Записки научных
семинаров ПОМИ
Том 344, 2007 г.

И. Н. Пономаренко, А. Рахнама Барги

О СТРУКТУРЕ p-СХЕМ

1. Введение

Хорошо известно, что если $G \leqslant \mathrm{Sym}(V)$ – группа перестановок конечного множества V и $\mathcal{R}$ – множество её орбит в естественном действии на V^2, то пара $\mathrm{Inv}(G) = (V, \mathcal{R})$ является схемой отношений на V (по поводу общей теории схем или, в другой терминологии, когерентных конфигураций см. [2, 4, 7], а также §4). Это обстоятельство позволяет рассматривать теорию схем как обобщение теории групп перестановок (в действительности далеко не каждая схема имеет вид $\mathrm{Inv}(G)$ для какой-либо группы перестановок G). В этом смысле естественно спросить, какие схемы соответствуют p-группам. Один из возможных ответов был предложен первым автором в [6]: схема отношений $\mathcal{C} = (V, \mathcal{R})$ называется *p-схемой* для простого числа p, если мощность $|R|$ каждого отношения $R \in \mathcal{R}$ является степенью p (определение 2.1). Однородные p-схемы изучались в [8, 9], где, в частности, найдено обобщение теоремы Силова. Однако общая теория p-схем далека от завершения.

В этой статье мы изучаем произвольные p-схемы. Доказано, что схема $\mathcal{C}$ является p-схемой тогда и только тогда, когда таковой является каждая её однородная компонента (теорема 3.4). Используя этот факт, мы получаем основные результаты настоящей работы, показывающие, в частности, что соответствие Галуа между схемами и группами перестановок (см. (10)) индуцирует соответствие между p-схемами и p-группами.

Теорема 1.1. *Каждое расширение p-схемы является p-схемой.*

Следствие 1.2. *Схема* $\mathrm{Inv}(G)$ *группы перестановок G является p-схемой тогда и только тогда, когда G является p-группой. В част-*

Работа первого автора поддержана грантами РФФИ 05-01-00899 и НШ-4329.2006.1. Автор также благодарит Институт IASBS (the Institute for Advanced Studies in Basic Sciences) за сотрудничество, в рамках которого была выполнена настоящая работа.

ности, группа автоморфизмов произвольной p-схемы является p-группой.

Доказательства теоремы 1.1 и следствия 1.2 содержатся в § 3. Чтобы сделать изложение замкнутым, в § 4 приводятся все необходимые обозначения и определения, касающиеся схем. Наконец, в § 2 доказываются некоторые результаты о p-схемах, используемые в доказательстве теоремы 1.1.

Обозначения. На протяжении всей статьи через V обозначается конечное множество из $n = |V|$ элементов. Мы полагаем $\Lambda(V) = V \times V$ и $\Delta(V) = \{(v, v) : v \in V\}$.

Множество $R \subseteq \Lambda(V)$ называется отношением на V. Носитель V_R отношения R определяется как объединение его области определения и множества значений. Будем говорить, что R – недиагональное отношение, если $R \not\subseteq \Delta(V)$. Мы полагаем $R^T = \{(u, v) : \ (v, u) \in R\}$.

Произведением отношений $R, S \subseteq \Lambda(V)$ называется отношение $RS = \{(u, v) \in \Lambda(V) : (u, w) \in R$ и $(w, v) \in S$ для некоторого $w \in V\}$.

Для множеств $X, Y \subseteq V$ и отношения $R \subseteq \Lambda(V)$ мы полагаем $R_{X,Y} = R \cap (X \times Y)$ и пишем R_X при $X = Y$. Для множества $\mathcal{R}$ отношений на V положим $\mathcal{R}_{X,Y} = \{R_{X,Y} : \ R \in \mathcal{R}\}$.

Под эквивалентностью E на V мы понимаем обычное отношение эквивалентности на подмножестве множества V (совпадающего с V_E). Для $X \subseteq V$ и $R \subseteq \Lambda(V)$ положим $X/E = X/(\Lambda(X) \cap E)$ и $R_{V/E} = \{(X, Y) \in \Lambda(V/E) : R_{X,Y} \neq \emptyset\}$.

Группа всех перестановок множества V обозначается через $\mathrm{Sym}(V)$.

2. p-схемы

На протяжении всей статьи мы фиксируем простое число p. Следующее определение распространяет понятие однородной p-схемы из [8] на неоднородный случай.

Определение 2.1. *Схема называется p-схемой, если мощность каждого её базисного отношения является степенью p.*

Пусть R – базисное отношение схемы $\mathcal{C}$. Тогда $|R| = d \cdot |X|$, где d – степень исхода или степень захода отношения R и X – соответствующая фибра схемы $\mathcal{C}$ (см. (11)). Таким образом, $\mathcal{C}$ – p-схема тогда и только тогда, когда мощность каждой её фибры, а также степень исхода и степень захода каждого её базисного отношения являются степенями числа p. В частности, p-схемами являются ограничения p-схемы на любые объединения её фибр (см. также теорему 3.4 ниже).

Тот факт, что степень однородной p-схемы является степенью числа p, влечёт, что любая такая схема содержит базисное отношение R, для которого $|R_{\mathrm{in}}(v)| = |R_{\mathrm{out}}(v)| = 1$ для всех $v \in V$; ниже каждое отношение произвольной схемы, обладающее этим свойством, называется *тонким*. При $n \geqslant 2$ отношение R может быть выбрано недиагональным. Более того, для любой эквивалентности E однородной схемы $\mathcal{C} = (V, \mathcal{R})$ имеют место равенства

$$|V| = |V/E| \cdot |X|, \quad |R| = |R_{V/E}| \cdot |R_{X,Y}|, \quad R \in \mathcal{R}, \tag{1}$$

для всех $X, Y \in V/E$, таких, что $R_{X,Y} \neq \emptyset$. Таким образом, каждая из схем $\mathcal{C}_X$ и $\mathcal{C}_{V/E}$ является p-схемой.

Пусть теперь $\mathcal{C}$ – произвольная схема. Множество $\mathcal{O} = \mathcal{O}(\mathcal{C})$ всех её тонких отношений назовём *тонким радикалом* этой схемы. Легко видеть, что это множество содержит отношение $\Delta(V)$ и замкнуто относительно произведения отношений. Для каждого $R \in \mathcal{O}$ отображение

$$g_R : V \to V, \quad v \mapsto v^{g_R}, \tag{2}$$

где v^{g_R} – единственный элемент множества $R_{\mathrm{out}}(v)$, является корректно определённой перестановкой множества V. Поскольку, очевидно, $S^{g_R} = R^T S R$ для всех $S \in \mathcal{R}^*$, эта перестановка сохраняет множество $\mathcal{R}^*$ и, следовательно, множество $\mathcal{R}$. Таким образом, $g_R \in \mathrm{Iso}\,(\mathcal{C})$ и множество

$$G_{\mathcal{O}} = \{g_R : \ R \in \mathcal{O}\}$$

является подгруппой группы $\mathrm{Iso}\,(\mathcal{C})$. Эта подгруппа действует естественным образом на множестве фибр схемы $\mathcal{C}$. Ядро $G^*_{\mathcal{O}}$ этого действия состоит из всех перестановок g_R, для которых отношение R является дизъюнктным объединением отношений R_X, где X пробегает множество всех фибр рассматриваемой схемы. Отсюда следует, что

$$G^*_{\mathcal{O}} = \prod_{X \in \mathrm{Fib}\,(\mathcal{C})} G^*_{\mathcal{O}_X}, \tag{3}$$

где $\mathcal{O}_X = \mathcal{O}(\mathcal{C}_X)$.

Теорема 2.2. *Пусть $\mathcal{C}$ – p-схема. Тогда группа $G_{\mathcal{O}}$ (соотв. $G^*_{\mathcal{O}}$) нетривиальна тогда и только тогда, когда схема $\mathcal{C}$ имеет степень $\geqslant 2$ (соотв. нетривиальна). Более того, $G^*_{\mathcal{O}}$ является p-группой.*

Доказательство. Если схема $\mathcal{C}$ тривиальна, то требуемые утверждения следуют из очевидных равенств $G_{\mathcal{O}} = \mathrm{Sym}(V)$ и $G^*_{\mathcal{O}} = \{\mathrm{id}_V\}$, где V – множество её точек. Пусть $\mathcal{C}$ нетривиальна. Тогда в силу равенства (3) можно считать, что $\mathcal{C}$ – однородная схема. Отсюда следует, что $G_{\mathcal{O}} = G^*_{\mathcal{O}}$, и, следовательно, первое утверждение вытекает из упомянутого выше замечания, что в случае нетривиальной однородной p-схемы всегда $\mathcal{O} \neq \{\Delta(V)\}$. Для завершения доказательства заметим, что для всех $R \in \mathcal{O}$ длина каждого цикла перестановки g_R равна $|X|$, где X – класс наименьшей эквивалентности на V, содержащей R. Поскольку последняя эквивалентность принадлежит множеству $\mathcal{E}(\mathcal{C})$, а $\mathcal{C}$ – однородная p-схема, левое равенство в формуле (1) влечёт, что число $|X|$ является степенью p. Таким образом, таковым является и порядок каждой перестановки $g_R \in G^*_{\mathcal{O}}$, и, следовательно, $G^*_{\mathcal{O}}$ – p-группа. □

Очевидно, что свойство "быть p-схемой" сохраняется при изоморфизмах схем. Более общо, пусть φ – *подобие* схемы $\mathcal{C} = (V, \mathcal{R})$ на схему $\mathcal{C}' = (V', \mathcal{R}')$. Это означает, что φ является биекцией из $\mathcal{R}$ на $\mathcal{R}'$, для которой

$$c^T_{R,S} = c^{T^\varphi}_{R^\varphi, S^\varphi}, \quad R, S, T \in \mathcal{R}.$$

Можно доказать (см. [2, лемма 2.2]), что $|R| = |R^\varphi|$ для всех $R \in \mathcal{R}$. Отсюда следует, что $\mathcal{C}$ является p-схемой тогда и только тогда, когда таковой является схема $\mathcal{C}'$. Множество всех подобий схемы $\mathcal{C}$ на схему $\mathcal{C}'$ обозначается через $\mathrm{Sml}(\mathcal{C}, \mathcal{C}')$. При $\mathcal{C} = \mathcal{C}'$ множество $\mathrm{Sml}(\mathcal{C}) = \mathrm{Sml}(\mathcal{C}, \mathcal{C})$ является группой, которая может быть естественным образом отождествлена с группой автоморфизмов алгебры смежности $\mathcal{A}$ схемы $\mathcal{C}$. Легко видеть, что для каждой группы $G \leqslant \mathrm{Sml}(\mathcal{C})$ алгебра $\mathcal{A}^G$ является алгеброй смежности некоторой схемы на V. Эта схема обозначается через $\mathcal{C}^G$.

Теорема 2.3. *Пусть $\mathcal{C}$ – однородная p-схема степени $n > 1$. Тогда существуют схема $\mathcal{D} > \mathcal{C}$ с фибрами одного и того же размера n/p и группа $G \leq \mathrm{Sml}(\mathcal{D})$ порядка p, такие, что $\mathcal{D}^G = \mathcal{C}$.*

Доказательство. Пусть $E \neq \Lambda(V)$ – максимальная эквивалентность схемы $\mathcal{C} = (V, \mathcal{R})$. Тогда схема $\mathcal{C}_{V/E}$ примитивна, т.е. содержит лишь две эквивалентности: $\Delta(V/E)$ и $\Lambda(V/E)$. С другой стороны, она является нетривиальной p-схемой и, следовательно, по теореме 2.2 содержит недиагональное тонкое отношение. Таким образом, в силу [7, с. 71] это означает, что $\mathcal{C}_{V/E}$ – регулярная схема степени p. Используя результат [5, предложение 3.1], легко видеть, что отношения $R_{X,Y}$, где $X, Y \in V/E$ и $R \in \mathcal{R}$, являются базисными отношениями некоторой схемы $\mathcal{D}$ на V, фибрами которой являются в точности классы эквивалентности E. В частности, поскольку $\mathcal{C}$ однородна и $|V/E| = p$, каждый из них имеет размер n/p. Более того, [5, предложение 3.2] влечёт, что для каждого отношения $S \in \mathcal{R}_{V/E}$ перестановка φ_S множества $\mathcal{R}(\mathcal{D})$, заданная формулой

$$\left(R_{X,Y}\right)^{\varphi_S} = R_{X^{g_S},Y^{g_S}}, \quad X, Y \in V/E, \quad R \in \mathcal{R},$$

где g_S – изоморфизм схемы $\mathcal{C}_{V/E}$, определённый формулой (2) при $R = S$, является подобием схемы $\mathcal{D}$. Легко видеть, что $G = \{\varphi_S : S \in \mathcal{R}_{V/E}\}$ – подгруппа группы $\mathrm{Sml}(\mathcal{D})$ порядка p. Для завершения доказательства достаточно заметить, что

$$\mathcal{R}(D^G) = \left\{ \bigcup_{S \in \mathcal{R}_{V/E}} R_{X^{g_S},Y^{g_S}} : R \in \mathcal{R} \right\} = \mathcal{R}$$

и потому $\mathcal{D}^G = \mathcal{C}$. □

3. Структурные свойства p-схем

Пусть $\mathcal{C}$ – нетривиальная p-схема. Тогда в силу теоремы 2.2 найдётся тонкое отношение $R \in \mathcal{O}$, такое, что $g_R \in G^*_{\mathcal{O}}$ и перестановка g_R имеет порядок p. Легко видеть, что наименьшая эквивалентность схемы $\mathcal{C}$, содержащая R, является объединением отношений R^i при $i = 0, \ldots, p-1$. Поэтому каждый её класс X является объединением p множеств $(R^i)_{\mathrm{out}}(u)$ для фиксированного $u \in X$. Отсюда следует, что $|X| \in \{1, p\}$, и, значит, схема $\mathcal{C}_X$ регулярна. Таким образом, каждая нетривиальная p-схема содержит недиагональную *p-эквивалентность* в смысле следующего определения.

Определение 3.1. *Пусть $\mathcal{C}$ – схема на V. Будем говорить, что $E \in \mathcal{E}(\mathcal{C})$ – p-эквивалентность схемы $\mathcal{C}$, если $V_E = V$ и для каждого $X \in V/E$ схема $\mathcal{C}_X$ является регулярной степени 1 или p.*

Пусть E – p-эквивалентность схемы $\mathcal{C}$. Тогда каждый класс этой эквивалентности содержится в некоторой фибре, а сама она является объединением (не обязательно дизъюнктных) тонких отношений схемы $\mathcal{C}$. Если R – одно из них, то $g_R \in G^*_{\mathcal{O}}$ и $R^p = \Delta(V)$. Поэтому множество

$$G_E = \{g_R : \ R \subset E, \ R \in \mathcal{O}\}$$

является p-подгруппой группы $G^*_{\mathcal{O}}$.

Теорема 3.2. *Пусть $\mathcal{C}$ – схема на V и E – её p-эквивалентность. Тогда $\mathcal{C}$ является p-схемой в том и только в том случае, если таковой является схема $\mathcal{C}_{V/E}$.*

Доказательство. В силу правого из равенств (1) (очевидно, справедливого и в неоднородном случае) необходимость тривиальна. По той же причине доказательство достаточности легко сводится к проверке того, что для всех $X, Y \in V/E$ и всех $R \in \mathcal{R}_{X,Y}$ число $|R_{X,Y}|$ является степенью p. Однако, по определению группы G_E её орбиты совпадают с классами эквивалентности E. Поэтому множество $X \times Y$ является орбитой группы $G = G_E \times G_E$ в её покомпонентном действии на $V \times V$. С другой стороны, поскольку $G_E \le \mathrm{Iso}(\mathcal{C})$, группа G действует на множестве $\mathcal{R}$ так, что если $g = (g_S, g_{S'}) \in G$, то $R^g = S^T R S'$ для всех $R \in \mathcal{R}$. Отсюда следует, что

$$(R_{X,Y})^g = R^g_{X^{g_S}, Y^{g_{S'}}} = R^g_{X,Y}, \quad R_{X,Y} \in \mathcal{R}_{X,Y}.$$

Таким образом, каждое множество $R_{X,Y} \in \mathcal{R}_{X,Y}$ является блоком группы перестановок, индуцированной (транзитивным) действием группы G на множестве $X \times Y$. Поэтому $|R_{X,Y}|$ делит число $|X \times Y| \in \{1, p, p^2\}$ (мы использовали тот факт, что E является p-эквивалентностью). □

Следующая теорема характеризует однородные p-схемы в терминах их p-эквивалентностей. Чтобы упростить обозначения, для эквивалентностей E и F на множестве V, удовлетворяющих условию $E \subseteq F$, будем писать F/E вместо $F_{V/E}$. Тогда в силу [8, теорема 1.7.6] мы получим, что

$$\mathcal{C}_{V/F} \simeq \mathcal{C}_{(V/E)/(F/E)}, \tag{4}$$

когда E и F являются эквивалентностями схемы $\mathcal{C}$.

Теорема 3.3.[1] *Пусть $\mathcal{C}$ – однородная схема на V. Тогда $\mathcal{C}$ является p-схемой тогда и только тогда, когда найдётся ряд*

$$\Delta(V) = E_0 \subseteq E_1 \subseteq \cdots \subseteq E_m = \Lambda(V), \tag{5}$$

такой, что E_i – эквивалентность схемы $\mathcal{C}$ и E_i/E_{i-1} – p-эквивалентность схемы $\mathcal{C}_{V/E_{i-1}}$ $(i = 1, \ldots, m)$.

Доказательство. Для доказательства необходимости не умаляя общности предположим, что $|V| > 1$. Тогда в силу замечания, сделанного перед определением 3.1, схема $\mathcal{C}$ имеет недиагональную p-эквивалентность E. По теореме 3.2 отсюда следует, что $\mathcal{C}' = \mathcal{C}_{V/E}$ является p-схемой на $V' = V/E$. По индукции можно считать, что найдётся ряд

$$\Delta(V') = E'_0 \subseteq E'_1 \subseteq \cdots \subseteq E'_{m'} = \Lambda(V') \tag{6}$$

такой, что E'_i – эквивалентность схемы $\mathcal{C}'$ и E'_i/E'_{i-1} – p-эквивалентность схемы $\mathcal{C}'_{V'/E'_{i-1}}$ $(i = 1, \ldots, m')$. Положим $E_0 = \Delta(V)$ и обозначим через E_i ту эквивалентность схемы $\mathcal{C}$, для которой $E \subseteq E_i$ и $E_i/E = E'_{i-1}$ для всех $i \geqslant 1$. Тогда, очевидно, $E_1 = E$ и включения (5) имеют место для $m = m' + 1$. Докажем, что E_i/E_{i-1} – p-эквивалентность схемы $\mathcal{C}_{V/E_{i-1}}$. Поскольку $E_1 = E$, можно считать, что $i > 1$. Из формулы (4) при $F = E_i$ следует, что

$$\mathcal{C}_{V/E_i} \simeq (\mathcal{C}_{V/E})_{(V/E)/(E_i/E)} = \mathcal{C}'_{V'/E'_{i-1}}.$$

Соответствующий изоморфизм переводит эквивалентность E_{i+1}/E_i схемы $\mathcal{C}_{V/E_i}$ в эквивалентность $(E_{i+1}/E)/(E_i/E) = E'_i/E'_{i-1}$ схемы $\mathcal{C}'_{V'/E'_{i-1}}$. Поскольку последняя эквивалентность является p-эквивалентностью, то таковой же является и E_{i+1}/E_i. Необходимость доказана.

В доказательстве достаточности не умаляя общности можно считать, что $m \geq 2$ и $E_0 \neq E_1$. Тогда E_1 – недиагональная p-эквивалентность схемы $\mathcal{C}$. С другой стороны, легко видеть, что схема $\mathcal{C}' = \mathcal{C}_{V/E_1}$ имеет ряд (6) и потому по индукции является p-схемой. Так что требуемое утверждение вытекает из теоремы 3.2. □

Следующая теорема показывает, что свойство "быть p-схемой" полностью определяется однородными компонентами.

[1] На другом языке это утверждение было доказано в [9, следствие 5.6.8].

Теорема 3.4. *Схема $\mathcal{C}$ является p-схемой тогда и только тогда, когда таковой является каждая схема $\mathcal{C}_X$ при $X \in \mathrm{Fib}\,(\mathcal{C})$.*

Доказательство. Необходимость очевидна. В доказательстве достаточности не умаляя общности можно считать, что схема $\mathcal{C}$ нетривиальна. Тогда найдётся фибра X, для которой схема $\mathcal{C}_X$ нетривиальна и потому содержит недиагональную p-эквивалентность E_X. Легко видеть, что отношение

$$E = E_X \cup \Delta(V \setminus X)$$

является p-эквивалентностью схемы $\mathcal{C}$. Каждая фибра Y' схемы $\mathcal{C}' = \mathcal{C}_{V/E}$ имеет вид Y/E для некоторой фибры Y схемы $\mathcal{C}$. Поэтому из теоремы 3.2 следует, что $\mathcal{C}'_{Y'} = (\mathcal{C}_Y)_{Y/E}$ – p-схема для всех Y'. Отсюда по индукции получаем, что $\mathcal{C}'$ – p-схема, и потому $\mathcal{C}$ является p-схемой по теореме 3.2. □

Доказательство теоремы 1.1. Пусть $\mathcal{C}$ – p-схема и $\mathcal{D}$ – её произвольное расширение. Если $\mathcal{C}$ тривиальна, то $\mathcal{D} = \mathcal{C}$ и утверждение очевидно. В противном случае по теореме 3.4 не умаляя общности можно считать, что $\mathcal{C}$ однородна. Тогда она содержит недиагональную p-эквивалентность E, каждый класс которой имеет мощность p. Ясно, что она также является эквивалентностью схемы $\mathcal{D}$. Докажем, что

$$U \subseteq X \quad \text{или} \quad |U \cap X| = 1, \quad X \in \mathrm{Fib}\,(\mathcal{D}), \tag{7}$$

для всех $U \in V/E$ с условием $U \cap X \neq \emptyset$. С этой целью возьмём такое множество U. Тогда для каждого $R \in \mathcal{R}(\mathcal{D}_{U\cap X})$ существует такое $T \in \mathcal{R}(\mathcal{C})$, что $R \subseteq T_{U\cap X} \subseteq T_U$. Поскольку $\mathcal{C}_U$ – регулярная схема степени p, её базисное отношение T_U есть либо ориентированный цикл длины p, либо отношение $\Delta(U)$. Однако $|R_{\mathrm{in}}(v)| = |R_{\mathrm{out}}(v)| > 0$ для всех $v \in U \cap X$. Поэтому либо $U \cap X = U$ и $R = T_U$, либо $R = \Delta(U \cap X)$. Если последнее верно для всех R, то $|U \cap X| = 1$, поскольку $\mathcal{D}_{U\cap X}$ – однородная схема. В противном случае, очевидно, $U \subseteq X$, что завершает доказательство формулы (7).

Из результата [1, лемма 2.6] следует, что эквивалентность E является дизъюнктным объединением однозначно определённых эквивалентностей $E_i \in \mathcal{E}(\mathcal{D})$, $i \in I$, никакая из которых не является дизъюнктным объединением двух непустых эквивалентностей схемы $\mathcal{D}$. Кроме того, для каждого $i \in I$ выполнено условие

$$|X \cap U| = |Y \cap U|, \quad X, Y \in \mathrm{Fib}\,(\mathcal{D}), \quad U \in V/E_i, \tag{8}$$

и множество $V_i = V_{E_i}$ является объединением некоторых фибр схемы $\mathcal{D}$. Наконец, поскольку $V_E = V$, множество V является дизъюнктным объединением всех множеств V_i. Для завершения доказательства теоремы нам необходима следующая вспомогательная лемма.

Лемма 3.6. *Во введённых обозначениях пусть $i \in I$. Тогда $V_i/E \in \mathrm{Fib}(\mathcal{D}_{V/E})$. Более того, если $V_i \notin \mathrm{Fib}(\mathcal{D})$, то $\mathcal{D}_{V_i/E} \simeq \mathcal{D}_X$ для всех $X \in \mathrm{Fib}(\mathcal{D})$ с условием $X \subseteq V_i$.*

Доказательство. Не умаляя общности можно считать, что множество V_i есть дизъюнктное объединение $k > 1$ фибр $X_1, \dots, X_k$ схемы $\mathcal{D}$. Предположим, что V_i/E – объединение по крайней мере двух фибр схемы $\mathcal{D}_{V/E}$. Тогда найдутся два непустых множества $X, Y \in \mathrm{Fib}^*(\mathcal{D})$, для которых

$$X \cup Y = V_i, \quad \Delta(X)_{V/E} \cap \Delta(Y)_{V/E} = \emptyset.$$

Правая часть означает, что X и Y – объединения классов эквивалентности E_i, и, следовательно, эквивалентности $(E_i)_X$ и $(E_i)_Y$ дизъюнктны. С другой стороны, левая часть показывает, что $E_i = (E_i)_X \cup (E_i)_Y$. Поскольку обе последние эквивалентности непусты, мы получаем противоречие с определяющим свойством эквивалентности E_i. Это доказывает первую часть утверждения.

Поскольку $k > 1$, из формулы (8) следует, что ни один класс эквивалентности E_i не содержится ни в каком множестве X_i. Поэтому из формулы (7) получаем, что

$$|U \cap X_j| = 1, \quad U \in V/E_i, \quad j = 1, \dots, k. \tag{9}$$

Пусть $X \subset V_i$ – фибра схемы $\mathcal{D}$, скажем, $X = X_j$ для некоторого j. Тогда из формулы (9) следует, что отображение

$$f : V/E_i \to X, \quad U \mapsto x_{U,j},$$

где $x_{U,j}$ – единственный элемент множества $U \cap X_j$, является биекцией. Покажем, что $f \in \mathrm{Iso}(\mathcal{D}_{V_i/E}, \mathcal{D}_X)$. С этой целью заметим, что каждое базисное отношение схемы $\mathcal{D}_{V_i/E}$ имеет вид $R_{V_i/E}$ для некоторого $R \in \mathcal{R}(\mathcal{D})$, такого, что $R \subseteq \Lambda(V_i)$. Достаточно проверить, что отношение R можно выбрать из множества $\mathcal{R}(\mathcal{D}_X)$ (тогда легко видеть, что $(R_{V_i/E})^f = R$). Для этого каждой паре элементов $a, b \in \{1, \dots, k\}$ сопоставим отображение

$$g_{a,b} : X_a \times X_b \to X_j \times X_j, \quad (x_{U,a}, x_{U',b}) \mapsto (x_{U,j}, x_{U',j}),$$

где U и U' пробегают все классы эквивалентности E_i. Поскольку $E_i \cap (X_a \times X_b)$ – отношение схемы $\mathcal{D}$ с единичной степенью исхода, отображение $g_{a,b}$ переводит множество $\mathcal{R}_{X_a,X_b}$ в множество $\mathcal{R}_{X_j,X_j} = \mathcal{R}(\mathcal{D}_{X_j})$. Кроме того, легко видеть, что

$$S_{V_i/E} = (S^{g_{a,b}})_{V_i/E}, \quad S \in \mathcal{R}(\mathcal{D}_{V_i}).$$

Таким образом, для каждого базисного отношения $R_{V_i/E}$ схемы $\mathcal{D}_{V_i/E}$ в качестве требуемого отношения можно выбрать отношение $R^{g_{a,b}}$, где индексы a, b однозначно определяются из включения $R \subseteq X_a \times X_b$. □

Вернёмся к доказательству теоремы 1.1. По теореме 3.4 достаточно проверить, что $\mathcal{D}_X$ – p-схема для каждого $X \in \mathrm{Fib}\,(\mathcal{D})$. Однако $\mathcal{D}_{V/E}$ – расширение схемы $\mathcal{C}_{V/E}$, которая является p-схемой по теореме 3.2. Отсюда по индукции заключаем, что таковой является и схема $\mathcal{D}_{V/E}$. С другой стороны, по лемме 3.6 множество V_i/E является фиброй последней схемы для всех i. Таким образом,

$$\mathcal{D}_{V_i/E} = (\mathcal{D}_{V_i})_{V_i/E} = (\mathcal{D}_{V/E})_{V_i/E}$$

является p-схемой по теореме 3.4. Отсюда следует, что и $\mathcal{D}_X$ является p-схемой для всех $X \in \mathrm{Fib}\,(\mathcal{D})$. Действительно, если $X \neq V_i$, то это следует из второй части леммы 3.6, а если $X = V_i$ – из теоремы 3.2 (поскольку E – p-эквивалентность схемы $\mathcal{D}_X$). □

Доказательство следствия 1.2. Достаточность, очевидно, следует из того, что мощность каждой 2-орбиты группы перестановок делит порядок этой группы. Необходимость очевидна при $|G| = 1$. В противном случае пусть X – орбита группы G, содержащая по крайней мере два элемента. Тогда для каждого $x \in X$ имеем

$$\mathrm{Inv}\,(G_x) \geq \mathrm{Inv}\,(G)_x > \mathrm{Inv}\,(G),$$

где $\mathrm{Inv}\,(G)_x$ – наименьшее расширение схемы $\mathrm{Inv}\,(G)$, содержащее одноэлементное отношение $\{(x,x)\}$. По теореме 1.1 схема $\mathrm{Inv}\,(G_x)$ является p-схемой. Следовательно, по индукции можно считать, что G_x – p-группа. Поскольку X – фибра p-схемы $\mathrm{Inv}\,(G)$, а $|G| = |G_x||X|$, отсюда следует, что G – p-группа.

Для доказательства второй части следствия предположим, что $\mathcal{C}$ – p-схема и $\mathcal{D} = \mathrm{Inv}\,(\mathrm{Aut}\,(\mathcal{C}))$. Поскольку $\mathcal{D}$ – расширение схемы $\mathcal{C}$, теорема 1.1 влечёт, что $\mathcal{D}$ является p-схемой. Следовательно, в силу доказанного выше $\mathrm{Aut}\,(\mathcal{D})$ – p-группа. Для завершения доказательства достаточно заметить, что $\mathrm{Aut}\,(\mathcal{C}) = \mathrm{Aut}\,(\mathcal{D})$. $\square$

4. Схемы отношений

Пусть V – конечное множество и $\mathcal{R}$ – разбиение множества V^2, замкнутое относительно перестановки координат.[2] Обозначим через $\mathcal{R}^*$ множество всевозможных объединений элементов из $\mathcal{R}$. Пара $\mathcal{C} = (V, \mathcal{R})$ называется *когерентной конфигурацией* или *схемой* на V, если отношение $\Delta(V)$ принадлежит множеству $\mathcal{R}^*$ и для всех $R, S, T \in \mathcal{R}$ число

$$c_{R,S}^T = |\{v \in V : (u,v) \in R,\ (v,w) \in S\}|$$

не зависит от выбора $(u,w) \in T$. Элементы множеств V, $\mathcal{R} = \mathcal{R}(\mathcal{C})$ и $\mathcal{R}^* = \mathcal{R}^*(\mathcal{C})$ называются соответственно *точками*, *базисными отношениями* и *отношениями* схемы $\mathcal{C}$. Числа $|V|$ и $|\mathcal{R}|$ называются *степенью* и *рангом* этой схемы.

Две схемы называются *изоморфными*, если существует биекция между их множествами точек, которая сохраняет базисные отношения. Любая такая биекция называется *изоморфизмом* этих схем. Множество всех изоморфизмов схемы $\mathcal{C}$ на себя образует группу, обозначаемую через $\mathrm{Iso}\,(\mathcal{C})$. Эта группа содержит нормальную подгруппу

$$\mathrm{Aut}\,(\mathcal{C}) = \{f \in \mathrm{Sym}\,(V) :\ R^f = R,\ R \in \mathcal{R}\},$$

называемую *группой автоморфизмов* схемы $\mathcal{C}$. Обратно, пусть $G \leqslant \mathrm{Sym}\,(V)$ – группа перестановок. Тогда пара $\mathrm{Inv}\,(G) = (V, \mathcal{R})$, где $\mathcal{R}$ – множество всех орбит в покомпонентном действии группы G на множестве V^2, является схемой, причём $G \leqslant \mathrm{Aut}\,(\mathcal{C})$. Эта схема называется *схемой 2-орбит* группы G.

Множество всех схем на V частично упорядочено так, что $\mathcal{C} \leqslant \mathcal{C}'$ в том и только в том случае, если $\mathcal{R}^* \subseteq (\mathcal{R}')^*$; в этом случае мы говорим, что $\mathcal{C}'$ является *расширением* схемы $\mathcal{C}$. Наибольшая схема называется *тривиальной*, её отношениями являются все бинарные отношения на V; наименьшая схема имеет ранг $\leqslant 2$ и совпадает со схемой 2-орбит группы $\mathrm{Sym}\,(V)$. Отображения

$$\mathcal{C} \to \mathrm{Aut}\,(\mathcal{C}), \quad G \to \mathrm{Inv}\,(G) \tag{10}$$

[2] Элементы из $\mathcal{R}$ предполагаются непустыми.

задают соответствие Галуа между схемами отношений на V и группами перестановок на V. Замкнутыми объектами в этом соответствии являются шуровы схемы и 2-замкнутые группы перестановок (см. [3]).

Для схемы $\mathcal{C} = (V, \mathcal{R})$ положим

$$\mathrm{Fib}\,(\mathcal{C}) = \{X \subseteq V:\ \Delta(X) \in \mathcal{R}\}, \quad \mathrm{Fib}^*(\mathcal{C}) = \{X \subseteq V:\ \Delta(X) \in \mathcal{R}^*\}.$$

Каждый элемент множества $\mathrm{Fib}\,(\mathcal{C})$ называется *фиброй* схемы $\mathcal{C}$. Очевидно, что множество V является дизъюнктным объединением фибр и что для каждого отношения $R \in \mathcal{R}$ существуют единственным образом определённые фибры X и Y, для которых $R \subseteq X \times Y$. Числа

$$d_{\mathrm{out}}(R) = c_{R,R^T}^{\Delta(X)}, \quad d_{\mathrm{in}}(R) = c_{R^T,R}^{\Delta(Y)} \tag{11}$$

называются соответственно *степенью исхода* и *степенью захода* отношения R. Легко видеть, что $d_{\mathrm{out}}(x) = |R_{\mathrm{out}}(x)|$ и $d_{\mathrm{in}}(x) = |R_{\mathrm{in}}(x)|$ для всех $x \in X$, где $R_{\mathrm{out}}(x) = \{y \in Y:\ (x,y) \in R\}$ и $R_{\mathrm{in}}(x) = \{y \in Y:\ (y,x) \in R^T\}$.

Множество всех эквивалентностей на V, принадлежащих множеству $\mathcal{R}^*$, обозначается через $\mathcal{E} = \mathcal{E}(\mathcal{C})$, и его элементы называются *эквивалентностями* схемы $\mathcal{C}$. Легко видеть, что $\Delta(X), \Lambda(X) \in \mathcal{E}$ для всех $X \in \mathrm{Fib}^*(\mathcal{C})$. Можно показать, что для каждого отношения $R \in \mathcal{R}^*$ наименьшая эквивалентность на V, содержащая R, также принадлежит множеству $\mathcal{E}$. Для любой эквивалентности $E \in \mathcal{E}$ и любого множества $X \in V/E$ множества

$$\mathcal{R}_X = \{R_X:\ R \in \mathcal{R},\ R_X \neq \emptyset\}, \quad \mathcal{R}_{V/E} = \{R_{V/E}:\ R \in \mathcal{R},\ R_{V/E} \neq \emptyset\}$$

являются множествами базисных отношений некоторых схем $\mathcal{C}_X$ на X и $\mathcal{C}_{V/E}$ на V/E соответственно; мы называем их *ограничением* схемы $\mathcal{C}$ на множество X и *фактор-схемой* схемы $\mathcal{C}$ по модулю E.

Однородной компонентой схемы $\mathcal{C}$ называется схема $\mathcal{C}_X$, где $X \in \mathrm{Fib}\,(\mathcal{C})$. Если имеется лишь одна однородная компонента, т.е. $|\mathrm{Fib}\,(\mathcal{C})| = 1$, мы говорим, что $\mathcal{C}$ – *однородная* схема. В этом случае $d_{\mathrm{in}}(R) = d_{\mathrm{out}}(R)$ для всех $R \in \mathcal{R}$ и мы обозначаем это число через $d(R)$. Однородная схема $\mathcal{C}$ называется *регулярной*, если $d(R) = 1$ для всех $R \in \mathcal{R}$. Можно доказать, что каждая регулярная схема на V имеет вид $\mathrm{Inv}\,(G)$, где $G \leqslant \mathrm{Sym}\,(V)$ – регулярная группа перестановок (см. [2, теорема 4.4]).

Литература

1. S. Evdokimov, M. Karpinski, I. Ponomarenko, *On a new high dimensional Weisfeiler-Leman algorithm.* — J. Algebraic Combin. **10** (1999), 29–45.
2. S. Evdokimov, I. Ponomarenko, *Separability number and Schurity number of coherent configurations.* — Electron. J. Combin. **7** (2000), #R31.
3. I. A. Faradžev, M. H. Klin, M. E. Muzychuk, *Cellular rings and groups of automorphisms of graphs.* — In: I. A. Faradžev et al. (eds), Investigations in Algebraic Theory of Combinatorial Objects, Kluwer Acad. Publ., Dordrecht (1994), pp. 1–152.
4. D. G. Higman, *Coherent configurations.* — Geom. Dedicata **4** (1975), 1–32.
5. M. Klin, M. Muzychuk, C. Pech, A. Woldar, P.-H. Zieschang, *Association schemes on 28 points as mergings of a half-homogeneous coherent configuration.* — European J. Combin. (2006), doi:10.1016/j.ejc.2006.08.010.
6. I. Ponomarenko, *Cellular algebras and graph isomorphism problem.* — Research Report No. 8592-CS, University of Bonn (April 1993).
7. B. Weisfeiler (ed.), *On Construction and Identification of Graphs.* — Springer Lecture Notes **558** (1976).
8. P.-H. Zieschang, *Algebraic Approach to Association Schemes.* Springer, Berlin–Heidelberg (1996).
9. P.-H. Zieschang, *Theory of Association Schemes.* — Springer Monographs in Mathematics (2005).

Ponomarenko I. N., Rahnamai Barghi A. On the structure of p-schemes.

We introduce and study an analog of p-groups in general scheme theory. It is proved that a scheme is a p-scheme if and only if so is each homogeneous component of it. Moreover, the automorphism group of a p-scheme is a p-group, and the 2-orbit scheme of a permutation group G is a p-scheme if and only if G is a p-group. Both of these statements follow from the fact that the class of p-schemes is closed with respect to extensions.

С.-Петербургское отделение
Математического института
им. В. А. Стеклова РАН

E-mail: inp@pdmi.ras.ru

Поступило 15 марта 2007 г.

Institute for Advanced Studies in Basic
Sciences, Gava Zang, Zanjan, Iran

E-mail: rahnama@iasbs.ac.ir