

Графы Деза, связанные с пересечениями сопряжённых подгрупп в группах $SL_2(q)$

М.П. Голубятников, Н.В. Маслова

ИММ УрО РАН

Пусть G конечная группа $H \leq G$. Обозначим

$$\mathcal{H} = \{H^g \mid g \in G\},$$

множество всех подгрупп G сопряжённых H .

Построим граф $\Gamma(G, H, d)$ следующим образом. Вершины графа являются элементами множества $\mathcal{H}$, и две вершины $H_1, H_2 \in \mathcal{H}$ смежны тогда и только тогда, когда $|H_1 \cap H_2| = d$.

Пример 1

Пусть $G = A_5$ и $H = \langle (3, 4, 5), (1, 2)(4, 5) \rangle < G$, тогда $H \cong S_3$ и $\Gamma(G, H, 2)$ является графом Петерсона.

Пример 2

Пусть $G = A_6$ и $H = \langle (3, 6)(4, 5), (1, 2)(3, 4) \rangle < G$, тогда $H \cong D_4$ и $\Gamma(G, H, 4)$ является дистанционно регулярным графом с массивом пересечений $\{4, 2, 2, 2; 1, 1, 1, 2\}$ (рёберный граф 8-клетки Татта)

Пример 3

Пусть $G = PSU_3(5)$ и $H \cong M_{10}$.

Тогда различные подгруппы из $\mathcal{H}$ могут пересекаться по 720, 60, 10 или по 8 элементам. Через A_0, A_1, A_2, A_3 обозначим матрицы смежности графов $\Gamma(G, H, 720)$, $\Gamma(G, H, 60)$, $\Gamma(G, H, 10)$ и $\Gamma(G, H, 8)$ соответственно.

Тогда матрицы $A_0 = E, A_1, A_2, A_3$ образуют P -полиномиальную схему отношений и $\Gamma(G, H, 60)$ является дистанционно регулярным графом с массивом пересечений $\{12, 6, 5; 1, 1, 4\}$ (рёберный граф графа Хоффмана-Синглтона).

Примеры

Пример 4

Пусть $G = PSp_4(3)$ и $H \cong C_3 \times ((C_3 \times C_3) \rtimes C_2)$.

Тогда различные подгруппы из $\mathcal{H}$ могут пересекаться по 54, 27, 3, 2 или по 1 элементам. И аналогично определённые матрицы $A_0 = E, A_1, A_2, A_3, A_4$ образуют схему отношений с 4 классами и матрицей собственных значений

$$\begin{pmatrix} 1 & 2 & 36 & 27 & 54 \\ 1 & 2 & 6 & -3 & -6 \\ 1 & 2 & -12 & 3 & 6 \\ 1 & -1 & 0 & 9 & -9 \\ 1 & -1 & 0 & -3 & 3 \end{pmatrix}.$$

Данная схема не является ни P - ни Q - полиномиальный.

Примеры

Пример 5

Пусть $G = PGL_3(4)$ и $H \cong A_6$.

Тогда различные подгруппы из $\mathcal{H}$ могут пересекаться по 360, 36, 18, 10 или по 8 элементам. И аналогично определённые матрицы $A_0 = E, A_1, A_2, A_3, A_4$ образуют схему отношений с 4 классами и матрицей собственных значений

$$\begin{pmatrix} 1 & 10 & 40 & 72 & 45 \\ 1 & 10 & -20 & -36 & 45 \\ 1 & 2 & 0 & 0 & -3 \\ 1 & -4 & 12 & -12 & 3 \\ 1 & -4 & -6 & 6 & 3 \end{pmatrix}$$

Данная схема является Q -полиномиальной с упорядочением 0, 3, 2, 4, 1.

Предварительная часть

Зафиксируем простое число p и целое число $m > 0$. Пусть $\mathbb{F} = GF(q)$ - поле с $q = p^m$ элементов и $SL_2(q) = SL_2(\mathbb{F})$ - специальная линейная группа, т. е. группа обратимых 2×2 матриц над $\mathbb{F}$ с определителем 1.

Мы изучаем граф $\Gamma(G, H, 8)$ для случая $G = SL_2(q)$, где $q \equiv 1 \pmod{4}$ и $H = \Delta$, где

$$\Delta = \left\{ \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \mid a \in \mathbb{F}^* \right\} \cup \left\{ \begin{pmatrix} 0 & a \\ -a^{-1} & 0 \end{pmatrix} \mid a \in \mathbb{F}^* \right\},$$

и $d = 8$, т.е. вершины A и B смежны тогда и только тогда, когда $|A \cap B| = 8$.

Предварительная часть

Множество Δ образует подгруппу порядка $2(q-1)$. Поскольку $\Delta/Z(G) = D_{\frac{q-1}{2}}$ и $D_{\frac{q-1}{2}}$ - максимальная подгруппа в $G/Z(G) = PSL_2(q)$, то подгруппа Δ является максимальной подгруппой в G . Следовательно $N_G(\Delta) = \Delta$. Пусть до конца работы $\Gamma = \Gamma(SL_2(q), \Delta, 8)$, $\mathbb{F} = GF(q)$ с $q \equiv 1 \pmod{4}$ и

$$\mathcal{D} = \left\{ \Delta^P \mid P \in G \right\}.$$

Через ξ обозначим элемент поля $\mathbb{F} = GF(q)$, обладающий свойством $\xi^2 = -1$. Основная цель работы доказать следующую теорему.

Теорема

Граф Γ является реберно-регулярным графом Деза с $\lambda = 1$ и параметрами:

$$\left(\frac{q(q+1)}{2}, \frac{q-1}{2}, 1, 0 \right).$$

Структура группы Δ и $\Delta \cap \Delta^P$

Обозначим

$$R_a = \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}, \quad S_a = \begin{pmatrix} 0 & a \\ -a^{-1} & 0 \end{pmatrix}$$

Справедлива следующая лемма

Лемма 1

Пусть $P \in G \setminus \Delta$, и $PT_aP^{-1} = T_b$, где $T \in \{R, S\}$ и некоторых $a, b \in \mathbb{F}^*$, то выполнено одно из следующих утверждений

- 1 $PR_aP^{-1} = R_b$, тогда и только тогда, когда $a = b$ и $a^2 = 1$;
- 2 $PR_aP^{-1} = S_b$, тогда и только тогда, когда $a^2 = -1$ и матрица P имеет вид

$$\begin{pmatrix} x \frac{b}{a} & -\frac{1}{2x} \\ x & \frac{a}{2xb} \end{pmatrix} \text{ для некоторого } x \in \mathbb{F}^*.$$

Структура группы Δ и $\Delta \cap \Delta^P$

Лемма (продолжение)

3 $PS_aP^{-1} = R_b$, тогда и только тогда, когда $b^2 = -1$ и матрица P имеет вид

$$\begin{pmatrix} \frac{x}{ab} & -x \\ \frac{1}{2x} & \frac{ab}{2x} \end{pmatrix} \text{ для некоторого } x \in \mathbb{F}^*.$$

4 $PS_aP^{-1} = S_b$, тогда и только тогда, когда матрица P имеет вид

$$\begin{pmatrix} xb & -aby \\ y & xa \end{pmatrix}, \text{ для некоторых } x, y \in \mathbb{F}^*, x^2 + y^2 = (ab)^{-1}.$$

Более того, для фиксированной матрицы P указанного вида, равенство $PS_{a'}P^{-1} = S_{b'}$ выполняется тогда и только тогда, когда $(a', b') = (a, b)$ или $(a', b') = (-a, -b)$.

Структура группы Δ и $\Delta \cap \Delta^P$

Набросок доказательства

Пусть

$$P = \begin{pmatrix} p_{11} & p_{12} \\ p_{21} & p_{22} \end{pmatrix}.$$

Рассмотрим случай $PR_aP^{-1} = S_b$. Имеем

$$PR_a - S_bP = \begin{pmatrix} ap_{11} - bp_{21} & a^{-1}p_{12} - bp_{22} \\ b^{-1}p_{11} + ap_{21} & b^{-1}p_{12} + a^{-1}p_{22} \end{pmatrix} = 0. \quad (1)$$

На матричное уравнение 1 можно смотреть как на систему линейных уравнений относительно $p_{11}, p_{12}, p_{21}, p_{22}$ с определителем

Структура группы Δ и $\Delta \cap \Delta^P$

Введём обозначения:

$$\mathcal{R} = \left\{ \begin{pmatrix} \alpha & -\frac{1}{2\beta} \\ \beta & \frac{1}{2\alpha} \end{pmatrix} \mid \alpha, \beta \in \mathbb{F}^* \right\}.$$

Заметим, что множество матриц $\mathcal{R}$ совпадает с множеством матриц вида (2) из леммы. Действительно, для матрицы $P_{\alpha,\beta} \in \mathcal{R}$ имеем

$$\begin{aligned} PR_{\xi}P^{-1} &= S_{\frac{\alpha}{\beta}\xi}, \\ PR_{-\xi}P^{-1} &= S_{-\frac{\alpha}{\beta}\xi}. \end{aligned}$$

Лемма 2

Пусть $\Delta^P \in \mathcal{D}$, тогда $|\Delta \cap \Delta^P| \in \{2(q-1), 8, 4, 2\}$. Более того, $|\Delta \cap \Delta^P| = 8$ тогда и только тогда, когда $P \in \mathcal{R}$.

Структура окрестности вершины Δ

Опишем структуру окрестности вершины Δ в графе Γ .

Введём на множестве матриц $\mathcal{R}$ отношение эквивалентности следующим образом:

$$P_1 \sim P_2 \Leftrightarrow P_2^{-1}P_1 \in \Delta.$$

Лемма

Пусть $\Gamma(\Delta)$ окрестность вершины Δ в графе Γ . $\Gamma(\Delta^P) = \Gamma(\Delta^Q)$ тогда и только тогда, когда $P \sim Q$. Более того,

$$|\Gamma(\Delta)| = |\mathcal{R}/\sim| = \frac{q-1}{2}$$

Количество элементов в пересечении двух окрестностей

Пусть $Q \in G$, тогда число $|\Gamma(\Delta) \cap \Gamma(\Delta^Q)|$ равно числу попарно неэквивалентных матриц $P \in \mathcal{R}$, таких что

$$P^{-1}QS \in \Delta$$

для некоторой матрицы $S \in \mathcal{R}$.

Действительно, множество смежных с Δ вершин совпадает с множеством Δ^P для P из $\mathcal{R}$. Множество смежных с Δ^Q вершин это множество Δ^Q сопряжённое с помощью матриц вида S^Q , где S из $\mathcal{R}$. Получаем, что пересечение окрестностей - это мощность множества пар верши P из R которых существует S из $\mathcal{R}$ со свойством $\Delta^P = (\Delta^Q)^{S^Q}$.

То есть,

$$P\Delta P^{-1} = (QSQ^{-1})Q\Delta Q^{-1}(QSQ^{-1})^{-1} = QS\Delta S^{-1}Q^{-1}.$$

Лемма

Пусть $Q \in G$, тогда $|\Gamma(\Delta) \cap \Gamma(\Delta^Q)| \leq 1$.

Более того, для матрицы $Q = \begin{pmatrix} q_{11} & q_{12} \\ q_{21} & q_{22} \end{pmatrix}$ выполнено

$|\Gamma(\Delta) \cap \Gamma(\Delta^Q)| = 1$, тогда и только тогда, когда $\frac{q_{12}q_{22}}{q_{11}q_{21}}$ является ненулевым квадратом в $\mathbb{F}$.

Количество элементов в пересечении двух окрестностей

Доказательство

Обозначим

$$P = \begin{pmatrix} x & -\frac{1}{2y} \\ y & \frac{1}{2x} \end{pmatrix}, \quad S = \begin{pmatrix} s_1 & -\frac{1}{2s_2} \\ s_2 & \frac{1}{2s_1} \end{pmatrix}, \quad Q = \begin{pmatrix} q_{11} & q_{12} \\ q_{21} & q_{22} \end{pmatrix}.$$

Тогда $M = P^{-1}QS =$

$$\begin{pmatrix} \frac{q_{21}s_1x + q_{22}s_2x + q_{11}s_1y + q_{12}s_2y}{2xy} & -\frac{q_{21}s_1x - q_{22}s_2x + q_{11}s_1y - q_{12}s_2y}{4s_1s_2xy} \\ q_{21}s_1x + q_{22}s_2x - q_{11}s_1y - q_{12}s_2y & -\frac{q_{21}s_1x - q_{22}s_2x - q_{11}s_1y + q_{12}s_2y}{2s_1s_2} \end{pmatrix}.$$

Для того, чтобы $M \in \Delta$ необходимо, чтобы $M_{0,0} = M_{1,1} = 0$
или $M_{1,0} = M_{0,1} = 0$.

Количество элементов в пересечении двух окрестностей

Доказательство

Рассматривая $M_{0,0} = M_{1,1} = 0$ и $M_{1,0} = M_{0,1} = 0$ как системы уравнений относительно x_1 и y_1 для системы $M_{0,0} = M_{1,1} = 0$ и относительно x_2 и y_2 для системы $M_{1,0} = M_{0,1} = 0$ с определителями

$$\begin{vmatrix} q_{21}s_1 + q_{22}s_2 & q_{11}s_1 + q_{12}s_2 \\ -q_{21}s_1 + q_{22}s_2 & q_{11}s_1 - q_{12}s_2 \end{vmatrix} = 2(q_{11}q_{21}s_1^2 - q_{12}q_{22}s_2^2)$$

и

$$\begin{vmatrix} q_{21}s_1 + q_{22}s_2 & -q_{11}s_1 - q_{12}s_2 \\ -q_{21}s_1 + q_{22}s_2 & -q_{11}s_1 + q_{12}s_2 \end{vmatrix} = 2(q_{11}q_{21}s_1^2 - q_{12}q_{22}s_2^2).$$

Количество элементов в пересечении двух окрестностей

Доказательство

Отсюда $\left(\frac{s_1}{s_2}\right)^2 = \frac{q_{12}q_{22}}{q_{11}q_{21}}$ и

$$\begin{aligned}\frac{x_1}{y_1} &= -\frac{q_{11}s_1 + q_{12}s_2}{q_{21}s_1 + q_{22}s_2} = \frac{q_{11}s_1 - q_{12}s_2}{q_{21}s_1 - q_{22}s_2} \\ \frac{x_2}{y_2} &= \frac{q_{11}s_1 + q_{12}s_2}{q_{21}s_1 + q_{22}s_2} = -\frac{q_{11}s_1 - q_{12}s_2}{q_{21}s_1 - q_{22}s_2} = -\frac{x_1}{y_1},\end{aligned}$$

Таким образом решениями матричного включения $P^{-1}QS \in \Delta$ являются матрицы:

$$P_1 = \begin{pmatrix} x_1 & -\frac{1}{2y_1} \\ y_1 & \frac{1}{2x_1} \end{pmatrix}, \quad P_2 = \begin{pmatrix} x_2 & -\frac{1}{2y_2} \\ y_2 & \frac{1}{2x_2} \end{pmatrix}.$$

При этом $\frac{x_1}{y_1} = -\frac{x_2}{y_2}$, отсюда $x_1y_2 + x_2y_1 = 0$ и матрицы P_1 и P_2 эквивалентны.

Доказательство основной теоремы

Зафиксируем вершину Δ . Окрестность вершины Δ состоит из $\frac{q-1}{2}$ вершины, и в силу транзитивности Γ — регулярный граф степени $\frac{q-1}{2}$.

Далее имеем, что для любой вершины Σ , отличной от Δ число $|\Gamma(\Delta) \cap \Gamma(\Sigma)| \in \{0, 1\}$ и в силу вершинной транзитивности для любых двух вершин Σ_1, Σ_2 имеем $|\Gamma(\Sigma_1) \cap \Gamma(\Sigma_2)| \in \{0, 1\}$.

Таким образом Γ является графом Деза с параметрами:

$$\left(\frac{q(q+1)}{2}, \frac{q-1}{2}, 1, 0 \right).$$

Доказательство основной теоремы

Заметим, что для матрицы $P \in \mathcal{R}$ число

$$\frac{q_{12}q_{22}}{q_{11}q_{21}} = -\frac{1}{4x^2y^2}$$

является ненулевым квадратом в $\mathbb{F}$ и $|\Gamma(\Delta) \cap \Gamma(\Delta^P)| = 1$,
отсюда для любых двух смежных вершин Σ_1 и Σ_2 имеем
 $|\Gamma(\Sigma_1) \cap \Gamma(\Sigma_2)| = 1$.

Существование совершенного 1-кода

Совершенный 1-код в графе Γ это множество вершин C для которого выполняются следующие свойства:

1. Для любых двух вершин $v_1, v_2 \in C$ выполнено
 $(v_1 \cup \Gamma(v_1)) \cap (v_2 \cup \Gamma(v_2)) = \emptyset;$
2. $\bigcup_{v \in C} (v \cup \Gamma(v)) = V(\Gamma).$

Теорема

Множество Δ^{Q_a} , где

$$Q_a = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$$

и $a \in \mathbb{F}$ является совершенным 1-кодом в графе Γ .

Существование совершенного 1-кода

Рассмотрим множество матриц следующего вида

$$\mathcal{C} = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} : a \in \mathbb{F} \right\},$$

Заметим, что $|\mathcal{C}| = |\mathbb{F}| = q$.

Пусть $C(a) = \Delta^{Q_a} \cup \Gamma(\Delta^{Q_a})$, где

$$Q_a = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$$

и $a \in \mathbb{F}$.

Существование совершенного 1-кода

Для любых двух $a, b \in \mathbb{F}$ если $\Delta^{Q_a} \in \Gamma(\Delta^{Q_b})$ то $Q_b^{-1}Q_a \in \mathcal{R}$, но

$$Q_b^{-1}Q_a = \begin{pmatrix} 1 & a-b \\ 0 & 1 \end{pmatrix} \notin \mathcal{R}, \text{ противоречие.}$$

Аналогично, поскольку $Q_b^{-1}Q_a \notin \Delta$ то $\Delta_b^Q \neq \Delta_a^Q$ и так как $\frac{1 \cdot 0}{(a-b) \cdot 1} = 0$ то $|\Gamma(\Delta^{Q_a}) \cap \Gamma(\Delta^{Q_b})| = 0$. Отсюда для любых двух $a, b \in \mathbb{F}$ имеем $C(a) \cap C(b) = \emptyset$.

Наконец для $a \in \mathbb{F}$ мы имеем $|C(a)| = 1 + \frac{q-1}{2} = \frac{q+1}{2}$ и $q \cdot |C(a)| = |V(\Gamma)|$, отсюда $\bigcup_{a \in \mathbb{F}} C(a) = V(\Gamma)$.