется $(v_1 + v_2, k)$ -матрица

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

Неприводимая перестановкой строк и столбцов к такому виду матрица L называется неразложимой.

Любая $(v, 1)$ -матрица является подстановочной и потому она разложима.

В настоящей работе наше внимание сосредоточено на неразложимых $(v, 3)$ -матрицах. При каждом четном $v \geq 4$ все известные неразложимые $(v, 3)$ -матрицы,

приведенные в работе [1], оказались комбинаторно (перестановками строк и столбцов) эквивалентными матрицам

$$\begin{pmatrix} J & I & 0 & 0 & \cdot & 0 & 0 & 0 \\ 0 & J & I & 0 & \cdot & 0 & 0 & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & 0 & \cdot & 0 & J & I \\ I & 0 & 0 & 0 & \cdot & 0 & 0 & J \end{pmatrix}, \quad I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad J = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix},$$

предложенным А. М. Зубковым и Е. Г. Красулиной.

Исчерпывающая классификация $(6, 3)$ -матриц и $(8, 3)$ -матриц не позволила выйти за пределы этого примера. К нему же приводило рассмотрение некоторых семейств инволютивных (удовлетворяющих условию $L = L^{-1}$) $(v, 3)$ -матриц.

Единственным известным примером $(v, 3)$ -матрицы с нечетным v является $(5, 3)$ -матрица. Она является матрицей инцидентности между пятью вершинами и пятью треугольниками, на которые разбивается лист Мебиуса. На рис. 1 край листа Мебиуса представлен внутренней звездой, а общие стороны соседних треугольников – внешним пятиугольником. Отсутствие $(7, 3)$ -матриц доказано в работе [1]. С помощью вычислений на компьютере отсутствие $(9, 3)$ -матриц и $(11, 3)$ -матриц проверено Тришиным [3].

Рис. 1

ТЕОРЕМА 1. Для каждого четного $v \geq 4$ имеется ровно одна неразложимая $(v, 3)$ -конфигурация. Для нечетного v единственная $(v, 3)$ -конфигурация имеется только при $v = 5$.

ДОКАЗАТЕЛЬСТВО. Пусть имеется $(v, 3)$ -матрица L с $v \geq 4$. Множество номеров ее строк $\{1, 2, \dots, v\}$ будем представлять в виде v вершин. Каждый столбец матрицы L задает треугольник с вершинами, отвечающими единицам этого столбца. Эти треугольники будем также считать векторами линейного пространства над $\text{GF}(2)$ с векторами в виде всевозможных подмножеств в множестве из v вершин. Для двух подмножеств X, Y полагаем $X + Y = (X \cup Y) \setminus (X \cap Y)$. Пустое подмножество является нулем векторного пространства.

Треугольником будем считать только v выделенных 3-х точечных подмножеств, отвечающих столбцам матрицы L . Остальные $\binom{v}{3} - v$ троек вершин не являются треугольниками.

С учетом сделанных замечаний при доказательстве будет удобно пользоваться другим эквивалентным определением для $(v, 3)$ -конфигурации.

Задание $(v, 3)$ -конфигурации на v вершинах равносильно выделению v треугольников (3-х точечных подмножеств вершин), удовлетворяющих следующим двум условиям:

- $\alpha)$ каждая вершина принадлежит трем различным треугольникам;
- $\beta)$ каждая вершина является суммой трех треугольников, причем каждый треугольник участвует ровно в трех таких суммах.

Далее доказательство разбивается на несколько отдельных утверждений. Под суммами при этом будут пониматься только суммы, упомянутые в условии $\beta)$.

Д. 1. Окрестность каждой вершины устроена одним из пяти способов, представленных на рис. 2.

Рис. 2

Д. 2. Ни у одной вершины не может быть окрестности типа $e)$.

При наличии у одной вершины окрестности типа $e)$ в соответствующей матрице L имели бы место две одинаковых строки, что противоречит невырожденности матрицы L . Невырожденность матрицы L следует из условия $\beta)$.

Д. 3. Представление вершин суммой трех треугольников может реализовываться одним из двух способов, представленных на рис. 3.

Рис. 3

Крестиком на рис. 3 указаны треугольники, входящие в сумму.

Д. 4. Если имеется вершина типа $a)$ на рис. 2, то $v = 4$ и утверждение теоремы справедливо.

В вершине A уже сходятся три треугольника $\Delta_{AB_1B_2}$, $\Delta_{AC_1C_2}$ и Δ_{ABC} , поэтому треугольник $\Delta_{AB_1B_2}$ не смежен с другими треугольниками со сторонами AB_1 и AB_2 . Таким образом, $\Delta_{AB_1B_2}$ содержится в единственной паре смежных треугольников с $\Delta_{CB_1B_2}$. (Напомним, что случай е) на рис. 2 невозможен). Треугольник AB_1B_2 участвует в трех суммах вида В) на рис. 3, но в качестве элемента смежной пары треугольников не более, чем в двух из этих сумм, так как сторона AC не может быть смежной трем треугольникам. Значит в третьей сумме S_3 треугольник AB_1B_2 будет участвовать в качестве верхнего треугольника на рис. 3 В). У нас $A = \Delta_{ABC} + \Delta_{BA_1A_2} + \Delta_{CA_1A_2}$, поэтому $S_3 = B_1$ или $S_3 = B_2$. Пусть $S_3 = B_2$. Тогда потребуется треугольник $B_1C_1C_2$ или треугольник B_1BC . В первом случае, к ребру C_1C_2 примыкало бы три треугольника, а во втором случае к вершине C примыкало бы четыре треугольника.

Далее отрезок, соединяющей две вершины и являющейся стороной ровно одного треугольника, будем представлять сплошной утолщенной линией. Если этот отрезок является стороной двух треугольников, то будем представлять его пунктирной линией. По утверждению Д. 2 более чем двум треугольникам стороны не могут принадлежать. По утверждению Д. 5 хотя бы одна сторона является пунктирной.

Д. 6. Вершины типа d) рис. 2 невозможны.

Доказывать будем от противного. Пусть такая вершина O имеется (см. рис. 6).

Рис. 6

Положим, для определенности, $O = \Delta_{OA_1A_2} + \Delta_{A_1A_3A_4} + \Delta_{A_2A_3A_4}$. В других суммах, в которые входит хоть один треугольник с вершиной O , участвуют обязательно два таких треугольника, поскольку вершина O должна сокращаться. В каждой из последних сумм должны сокращаться обе вершины одного из ребер A_1A_2 , B_1B_2 , C_1C_2 . Согласно утверждению Д. 2 каждому из этих ребер отвечает не более одной суммы. В результате имеем не более четырех сумм, содержащих треугольники с вершиной O . Данные треугольники будут играть роль не более семи слагаемых в рассматриваемых суммах, тогда как, по условию β), таких слагаемых должно быть девять.

Далее самую верхнюю вершину в верхнем треугольнике на рис. 3 В) будем называть *отмеченной* в этом треугольнике.

Д. 7. В каждом треугольнике ровно одна отмеченная вершина.

Согласно принципу Дирихле, чтобы в этом убедиться достаточно проверить, что в треугольнике не может быть двух отмеченных вершин. Последнее будем доказывать от противного с помощью рис. 7.

Рис. 7

Пусть там в треугольнике ABC вершины B и C отмечены. В соответствии с рис. 3 В) должны быть четыре треугольника – $\triangle AC_1C_2$, $\triangle BC_1C_2$, $\triangle AB_1B_2$, $\triangle CB_1B_2$. В результате в вершине A сходятся три треугольника, противоречащие утверждению Д. 6.

В качестве следствия утверждения Д. 7 можно сформулировать следующее утверждение.

Д. 8. Каждый треугольник участвует в одной сумме в качестве верхнего треугольника на рис. 3 В) и в двух суммах в качестве нижнего элемента смежной пары треугольников.

Отметим еще, что одна и та же вершина не может быть отмеченной в двух треугольниках в силу невырожденности матрицы L .

Рис. 8

Д. 9. Все три стороны у треугольника не могут быть пунктирными, т.е. у него могут быть одна или две пунктирные стороны.

Докажем это от противного с помощью рис. 8. Пусть все стороны Δ_{ABC} пунктирные.

Достроим смежные ему треугольники с вершинами A_1, B_1, C_1 . Вершины A, B, C относятся к типу b) на рис. 2, поэтому все шесть ребер внешнего треугольника на рис. 8 являются сплошными утолщенными. Треугольник ABC входит в одну из сумм в качестве слагаемого из смежной пары, например с Δ_{BCA_1} . Тогда должен быть треугольник со стороной AA_1 , примыкающий к вершине A в качестве четвертого треугольника.

Согласно доказанному утверждению вершины типа b) и c) на рис. 2 представляются в виде, изображенном на рис. 9. Тонкой линией там представлены стороны неопределенного типа. Они могут быть, вообще говоря, как утолщенными, так и пунктирными. Связная компонента графа из пунктирных ребер может быть цепью из $l \geq 1$ ребер или циклом из $r \geq 3$ ребер.

Рис. 9

Д. 10. Для цикла из пунктирных ребер имеется единственная возможность $r = 5$.

Рис. 10

Цикл длины 3 исключается, потому как, наряду с утверждением Д. 9, в одной вершине не могут сходиться четыре треугольника. При цикле длины четыре все его диагонали являлись бы одновременно утолщенными и пунктирными линиями. Возможность $r \geq 6$ исключается следующим рассуждением (см. рис. 10).

Вершины на рассматриваемом цикле через одну соединены утолщенным ребром. У каждого из образовавшихся треугольников по два пунктирных ребра. Треугольник по утверждению Д. 8 только в одной сумме участвует в качестве верхнего треугольника рис. 3 В). Имеется сумма, например, с Δ_{ABC} и с Δ_{CBD} рис. 10 в качестве нижних смежных треугольников на рис. 3 В). В этой сумме должен быть третий верхний треугольник с ребром AD , который будет примыкать как к вершине A , так и к вершине D , в качестве четвертого треугольника. Оставшийся случай $r = 5$ возможен. Он как раз предоставляет приведенную в начале статьи $(5, 3)$ -конфигурацию, отвечающую разбиению листа Мебиуса на пять треугольников. Соответствующий граф из 5 утолщенных и 5 пунктирных ребер представлен на рис. 11.

Рис. 11

Д. 11. Цепь из $l \geq 2$ пунктирных ребер невозможна.

Самым трудным является случай $l = 2$ (см. рис. 12). В этом случае треугольник CDE участвовал бы в двух суммах в качестве нижнего треугольника рис. 3 В) и оба раза в паре с Δ_{ACE} . Это означает, что к вершине A , кроме Δ_{ABC} и Δ_{CAE} примыкают еще два треугольника. Случай $l > 2$ исключается аналогичным образом.

Рис. 12

Таким образом, если пунктирные ребра не образуют цикла, то в каждом треугольнике только одна пунктирная линия и он образует одну смежную пару еще с одним треугольником. Множество треугольников тем самым разбивается на смежные пары, поэтому v четно.

По свойству β на рис. 3 В) на самом верху должна быть еще одна вершина (см. рис. 13). Другими словами, над каждой смежной парой должна располагаться другая пара смежных треугольников.

Рис. 13

Надстраиванием вверх подобным образом пар смежных треугольников, ввиду конечности v замкнемся на самых нижних вершинах, причем на обеих вершинах сразу. Если бы замкнулись только на одну самую нижнюю вершину, то к ней прикрепило бы 5 треугольников (см. рис. 14).

Рис. 14

Число вершин v здесь четно и $v \geq 6$. При $v = 4$ все вершины были бы устроены по типу а) на рис. 2. Этот случай был рассмотрен в самом начале доказательства. Теорема доказана.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

- [1] Ф. М. Малышев, В. Е. Тараканов, “О (v, k) -конфигурациях”, *Матем. сб.*, **192**:9 (2001), 85–108.
- [2] М. Холл, *Комбинаторика*, Мир, М., 1970.
- [3] А. Е. Тришин, “Примеры (v, k) -матриц”, *Вестн. ИКСИ. Сер. «К»*, 2003, Специальный выпуск, посвященный 100-летию академика А. Н. Колмогорова, 179–185.

Ф. М. Малышев

Академия криптографии РФ, г. Москва

E-mail: malyshevf@yandex.ru

Поступило

12.11.2010

А. А. Фролов

Академия криптографии РФ, г. Москва

E-mail: faa75@yandex.ru