

**Известные и коммутативно групповые
5-конфигурации**

Ф.М. Малышев

В. Новгород – 2025

Совокупность $\mathcal{X} \subset 2^X$ из v подмножеств мощности k множества X называем k -конфигурацией, если:

i) каждый элемент $x \in X$ принадлежит ровно k подмножествам из $\mathcal{X}$,

ii) каждый элемент $x \in X$ является суммой (как подмножество $\{x\}$) ровно k подмножеств из $\mathcal{X}$, причём каждое подмножество из $\mathcal{X}$ участвует в качестве слагаемого ровно в k таких суммах.

В построении k -конфигураций в разное время принимали участие Брославский М.В., Зубков А.М., Комягин М.М., Красулина Е.Г., Малышев Ф.М., Сачков В.Н., Тараканов В.Е., Тришин А.Е., Фролов А.А.

Т.1.(1999,МФМ) Все $(v, 3)$ -группы являются абелевыми. Любая неразложимая $(v, 3)$ -группа эквивалентна одной из следующих $(v, 3)$ -групп:

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

Т. 2. (2001, Тараканов В.Е.) Пусть p простое, R – множество ненулевых квадратичных вычетов кольца $\mathbb{Z}_p = \{0, 1, \dots, p-1\}$, $\mathcal{R} = \{i + R \mid i \in \mathbb{Z}_p\}$ при $p \equiv 3 \pmod{8}$ и $\mathcal{R} = \{i + (R \cup \{0\}) \mid i \in \mathbb{Z}_p\}$ при $p \equiv 5 \pmod{8}$. Тогда $\mathcal{R}$ будет $(p, (p-1)/2)$ -конфигурацией при $p \equiv 3 \pmod{8}$ и $(p, (p+1)/2)$ -конфигурацией при $p \equiv 5 \pmod{8}$.

Т. 3. (2003, Тришин А.Е.) Неразложимая циклическая $(v, 5)$ -группа $(\mathbb{Z}_v, H, S)$, $H \setminus \{0\} = \{x_1, x_2, x_3, x_4\}$, $S \setminus \{0\} = \{y_1, y_2, y_3, y_4\}$, существует тогда и только тогда, когда v кратно 2 или 3, либо равно одному из чисел 11, 13, 17, 19. С точностью до эквивалентности неразложимые циклические $(v, 5)$ -группы исчерпываются двумя бесконечными сериями:

1) $H = -S = \{0, u, u+t, z, z+t\}$, где $v = 2t$, $u, z \in \mathbb{Z}_v \setminus \{0, t\}$, $u \neq z$, $u - z \neq t$, $\text{НОД}(u, z, t) = 1$, $t \geq 3$;

2) $H = S = \{0, -z, t, 2t, 2t - z\}$, где $v = 3t$, $z \in \mathbb{Z}_v \setminus \{0\}$, $\text{НОД}(z, t) = 1$, $t \geq 3$;
и двадцатью двумя исключительными случаями с $v \in \{10, \dots, 19\}$

Т. 4. (2005, Фролов А.А.) Абелевы нециклические неразложимые инволютивные $(v, 5)$ -группы исчерпываются единственной бесконечной серией: $(\mathbb{Z}_3 \times \mathbb{Z}_{3n}, \{(0, 0), (1, 0), (2, 0), (1, 1), (2, 1)\})$ с $S = H$. Все абелевы инволютивные (v, k) -группы являются факторами $(k - 1)/2$ -й декартовой степени группы $G = \mathbb{Z}_{2n} \times \mathbb{Z}_2$ из теоремы 1.

Т. 5. (2005, Фролов А.А.) Все неразложимые инволютивные абелевы $(v, 5)$ -группы являются образами группы $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z} \times \mathbb{Z}$ при некотором эпиморфизме ψ , при этом $H = \{0, \psi(0, 0, 0, 1), \psi(0, 1, 0, 1), \psi(0, 0, 1, 0), \psi(1, 0, 1, 0)\}$.

Т. 6. (2010, МФМ) Для каждого чётного $v \geq 4$ имеется ровно одна неразложимая $(v, 3)$ -конфигурация. Для нечётного v неразложимая $(v, 3)$ -конфигурация имеется только при $v = 5$.

Т. 7. (1999-2021,МФМ) При любых чётном v и нечётном k , $0 < k < v$, существует неразложимая (v, k) -конфигурация. Если при нечётных v и $k \geq 1$ существует (v, k) -конфигурация, то

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

Для нечётных $k \leq 17$ и всех v , удовлетворяющих неравенству (1), существует (v, k) -конфигурация за исключением случая $k = 3$, $v = 7$, когда её не существует.

Т. 8. (2024,2025,Комягин М.М.) С точностью до комбинаторной эквивалентности для $v = 9, 10, 11, 12$ имеется, соответственно, ровно 1, 34, 386, $71355 = 71330 + 5 \cdot 5$ $(v, 5)$ -конфигураций.

Под 2-графом Γ понимаем связный ориентированный граф на конечном или счётном множестве вершин P без петель и параллельных дуг с двумя входящими и двумя выходящими дугами для каждой вершины. В конечном случае полагаем $|P| = p$. Ориентированные циклы и граф на множестве вершин $\mathbb{Z}$ с дугами $i \rightarrow i + 1$, $i \in \mathbb{Z}$, считаем 1-графами.

Серия $\mathcal{A}$. Пусть Γ – 2-граф с множеством вершин P , $|P| \geq 3$. Концы дуг 2-графа Γ , выходящих из вершины $v \in P$, обозначаем $v_{\hat{0}}$ и $v_{\hat{1}}$. Полагаем $X = P \times \{0, 1\}$, $X_x = \{(v, \varepsilon), (v_{\hat{0}}, 0), (v_{\hat{0}}, 1), (v_{\hat{1}}, 0), (v_{\hat{1}}, 1)\}$, $x = (v, \varepsilon) \in P \times \{0, 1\}$, $\mathcal{X} = \{X_x | x \in X\}$. Обозначаем эту 5-конфигурацию символом $\mathcal{A}(\Gamma)$. Прототипами 5-конфигураций серии $\mathcal{A}$ являются конфигурации из Предложения 7 работы [1], полученные Ф.М. Малышевым.

Серия $\mathcal{B}$. Пусть Γ – 2-граф с множеством вершин P , $|P| \geq 3$, у которого дуги помечены либо 0, либо 1 так, что как входящие, так и выходящие дуги каждой вершины $v \in P$ помечены различно. Через v_{ε} обозначаем конец дуги, выходящей из вершины $v \in P$ с меткой $\varepsilon \in \{0, 1\}$. Предполагается, что $v_{\hat{0}\hat{1}} = v_{\hat{1}\hat{0}}$ для всех $v \in P$. Тогда 2-граф Γ называем *помеченным 2-графом*. Полагаем $X = P \times \{0, 1\} \times \{0, 1\}$, $X_x = \{(v, \varepsilon, \nu), (v_{\hat{0}}, 0, \nu), (v_{\hat{0}}, 1, \nu), (v_{\hat{1}}, \varepsilon, 0), (v_{\hat{1}}, \varepsilon, 1)\}$, $\mathcal{X} = \{X_x | x \in X\}$, $x = (v, \varepsilon, \nu) \in P \times \{0, 1\} \times \{0, 1\}$. Обозначаем эту 5-конфигурацию $\mathcal{B}(\Gamma)$. Прототипом 5-конфигураций серии $\mathcal{B}$ явилось Следствие 2 в работе А.А. Фроолова [6].

Серия $\mathcal{C}$. Пусть Γ – 1-граф с множеством вершин P , $|P| \geq 3$. Конец дуги 1-графа Γ , выходящей из вершины v , обозначаем $v_{\hat{0}}$. Полагаем $X = P \times \{0, 1, 2\}$, $X_x = \{(v, 0), (v, 1), (v, 2), (v_{\hat{0}}, \nu), \nu \in \{0, 1, 2\} \setminus \{\varepsilon\}\}$, $x = (v, \varepsilon) \in P \times \{0, 1, 2\}$, $\mathcal{X} = \{X_x | x \in X\}$. Прототипами 5-конфигураций серии $\mathcal{C}$ являются конфигурации из Примера 6 работы [1], полученного В.Е. Таракановым.

Серия $\mathcal{D}$. Пусть Γ – 1-граф с множеством вершин $\mathbb{Z}$. Концом дуги 1-графа Γ , выходящей из вершины $v \in \mathbb{Z}$, будет $v + 1$. Полагаем $X = \mathbb{Z} \times \mathbb{Z}_7$,

$$X_x = \{(v, \varepsilon), (v+1, \varepsilon), (v+1, \varepsilon+(-1)^v), (v+1, \varepsilon+(-1)^v 2), (v+1, \varepsilon+(-1)^v)\}$$

$x = (v, \varepsilon) \in \mathbb{Z} \times \mathbb{Z}_7$, $\mathcal{X} = \{X_x | x \in X\}$. Факторизуя данную 5-конфигурацию по группе автоморфизмов в виде $(v, \varepsilon) \mapsto (v + d, \varepsilon)$, $(v, \varepsilon) \in X$, по всем $d \in \mathbb{Z}$, кратным $2p$, $p \in \mathbb{N}$, получаем 5-конфигурацию на $14p$ вершинах. Прототипами 5-конфигураций серии $\mathcal{D}$ являются некоммутативные $(14p, 5)$ -группы из работы Фролова А.А. [4].

$$G_1 = \mathbb{Z} \times D_4, \mathbb{Z} = \langle d \rangle, D_4 = \langle z, \tau | z^2 = \tau^4 = e, z\tau z = \tau^{-1} \rangle, H = \{e, dz, dz\tau, dz\tau^2, d\},$$

$$G_2 = \mathbb{Z}_2 \times G, \mathbb{Z}_2 = \langle z \rangle, G = \langle a, \tau | \tau^4 = e, a^{-1}\tau a = \tau^{-1} \rangle, H = \{e, a, a\tau, a\tau^2, a\tau z\}.$$

Т. 9. (2025, МФМ) *5-конфигурации на группах G_1 и G_2 являются комбинаторно эквивалентными 5-конфигурации $\mathcal{B}_4(\mathbb{Z})$.*

Т. 10. (2024,МФМ) *5-конфигурации $\mathcal{A}(\Gamma')$ и $\mathcal{A}(\Gamma'')$ комбинаторно эквивалентны тогда и только тогда, когда 2-графы Γ' и Γ'' изоморфны*

Спецификации частот встречаемости вершин в окрестностях точек. Каждому $y \in X$ поставим в соответствие подмножество $Y_y = \cup_{x \in X: y \in X_x} X_x = \cup_{X_x \in \mathcal{X}: y \in X_x} X_x$. Для $z \in X$ определим $\iota(z, y) = |\{X_x \in \mathcal{X} | y \in X_x \text{ и } z \in X_x\}|$ – частоту встречаемости z в Y_y , $\iota(y, y) = 5$, $\iota(z, y) < 5$ для $z \neq y$ [12]. Пусть $\alpha_n = |\{z \in Y_y | \iota(z, y) = n\}|$, $n \in \mathbb{N}$, $N = \{n \in \mathbb{N} | \alpha_n \neq 0\}$. Наконец, точке $y \in X$ поставим в соответствие инвариант в виде произвольно упорядоченной строки Λ_y из символов n^{α_n} , $n \in N$, называемый спецификациями частот встречаемости в Y_y различных элементов из Y_y .

Типы вершин. Пусть $y \in X$ и X_i , $i = 1, 2, 3, 4, 5$, подмножества из $\mathcal{X}$, содержащие y . Рассматривается симплекс с вершинами $i \in \{1, 2, 3, 4, 5\}$. Каждой его j -мерной грани с вершинами $i_1, \dots, i_{j+1}$, $j = 0, 1, 2, 3, 4$, приписываем пометки в виде мощностей пересечений $\cap_{s=1}^{j+1} X_{i_s}$. Инвариантом является так помеченный четырёхмерный симплекс, рассматриваемый с точностью до его симметрий.

Вторичные спецификации частот встречаемости вершин в окрестностях точек. Для $y \in X$ рассмотрим одно из максимальных подмножеств $U_n \subset Y_y \setminus \{y\}$, состоящее из вершин $y_1, \dots, y_{\alpha_n}$, для которых $\iota(y_i, y) = n$. При каждом $i = 1, \dots, \alpha_n$ для $z \in Y_y \cup Y_{y_i}$ имеем две частоты $\iota(z, y)/\iota(z, y_i)$. Для $n, m \in \mathbb{N} \sqcup \{0\}$ рассмотрим $\alpha'_{n,m}(i) = |\{z \in Y_y \cup Y_{y_i} \mid \iota(z, y) = n, \iota(z, y_i) = m\}|$, а для $y \in X$ – инвариант в виде семейства из α_n произвольно упорядоченных строк $\Lambda'_y(i)$ из символов $(n/m)^{\alpha'_{n,m}(i)}$, $n, m \in \mathbb{N} \sqcup \{0\} : n \neq 0 \vee m \neq 0$, $i = 1, \dots, \alpha_n$.

Т. 11. (2024,МФМ) *С точностью до изоморфизма помеченными 2-графами являются:*

$$\mathcal{B}_1(p), p \geq 3, \mathcal{B}_1(\mathbb{Z}), \mathcal{B}'_1(4)$$

$$\mathcal{B}_2(2k), k \geq 3, \mathcal{B}_2(\mathbb{Z}), \mathcal{B}'_2(2k), k \geq 2,$$

$$\mathcal{B}_3(2k), k \geq 3, \mathcal{B}_3(\mathbb{Z}), \mathcal{B}'_3(2k+1), k \geq 2,$$

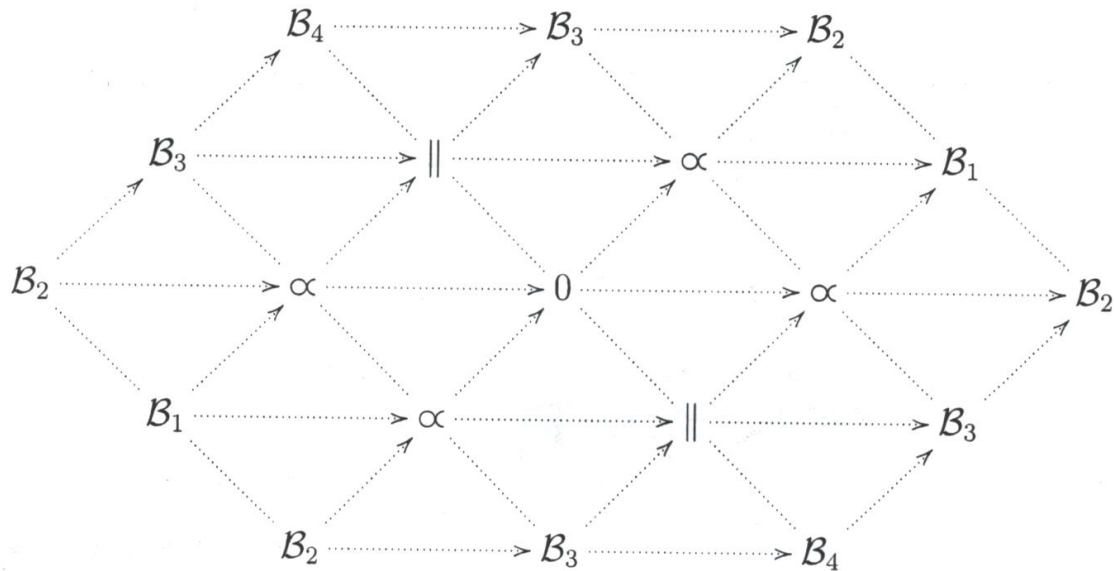
$$\mathcal{B}_4(2k), k \geq 3, \mathcal{B}_4(\mathbb{Z}), \mathcal{B}'_4(4k), k \geq 2,$$

$$\mathcal{B}_5^{(0)}, \mathcal{B}_5^{(1)}(u), \mathcal{B}_5^{(2,1)}(u, n, w), [w] = n > [u] \geq 3,$$

$$\mathcal{B}_5^{(2,2)}(u, w), [w] = [u] > [w - u] \geq 3,$$

$$\mathcal{B}_5^{(2,3)}(u), [w] = [u] = [w - u] \geq 3.$$

Помеченные 2-графы из приведённого списка не изоморфны друг другу.



М.М. Комягин установил комбинаторную эквивалентность $\mathcal{B}_1(4)$ и $\mathcal{B}'_2(4)$, $\mathcal{B}_2(2s)$ и $\mathcal{B}'_2(2s)$ для нечётных $s \geq 3$. Пары $\mathcal{B}_2(4s)$ и $\mathcal{B}'_2(4s)$, $\mathcal{B}_4(4s)$ и $\mathcal{B}'_4(4s)$, $s \geq 2$ комбинаторно не эквивалентны.

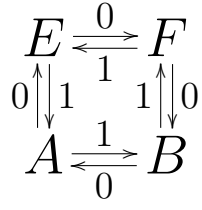


Рис. 1

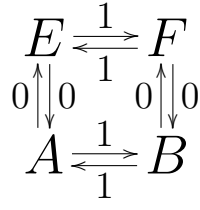


Рис. 2

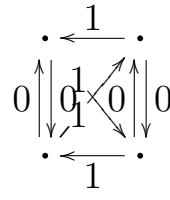


Рис. 3

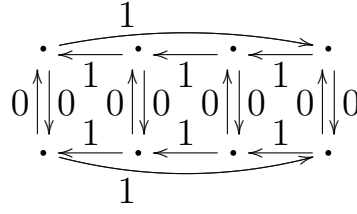


Рис. 4

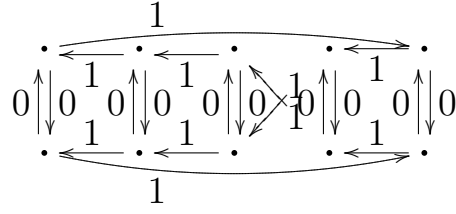


Рис. 5

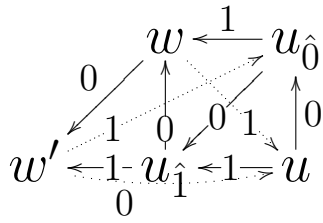


Рис. 6

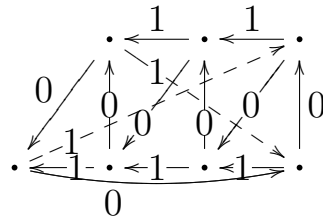


Рис. 7

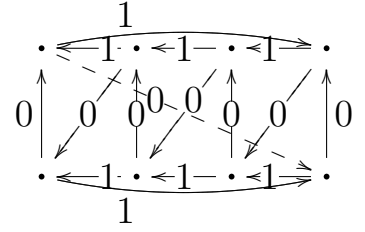


Рис. 8

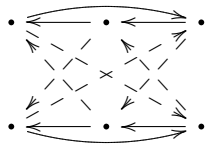


Рис. 9

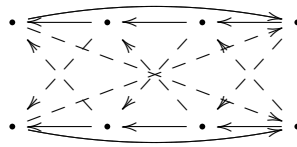


Рис. 10

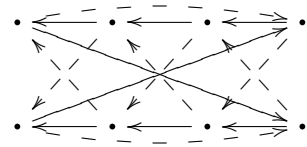


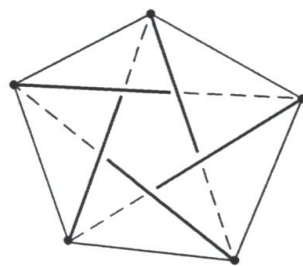
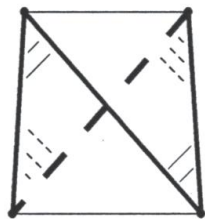
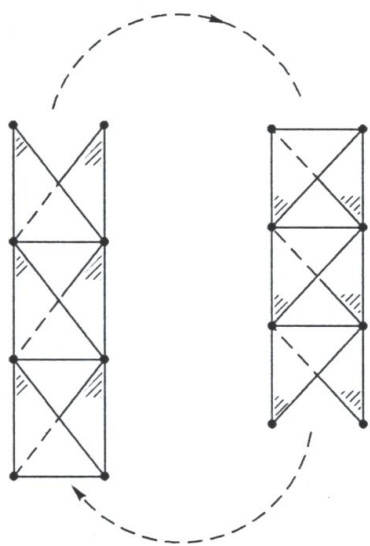
Рис. 11

Т. 12. (2025,МФМ) Любые две 5-конфигурации, принадлежащие различным сериям $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$, $\mathcal{D}$, комбинаторно не эквивалентны.

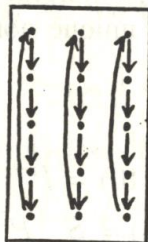
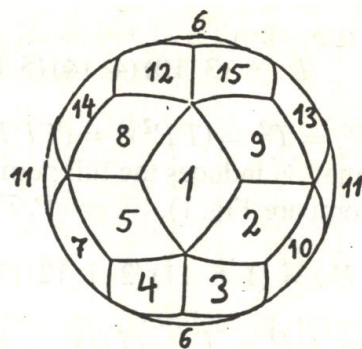
Т. 13. (2025,МФМ) Коммутативно групповые 5-конфигурации серии $\mathcal{A}$ строятся по помеченным 2-графам.

Т. 14. (2025,МФМ) За исключением нескольких циклических $(v, 5)$ -групп с $v \in \{10, \dots, 19\}$, любая коммутативно-групповая 5-конфигурация либо относится к одной из серий $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$, либо комбинаторно эквивалентна 5-конфигурации серии $\mathcal{A}$, профакторизованной по автоморфизму второго порядка, либо комбинаторно эквивалентна 5-конфигурации серии $\mathcal{B}$, профакторизованной или по автоморфизму второго порядка, или по группе автоморфизмов, изоморфной четверной группе Клейна.

Серия $\mathcal{KB}$



1	6	11
2	7	12
3	8	13
4	9	14
5	10	15



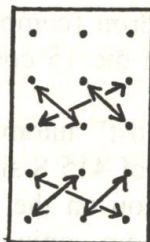
P rotation by 72°



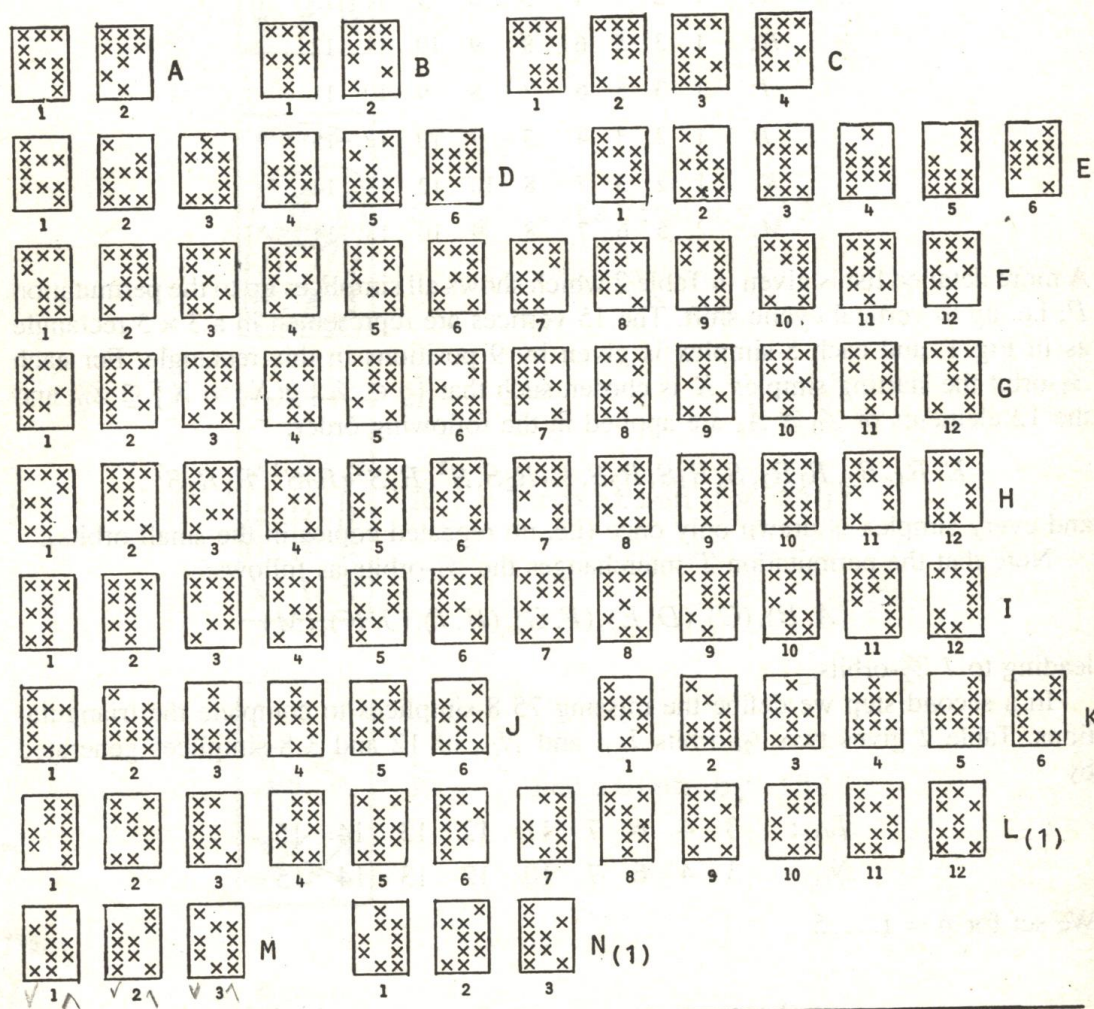
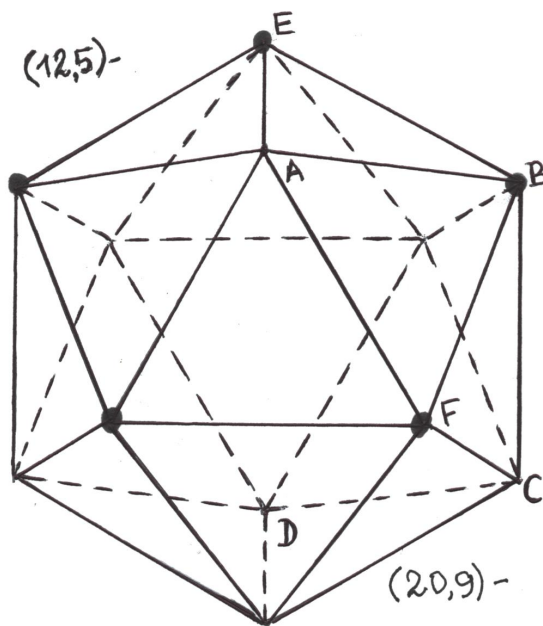
S rotation by 120°

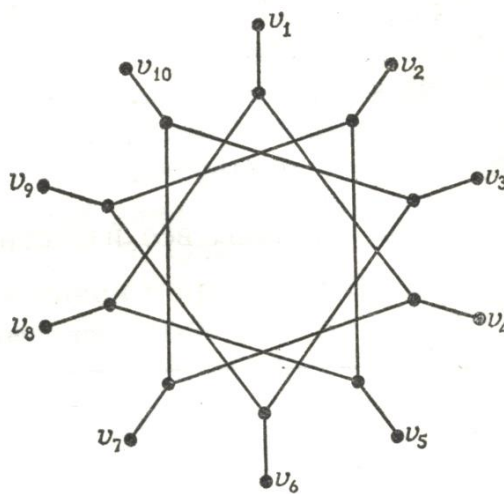
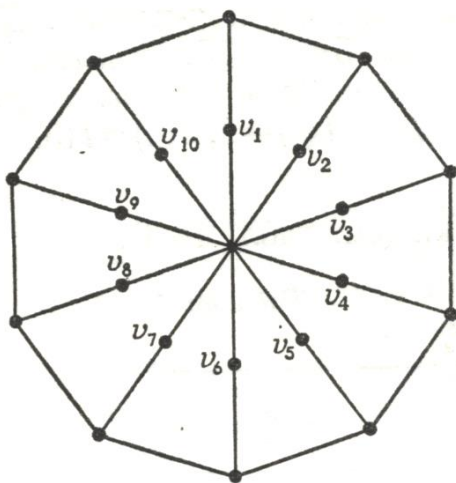


R_1 rotation by 180°

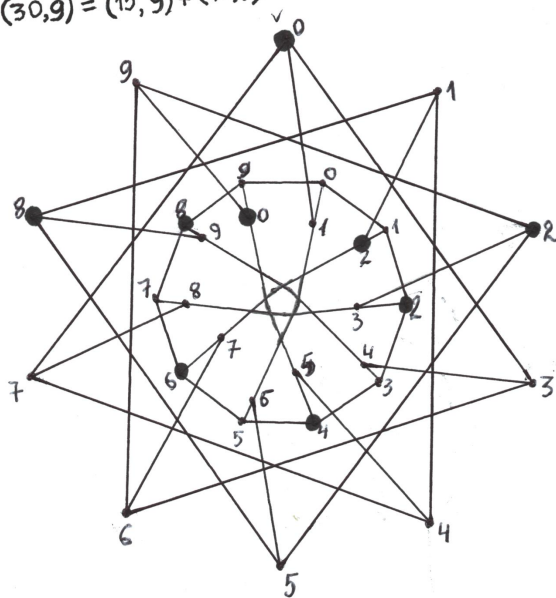


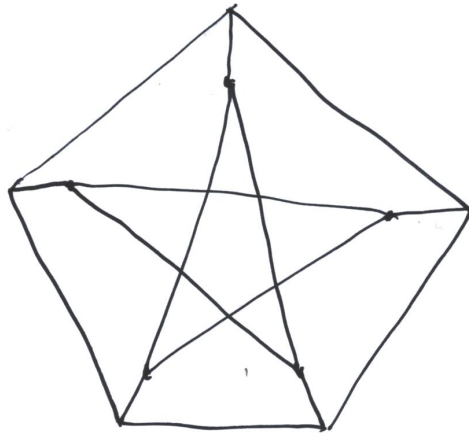
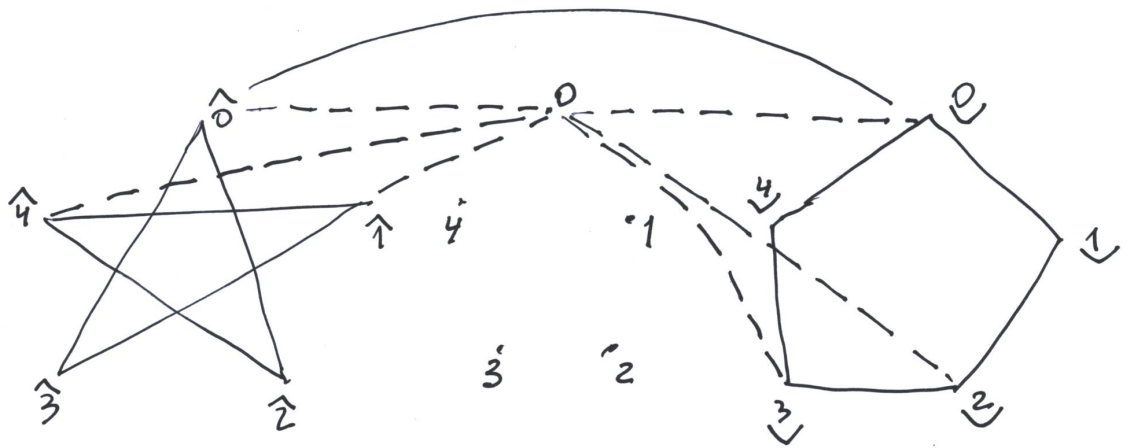
R_2 rotation by 180°





$$(30, 9) = (15, 9) + (15, 9)$$





Список литературы

- [1] Малышев Ф.М., Тараканов В.Е. О (v, k) -конфигурациях. Мат. сборник, **192**:9 (2001), 85-108.
- [2] Тришин А.Е. Примеры (v, k) -матриц. Вестник ИКСИ (серия К), специальный выпуск, посвящённый 100-летию академика А. Н. Колмогорова – М., 2003, 179-185.
- [3] Тришин, А.Е. Классификация циркулянтных $(v, 5)$ -матриц / А.Е. Тришин – Обзорение прикладной и промышленной математики, т. 11, вып. 2. – М.:ОПиПМ, 2004, с. 258-259.
- [4] Фролов А.А. Класс инволютивных неабелевых $(v, 5)$ -групп. – Обзорение прикладной и промышленной математики, т. 12, вып. 1. – М.:ОПиПМ, 2005, с. 197-199.
- [5] Тришин А.Е., Фролов А.А. Способ построения (v, k) -матриц при помощи функции след. 7-й Всероссийский симпозиум по прикладной и промышленной математике: “Обзорение прикладной и промышленной математики”, 2006, 362-364.
- [6] Фролов, А.А. Классификация неразложимых абелевых $(v, 5)$ -групп. Дискретная математика, **20**:1 (2008), 94–108.
- [7] Малышев Ф.М., Фролов А.А. Классификация $(v, 3)$ -конфигураций. Математические заметки, **91**:5 (2012) 741-749.
- [8] Малышев Ф.М. Три семейства 5-конфигураций. Математическме вопросы криптографии, **4**:3 (2013), 83–97.
- [9] Малышев, Ф.М. Четыре бесконечные серии k -конфигураций. Математическме вопросы криптографии, **4**:4 (2013), 65–75.
- [10] Малышев Ф. М. k -конфигурации. Труды МИАН, **316** (2022), 233–253.
- [11] Комягин М.М. Классификация $(v, 5)$ -конфигураций для $v \leq 11$. Дискретная математика, **36**:1 (2024), 46–66.
- [12] Малышев Ф.М. Классификация трех семейств 5-конфигураций. Дискрет. матем., **36**:4 (2024), 74–100.

- [13] Комягин М.М. Классификация и свойства $(12, 5)$ -конфигураций. Дискретная математика, **37**:1 (2025), 22–38.
- [14] Малышев Ф.М. Методы линейных и разностных соотношений в криптографии. Дискрет. матем. **34**:1 (2022), 36–63.
- [15] Гайфуллин А.А. О возможных группах симметрий 27-вершинных триангуляций многообразий, похожих на октавную проективную плоскость. Мат. сборник, **215**:7 (2024), 3-51.
- [16] Bagchi B., Datta B. On Künel's 9-vertex complex projective plane. Geom. Dedicata, **50**:1 (1994), 1-13.
- [17] Холл М. Комбинаторика. М.:Мир, 1970, 424 с.
- [18] Новиков Ф.А. Дискретная математика для программистов. СПб.: Питер, 2003, 304 с.
- [19] Понтрягин Л.С. Непрерывные группы. 4-е издание, М.: "Наука", 1984, 520 с.
- [20] Никулин В.В., Шафаревич И.Р. Геометрии и группы. М. "Наука", 1983, 240 с.
- [21] Магнус В., Каррас А., Солитер Д. Комбинаторная теория групп. М. "Наука", 1974, 456 с.
- [22] Серр Ж.-П. Деревья, амальгамы и SL_2 . Математика (сб. переводов), **18**:1 (1974), 3-51.
- [23] Харари Ф. Теория графов. М.: Мир, 1973, 302 с.