Math-Net.Ru

All Russian mathematical portal

I. T. Mukhametyanov, Associations scheme with nonconstant intersection numbers, associated with group $SL_2(q)$, *Sib. Èlektron. Mat. Izv.*, 2019, Volume 16, 648–672

DOI: <https://doi.org/10.33048/semi.2019.16.042>

Use of the all-Russian mathematical portal Math-Net.Ru implies that you have read and agreed to these terms of use

<http://www.mathnet.ru/eng/agreement>

Download details:

IP: 54.209.52.79

April 26, 2023, 14:57:09

СИБИРСКИЕ ЭЛЕКТРОННЫЕ МАТЕМАТИЧЕСКИЕ ИЗВЕСТИЯ

Siberian Electronic Mathematical Reports

<http://semr.math.nsc.ru>

Том 16, стр. 648–672 (2019)

DOI 10.33048/semi.2019.16.042

УДК 512.542, 519.172

MSC 20D15, 05C25

СХЕМА ОТНОШЕНИЙ С НЕПОСТОЯННЫМИ ЧИСЛАМИ ПЕРЕСЕЧЕНИЙ, АССОЦИИРОВАННАЯ С ГРУППОЙ $SL_2(q)$

И.Т. МУХАМЕТЬЯНОВ

ABSTRACT. Considered one of generalizations of association schemes, with variability of intersection numbers is allowed. Generalization of scheme is considered on set of elements of prime order p of group $SL_2(q)$ where q is a degree of p . Intersection numbers of this scheme are calculated and intersection arrays of it's graphs are found.

Keywords: association scheme, intersection numbers, group, distance-regular graph.

ВВЕДЕНИЕ

Пусть X – конечное множество и пусть $R_i (i = 0, 1, \dots, d)$ – бинарные отношения на X . $\mathfrak{X}(X) = (X, \{R_i\}_{0 \leq i \leq d})$ называется *схемой отношений на d классах*, если выполняются следующие условия:

- (1) $R_0 = \{(x, x) | x \in X\}$;
- (2) $X \times X = R_0 \cup R_1 \cup \dots \cup R_d$ и $R_i \cap R_j = \emptyset$ при $i \neq j$;
- (3) ${}^t R_{i'} = R_i$ для некоторого $i' \in \{0, 1, \dots, d\}$, где ${}^t R_i = \{(x, y) | (y, x) \in R_i\}$;
- (4) для любых $x, y \in X$ таких, что $(x, y) \in R_k$, число p_{ij}^k элементов z из X с условием $(x, z) \in R_i$ и $(z, y) \in R_j$, является постоянным ($i, j, k \in \{0, 1, \dots, d\}$).

Неотрицательные целые числа p_{ij}^k называются *числами пересечений* схемы $\mathfrak{X}(X)$.

Если выполнено условие

- (5) $p_{ij}^k = p_{ji}^k$ для всех $i, j, k \in \{0, 1, \dots, d\}$,

то схема $\mathfrak{X}(X)$ называется *коммутативной*. При выполнении условия

- (6) все отношения $R_i (i \in \{0, 1, \dots, d\})$ симметричны: ${}^t R_i = R_i$,

MUKHMETYANOV, I.T., ASSOCIATIONS SCHEME WITH NONCONSTANT INTERSECTION NUMBERS, ASSOCIATED WITH GROUP $SL_2(q)$.

© 2019 Мухаметьянов И.Т.

Поступила 9 апреля 2018 г., опубликована 17 мая 2019 г.

схема $\mathfrak{X}(X)$ называется *симметричной*.

Несколько обобщим это понятие, убрав условие (4). Тогда $\mathfrak{X}(X)$ назовём *схемой отношений на d классах с непостоянными числами пересечений*. "Подкорректировав" условие (5):

(5') $p_{ij}^k(x, y) = p_{ji}^k(x, y)$, где $p_{ij}^k(x, y)$ – число z из X таких, что $(x, z) \in R_i$ и $(z, y) \in R_j$ для $(x, y) \in R_k$,

и добавив его к условиям (1) – (3), получим *коммутативную схему отношений с непостоянными числами пересечений*. Если при этом выполнено условие (6), то её будем также называть *симметричной*.

Может оказаться, что для каких-то $i, j, k \in \{0, 1, \dots, d\}$ число $p_{ij}^k(x, y)$ не зависит от выбора пары $(x, y) \in R_k$. В этом случае в обозначении $p_{ij}^k(x, y)$ пару (x, y) будем опускать: $p_{ij}^k(x, y) = p_{ij}^k$.

В общем случае коммутативную схему отношений с непостоянными числами пересечений будем называть просто *схемой*. Так как речь в статье пойдёт исключительно о таких схемах, то путаницы с обычной схемой (с постоянными числами пересечений p_{ij}^k) не будет.

Графом i -го отношения схемы $\mathfrak{X}(X)$ называется граф $\Gamma^{(i)} = (X, R_i)$ ($0 \leq i \leq d$) с множеством вершин X и множеством рёбер R_i . Обозначим через n_i степень графа $\Gamma^{(i)}$.

В данной работе мы рассматриваем схему $\mathfrak{X}(X) = (X, \{R_i\}_{0 \leq i \leq d})$, обладающую следующими свойствами:

1. Схема $\mathfrak{X}(X)$ – симметричная.
2. Граф $\Gamma^{(1)}$ 1-го отношения является несвязным, каждая компонента связности которого является кликой из $d - 1$ точек. Обозначим эти клики через $K_1, K_2, \dots, K_{n+1}$ и назовём их *R_1 -кликами* схемы $\mathfrak{X}(X)$.
3. Если x – (произвольная) фиксированная точка некоторой R_1 -клики K_s , K_t – R_1 -клика, отличная от K_s , и y пробегает точки из K_t , то в $(x, y) \in R_i$ индекс i пробегает подмножество $I = \{2, 3, \dots, d\}$ индексов, которая определённым образом связана с группой $SL_2(q)$ ($q = p^m \geq 4$, p – простое число). А именно, в качестве X берём множества элементов порядка p (как всё множество, так и отдельный класс сопряжённости), на котором вводятся отношения R_i по правилу: $(x, x) \in R_0$, $(x, y) \in R_1 \Leftrightarrow yx^{-1}$ – элемент порядка p , $(x, y) \in R_i \Leftrightarrow yx^{-1} \in C_i$ или $yx^{-1} \in -X$ (здесь и ниже $-X$ – множество противоположных элементов к элементам из X (в кольце матриц размерности 2×2)), где C_i – фиксированный класс сопряжённых p' -элементов группы $SL_2(q)$. Нами вычисляются числа пересечений $p_{ij}^k(x, y)$ этой схемы и описываются параметры графов $\Gamma^{(i)}$ этих схем.

Назовём схему, удовлетворяющую условиям 1 и 2 (но не обязательно связанную с группой $SL_2(q)$), *кликковой*. Если она удовлетворяет всем трём условиям, то назовём её *равномерно кликковой относительно множества I* .

Отметим, что в работе [1] фактически дано описание графов $\Gamma^{(i)}$ схем, связанных с группой $SL_2(2^m) \simeq L_2(2^m)$. В работе [2] дано описание графа $\Gamma^{(i)}$, связанного с группой $L_2(p^m)$ при нечётном $p^m \geq 5$ для отдельно взятого индекса i , соответствующего классу C_i инволюций группы $L_2(p^m)$. Наконец, в работе [3] дано описание индуцированных подграфов графов $\Gamma^{(i)}$ на отдельном классе сопряжённых элементов порядка p , связанных с группой $L_2(p^m)$ при нечётном $p^m \geq 5$ для произвольного i .

1. ПРЕДВАРИТЕЛЬНЫЕ СВЕДЕНИЯ И ФОРМУЛИРОВКА ОСНОВНЫХ РЕЗУЛЬТАТОВ

Всюду в статье $q = p^m \geq 4$, p – простое число. Далее, $C_G(g) = \{x \in G | gx = xg\}$ – централизатор элемента g в группе G , $Z(G) = \{z \in G | zx = xz \quad \forall x \in G\}$ – центр группы G , $o(g)$ – порядок элемента g группы (поля), e – единица группы G .

Также напомним, что $\left(\frac{a}{q}\right)$ – символ Лежандра – это 1 или -1 в зависимости от того, разрешимо или нет квадратное уравнение $x^2 = a$ в поле F_q при $a \neq 0$. При этом, если $\left(\frac{a}{q}\right) = 1$, то a называется *квадратичным вычетом* поля F_q . Если $\left(\frac{a}{q}\right) = -1$, то a – *квадратичный невычет* поля F_q . Множество квадратичных вычетов поля F_q будем обозначать через F_q^2 .

Ясно, что граф отношения симметричной схемы является неориентированным без петель и кратных рёбер, так что мы рассматриваем неориентированные графы без петель и кратных рёбер.

Если вершины x и y графа лежат на расстоянии i друг от друга, то этот факт будем обозначать через $d(x, y) = i$. Для вершины x графа Γ через $\Gamma_i(x)$ обозначим i -окрестность вершины x , то есть подграф, индуцированный Γ на подмножестве всех вершин, находящихся на расстоянии i от x . *Окрестность вершины* – её 1-окрестность. Положим $\Gamma_1(x) = \Gamma(x) = [x]$ – окрестность вершины x , $x^\perp = \{x\} \cup \Gamma(x)$ – *замкнутая окрестность* вершины x . Через Γ_i обозначим граф i -расстояний графа Γ , то есть граф с множеством вершин Γ , в котором две вершины соединены ребром тогда и только тогда, когда они находятся в Γ на расстоянии i .

Регулярный граф степени k – это граф, степени вершин которого равны одному и тому же числу k . *Сильно регулярный граф с параметрами (v, k, λ, μ)* – это регулярный граф, любая пара смежных вершин которого имеет постоянное число λ общих соседей и любая пара несмежных вершин имеет постоянное число μ общих соседей.

Если вершины x и y регулярного графа Γ находятся на расстоянии i друг от друга, то через $a_i(x, y)$, $b_i(x, y)$, $c_i(x, y)$ обозначим число вершин соответственно в пересечениях $\Gamma_i(x) \cap \Gamma(y)$, $\Gamma_{i+1}(x) \cap \Gamma(y)$, $\Gamma_{i-1}(x) \cap \Gamma(y)$. Назовём их *числами пересечений графа Γ* .

Если числа пересечений не зависят от выбора вершин x и y (а зависят только от выбора расстояния $i = d(x, y)$) то они обозначаются соответственно через a_i , b_i , c_i , граф называется *дистанционно регулярным с массивом пересечений* $\{b_0, b_1, \dots, b_{d-1}; c_1, c_2, \dots, c_d\}$. Числа пересечений a_i , b_i , c_i связаны соотношением $a_i + b_i + c_i = b_0$, при этом $b_0 = k$ – степень графа, $c_1 = 1$. Ясно, что дистанционно регулярный граф диаметра 2 – это связный сильно регулярный граф.

Очевидно, в регулярном графе i -окрестность $\Gamma_i(x)$ вершины x "распадается" на классы $Y_{i1}(x)$, $Y_{i2}(x)$, $\dots$, $Y_{i,s(i)}(x)$ вершин y с одинаковыми значениями $a_i(x, y)$, $b_i(x, y)$, $c_i(x, y)$. При этом может оказаться, что для любой вершины x и любого i число таких классов одинаково, и для каждой x их можно проиндексировать так, чтобы для различных x_1 и x_2 из того, что $y_1 \in Y_{ij}(x_1)$ и $y_2 \in Y_{ij}(x_2)$ вытекало $a_i(x_1, y_1) = a_i(x_2, y_2)$, $b_i(x_1, y_1) = b_i(x_2, y_2)$, $c_i(x_1, y_1) = c_i(x_2, y_2)$. Такой граф назовём *почти дистанционно регулярным*. Упорядоченный набор

$$\{b_0(x, y), b_1(x, y), \dots, b_{d-1}(x, y); c_1(x, y), c_2(x, y), \dots, c_d(x, y)\}$$

– массив пересечений почти дистанционно регулярного графа.

Вообще говоря, корректнее было бы в массиве пересечений почти дистанционно регулярного графа воспользоваться обозначениями типа $b_i(x, y_i)$, $c_i(x, y_i)$, так как в числах пересечений для разных i вершины y различны. Но для удобства будем придерживаться обозначений $b_i(x, y)$, $c_i(x, y)$.

Лемма 1.1. *Вершинно-транзитивный граф является почти дистанционно регулярным. В частности, если Γ – граф с множеством вершин $V = g^G \cup (g^{-1})^G$ и множеством рёбер $\{\{x, y\} | xy^{-1} \in h^G \cup (h^{-1})^G\}$, где g^G и h^G некоторые классы сопряжённых элементов произвольной группы G , то Γ – почти дистанционно регулярный.*

Доказательство. См. [2], лемма 1. □

Антиподальный дистанционно регулярный граф диаметра 3 – это дистанционно регулярный граф, множество вершин которого разбивается на классы эквивалентности отношением $\sim$, определённым по правилу: $x \sim y$ тогда, и только тогда, когда $d(x, y) = 3$ или $x = y$. Класс $\bar{x}$ называется *антиподальным*. Известно, что если $\bar{x}$ – фиксированный класс антиподального графа с $\lambda = \mu$, то $|\bar{x}| = (k-1)/\mu$, имеется в точности $k+1$ антиподальных классов (см. [4]), если $\bar{x} = \{x_1, x_2, \dots, x_{(k-1)/\mu}\}$, то $x_1^\perp, x_2^\perp, \dots, x_{(k-1)/\mu}^\perp$ попарно не пересекаются и их объединение образует множество вершин всего графа. Такой граф имеет массив пересечений $\{k, k-\mu-1, 1; 1, \mu, k\}$.

Граф $x^\perp$ называется *т-мельницей*, если он является объединением t треугольников с единственной общей вершиной x .

Граф $x^\perp$ называется *т-пирамидой*, если $\Gamma(x)$ является простым циклом длины t . Этот цикл назовём *основанием* пирамиды. Граф $x^\perp$ называется *связкой пирамид* с общей вершиной x , если $\Gamma(x)$ есть объединение изолированных простых циклов. Граф $x^\perp$ называется *т-звездой* с центром x , если $\Gamma(x)$ является t -кликкой.

Кодом в графе Γ с множеством вершин V называется непустое подмножество C из V . Число $\delta(C) = \min\{d(x, y) | x, y \in C, x \neq y\}$ при $|C| \neq 1$ называется *минимальным расстоянием* в C . Расстояние от $x \in V$ до C – это число $d(x, C) = \min\{d(x, y) | y \in C\}$, а число $r(C) = \max\{d(x, C) | x \in V\}$ называется *радиусом накрытия*. Минимальное расстояние в C и радиус накрытия связаны неравенством $\delta(C) \leq 2r(C) + 1$ (см. [4], с.345), равенство имеет место тогда и только тогда, когда шары радиуса $r(C)$ с центром в точках C образует разбиение V . Код с таким свойством называется *совершенным*.

Пусть $\mu \in \{1, 2\}$. *Обобщённым икосаэдром с параметрами q и μ* назовём граф $I(q, \mu)$ со следующими свойствами:

1. Граф состоит из $(q^2 - 1)/\mu$ вершин.
2. При $\mu = 2$ замкнутая окрестность любой вершины графа является связкой из p^{m-1} p -пирамид. При $\mu = 1$ замкнутая окрестность любой вершины графа является 2^{m-1} -мельницей.
3. Для любой вершины g графа в нём существует совершенный код $C(g)$ накрывающего радиуса 1, содержащий g .
4. Для любых вершин x, y из $C(g)$ любая вершина $u \in \Gamma(x)$ смежна в точности с μ вершинами из $\Gamma(y)$.

Наряду с обобщённым икосаэдром будем рассматривать *псевдоикосаэдр* $PI(q)$ с параметром q со следующими свойствами:

1. Граф состоит из $q^2 - 1$ вершин.
2. Замкнутая окрестность любой вершины графа является q -звездой.
3. Для любой вершины g графа в нём существует совершенный код $C(g)$ накрывающего радиуса 1, содержащий g .
4. Множество V вершин графа $\Gamma = PI(q)$ разбивается на два подмножества V_1 и V_2 таких, что для любой вершины $g \in V$ в точности половина элементов из $C(g)$ лежит в V_1 , а другая половина – в V_2 , при этом для любых $x \in V_1 \cap C(g)$ и $y \in V_2 \cap C(g)$ любая вершина $u \in \Gamma(x)$ смежна в точности с двумя вершинами из $\Gamma(y)$, любая вершина из $\Gamma(y)$ смежна в точности с двумя вершинами из $\Gamma(x)$, и для любых $x, z \in V_s \cap C(g)$ ($s = 1, 2$) никакая вершина из $\Gamma(x)$ не смежна с вершинами из $\Gamma(z)$.

Назовём подмножества V_1 и V_2 графа $PI(q)$ *половинками множества вершин* $PI(q)$.

Предложение 1. *Справедливы следующие утверждения:*

1. Граф $I(q, \mu)$ является дистанционно регулярным графом диаметра 3 с массивом пересечений $\{q, q - \mu - 1, 1; 1, \mu, q\}$.
2. $PI(q)$ является почти дистанционно регулярным (но не дистанционно регулярным) с массивом пересечений $\{q, q - 1, q - 2, b_3(x, y); 1, 2, c_3(x, y), q\}$, где

$$b_3(x, y) = \begin{cases} 0, & \text{если } y \in C(x), \\ 1, & \text{если } y \notin C(x), \end{cases} \quad c_3(x, y) = \begin{cases} q, & \text{если } y \in C(x), \\ q - 1, & \text{если } y \notin C(x). \end{cases}$$

При этом граф 2-расстояний псевдокосаэдра $PI(q)$ имеет в точности две компоненты связности, каждая из которых является сильно регулярным графом с параметрами $((q^2 - 1)/2, q(q - 1)/2, (q - 1)^2/2, q(q - 1)/2)$.

Доказательство. См. в [1], предложение 1, и [2], теорема 1. □

Нам потребуется информация о классах сопряжённых элементов группы $G = SL_2(q)$, которую мы почерпнём из [5], где она приведена, в свою очередь, со ссылкой на [6].

При $q = 2^m$ – чётном в $G \simeq L_2(q)$ имеются следующие классы сопряжённых элементов:

- 1) $C_0 = \{e\}$;
- 2) C_1 – класс инволюций;
- 3) $X_i = (x^i)^G$, где $o(x) = q - 1$, $1 \leq i \leq q/2 - 1$ (всего $q/2 - 1$ классов), $X_i^{-1} = X_i$ для всех $i \in \{1, 2, \dots, q/2 - 1\}$;
- 5) $Y_j = (y^j)^G$, где $o(y) = q + 1$, $1 \leq j \leq q/2$ (всего $q/2$ классов), $Y_j^{-1} = Y_j$ для всех $j \in \{1, 2, \dots, q/2\}$.

При q нечётном в G имеются следующие классы сопряжённых элементов:

- 1) $C_0 = \{e\}$; $C_1 = \{z\}$, $z \in Z(G) \setminus \{e\}$;
- 2) C_2, C_3 – два класса сопряжённых неединичных p -элементов, и если $q \equiv 1 \pmod{4}$, то $C_2^{-1} = C_2$ и $C_3^{-1} = C_3$, а если $q \equiv -1 \pmod{4}$, то $C_2^{-1} = C_3$ и $C_3^{-1} = C_2$;
- 3) $C_4 = zC_2$, $C_5 = zC_3$ – два класса сопряжённых неединичных элементов порядка $2p$;
- 4) $X_i = (x^i)^G$, где $o(x) = q - 1$, $1 \leq i \leq (q - 3)/2$, $X_i^{-1} = X_i$ для всех $i \in \{1, 2, \dots, (q - 3)/2\}$;
- 5) $Y_j = (y^j)^G$, где $o(y) = q + 1$, $1 \leq j \leq (q - 1)/2$, $Y_j^{-1} = Y_j$ для всех $j \in \{1, 2, \dots, (q - 1)/2\}$.

Обозначим множество индексов у X_i через I_1 , а множество индексов у Y_j — через I_2 .

Следующие **леммы 1.2** и **1.3** дают описание параметрами множество X неединичных p -элементов, классов сопряжённых неединичных p -элементов и классов p' -элементов X_i ($i \in I_1$), Y_j ($j \in I_2$) группы $G = SL_2(p^m)$.

Лемма 1.2. *Множество X неединичных p -элементов группы $SL_2(q)$ задаётся равенствами*

$$X = \left\{ \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix} \middle| \alpha \in F_q^* \right\} \cup \left(\bigcup_{i=1}^q \left\{ \begin{pmatrix} 1 - \beta\delta_i & -\beta\delta_i^2 \\ \beta & 1 + \beta\delta_i \end{pmatrix} \middle| \beta \in F_q^* \right\}, \delta_i \in F_q \right), \quad (1.1)$$

$$X = \left\{ \begin{pmatrix} 1 & 0 \\ \beta & 1 \end{pmatrix} \middle| \beta \in F_q^* \right\} \cup \left(\bigcup_{i=1}^q \left\{ \begin{pmatrix} 1 + \alpha\delta_i & \alpha \\ -\alpha\delta_i^2 & 1 - \alpha\delta_i \end{pmatrix} \middle| \alpha \in F_q^* \right\}, \delta_i \in F_q \right). \quad (1.2)$$

При этом при $p = 2$ X образует один класс сопряжённых инволюций группы G , а при $p \neq 2$ X образует два класса сопряжённых элементов C_2 и C_3 , и если в качестве класса, который содержит $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, взять C_2 , то C_2 и C_3 определяются равенствами

$$\begin{aligned} C_2 &= \left\{ \begin{pmatrix} 1 & \alpha^2 \\ 0 & 1 \end{pmatrix} \middle| \alpha \in F_q^* \right\} \cup \left(\bigcup_{i=1}^q \left\{ \begin{pmatrix} 1 + \beta^2\delta_i & \beta^2\delta_i^2 \\ -\beta^2 & 1 - \beta^2\delta_i \end{pmatrix} \middle| \beta \in F_q^* \right\}, \delta_i \in F_q \right) = \\ &= \left\{ \begin{pmatrix} 1 & 0 \\ -\beta^2 & 1 \end{pmatrix} \middle| \beta \in F_q^* \right\} \cup \left(\bigcup_{i=1}^q \left\{ \begin{pmatrix} 1 + \alpha^2\delta_i & \alpha^2 \\ -\alpha^2\delta_i^2 & 1 - \alpha^2\delta_i \end{pmatrix} \middle| \alpha \in F_q^* \right\}, \delta_i \in F_q \right), \\ C_3 &= \left\{ \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix} \middle| \alpha \in F_q \setminus F_q^2 \right\} \cup \left(\bigcup_{i=1}^q \left\{ \begin{pmatrix} 1 - \beta\delta_i & -\beta\delta_i^2 \\ \beta & 1 + \beta\delta_i \end{pmatrix} \middle| \beta \in F_q \setminus F_q^2 \right\}, \delta_i \in F_q \right) = \\ &= \left\{ \begin{pmatrix} 1 & 0 \\ -\beta & 1 \end{pmatrix} \middle| \beta \in F_q \setminus F_q^2 \right\} \cup \left(\bigcup_{i=1}^q \left\{ \begin{pmatrix} 1 + \alpha\delta_i & \alpha \\ -\alpha\delta_i^2 & 1 - \alpha\delta_i \end{pmatrix} \middle| \alpha \in F_q \setminus F_q^2 \right\}, \delta_i \in F_q \right). \end{aligned}$$

В частности, $\begin{pmatrix} 1 - \beta\delta_i & -\beta\delta_i^2 \\ \beta & 1 + \beta\delta_i \end{pmatrix}$ и $\begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}$ лежат в одном классе сопряжённости тогда и только тогда, когда α и $-\beta$ одновременно либо квадратичные вычеты, либо таковыми не являются. Аналогично с парой элементов $\begin{pmatrix} 1 + \alpha\delta_i & \alpha \\ -\alpha\delta_i^2 & 1 - \alpha\delta_i \end{pmatrix}$ и $\begin{pmatrix} 1 & 0 \\ -\beta & 1 \end{pmatrix}$.

Доказательство. Для $p = 2$ см. в [1], **лемма 1**. При $p \neq 2$ эта **лемма** фактически доказана в [2] (**лемма 4**), только для группы $L_2(q) = G/Z(G)$. Доказательство дословно, но мы здесь приведём некоторые фрагменты доказательства по причине, что в упомянутое по вине автора вкрались досадные опечатки.

Прежде всего, доказано, что если X — множество неединичных p -элементов группы $L_2(q)$, q — нечётно, то имеем равенства

$$\begin{aligned} X &= \left\{ \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix} \middle| \alpha \in F_q^* \right\} \cup \left(\bigcup_{i=1}^q \left\{ \begin{pmatrix} 1 - \beta\delta_i & -\beta\alpha_i^2 \\ \beta & 1 + \beta\alpha_i \end{pmatrix} \middle| \beta \in F_q^* \right\}, \alpha_i \in F_q \right), \\ X &= \left\{ \begin{pmatrix} 1 & 0 \\ \beta & 1 \end{pmatrix} \middle| \beta \in F_q^* \right\} \cup \left(\bigcup_{i=1}^q \left\{ \begin{pmatrix} 1 + \alpha\delta_i & \alpha \\ -\alpha\delta_i^2 & 1 - \alpha\delta_i \end{pmatrix} \middle| \alpha \in F_q^* \right\}, \delta_i \in F_q \right). \end{aligned}$$

Далее, если $g = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $a = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix}$, где α – ненулевой элемент поля F_q , то $aga^{-1} = \begin{pmatrix} 1 & \alpha^2 \\ 0 & 1 \end{pmatrix}$ и

$$\begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & \alpha^2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 1 - \alpha^2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -\alpha^2 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}.$$

Поэтому при нечётном q для произвольного $\alpha \in F_q^*$ имеем, что $\begin{pmatrix} 1 & \alpha^2 \\ 0 & 1 \end{pmatrix}$ и $\begin{pmatrix} 1 & 0 \\ -\alpha^2 & 1 \end{pmatrix}$ лежат в C_2 (это и есть уточнение доказательства **Леммы**). Равенства для C_3 очевидным образом вытекают из того, что в C_2 попадают те матрицы из X , для которых в равенствах (1.1) и (1.2) α и $-\beta$ являются квадратичными вычетами. Значит, в C_3 попадают те, в которых α и $-\beta$ являются квадратичными невычетами.

Лемма доказана. $\square$

Элементы вида $\begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}$ будем называть *элементами первого типа* по отношению к $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$, а элементы вида $\begin{pmatrix} 1 - \beta\delta_i & -\beta\alpha_i^2 \\ \beta & 1 + \beta\alpha_i \end{pmatrix}$ – *элементами второго типа* (по отношению к $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$). Аналогично, элементы $\begin{pmatrix} 1 & 0 \\ \beta & 1 \end{pmatrix}$ и $\begin{pmatrix} 1 + \alpha\delta_i & \alpha \\ -\alpha\delta_i^2 & 1 - \alpha\delta_i \end{pmatrix}$ – элементы соответственно *первого* и *второго типов* по отношению к $\begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix}$.

Лемма 1.3. Если $i \in I_1$, то класс X_i состоит из матриц вида

$$\begin{pmatrix} \gamma^i x_{11} x_{22} - \gamma^{-i} x_{12} x_{21} & (\gamma^i - \gamma^{-i}) x_{12} x_{22} \\ (\gamma^{-i} - \gamma^i) x_{11} x_{21} & \gamma^{-i} x_{11} x_{22} - \gamma^i x_{12} x_{21} \end{pmatrix},$$

где γ – первообразный элемент поля F_q , $\begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix} \in SL_2(q)$, а если $i \in I_2$, то класс Y_i состоит из матриц вида

$$\begin{pmatrix} \gamma^{i(q-1)} x_{11} x_{22} - \gamma^{-i(q-1)} x_{12} x_{21} & (\gamma^{i(q-1)} - \gamma^{-i(q-1)}) x_{12} x_{22} \\ (\gamma^{-i(q-1)} - \gamma^{i(q-1)}) x_{11} x_{21} & \gamma^{-i(q-1)} x_{11} x_{22} - \gamma^{i(q-1)} x_{12} x_{21} \end{pmatrix},$$

где γ – первообразный элемент поля F_{q^2} , $\begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix} \in SL_2(q^2)$.

Доказательство. Хорошо известно (впрочем, это – очевидный факт), что если γ – первообразный элемент поля F_q , то $g = \begin{pmatrix} \gamma & 0 \\ 0 & \gamma^{-1} \end{pmatrix}$ – элемент порядка $q-1$ из $SL_2(q)$.

Пусть $x = \begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix} \in SL_2(q)$. Тогда имеем

$$\begin{aligned}
x^{-1}g^ix &= \begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix}^{-1} \begin{pmatrix} \gamma^i & 0 \\ 0 & \gamma^{-i} \end{pmatrix} \begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix} = \\
&= \begin{pmatrix} x_{22} & -x_{12} \\ -x_{21} & x_{11} \end{pmatrix} \begin{pmatrix} \gamma^i & 0 \\ 0 & \gamma^{-i} \end{pmatrix} \begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix} = \\
&= \begin{pmatrix} \gamma^i x_{11} x_{22} - \gamma^{-i} x_{12} x_{21} & (\gamma^i - \gamma^{-i}) x_{12} x_{22} \\ (\gamma^{-i} - \gamma^i) x_{11} x_{21} & \gamma^{-i} x_{11} x_{22} - \gamma^i x_{12} x_{21} \end{pmatrix} \in (g^i)^G.
\end{aligned}$$

Поэтому утверждение леммы относительно состава X_i доказано.

Далее, если γ – первообразный элемент поля F_{q^2} , то $u = \begin{pmatrix} \gamma^{q-1} & 0 \\ 0 & \gamma^{-(q-1)} \end{pmatrix}$

– элемент порядка $q+1$ группы $SL_2(q^2)$,

$$u^j = \begin{pmatrix} \gamma^{q-1} & 0 \\ 0 & \gamma^{-(q-1)} \end{pmatrix}^j = \begin{pmatrix} \gamma^{j(q-1)} & 0 \\ 0 & \gamma^{-j(q-1)} \end{pmatrix}$$

– элемент из $SL_2(q^2)$, порядок которого делит $q+1$. Ясно, что если $K_i = (g^i)^G$ – класс сопряжённых элементов группы $SL_2(q^2)$, порядки которых делят q^2-1 , $o(g) = q^2-1$, $i \in I(q^2)$, где $I(q^2)$ – множество индексов классов элементов группы $SL_2(q^2)$, порядки которых делят q^2-1 , то $\bigcup_{j \in I_2} Y_j \subseteq \bigcup_{i \in I(q^2)} K_i$. Поэтому утверждение леммы относительно состава Y_j также доказано, и лемма доказана полностью. $\square$

Всюду ниже в символ γ мы вкладываем смысл, вложенный в **лемме 1.3**. При этом в γ^{is} и γ^{-is} полагаем $s=1$, если $i \in I_1$ и $s=q-1$, если $i \in I_2$ и, наоборот, $i \in I_1$, если $s=1$ и $i \in I_2$, если $s=q-1$, а $\gamma \in F_q$ или $\gamma \in F_{q^2}$, будет ясно из контекста или оговорено особо.

Заметим, что силовские p -подгруппы группы G попарно пересекаются тривиально, так как если $P = \left\{ \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix} \middle| \alpha \in F_q \right\}$ и $Q = \left\{ \begin{pmatrix} 1 & 0 \\ \beta & 1 \end{pmatrix} \middle| \beta \in F_q \right\}$ – элементы множества $Syl_p(G)$ силовских p -подгрупп группы G , для $x = \begin{pmatrix} 1 & 0 \\ \delta & 1 \end{pmatrix}$ $P^x = \left\{ \begin{pmatrix} 1 + \alpha\delta & \alpha \\ -\alpha\delta^2 & 1 - \alpha\delta \end{pmatrix} \middle| \alpha \in F_q \right\}$, то $Syl_p(G) = \{Q\} \cup \{P^x | x \in Q\}$, и непосредственно проверяется, что $Q \cap P^x = \{e\}$ и $P^x \cap P^y = \{e\}$ для $x \neq y \in Q$. Аналогично, $Syl_p(G) = \{P\} \cup \{Q^y | y \in P\}$. В частности, $S \in Syl_p(G)$ действует транзитивно на $Syl_p(G) \setminus \{S\}$.

За обозначениями P и Q закрепим обозначения упомянутых силовских подгрупп. Также положим $P^\# = P \setminus \{e\}$ и $Q^\# = Q \setminus \{e\}$.

Введём параллельную индексацию классов элементов группы G , порядки которых делят $q \pm 1$, положив $K_{1+i} = X_i$ для $i \in I_1$, и $K_{q/2+j} = Y_j$, или $K_{(q-1)/2+j} = Y_j$ для $j \in I_2$ в зависимости от того, q чётно или нечётно. Кроме того положим $K_1 = X$, а при нечётном q также положим $K_q = -X$. Наконец, при чётном q положим $I = \{2, 3, \dots, q\}$, а при нечётном q положим $I = \{2, 3, \dots, q-1\}$ и $J = I \cup \{q\}$. При этом кроме обозначения $i \in I$ ($i \in J$) будем применять обозначение $i_s \in I$ ($i_s \in J$), что будет означать $i_s = 1+i$ с $i \in I_1$, либо $i_s = 1 + |I_1| + i$ с $i \in I_2$, либо $i_s = q$. Для удобства при чётном q также положим $J = I$, так что в любом случае $|J| = q-1$.

Таким образом, мы будем применять двойную систему индексации одной и той же фиксированной системы нормальных подмножеств группы G . Множество индексов первой системы – это $\{0, 1\} \cup I_1 \cup I_2$ при чётном q , и $\{0, 1\} \cup I_1 \cup I_2 \cup \{q\}$ при нечётном q , а множество индексов второй системы – это $\{0, 1\} \cup J$. При этом договоримся обозначать классы K_i как при $i \in I_1 \cup I_2 \cup \{q\}$, так и при $i \in J$, одинаково.

Определим на X отношения $R_i (0 \leq i \leq q)$ по следующему правилу:

- 1) для любого $x \in X$ положим $(x, x) \in R_0$;
- 2) для любых x и y из одной и той же силовой p -подгруппы положим $(x, y) \in R_1$ (что равносильно $yx^{-1} \in X = K_1$);
- 3) для $i \in \{2, 3, \dots, q\}$ положим $(x, y) \in R_i \Leftrightarrow yx^{-1} \in K_i$.

Условимся, что для отношений R_i тоже будем применять двойную систему индексации. Например, в формулировке **теоремы 1** (ниже) используется вторая система индексации, а в формулировке **теоремы 2** – первая, в формулировке **теоремы 3** – обе. Наконец, будем применять обозначение как $(x, y) \in R_i$, так и $\{x, y\} \in R_i$. В первом случае – это пара (x, y) , находящаяся в отношении R_i , во втором – это ребро $\{x, y\}$, лежащее во множестве рёбер R_i . В любом случае из контекста будет ясно, что обозначает R_i – отношение или множество рёбер.

Напомним, что n_i – степень графа $\Gamma^{(i)}$. Напомним также, что δ_{ij} (равный 1 или 0 в зависимости от того, $i = j$ или $i \neq j$) – символ Кронекера.

Пусть q – нечётно, $(x, y) \in R_i$. Если при этом x и y сопряжены, то индекс i назовём *индексом первого типа* (для пары (x, y)), а если x и y не сопряжены, то индекс i назовём *индексом второго типа* (для пары (x, y)). Корректность этих понятий вытекает из **лемм 2.1 – 2.3**.

Говоря о типах индексов в числах пересечений p_{ij}^k , мы имеем в виду типы для соответствующих пар. Так, говоря о типе индекса k мы имеем в виду для пар $(x, y) \in R_k$, а говоря о типах индексов i и j , мы имеем в виду пары $(x, z) \in R_i$ и $(z, y) \in R_j$.

Пусть $\mathfrak{X}(X)$ – схема на множестве X элементов порядка p группы $SL_2(q)$, и с отношениями, введёнными выше.

Нами доказаны следующие теоремы:

Теорема 1. *Схема $\mathfrak{X}(X)$ является равномерно кликовой относительно подмножества индексов J , коммутативной с q классами со следующими числами пересечений:*

- 1) $p_{0j}^k = \delta_{jk}$, $p_{i0}^k = \delta_{ik}$, $p_{ij}^0 = n_i \delta_{ij}$, где $n_i = \begin{cases} q-2, & \text{если } i = 1, \\ q, & \text{если } i \in J. \end{cases}$
- 2) $p_{11}^k = p_{1k}^1 = p_{k1}^1 = \begin{cases} q-3, & \text{если } k = 1, \\ 0, & \text{если } k \in J. \end{cases}$
- 3) $p_{ii}^1 = 0$ для любого $i \in J$, и для любых i и j из J число $p_{ij}^1(x, y)$ зависит от выбора элементов x и y , и $p_{ij}^1(x, y) \in \{0, q\}$.
- 4) Если q – чётно, то для любых i, j и k из J имеет место равенство $p_{ij}^k = 1$.

Далее, пусть q – нечётно, i, j и k – произвольные индексы из J . Тогда если k – индекс первого типа, то

$$p_{ij}^k = \begin{cases} 2, & \text{если } i \text{ и } j - \text{индексы одного типа,} \\ 0, & \text{если } i \text{ и } j - \text{индексы разных типов.} \end{cases}$$

Если k – индекс второго типа, то

$$p_{ij}^k = \begin{cases} 0, & \text{если } i \text{ и } j - \text{индексы одного типа,} \\ 2, & \text{если } i \text{ и } j - \text{индексы разных типов.} \end{cases}$$

В частности, если x и y лежат в одном классе сопряжённых элементов, то для любых $i, k \in J$ имеет место равенство $p_{ii}^k = 2$, а если x с y лежат в разных классах сопряжённости, то $p_{ii}^k = 0$.

Теорема 2. Если q – чётное, то для любого $i \in I_1 \cup I_2$ граф $\Gamma^{(i)}$ i -го отношения схемы $\mathfrak{X}(X)$ является дистанционно регулярным с массивом пересечений $\{q, q-2, 1; 1, 1, q\}$.

Если q – нечётно, то в следующих случаях для $i \in I_1 \cup I_2 \cup \{q\}$ граф $\Gamma^{(i)}$ i -го отношения схемы $\mathfrak{X}(X)$ является несвязным с двумя компонентами – дистанционно регулярными графами с одинаковыми массивами пересечений $\{q, q-3, 1; 1, 2, q\}$:

- 1) $i \in I_1$ – чётное;
- 2) $i \in I_2$ – нечётное;
- 3) при $q \equiv 1 \pmod{4}$ $i = q$.

При нечётном q в следующих случаях для $i \in I_1 \cup I_2 \cup \{q\}$ граф $\Gamma^{(i)}$ является почти дистанционно регулярным (но не дистанционно регулярным) со следующими массивами пересечений $\{q, q-1, q-2, b_3(x, y); 1, 2, c_3(x, y), q\}$, где

$$b_3(x, y) = \begin{cases} 0, & \text{если } y \in C_G(x), \\ 1, & \text{если } y \notin C_G(x), \end{cases} \quad c_3(x, y) = \begin{cases} q, & \text{если } y \in C_G(x), \\ q-1, & \text{если } y \notin C_G(x) : \end{cases}$$

- 1) $i \in I_1$ – нечётное;
- 2) $i \in I_2$ – чётное;
- 3) при $q \equiv -1 \pmod{4}$ $i = q$.

При этом граф 2-расстояний графа $\Gamma^{(i)}$ имеет в точности две компоненты связности, каждая из которых является сильно регулярным графом с параметрами $((q^2-1)/2, q(q-1)/2, (q-1)^2/2, q(q-1)/2)$.

Теорема 3. Если q нечётно, то для того, чтобы отношения R_i определяли схему отношений $\mathfrak{X}(C)$ на отдельном классе C сопряжённых элементов порядка p группы $SL_2(q)$, необходимо и достаточно, чтобы индексы $i \in I_1 \cup I_2 \cup \{q\}$ удовлетворяли одному из следующих условий:

- (i) $i \in I_1$ – чётное;
- (ii) $i \in I_2$ – нечётное;
- (iii) $i = q$ и $q \equiv 1 \pmod{4}$.

При этом схема $\mathfrak{X}(C)$ имеет следующие числа пересечений:

- 1) $p_{0j}^k = \delta_{jk}$, $p_{i0}^k = \delta_{ik}$, $p_{ij}^0 = n_i \delta_{ij}$, где $n_i = \begin{cases} (q-3)/2, & \text{если } i = 1, \\ q, & \text{если } i \in J. \end{cases}$
- 2) $p_{11}^k = p_{1k}^1 = p_{k1}^1 = \begin{cases} (q-5)/2, & \text{если } k = 1, \\ 0, & \text{если } k \in J. \end{cases}$
- 3) $p_{ii}^1 = 0$ для любого $i \in J$, и для любых i и j из J число $p_{ij}^1(x, y)$ зависит от выбора элементов x и y , и $p_{ij}^1(x, y) \in \{0, q\}$.
- 4) $p_{ij}^k = 2$ для любых i, j и k из J .

Наконец, для любого $i \in I_1 \cup I_2 \cup \{q\}$ граф $\Gamma^{(i)}$ i -го отношения схемы $\mathfrak{X}(C)$ является дистанционно регулярным с массивом пересечений $\{q, q-3, 1; 1, 2, q\}$.

Мы не касаемся вопроса изоморфизма упомянутых в теоремах дистанционно регулярных графов ранее построенным, например, в [2] и [4]. Отметим лишь, что в свете [7] мы не сомневаемся в этом изоморфизме.

Нам потребуется определённый анализ некоторых уравнений и их систем над полем F_q . В частности, уравнений $x^2 = a$ и

$$\gamma^{js} + \gamma^{-js} = 2 - \alpha x, \quad (1.3)$$

в котором будем предполагать, что α – элемент поля F_q , γ – первообразный элемент поля F_q или F_{q^2} в зависимости от того, $s = 1$ или $s = q - 1$.

Хорошо известна следующая

Лемма 1.4. *Если q – чётно, то квадратное уравнение $x^2 = a$ в поле F_q для любого a имеет единственное решение. Если q – нечётно, то имеет место равенство $a^{(q-1)/2} = \left(\frac{a}{q}\right)$. Другими словами, квадратное уравнение $x^2 = a$ в поле F_q разрешимо тогда и только тогда, когда $a^{(q-1)/2} = 1$. При этом при наличии решения для ненулевого a их имеется в точности два.*

Если a и b одновременно являются либо не являются квадратичными вычетами поля F_q , то будем говорить, что a и b имеют одинаковый тип квадратичности. В противном случае они имеют разный тип квадратичности.

Напоминаем, что q – это степень простого числа. Оно может быть как чётным, так и нечётным. Поэтому, когда речь заходит о квадратичных вычетах поля F_q (в частности, о типах квадратичности элементов поля), то автоматически будем подразумевать, что q – нечётное. Так, в первой части **леммы 1.5** речь идёт о поле для произвольного q , а во второй части – для нечётного q .

Лемма 1.5. *Если $1 \leq j \leq (q-1)/2$, то $\gamma^{js} + \gamma^{-js} \in F_q$ и уравнение (1.3) в поле F_q имеет единственное решение, которое является ненулевым. При этом $\gamma^{js} + \gamma^{-js} - 2$ – квадратичный вычет поля F_q тогда и только тогда, когда $j \in I_1$ – чётное или $j \in I_2$ – нечётное.*

Доказательство. Напоминаем, что α – элемент поля F_q , и речь идёт о решении уравнения (1.3) в поле F_q .

Ясно, что $x = -\alpha^{-1}(\gamma^{js} + \gamma^{-js} - 2)$ – единственное решение уравнения (1.3), и оно ненулевое тогда и только тогда, когда $\gamma^{js} + \gamma^{-js} - 2 \neq 0$. То, что x – ненулевое решение, при чётном q вытекает из того, что $\gamma^{js} + \gamma^{-js} - 2 = \gamma^{js} + \gamma^{-js}$ и γ – первообразный элемент поля F_q . А то, что при нечётном q и при $1 \leq j \leq (q-1)/2$ имеет место условие $\gamma^{js} + \gamma^{-js} - 2 \neq 0$, и тем самым $x \neq 0$, мы будем доказывать по ходу доказательства второй части **леммы**. Так же по ходу показываем, что $\gamma^{js} + \gamma^{-js} - 2 \in F_q$, откуда будет вытекать, что $\gamma^{js} + \gamma^{-js} \in F_q$.

Пусть $s = 1$. Тогда включение $\gamma^{js} + \gamma^{-js} - 2 \in F_q$ имеет место по определению (то есть вытекает из того, что γ – первообразный корень поля F_q). При этом уравнение (1.3) равносильно

$$(\gamma^j - 1)^2 = -\alpha \gamma^j. \quad (1.4)$$

Если $\gamma^{js} + \gamma^{-js} - 2 = \gamma^j + \gamma^{-j} = 0$, то (1.4) равносильно $(\gamma^j - 1)^2 = 0$, то есть $\gamma^j = 1$, откуда $j \geq q - 1$, что противоречит условию **леммы**. Таким образом, $\gamma^{js} + \gamma^{-js} - 2 = \gamma^j + \gamma^{-j} \neq 0$.

Если j – чётно, то $\mu = \gamma^j + \gamma^{-j} - 2 = (\gamma^{j/2} - \gamma^{-j/2})^2$ – квадратичный вычет поля F_q . Обратно, если $\mu = \lambda^2$ – квадратичный вычет поля F_q , то в силу

цепочки равносильностей и импликации в последнем звене цепочки

$$\begin{aligned}\mu &= \gamma^j + \gamma^{-j} - 2 \Leftrightarrow \mu\gamma^j = \gamma^{2j} - 2\gamma^j + 1 \Leftrightarrow \mu\gamma^j = (\gamma^j - 1)^2 \Leftrightarrow \\ &\Leftrightarrow \gamma^j = (\gamma^j - 1)^2\mu^{-1} \Leftrightarrow \gamma^j = (\gamma^j - 1)^2\lambda^{-2} \Rightarrow \gamma^{((q-1)/2)j} = 1\end{aligned}$$

имеем, что $((q-1)/2)j$ делится на $q-1$. Это означает, что для некоторого целого t имеем $((q-1)/2)j = t(q-1)$, откуда $j = 2t$ – чётно.

Таким образом, $\gamma^j + \gamma^{-j} - 2$ – квадратичный вычет поля F_q тогда и только тогда, когда $j \in I_1$ – чётное.

Пусть $s = q-1$. Тогда $\gamma^{js} + \gamma^{-js} - 2 = (\gamma^{js/2} - \gamma^{-js/2})^2$, и для того, чтобы $\gamma^{js} + \gamma^{-js} - 2 \in F_q$, необходимо и достаточно, чтобы $((\gamma^{js/2} - \gamma^{-js/2})^2)^q = (\gamma^{js/2} - \gamma^{-js/2})^2$, при этом для того, чтобы $\gamma^{js} + \gamma^{-js} - 2$ был квадратичным вычетом поля F_q , необходимо и достаточно, чтобы $\gamma^{js/2} + \gamma^{-js/2} - 2 \in F_q$, что равносильно $(\gamma^{js/2} - \gamma^{-js/2})^q = \gamma^{js/2} - \gamma^{-js/2}$.

$$\begin{aligned}\text{Имеем} \\ (\gamma^{js/2} - \gamma^{-js/2})^q &= \gamma^{j(q^2-q)/2} - \gamma^{-j(q^2-q)/2} = \\ &= \gamma^{j((q^2-1)/2+(1-q)/2)} - \gamma^{-j((q^2-1)/2+(1-q)/2)}.\end{aligned}$$

Так как γ – первообразный элемент поля F_{q^2} , то $\gamma^{(q^2-1)/2} = -1$, и последнее выражение полученной цепочки равенств принимает вид

$$(-1)^j \gamma^{j(1-q)/2} - (-1)^j \gamma^{-j(1-q)/2}.$$

Имеем

$$(-1)^j \gamma^{j(1-q)/2} - (-1)^j \gamma^{-j(1-q)/2} = (-1)^j \gamma^{-j(q-1)/2} - (-1)^j \gamma^{j(q-1)/2}.$$

Последнее выражение совпадает с $\gamma^{j(q-1)/2} - \gamma^{-j(q-1)/2}$ тогда и только тогда, когда j – нечётно. Другими словами,

$$(\gamma^{j(q-1)/2} - \gamma^{-j(q-1)/2})^q = \gamma^{j(q-1)/2} - \gamma^{-j(q-1)/2}$$

тогда и только тогда, когда j – нечётно. Таким образом, $\gamma^{js} + \gamma^{-js} - 2$ – квадратичный вычет поля F_q тогда и только тогда, когда j – нечётно.

$$\begin{aligned}\text{Если } j \text{ – чётно, то имеем} \\ (-1)^j \gamma^{-j(q-1)/2} - (-1)^j \gamma^{j(q-1)/2} &= \gamma^{-j(q-1)/2} - \gamma^{j(q-1)/2} = \\ &= -(\gamma^{j(q-1)/2} - \gamma^{-j(q-1)/2}),\end{aligned}$$

и $((\gamma^{js/2} - \gamma^{-js/2})^q)^2 = (\gamma^{js/2} - \gamma^{-js/2})^2$, то есть

$$((\gamma^{js/2} - \gamma^{-js/2})^2)^q = (\gamma^{js/2} - \gamma^{-js/2})^2,$$

и в любом случае имеем $(\gamma^{js/2} - \gamma^{-js/2})^2 \in F_q$, то есть

$$\gamma^{js} + \gamma^{-js} - 2 = (\gamma^{js/2} - \gamma^{-js/2})^2 \in F_q,$$

откуда $\gamma^{js} + \gamma^{-js} \in F_q$.

В частности, мы также доказали, что $\gamma^{js} + \gamma^{-js} - 2$ – квадратичный вычет поля F_q тогда и только тогда, когда $j \in I_1$ – чётное или $j \in I_2$ – нечётное.

Лемма доказана. $\square$

Лемма 1.6. Пусть $1 \leq j \leq (q-3)/2$ при $s = 1$ и $1 \leq j \leq (q-1)/2$ при $s = q-1$. Тогда система

$$\begin{cases} \gamma^{js}x_{11}x_{22} - \gamma^{-js}x_{12}x_{21} = 1 - \beta\delta_i, \\ \gamma^{-js}x_{11}x_{22} - \gamma^{js}x_{12}x_{21} = 1 + \beta\delta_i - \beta\alpha, \\ (\gamma^{-js} - \gamma^{js})x_{11}x_{21} = \beta \\ (\gamma^{js} - \gamma^{-js})x_{12}x_{22} = -\alpha + \alpha\beta\delta_i - \beta\delta_i^2 \end{cases} \quad (1.6)$$

над полем F_q относительно $x_{11}, x_{12}, x_{21}, x_{22}, \beta, \delta$ при фиксированных ненулевых γ, js, α , совместна. При этом для всех решений системы значение β единственно, которое является ненулевым, и удовлетворяет уравнению (1.3), в то время, как δ пробегает все элементы поля F_q , а значения $x_{11}, x_{12}, x_{21}, x_{22}$ можно считать зависящими от δ .

Доказательство. Сложим первые два уравнения системы:

$$\gamma^{js}(x_{11}x_{22} - x_{12}x_{21}) + \gamma^{-js}(x_{11}x_{22} - x_{12}x_{21}) = 2 - \alpha\beta,$$

и, учитывая равенство $x_{11}x_{22} - x_{12}x_{21} = 1$, приходим к уравнению (1.3):

$$\gamma^{js} + \gamma^{-js} = 2 - \alpha\beta.$$

Так как $1 \leq j \leq (q-1)/2$, то по лемме 1.5 это уравнение имеет единственное решение β , которое является ненулевым. Будем считать, что оно найдено.

Осталось показать, что система (1.6) совместна относительно $x_{11}, x_{12}, x_{21}, x_{22}, \delta$, и при этом δ принимает все значения из поля F_q , а значения $x_{11}, x_{12}, x_{21}, x_{22}$, можно считать, зависят от δ .

Зафиксируем произвольное $\delta \in F_q$ и введём новые неизвестные для системы: $u = x_{11}x_{22}, v = x_{12}x_{21}, w = x_{11}x_{21}, z = x_{12}x_{22}$. Покажем, что достаточно найти решение (u, v, w, z) нашей системы относительно новых неизвестных. Допустим, это решение найдено. Рассмотрим новую систему:

$$u = x_{11}x_{22}, v = x_{12}x_{21}, w = x_{11}x_{21}, z = x_{12}x_{22}. \quad (1.7)$$

Из первого уравнения системы (1.7) выразим x_{22} через x_{11} , из третьего выразим x_{21} через x_{11} : $x_{22} = ux_{11}^{-1}, x_{21} = wx_{11}^{-1}$. Из второго уравнения выразим x_{12} посредством x_{21} через x_{11} : $x_{12} = vx_{21}^{-1} = v(wx_{11}^{-1})^{-1} = vw^{-1}x_{11}$. Таким образом, x_{12}, x_{21} и x_{22} выражаются через свободную неизвестную x_{11} . Наконец, покажем, что при этом последнее уравнение системы (1.7) не противоречит трём предыдущим. Для этого x_{12} выразим через x_{11} посредством x_{22} : $x_{12} = zx_{22}^{-1} = z(ux_{11}^{-1})^{-1} = zu^{-1}x_{11}$, откуда, приравняв разные выражения для x_{12} , получаем $vw^{-1}x_{11} = zu^{-1}x_{11}$. Теперь подставив в полученное равенство вместо z, u, w их выражения через x_{11}, x_{12}, x_{21} и x_{22} , получаем тождество.

Осталось показать, что система (1.6) совместна относительно новых неизвестных u, v, w, z .

Покажем, что $\gamma^{js} - \gamma^{-js} \neq 0$. Действительно, если $\gamma^{js} - \gamma^{-js} = 0$, то $\gamma^{2js} = 1$, откуда имеем, что при $s = 1$ $q-1$ делит $2j$, что означает $(q-1)/2$ делит j , то есть $(q-1)/2 \leq j$ — противоречие с условием. При $s = q-1$ получаем, что $q^2 - 1$ делит $2j(q-1)$, что означает $q+1$ делит $2j$, то есть $(q+1)/2$ делит j , и $(q+1)/2 \leq j$ — снова противоречие с условием **леммы**.

Теперь значения w и z находятся с очевидностью, так как $\gamma^{js} - \gamma^{-js} \neq 0$.

Покажем, что также можно найти u и v . Система, составленная из первых двух уравнений, имеет определитель $\Delta = \begin{vmatrix} \gamma^{js} & -\gamma^{-js} \\ \gamma^{-js} & -\gamma^{js} \end{vmatrix} = -\gamma^{2js} + \gamma^{-2js}$,

причём имеем следующую цепочку равносильностей:

$$\Delta = 0 \Leftrightarrow \gamma^{-2js} - \gamma^{2js} = 0 \Leftrightarrow (\gamma^{-js} + \gamma^{js})(\gamma^{-js} - \gamma^{js}) = 0 \Leftrightarrow \gamma^{js} + \gamma^{-js} = 0.$$

Поэтому если $\gamma^{js} + \gamma^{-js} \neq 0$ (это обязательно имеет место при чётном q), то первые два уравнения системы (1.6) относительно неизвестных $u = x_{11}x_{22}$ и $v = x_{12}x_{21}$ имеют единственное решение (u, v) . Если $\gamma^{js} + \gamma^{-js} = 0$ (что возможно только при нечётном q), то первые два уравнения образуют неопределённую систему относительно неизвестных u и v , которые являются также решениями уравнения $u - v = 1$ (так как $x_{11}x_{22} - x_{12}x_{21} = 1$).

Таким образом, система (1.6) совместна относительно неизвестных u, v, w, z . Следовательно, она совместна и относительно x_{11}, x_{12}, x_{21} и x_{22} . При этом значение $\delta \in F_q$ было зафиксировано произвольным. Поэтому лемма доказана. $\square$

2. ДОКАЗАТЕЛЬСТВО ТЕОРЕМ

Доказательство теорем разобьём на доказательство отдельных лемм. Но прежде напомним, что $\Gamma^{(j)} = (X, R_j)$ – граф с множеством вершин X и множеством рёбер $R_j = \{\{x, y\} | yx^{-1} \in K_j\}$. При этом индекс j может быть как из $\{0, 1\} \cup I_1 \cup I_2 \cup \{q\}$, так и из $\{0, 1\} \cup J$.

Лемма 2.1. Пусть $a = \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}$ и $b = \begin{pmatrix} 1 & 0 \\ -\beta & 1 \end{pmatrix}$. Тогда для любого $j \in I_1 \cup I_2$ имеют место равенства

$$\begin{aligned} \Gamma^{(j)}(a) &= \left\{ \begin{pmatrix} 1 - \eta\delta & -\eta\delta^2 \\ \eta & 1 + \eta\delta \end{pmatrix} \middle| \gamma^{js} + \gamma^{-js} = 2 - \alpha\eta, \delta \in F_q \right\}, \\ \Gamma^{(j)}(b) &= \left\{ \begin{pmatrix} 1 + \varepsilon\delta & \varepsilon \\ -\varepsilon\delta^2 & 1 - \varepsilon\delta \end{pmatrix} \middle| \gamma^{js} + \gamma^{-js} = 2 - \beta\varepsilon, \delta \in F_q \right\}. \end{aligned} \quad (2.1)$$

Доказательство. Пусть $j \in I_1 \cup I_2 \cup \{q\}$, $a = \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}$ и $x \in \Gamma^{(j)}(a)$. Ясно, что x является элементом второго типа по отношению к a : $x = \begin{pmatrix} 1 - \eta\delta & -\eta\delta^2 \\ \eta & 1 + \eta\delta \end{pmatrix}$. Тогда

$$xa^{-1} = \begin{pmatrix} 1 - \eta\delta & -\eta\delta^2 \\ \eta & 1 + \eta\delta \end{pmatrix} \cdot \begin{pmatrix} 1 & -\alpha \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 - \eta\delta & -\alpha + \alpha\eta\delta - \eta\delta^2 \\ \eta & 1 + \eta\delta - \alpha\eta \end{pmatrix},$$

и имеем следующую цепочку равносильностей:

$$\begin{aligned} x \in \Gamma^{(j)}(a) &\Leftrightarrow xa^{-1} \in K_j \Leftrightarrow \begin{pmatrix} 1 - \eta\delta & -\alpha + \alpha\eta\delta - \eta\delta^2 \\ \eta & 1 + \eta\delta - \alpha\eta \end{pmatrix} = \\ &= \begin{pmatrix} \gamma^{js}x_{11}x_{22} + \gamma^{-js}x_{12}x_{21} & (\gamma^{js} + \gamma^{-js})x_{12}x_{22} \\ (\gamma^{-js} + \gamma^{js})x_{11}x_{21} & \gamma^{-js}x_{11}x_{22} + \gamma^{js}x_{12}x_{21} \end{pmatrix} \end{aligned}$$

Последнее равенство равносильно системе

$$\begin{cases} \gamma^{js}x_{11}x_{22} - \gamma^{-js}x_{12}x_{21} &= 1 - \eta\delta, \\ \gamma^{-js}x_{11}x_{22} - \gamma^{js}x_{12}x_{21} &= 1 + \eta\delta - \eta\alpha, \\ (\gamma^{-js} - \gamma^{js})x_{11}x_{21} &= \eta \\ (\gamma^{js} - \gamma^{-js})x_{12}x_{22} &= -\alpha + \alpha\eta\delta - \eta\delta^2 \end{cases} \quad (2.2)$$

Таким образом, для того, чтобы $x \in \Gamma^{(j)}(a)$, необходимо и достаточно, чтобы была совестной система (2.2). По **лемме 1.6** она совместна. Более того, при фиксированных γ , j и α существует единственное значение η , удовлетворяющее системе (2.2) и уравнению $\gamma^{js} + \gamma^{-js} = 2 - \alpha\eta$, в то время, как δ пробегает все q значений из F_q , и равенство (2.1) выполнено (согласно той же **леммы 1.6**).

Докажем лемму относительно равенства для $\Gamma^{(j)}(b)$. Если $x \in \Gamma^{(j)}(b)$, где $b = \begin{pmatrix} 1 & 0 \\ \beta & 1 \end{pmatrix}$, то x – элемент второго типа относительно b : $x = \begin{pmatrix} 1 + \varepsilon\delta & \varepsilon \\ -\varepsilon\delta^2 & 1 - \varepsilon\delta \end{pmatrix}$. Тогда

$$xb^{-1} = \begin{pmatrix} 1 + \varepsilon\delta & \varepsilon \\ -\varepsilon\delta^2 & 1 - \varepsilon\delta \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ -\beta & 1 \end{pmatrix} = \begin{pmatrix} 1 + \varepsilon\delta - \varepsilon\beta & \varepsilon \\ -\beta + \varepsilon\beta\delta - \varepsilon\delta^2 & 1 - \varepsilon\delta \end{pmatrix}.$$

Теперь получаем аналог системы (2.2):

$$\begin{cases} \gamma^{js}x_{11}x_{22} - \gamma^{-js}x_{12}x_{21} &= 1 + \varepsilon\delta - \varepsilon\beta, \\ \gamma^{-js}x_{11}x_{22} - \gamma^{js}x_{12}x_{21} &= 1 - \varepsilon\delta, \\ (\gamma^{-js} - \gamma^{js})x_{11}x_{21} &= -\beta + \varepsilon\beta\delta - \varepsilon\delta^2 \\ (\gamma^{js} - \gamma^{-js})x_{12}x_{22} &= \varepsilon. \end{cases}$$

Остальное для $\Gamma^{(j)}(b)$ дословно (как и для $\Gamma^{(j)}(a)$).

Лемма доказана. $\square$

Лемма 2.2. Пусть q нечётно. Тогда в условиях **леммы 2.1** элементы из $\Gamma^{(j)}(a)$ и $\Gamma^{(j)}(b)$ лежат в одном классе сопряжённости с a и b , соответственно, тогда и только тогда, когда $j \in I_1$ – чётное или $j \in I_2$ – нечётное, и лежат в классах, отличных от a^G и b^G , соответственно, тогда и только тогда, когда $j \in I_1$ – нечётное или $j \in I_2$ – чётное.

Доказательство. По **лемме 2.1** $x = \begin{pmatrix} 1 - \eta\delta & -\eta\delta^2 \\ \eta & 1 + \eta\delta \end{pmatrix} \in \Gamma^{(j)}(a)$ тогда и только тогда, когда $\gamma^{js} + \gamma^{-js} - 2 = -\alpha\eta$. При этом $x \subseteq a^G$ тогда и только тогда, когда α и $-\eta$ имеют одинаковый тип квадратичности, что равносильно квадратичности $-\alpha\eta$ в поле F_q (**лемма 1.2**). Последнее означает, что $\gamma^{js} + \gamma^{-js} - 2$ – квадратичный вычет поля F_q . Но тогда по **лемме 1.5** имеем, что $j \in I_1$ – чётное или $j \in I_2$ – нечётное.

Таким образом, $\Gamma^{(j)}(a) \subseteq a^G$ тогда и только тогда, когда $j \in I_1$ – чётное или $j \in I_2$ – нечётное.

Дословно доказывается утверждение леммы относительно включения $\Gamma^{(j)}(b) \subseteq b^G$. Ясно, что отсюда вытекает утверждение леммы относительно $\Gamma^{(j)}(a) \not\subseteq a^G$ и $\Gamma^{(j)}(b) \not\subseteq b^G$.

Лемма доказана. $\square$

Лемма 2.3. Пусть $a = \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}$ и $b = \begin{pmatrix} 1 & 0 \\ -\beta & 1 \end{pmatrix}$. Тогда для индекса q имеют место равенства

$$\begin{aligned} \Gamma^{(q)}(a) &= \left\{ \begin{pmatrix} 1 - 4\alpha^{-1}\delta & -4\alpha^{-1}\delta^2 \\ 4\alpha^{-1} & 1 + 4\alpha^{-1}\delta \end{pmatrix} \middle| \delta \in F_q \right\}, \\ \Gamma^{(q)}(b) &= \left\{ \begin{pmatrix} 1 + 4\beta^{-1}\delta & 4\beta^{-1} \\ -4\beta^{-1}\delta^2 & 1 - 4\beta^{-1}\delta \end{pmatrix} \middle| \delta \in F_q \right\}. \end{aligned} \quad (2.3)$$

При этом элементы из $\Gamma^{(q)}(a)$ и $\Gamma^{(q)}(b)$ лежат в одном классе с a и b , соответственно, когда $q \equiv 1 \pmod{4}$, и лежат в классе, отличном от a^G и b^G (соответственно) при $q \equiv -1 \pmod{4}$.

Доказательство. Для индекса q имеем следующую цепочку равносильностей:

$$\begin{aligned} x \in \Gamma^{(q)}(a) &\Leftrightarrow xa^{-1} \in -X \Leftrightarrow \\ &\Leftrightarrow \begin{pmatrix} 1 - \eta\delta & -\alpha + \alpha\eta\delta - \eta\delta^2 \\ \eta & 1 + \eta\delta - \alpha\eta \end{pmatrix} = - \begin{pmatrix} 1 - \beta\varepsilon & -\beta\varepsilon^2 \\ \beta & 1 + \beta\varepsilon \end{pmatrix} \Leftrightarrow \\ &\Leftrightarrow \begin{cases} 1 - \eta\delta = -1 + \beta\varepsilon, \\ \eta = -\beta, \\ -\alpha + \alpha\eta\delta - \eta\delta^2 = \beta\varepsilon^2, \\ 1 + \eta\delta - \alpha\eta = -1 - \beta\varepsilon, \end{cases} \Leftrightarrow \begin{cases} \eta\delta + \beta\varepsilon = 2, \\ \eta = -\beta, \\ -\alpha + \alpha\eta\delta - \eta\delta^2 = \beta\varepsilon^2, \\ -\eta\delta + \alpha\eta - \beta\varepsilon = 2, \end{cases} \Leftrightarrow \\ &\Leftrightarrow \begin{cases} \eta\delta - \eta\varepsilon = 2, \\ \eta = -\beta, \\ -\alpha + \alpha\eta\delta - \eta\delta^2 = -\eta\varepsilon^2, \\ -\eta\delta + \alpha\eta + \eta\varepsilon = 2. \end{cases} \end{aligned} \quad (2.4)$$

Покажем, что из системы (2.4) можно исключить третье уравнение. Первое уравнение системы равносильно уравнению $\eta(\delta - \varepsilon) = 2$, а последнее – уравнению $-\eta(\delta + \alpha + \varepsilon) = 2$, откуда получаем (в силу $\eta \neq 0$) $\delta - \varepsilon = -\delta + \alpha + \varepsilon$, то есть $\alpha = 2\delta - 2\varepsilon$, которое подставляем в третье и подвергаем очевидным равносильным преобразованиям (с учётом $\delta - \varepsilon \neq 0$, иначе $\alpha = 0$):

$$\begin{aligned} 2\varepsilon - 2\delta + (2\delta - 2\varepsilon)\eta\delta - \eta\delta^2 &= -\eta\varepsilon^2 \Leftrightarrow \\ \Leftrightarrow 2\varepsilon - 2\delta + 2\delta\eta\delta - 2\varepsilon\eta\delta - \eta\delta^2 &= -\eta\varepsilon^2 \Leftrightarrow \\ \Leftrightarrow 2\varepsilon - 2\delta - 2\varepsilon\eta\delta + \eta\delta^2 &= -\eta\varepsilon^2 \Leftrightarrow \\ \Leftrightarrow \eta\varepsilon^2 - 2\varepsilon\eta\delta + \eta\delta^2 &= -2(\varepsilon - \delta) \Leftrightarrow \\ \Leftrightarrow \eta(\varepsilon - \delta)^2 &= -2(\varepsilon - \delta) \Leftrightarrow \eta(\varepsilon - \delta) = -2. \end{aligned}$$

Это означает, что система (2.4) равносильна системе

$$\begin{cases} \eta(\delta - \varepsilon) = 2, \\ \eta = -\beta, \\ \eta(-\delta + \alpha + \varepsilon) = 2. \end{cases} \quad (2.5)$$

В этой системе α фиксирована и равна $2\delta - 2\varepsilon = 2(\delta - \varepsilon)$. Значит, фиксировано и $\delta - \varepsilon$, то есть фиксирована η . Более того, из первого уравнения системы (2.5) получаем $\delta - \varepsilon = 2\eta^{-1}$, откуда $\alpha = 2\delta - 2\varepsilon = 4\eta^{-1}$, то есть $\eta = 4\alpha^{-1}$. Значит,

$$\Gamma^{(q)}(a) = \left\{ \begin{pmatrix} 1 - 4\alpha^{-1}\delta & -4\alpha^{-1}\delta^2 \\ 4\alpha^{-1} & 1 + 4\alpha^{-1}\delta \end{pmatrix} \middle| \delta \in F_q \right\}.$$

Выясним принадлежность элементов из $\Gamma^{(q)}(a)$ классам C_2 и C_3 . Как и выше, для определённости считаем, что $a \in C_2$, то есть α – квадратичный вычет поля F_q . Тогда имеем $\Gamma^{(q)}(a) \subseteq a^G \Leftrightarrow 4\alpha^{-1} = -\beta^2 \Leftrightarrow \beta^2 = -4\alpha^{-1}$, то есть $\Gamma^{(q)}(a) \subseteq a^G$ тогда и только тогда, когда $-4\alpha^{-1}$ является квадратичным вычетом поля F_q , что равносильно $(-4\alpha^{-1})^{(q-1)/2} = (-1)^{(q-1)/2}\alpha^{(q-1)/2} = (-1)^{(q-1)/2} = 1$, что в свою очередь равносильно $q \equiv 1 \pmod{4}$. Таким образом, $\Gamma^{(q)}(a) \subseteq C_2 = a^G \Leftrightarrow q \equiv 1 \pmod{4}$, и $\Gamma^{(q)}(a) \subseteq C_3 \neq a^G \Leftrightarrow q \equiv -1 \pmod{4}$.

Аналогично, для $x = \begin{pmatrix} 1 + \varepsilon\delta & \varepsilon \\ -\varepsilon\delta^2 & 1 - \varepsilon\delta \end{pmatrix}$ имеем

$$\begin{aligned}
x \in \Gamma^{(q)}(b) &\Leftrightarrow xb^{-1} \in -X \Leftrightarrow \\
&\Leftrightarrow \begin{pmatrix} 1 + \varepsilon\delta - \varepsilon\beta & \varepsilon \\ -\beta + \varepsilon\beta\delta - \varepsilon\delta^2 & 1 - \varepsilon\delta \end{pmatrix} = - \begin{pmatrix} 1 + \eta\varepsilon_1 & \eta \\ -\eta\varepsilon_1^2 & 1 - \eta\varepsilon_1 \end{pmatrix} \Leftrightarrow \\
&\Leftrightarrow \begin{cases} 1 + \varepsilon\delta - \varepsilon\beta = -1 - \eta\varepsilon_1, \\ \varepsilon = -\eta, \\ -\beta + \varepsilon\beta\delta - \varepsilon\delta^2 = \eta\varepsilon_1^2, \\ 1 - \varepsilon\delta = -1 + \eta\varepsilon_1, \end{cases} \Leftrightarrow \begin{cases} -\eta\varepsilon_1 - \varepsilon\delta + \varepsilon\beta = 2, \\ \varepsilon = -\eta, \\ -\beta + \varepsilon\beta\delta - \varepsilon\delta^2 = \eta\varepsilon_1^2, \\ \eta\varepsilon_1 + \varepsilon\delta = 2, \end{cases} \Leftrightarrow \\
&\Leftrightarrow \begin{cases} -\varepsilon\delta + \varepsilon\beta + \varepsilon\varepsilon_1 = 2, \\ \varepsilon = -\eta, \\ -\beta + \varepsilon\beta\delta - \varepsilon\delta^2 = -\varepsilon\varepsilon_1^2, \\ \varepsilon\delta - \varepsilon\varepsilon_1 = 2. \end{cases} \quad (2.6)
\end{aligned}$$

Так же, как и выше, показываем, что система (2.6) равносильна системе

$$\begin{cases} \varepsilon(\delta - \varepsilon_1) = -2, \\ \eta = -\varepsilon, \\ \varepsilon(-\delta + \beta + \varepsilon_1) = 2. \end{cases} \quad (2.7)$$

Снова $\delta - \varepsilon_1 = 2\varepsilon^{-1}$, откуда $\beta = 2(\delta - \varepsilon_1) = 4\varepsilon^{-1}$, то есть $\varepsilon = 4\beta^{-1}$. Значит,

$$\Gamma^{(q)}(b) = \left\{ \begin{pmatrix} 1 + 4\beta^{-1}\delta & 4\beta^{-1} \\ -4\beta^{-1}\delta^2 & 1 - 4\beta^{-1}\delta \end{pmatrix} \middle| \delta \in F_q \right\}.$$

а анализ включения $\Gamma^{(q)}(b)$ в b^G проводится практически дословно, как и для случая с $\Gamma^{(q)}(a)$. Лемма доказана. $\square$

Будем говорить, что параметр η в равенстве (2.1) определяет окрестность $\Gamma^{(j)}(a)$. Аналогично, ε определяет окрестность $\Gamma^{(j)}(b)$.

Лемма 2.4. Схема $\mathfrak{X}(X) = (X, \{R_i\}_{0 \leq i \leq q})$ – равномерно кликовая схема отношений относительно множества индексов J с q классами и $q+1$ кликами.

Доказательство. То, что для $\mathfrak{X}(X)$ выполнено условие (1) определения схемы отношений, вытекает из её определения. Мы уже заметили, что $|J| = q - 1$. Поэтому выполнение условия (2) с $d = q$ вытекает из лемм 2.1 и 2.3. То, что выполняется условие (3), вытекает из свойства $K_i = K_i^{-1}$ для любого $i \in J$.

Таким образом, $\mathfrak{X}(X)$ – схема отношений с $d = q$ классами. Покажем, что она является кликовой с $q+1$ кликами. То, что $\mathfrak{X}(X)$ симметрична, доказано. Ясно, что R_1 -клику образуют неединичные элементы одной и той же силовой p -подгруппы. Так как такие подгруппы между собой пересекаются тривиально, то клики между собой попарно не пересекаются. Так как $|Syl_p(G)| = q+1$, то и клик у схемы всего $q+1$, и $\mathfrak{X}(X)$ – кликовая схема с $q+1$ кликами.

Если x – фиксированная точка некоторой R_1 -клики K_s , K_t – R_1 -клики, отличная от K_s , y пробегает точки из K_t , то в $(x, y) \in R_i$ индекс обязан i пробегать элементы всего множества J , так как при действии сопряжениями на x всевозможными элементами α из силовой p -подгруппы P , содержащей x , при фиксированном i в $(x, y)^\alpha = (x, y^\alpha) \in R_i$ y^α пробегает все клики, отличные от K_s . Поэтому $\mathfrak{X}(X)$ – равномерно кликовая относительно множества индексов J .

Лемма доказана. $\square$

Лемма 2.5. Для чисел пересечений $p_{0j}^k, p_{i0}^k, p_{ij}^0, p_{11}^k, p_{1k}^1, p_{k1}^1$ схемы $\mathfrak{X}(X)$ имеют место следующие равенства:

$$\begin{aligned} 1) \quad & p_{0j}^k = \delta_{jk}, p_{i0}^k = \delta_{ik}, p_{ij}^0 = n_i \delta_{ij}, \text{ где } n_i = \begin{cases} q-2, & \text{если } i = 1, \\ q, & \text{если } i \in J. \end{cases} \\ 2) \quad & p_{11}^k = p_{1k}^1 = p_{k1}^1 = \begin{cases} q-3, & \text{если } k = 1, \\ 0, & \text{если } k \neq 1. \end{cases} \end{aligned}$$

Доказательство. 1) Равенства $p_{0j}^k(x, y) = \delta_{jk}, p_{i0}^k(x, y) = \delta_{ik}, p_{ij}^0(x, y) = n_i \delta_{ij}$, где n_i – степень графа $\Gamma^{(i)}$, вытекают непосредственно из определения схемы отношений (с непостоянными числами пересечений). При этом их значения не зависят от x и y . Поэтому имеем $p_{0j}^k = \delta_{jk}, p_{i0}^k = \delta_{ik}, p_{ij}^0 = n_i \delta_{ij}$. Они также совпадают с аналогичными равенствами для постоянных чисел пересечений (см. например, [4], [8]). Поэтому подробности доказательства опускаем. Докажем равенства для значений n_i .

То, что при $i = 1$ имеем $n_i = q - 2$, очевидно: $x \in \Gamma^{(i)}(a)$ тогда и только тогда, когда a и x лежат в одной клике, и для фиксированного a имеется $q - 2$ вершин, лежащих в одной клике с a и отличной от неё.

Пусть $i \in J$. Тогда в равенствах для $\Gamma^{(i)}(a)$ (см. равенства (2.1) и (2.3)) имеем, что η и α определены однозначно, в то время, как δ_i пробегает все q значений из F_q . Поэтому при $i \in J$ имеем $|\Gamma^{(i)}(a)| = q$.

2) Пусть $(x, y) \in R_k$ и z – такой, что $(x, z) \in R_1$ и $(z, y) \in R_1$. Тогда z лежит в одной клике с x и y , откуда $k = 1$. Так как клика содержит $q - 1$ элементов, то таких z будет в точности на две меньше, чем $q - 1$. Таким образом,

$$p_{11}^k(x, y) = \begin{cases} q-3, & \text{если } k = 1, \\ 0, & \text{если } k \in J. \end{cases}$$

Если $(x, y) \in R_1$ и z – такой, что $(x, z) \in R_1, (z, y) \in R_k$, то снова z лежит в одной клике с x и y , и тогда $k = 1$, причём это справедливо для любой пары $(x, y) \in R_1$. Поэтому $p_{1k}^1(x, y) = p_{1k}^1 = \begin{cases} q-3, & \text{если } k = 1, \\ 0, & \text{если } k \in J. \end{cases}$ Аналогично

$$p_{k1}^1 = \begin{cases} q-3, & \text{если } k = 1, \\ 0, & \text{если } k \in J. \end{cases}$$

Лемма доказана. $\square$

Лемма 2.6. Справедливы следующие утверждения:

- 1) Для любого $i \in J$ имеет место равенство $p_{ii}^1 = 0$.
- 2) Для любой пары $(i, j) \in J \times J$ с условием $i \neq j$ существует пара $(x, y) \in R_1$ такая, что $p_{ij}^1(x, y) \neq 0$, и тогда $p_{ij}^1(x, y) = q$, и существует пара $(u, v) \in R_1$, такая, что $p_{ij}^1(u, v) = 0$. Другими словами, для любых i и j из J с условием $i \neq j$ число $p_{ij}^1(x, y)$ зависит от выбора элементов x и y , и $p_{ij}^1(x, y) \in \{0, q\}$. Более того, для любой пары $(i, j) \in J \times J$ с условием $i \neq j$ в каждой R_1 -клике существует в точности $q - 1$ пар элементов x и y таких, что $p_{ij}^1(x, y) \neq 0$. При этом, если для фиксированных x и y $p_{ij}^1(x, y) \neq 0$, то для любого $k \in J \setminus \{j\}$ имеет место равенство $p_{ik}^1(x, y) = 0$.

Доказательство. 1) Если $(x, y) \in R_1$, то x и y лежат в одной R_1 -клике. Тогда для любого $i \in J$ элемента z такого, что $(x, z) \in R_i$ и $(z, y) \in R_i$, не существует, так как если $(x, z) \in R_i$ и $(z, y) \in R_j$, где x и y лежат в одной клике, то $i \neq j$.

Это вытекает из построения нашей схемы. Поэтому $p_{ij}^1(x, y) = 0$ при $i = j$, и это число не зависит от x и y : $p_{ii}^1 = 0$.

2) Зафиксируем пару $(x, y) \in R_1$. Тогда x и y лежат в одной и той же силовой p -подгруппе. Можем считать, что $x = \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}$, $y = \begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix}$.

Пусть q – произвольное и $(i_{s_1}, j_{s_2}) \in I \times I$, $i_{s_1} \neq j_{s_2}$ и z – такой, что $(x, z) \in R_{i_{s_1}}$ и $(z, y) \in R_{j_{s_2}}$:

$$z = \begin{pmatrix} 1 - \eta\delta & -\eta\delta^2 \\ \eta & 1 + \eta\delta \end{pmatrix} = \begin{pmatrix} 1 - \varepsilon\delta_1 & -\varepsilon\delta_1^2 \\ \varepsilon & 1 + \varepsilon\delta_1 \end{pmatrix} = \Gamma^{(i_{s_1})}(x) \cap \Gamma^{(j_{s_2})}(y).$$

(напоминаем, что при второй системе индексации имеем $t_s = 1 + t$, где $t \in I_1$, либо $t_s = 1 + |I_1| + t$, где $t \in I_2$). Из строения $\Gamma^{(i_{s_1})}(x)$ и $\Gamma^{(j_{s_2})}(y)$ (лемма 2.1) имеем что $\gamma^{is_1} + \gamma^{-is_1} = 2 - \alpha\eta$ и $\gamma^{js_2} + \gamma^{-js_2} = 2 - \beta\varepsilon$. При этом ясно, что $\eta = \varepsilon$ определено однозначно, в то время, как δ и δ_1 пробегает элементы из F_q . Поэтому $p_{i_{s_1}j_{s_2}}^1(x, y) = |\Gamma^{(i_{s_1})}(x) \cap \Gamma^{(j_{s_2})}(y)| = q$. Найдём необходимые и достаточные условия того, что $\Gamma^{(i_{s_1})}(x) \cap \Gamma^{(j_{s_2})}(y) \neq \emptyset$ для x и y с $(x, y) \in R_1$. Имеем

$$\eta = -\alpha^{-1}(\gamma^{is_1} + \gamma^{-is_1} - 2) = -\beta^{-1}(\gamma^{js_2} + \gamma^{-js_2} - 2),$$

откуда $\alpha\beta^{-1} = (\gamma^{js_2} + \gamma^{-js_2} - 2)(\gamma^{is_1} + \gamma^{-is_1} - 2)^{-1}$ – это и есть упомянутое необходимое и достаточное условия.

Так как i_{s_1} и j_{s_2} фиксированы, то фиксированы $\gamma^{is_1} + \gamma^{-is_1} - 2$ с $\gamma^{js_2} + \gamma^{-js_2} - 2$. Если вершина $x = \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}$ фиксирована, то фиксирован и α . Тогда существует единственный β с условием

$$\alpha\beta^{-1} = (\gamma^{js_2} + \gamma^{-js_2} - 2)(\gamma^{is_1} + \gamma^{-is_1} - 2)^{-1},$$

что означает существование единственного $y = \begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix}$ с условиями $(x, y) \in R_1$ и $p_{i_{s_1}j_{s_2}}^1(x, y) \neq 0$. Таким образом, для фиксированных i_{s_1}, j_{s_2} (таких, что $i_s \neq j_s$), и x существует единственный y с условием $p_{i_{s_1}j_{s_2}}^1(x, y) \neq 0$. Значит, в каждой клике существует в точности $q - 1$ пар элементов x и y таких, что $p_{i_{s_1}j_{s_2}}^1(x, y) \neq 0$.

Покажем, что, с другой стороны, для любой пары $(i_{s_1}, j_{s_2}) \in I \times I$ с условием $i_{s_1} \neq j_{s_2}$ существует пара $(u, v) \in R_1$ такая, что $p_{i_{s_1}j_{s_2}}^1(x, y) = 0$. Действительно,

возьмём в качестве u элемент $x = \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}$. Так как $q - 1 \geq 3$, то кроме

$y = \begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix}$ такого, что $\alpha\beta^{-1} = (\gamma^{js_2} + \gamma^{-js_2} - 2)(\gamma^{is_1} + \gamma^{-is_1} - 2)^{-1}$, существует $v = \begin{pmatrix} 1 & \mu \\ 0 & 1 \end{pmatrix} \neq y$. Для μ имеем неравенство

$$\alpha\mu^{-1} \neq (\gamma^{js_2} + \gamma^{-js_2} - 2)(\gamma^{is_1} + \gamma^{-is_1} - 2)^{-1},$$

и тогда $\Gamma^{(i_{s_1})}(u) \cap \Gamma^{(j_{s_2})}(v) = \emptyset$, то есть $p_{i_{s_1}j_{s_2}}^1(u, v) = 0$.

Наконец, пусть снова $x = \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}$, $y = \begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix}$ зафиксированы, i, j, k из J – такие, что $p_{ij}^1(x, y) \neq 0$ и $p_{ik}^1(x, y) \neq 0$. Тогда существуют z и u такие, что $(x, z) \in R_i$, $(z, y) \in R_j$, $(x, u) \in R_i$, $(u, y) \in R_k$. Так как силовая p -подгруппа

P (она содержит x и y) действует транзитивно на $Syl_p(G) \setminus \{P\}$, из x исходит в точности q рёбер, и все в разные силовские p -подгруппы группы $SL_2(q)$, то для некоторого $g \in P$ имеем $(x, z)^g = (x, z^g) = (x, u) \in R_i$, то есть $z^g = u$. Тогда $(z, y)^g = (z^g, y) = (u, y) \in R_j$, то есть $j = k$. Отсюда вытекает, что если для фиксированных x и y имеет место $p_{ij}^1(x, y) \neq 0$, то для любого $k \in J \setminus \{j\}$ имеет место равенство $p_{ik}^1(x, y) = 0$.

Пусть теперь q – нечётно, и один из индексов i_{s_1} или j_{s_2} равен q , скажем, $j_{s_2} = q$. В этом случае $s_1 = s$. Снова рассуждаем как в предыдущем случае (как в случае $i_{s_1}, j_{s_2} \notin \{q\}$):

Если $z \in \Gamma^{(i_{s_1})}(x) \cap \Gamma^{(q)}(y)$, то

$$z = \begin{pmatrix} 1 - \eta\delta & -\eta\delta^2 \\ \eta & 1 + \eta\delta \end{pmatrix} = \begin{pmatrix} 1 - 4\beta^{-1}\delta_1 & -4\beta^{-1}\delta_1^2 \\ 4\beta^{-1} & 1 + 4\beta^{-1}\delta_1 \end{pmatrix},$$

откуда $\eta = 4\beta^{-1}$. При этом $\gamma^{is} + \gamma^{-is} = 2 - \alpha\eta$, то есть

$$\eta = -\alpha^{-1}(\gamma^{is} + \gamma^{-is} - 2) = 4\beta^{-1}.$$

Значит, $4\alpha\beta^{-1} = -(\gamma^{is} + \gamma^{-is} - 2)$. Теперь фиксируем is , что означает фиксацию $\gamma^{is} + \gamma^{-is} - 2$, и так же, как и в случае $(i_s, j_s) \in I \times I$, получаем, что для некоторого фиксированного x существует единственный y с $p_{isq}^1(x, y) \neq 0$, и в каждой R_1 -кликке всего имеется в точности $q-1$ пар элементов x и y указанным условием.

Ясно, что для данной пары (i_{s_1}, j_{s_2}) ($j_{s_2} = q$) также существуют u и v , такие, что $p_{is_1q}^1(u, v) = 0$.

Наконец, если $p_{iq}^1(u, v) \neq 0$, то для любого $k \in J$ имеем $p_{ik}^1(x, y) = 0$.

Лемма доказана. $\square$

Лемма 2.7. Если q – чётно, то для любых i, j, k из J имеет место равенство $p_{ij}^k = 1$.

Пусть q – нечётно. Тогда если k – индекс первого типа, то

$$p_{ij}^k = \begin{cases} 2, & \text{если } i \text{ и } j - \text{индексы одного типа,} \\ 0, & \text{если } i \text{ и } j - \text{индексы разных типов.} \end{cases}$$

Если k – индекс второго типа, то

$$p_{ij}^k = \begin{cases} 0, & \text{если } i \text{ и } j - \text{индексы одного типа,} \\ 2, & \text{если } i \text{ и } j - \text{индексы разных типов.} \end{cases}$$

В частности, если x и y лежат в одном классе сопряжённых элементов, то для любых $i, k \in J$ имеет место равенство $p_{ii}^k = 2$, а если x с y лежат в разных классах сопряжённости, то $p_{ii}^k = 0$.

Доказательство. Доказательство сначала проведём для нечётного q .

Пусть $k \in J$ и $(x, y) \in R_k$. Будем считать, что $x \in P^\sharp$: $x = \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}$. Покажем, что можно считать $y \in Q^\sharp$. Действительно, если $y = \begin{pmatrix} 1 - \beta\delta & -\beta\delta^2 \\ \beta & 1 + \beta\delta \end{pmatrix}$, то, подействовав элементом $u = \begin{pmatrix} 1 & -\delta \\ 0 & 1 \end{pmatrix}$ на пару (x, y) сопряжением, получим $(x, y)^u = (x^u, y^u) = (x, y^u) \in R_k$, где

$$y^u = \begin{pmatrix} 1 & \delta \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 - \beta\delta & -\beta\delta^2 \\ \beta & 1 + \beta\delta \end{pmatrix} \cdot \begin{pmatrix} 1 & -\delta \\ 0 & 1 \end{pmatrix} =$$

$$= \begin{pmatrix} 1 & \delta \\ \beta & 1 + \beta\delta \end{pmatrix} \cdot \begin{pmatrix} 1 & -\delta \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ \beta & 1 \end{pmatrix},$$

так что можем считать, что $y = \begin{pmatrix} 1 & 0 \\ \beta & 1 \end{pmatrix}$.

Отдельно рассмотрим случаи $(i, j) \in I \times I$, $(i, j) \in I \times \{q\}$, $(i, j) \in \{q\} \times I$ и $(i, j) = (q, q)$.

Случай 1. $(i, j) \in I \times I$. Пусть z – такой, что $(x, z) \in R_i$ и $(z, y) \in R_j$. Тогда, с одной стороны, $z = \begin{pmatrix} 1 - \eta\delta & -\eta\delta^2 \\ \eta & 1 + \eta\delta \end{pmatrix} \in \Gamma^{(i)}(x)$, а с другой стороны $z = \begin{pmatrix} 1 + \varepsilon\delta_1 & \varepsilon \\ -\varepsilon\delta_1^2 & 1 - \varepsilon\delta_1 \end{pmatrix} \in \Gamma^{(j)}(y)$. Приходим к системе

$$\begin{cases} 1 - \eta\delta = 1 + \varepsilon\delta_1, \\ -\eta\delta^2 = \varepsilon, \\ \eta = -\varepsilon\delta_1^2, \\ 1 + \eta\delta = 1 - \varepsilon\delta_1, \end{cases}$$

которая равносильна системе

$$\begin{cases} -\eta\delta = \varepsilon\delta_1, \\ -\eta\delta^2 = \varepsilon, \\ \eta = -\varepsilon\delta_1^2, \end{cases}$$

откуда получаем, что $\varepsilon = -\eta\delta^2$ и $\delta = -\varepsilon\eta^{-1}\delta_1$. В частности, это означает, что $\delta^2 = -\varepsilon\eta^{-1}$ – квадратичный вычет поля F_q , а также что $-\varepsilon$ и η имеют одинаковый тип квадратичности.

Таким образом, если

$$z = \begin{pmatrix} 1 - \eta\delta & -\eta\delta^2 \\ \eta & 1 + \eta\delta \end{pmatrix} = \begin{pmatrix} 1 + \varepsilon\delta_1 & \varepsilon \\ -\varepsilon\delta_1^2 & 1 - \varepsilon\delta_1 \end{pmatrix} \in \Gamma^{(i)}(x) \cap \Gamma^{(j)}(y),$$

то $-\varepsilon\eta^{-1} = \delta^2$ – квадратичный вычет поля F_q . Ясно, что верно и обратное: если η и ε определяют окрестности $\Gamma^{(i)}(x)$ и $\Gamma^{(j)}(y)$ соответственно $x = \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}$ и $y = \begin{pmatrix} 1 & 0 \\ \beta & 1 \end{pmatrix}$, и $-\varepsilon\eta^{-1}$ – квадратичный вычет поля F_q , то существует z такой, что $(x, z) \in R_i$ и $(z, y) \in R_j$. Очевидно, z можно найти по уравнениям $-\varepsilon\eta^{-1} = \delta^2$, $\delta_1 = -\varepsilon\eta^{-1}\delta_1$. Решений квадратичного уравнения

$$x^2 = -\varepsilon\eta^{-1} \quad (2.8)$$

либо не существует, либо их в точности два. Но это уравнение разрешимо в точности тогда, когда $-\varepsilon$ и η имеют одинаковый тип квадратичности.

Таким образом, для того, чтобы $p_{ij}^k(x, y) = 2$, необходимо и достаточно, чтобы $-\varepsilon$ и η имели одинаковую чётность, где η и ε определяют окрестности соответственно $\Gamma^{(i)}(x)$ и $\Gamma^{(j)}(y)$. При этом число $p_{ij}^k(x, y)$ не зависит от выбора x и y : $p_{ij}^k(x, y) = p_{ij}^k = 2$. Осталось перевести это условие равенства $p_{ij}^k = 2$ в термины видов индексов k, i, j .

Пусть k – индекс первого типа, то есть x и y сопряжены. Тогда если $z \in \Gamma^{(i)}(x) \cap \Gamma^{(j)}(y)$, то либо z лежит в $x^G = y^G$, и тогда оба индекса i и j – индексы

первого типа, либо $z \notin x^G = y^G$, и тогда i и j – индексы второго типа. В любом случае i и j – индексы одного типа. И в этом случае $p_{ij}^k(x, y) = p_{ij}^k = 2$. Ясно, что если i и j – индексы разных типов, то $p_{ij}^k(x, y) = p_{ij}^k = 0$.

Пусть k – индекс второго типа, то есть $x^G \neq y^G$. Тогда если $z \in \Gamma^{(i)}(x) \cap \Gamma^{(j)}(y)$, то z лежит либо в x^G , либо в y^G . В любом случае i и j – индексы разных типов, и при этом $p_{ij}^k(x, y) = p_{ij}^k = 2$. Если же i и j – индексы одного типа, то $p_{ij}^k(x, y) = p_{ij}^k = 0$.

Случай 2. $(i, j) \in I \times \{q\}$. Тогда

$$z = \begin{pmatrix} 1 - \eta\delta & -\eta\delta^2 \\ \eta & 1 + \eta\delta \end{pmatrix} = \begin{pmatrix} 1 + 4\beta^{-1}\delta_1 & 4\beta^{-1} \\ -4\beta^{-1}\delta_1^2 & 1 - 4\beta^{-1}\delta_1 \end{pmatrix} \in \Gamma^{(i)}(x) \cap \Gamma^{(j)}(y).$$

Приходим к системе

$$\begin{cases} 1 - \eta\delta = 1 + 4\beta^{-1}\delta_1, \\ -\eta\delta^2 = 4\beta^{-1}, \\ \eta = -4\beta^{-1}\delta_1^2, \\ 1 + \eta\delta = 1 - 4\beta^{-1}\delta_1, \end{cases}$$

которая равносильна системе

$$\begin{cases} \eta\delta = 4\beta^{-1}\delta_1, \\ -\eta\delta^2 = 4\beta^{-1}, \\ \eta = -4\beta^{-1}\delta_1^2, \end{cases}$$

откуда получаем, что $\delta^2 = -4\beta^{-1}\eta^{-1}$ – квадратичный вычет поля F_q .

Обратно, если η и β такие, что $-4\beta^{-1}\eta^{-1}$ – квадратичный вычет поля F_q , то существует z такой, что $(x, z) \in R_i$ и $(z, y) \in R_q$. А для этого необходимо и достаточно, чтобы -4β и η имели одинаковый тип квадратичности. Остальное для этого случая доказывается дословно предыдущему.

Случай 3. $(i, j) \in \{q\} \times I$. Рассматривается аналогично.

Случай 4. $(i, j) = (q, q)$. Тогда,

$$z = \begin{pmatrix} 1 - 4\alpha^{-1}\delta & -4\alpha^{-1}\delta^2 \\ 4\alpha^{-1} & 1 + 4\alpha^{-1}\delta \end{pmatrix} = \begin{pmatrix} 1 + 4\beta^{-1}\delta_1 & 4\beta^{-1} \\ -4\beta^{-1}\delta_1^2 & 1 - 4\beta^{-1}\delta_1 \end{pmatrix} \in \Gamma^{(q)}(x) \cap \Gamma^{(q)}(y),$$

откуда приходим к системе

$$\begin{cases} 1 - 4\alpha^{-1}\delta = 1 + 4\beta^{-1}\delta_1, \\ -4\alpha^{-1}\delta^2 = 4\beta^{-1}, \\ 4\alpha^{-1} = -4\beta^{-1}\delta_1^2, \\ 1 + 4\alpha^{-1}\delta = 1 - 4\beta^{-1}\delta_1, \end{cases}$$

которая равносильна системе

$$\begin{cases} \alpha^{-1}\delta = -\beta^{-1}\delta_1, \\ \delta^2 = -\alpha\beta^{-1}, \\ \delta_1^2 = -\alpha^{-1}\beta, \end{cases} \quad (2.9)$$

Ясно, что $-4\alpha^{-1}$ и $4\beta^{-1}$ имеют одинаковый тип квадратичности тогда и только тогда, когда $-\alpha^{-1}$ и β имеют одинаковый тип квадратичности. Поэтому требуемый z существует тогда и только тогда, когда $-\alpha^{-1}\beta$ – квадратичный вычет, и $p_{ij}^k(x, y) = \begin{cases} 2, \text{ если } x^G = y^G, \\ 0, \text{ если } x^G \neq y^G. \end{cases}$

Случай чётного q рассматривается аналогично нечётному случаю. Нюанс только в том, что рассмотрение свободно от подслучаев 2 – 4 предыдущего нечётного для q случая, понятий квадратичности вычетов поля, и ввиду того,

что аналог уравнения (2.8) (который совпадает с ним) всегда имеет решение, и оно единственно, получается равенство $p_{ij}^k(x, y) = 1$, которое не зависит от выбора x и y : $p_{ij}^k(x, y) = p_{ij}^k = 1$.

Лемма доказана. $\square$

Теперь доказательство **теоремы 1** вытекает из **лемм 2.4 – 2.7**.

Лемма 2.8. Пусть q – чётно и $i \in J$. Тогда граф $\Gamma^{(i)}$ является дистанционно регулярным графом с массивом пересечений $\{q, q - 2, 1; 1, 1, q\}$.

Доказательство. В силу **предложения 1.1** достаточно показать, что $\Gamma^{(i)}$ является обобщённым икосаэдром $I(q, 1)$.

То, что граф $\Gamma^{(i)}$ состоит из $q^2 - 1$ вершин, вытекает из выбора множества вершин.

Так как q – чётно, то $p_{ii}^i = |\Gamma^{(i)}(x) \cap \Gamma^{(i)}(y)| = 1$ для любых двух смежных вершин x и y . Поэтому для $x \in \Gamma^{(i)}(g)$ существует единственная вершина y такая, что $y \in \Gamma^{(i)}(g) \cap \Gamma^{(i)}(x)$. Кроме того, $n_i = \deg \Gamma^{(i)} = q$. Поэтому $[g]$ – объединение $q/2$ треугольников с единственной общей вершиной g , и $[g]$ – 2^{m-1} -мельница.

Для любой вершины g совершенным кодом $C(g)$ радиуса 1, содержащим g , является $C_G(g) \cap g^G$, так как для любых x и y из $C_G(g) \cap g^G$ имеем $[x] \cap [y] = \emptyset$ и $|\bigcup_{x \in C(g)} x^\perp| = \sum_{i=1}^{q-1} |x^\perp| = (q-1)(q+1) = (q^2-1)$, то есть шары $x^\perp$ радиуса 1 с центрами из $C_G(g) \cap g^G$ образуют разбиение множества вершин графа $\Gamma^{(i)}$.

Пусть x и y – произвольные вершины из $C(g) = C_G(g) \cap g^G$ и $u \in \Gamma^{(i)}(x)$. Тогда $(y, u) \in R_k$ для некоторого $k \in J$. По **лемме 2.7** $p_{ii}^k = 1$. Это означает, что u смежна в точности с одной вершиной из $\Gamma^{(i)}(y)$.

Лемма доказана. $\square$

Лемма 2.9. Пусть $i \in J$ и q – нечётно. Если i – индекс первого типа, то граф $\Gamma^{(i)}$ является несвязным с двумя компонентами связности – дистанционно регулярными графами с массивами пересечений $\{q, q - 3, 1; 1, 2, q\}$.

Доказательство. Ясно, что оба класса сопряжённых неединичных p -элементов составляют множества вершин двух связных компонент графа $\Gamma^{(i)}$.

Покажем, что отдельно взятая компонента связности графа $\Gamma^{(i)}$ является дистанционно регулярным графом с массивом пересечений $\{q, q - 3, 1; 1, 2, q\}$. Для этого, как и в чётном случае, достаточно доказать, что связная компонента графа $\Gamma^{(i)}$ является обобщённым икосаэдром.

То, что связная компонента состоит из $(q^2-1)/2$ вершин, вытекает из выбора множества вершин.

Пусть g – произвольная вершина графа $\Gamma^{(i)}$. Так как $|g^\perp| = q$ и $|C_G(g)| = q$, то $C_G(g)$ действует на $\Gamma^{(i)}(g)$ транзитивно. Пусть x и y – смежные вершины из $\Gamma^{(i)}(g)$, то есть пусть $(x, y) \in R_i$.

В силу транзитивности $C_G(g)$ на $\Gamma^{(i)}(g)$ существует $\alpha \in C_G(g)$ такой, что $x^\alpha = y$. Но все элементы из $C_G(g) \setminus \{e\}$ имеют порядок p . Это означает, что x и y лежат в орбите длины p , которая в силу $p_{ii}^k(x, y) = 2 \neq 0$ (по **лемме 2.7**) является простым циклом длины p (в графе $\Gamma^{(i)}$). Отсюда вытекает, что $\Gamma^{(i)}(g)$ разбивается на p^{m-1} простых циклов длины p , а подграф $x^\perp$ графа $\Gamma^{(i)}$ представляет собой связку из p^{m-1} p -пирамид.

Для любой вершины g совершенным кодом $C(g)$ радиуса 1, содержащим g , является $C_G(g) \cap g^G$, так как для любых x и y из $C_G(g) \cap g^G$ имеем $[x] \cap [y] = \emptyset$ и $|\bigcup_{x \in C(g)} x^\perp| = \sum_{i=1}^{(q-1)/2} |x^\perp| = ((q-1)/2)(q+1) = (q^2-1)/2$, то есть шары $x^\perp$ радиуса 1 с центрами из $C_G(g) \cap g^G$ образуют разбиение множества вершин связной компоненты, содержащей g .

Пусть x и y – произвольные вершины из $C(g) = C_G(g) \cap g^G$ и $u \in \Gamma^{(i)}(x)$. Тогда $(y, u) \in R_k$ для некоторого $k \in J$, и u лежит в той же компоненте, где лежат x и y . По **лемме 2.7** $p_{ii}^k(y, u) = 2$, что означает, что u смежна в точности с двумя вершинами из $\Gamma^{(i)}(y)$.

Лемма доказана. $\square$

Лемма 2.10. Пусть $i \in J$ и q – нечётно. Если i – индекс второго типа, то граф $\Gamma^{(i)}$ является почти дистанционно регулярным графом диаметра 4 с массивом пересечений $\{q, q-1, q-2, b_3(x, y); 1, 2, c_3(x, y), q\}$, где

$$b_3(x, y) = \begin{cases} 0, & \text{если } y \in C_G(x), \\ 1, & \text{если } y \notin C_G(x), \end{cases} \quad c_3(x, y) = \begin{cases} q, & \text{если } y \in C_G(x), \\ q-1, & \text{если } y \notin C_G(x). \end{cases}$$

При этом граф 2-расстояний графа $\Gamma^{(i)}$ имеет в точности две компоненты связности, каждая из которых является сильно регулярным графом с параметрами $((q^2-1)/2, q(q-1)/2, (q-1)^2/2, q(q-1)/2)$.

Доказательство. Так же, как и в предыдущей лемме, достаточно показать, что граф $\Gamma^{(i)}$ является псевдоикосаэдром $PI(q)$.

То, что $\Gamma^{(i)}$ удовлетворяет пункту 1 определения псевдоикосаэдра, тривиально, а то, что удовлетворяет пункту 3, доказывается дословно предыдущей лемме с той лишь разницей, что теперь в качестве $C(g)$ выступает $C_G(g) \setminus \{e\}$.

То, что $g^\perp$ является звездой (и тем самым $\Gamma^{(i)}$ удовлетворяет пункту 2), вытекает из того, что если x и y лежат в $\Gamma^{(i)}(g)$, то они лежат в одном классе (отличном от g^G) и поэтому не могут лежать в окрестности друг друга.

Для того, чтобы показать, что $\Gamma^{(i)}$ удовлетворяет пункту 4 определения псевдоикосаэдра, покажем, что в качестве V_1 и V_2 можно взять соответственно C_2 и C_3 . Пусть $x \in C_2 \cap C_G(g)$ и $y \in C_3 \cap C_G(g)$, $u \in \Gamma^{(i)}(x)$. Но тогда по условию x и u лежат в разных классах. Значит, u и y лежат в одном классе. Тогда по **лемме 2.7** $p_{ii}^k = 2$, то есть вершина u из $\Gamma^{(i)}(x)$ смежна в точности с двумя вершинами из $\Gamma^{(i)}(y)$, и, наоборот, любая вершина из $\Gamma^{(i)}(y)$ смежна в точности с двумя вершинами из $\Gamma^{(i)}(x)$. Наконец, если $x, z \in C_s \cap C_G(g)$ ($s = 2, 3$), то вершины из $\Gamma^{(i)}(x)$ и $\Gamma^{(i)}(z)$ не могут быть смежными, так как они лежат в одном классе сопряжённости.

Лемма доказана. $\square$

Теперь из доказанных **лемм 2.2, 2.3, 2.9** и **2.10** вытекает доказательство **теоремы 2**. Например, покажем вывод **теоремы** для первого случая.

Пусть $i \in I_1$ – чётное, или $i \in I_2$ – нечётное, или $q \equiv 1 \pmod{4}$ и $i = q$. В этих случаях по **леммам 2.2** и **2.3** из того, что $(x, y) \in R_i$ вытекает, что x и y лежат в одном классе сопряжённых элементов, то есть индекс i является индексом первого типа. Но тогда из **леммы 2.9** вытекает, что $\Gamma^{(i)}$ является несвязным с двумя компонентами связности – почти дистанционно регулярными графами с одинаковыми массивами пересечений $\{q, q-3, 1; 1, 2, q\}$.

Если $i \in I_1$ – нечётное, или $i \in I_2$ – чётное, или $q \equiv -1 \pmod{4}$ и $i = q$, то снова по **леммам 2.2** и **2.3** индекс i является индексом второго типа. Тогда из **леммы 2.10** вытекает, что $\Gamma^{(i)}$ является почти дистанционно регулярным (но не дистанционно регулярным) с указанным массивом пересечений и указанным свойством графа $\Gamma_2^{(i)}$ 2-расстояний.

Теорема доказана.

Наконец, докажем **теорему 3**.

Ясно, что при $\{0, 1\} \cup I_1 \cup I_2 \cup \{q\}$ отношения R_i определяют схему на одном и том же классе C сопряжённых элементов порядка p тогда и только тогда, когда i – индексы первого типа. По **леммам 2.2** и **2.3** это имеет место тогда и только тогда, когда либо $i \in I_1$ – чётное, либо $i \in I_2$ – чётное, либо $i = q$ и $q \equiv 1 \pmod{4}$. Остальные утверждения теоремы непосредственно вытекают из **теорем 1** и **2**.

Теорема доказана.

REFERENCES

- [1] I.T. Mukhametianov, *Graphs on conjugate involutions class of group $L_2(2^m)$* , Nauchnoe obozrenie, **5** (2013), 133–141.
- [2] I.T. Mukhametianov, *About distance-regular graphs on set of non-unit p -lements of group $L_2(p^m)$* , Trudy Inst. Mat. Mekh. UrO RAN, **18**:3 (2012), 164–178.
- [3] I.T. Mukhametianov, *Graphs on conjugate p -elements class of group $L_2(p^m)$* , Nauchnoe obozrenie, **9** (2013), 105 – 113.
- [4] A.E. Brouwer, A.M. Cohen, A. Neumaier, *Distance-Regular Graphs*, Berlin; Heidelberg; New York: Springer-Verlag, 1989. Zbl 0747.05073
- [5] V.A. Belonogov, *About small interactions in finite groups*, Trudy Inst. Mat. Mekh. UrO RAN, **2** (1992), 3–18. Zbl 0816.20011
- [6] L. Dornhoff, *Group representation theory*, Pt. A.N.Y.: Marcel Dekker, 1971. Zbl 0227.20002
- [7] S.V. Goryainov, *On isomorphism between distance-regular graphs*, Siberian Electronic Mathematical Reports, **11** (2014), 311–320. Zbl 1326.05094
- [8] Eiichi Bannai, Tatsuro Ito, *Algebraic Combinatorics I: Association Schemes*: Translated from English: Mir, 1987. Zbl 0685.05030

ILDAR TALGATOVICH MUKHAMETIANOV

LYSVA BRANCH OF PERM NATIIONAL RESEARCH POLYTECHNIC UNIVERSITY,
2, LENINA ST.

LYSVA, 618900, PERM KRAY, RUSSIA

E-mail address: muiltal@yandex.ru