Записки научных
семинаров ПОМИ
Том 321, 2005 г.

И. Н. Пономаренко

НАХОЖДЕНИЕ ГРУППЫ АВТОМОРФИЗМОВ ЦИРКУЛЯНТНОЙ АССОЦИАТИВНОЙ СХЕМЫ ЗА ПОЛИНОМИАЛЬНОЕ ВРЕМЯ

1. Введение

Конечный граф называется *циркулянтным*, если его группа автоморфизмов содержит полный цикл, то есть перестановку, циклическое разложение которой состоит из единственного цикла полной длины. Такой граф допускает регулярную циклическую группу автоморфизмов и, следовательно, изоморфен графу Кэли над циклической группой. Проблема изоморфизма циркулянтных графов широко изучалась в последние десятилетия [8] и, наконец, была независимо решена в работах [2, 11]. Отметим, что в [2] были также найдены эффективные алгоритмы распознавания циркулянтных графов и построения для них полного множества неэквивалентных представлений Кэли. Однако, вплоть до настоящего времени не было известно ни одного эффективного алгоритма нахождения группы автоморфизмов произвольного циркулянтного графа (для класса циркулянтных турниров такой алгоритм был построен в работе [12]). Одно из объяснений этому состоит в том, что хотя проблема нахождения группы автоморфизмов произвольного графа (а точнее, какого-либо множества её образующих, имеющего полиномиальную от числа вершин графа мощность) полиномиально эквивалентна проблеме изоморфизма графов (см. [10]), соответствующая редукция не проходит в классе всех циркулянтных графов. Одним из основных результатов настоящей работы является решение проблемы нахождения группы автоморфизмов в классе всех циркулянтных графов (следствие 1.2).

Как было замечено в работах [1, 13], для любого графа $\mathfrak{G}$ с множеством вершин V существует эффективно вычислимая ассо-

Поддержано грантами РФФИ 03-01-00349, 02-01-00093, NSH-2251.2003.1.

циативная схема $\mathcal{C}(\mathfrak{G})$ на том же множестве, для которой

$$\mathrm{Aut}\,(\mathfrak{G}) = \mathrm{Aut}\,(\mathcal{C}(\mathfrak{G})), \qquad (1)$$

где ассоциативную схему $\mathcal{C} = \mathcal{C}(\mathfrak{G})$ можно представлять себе как специальное разбиение полного графа с множеством вершин V в регулярные остовные подграфы (точное определение ассоциативной схемы и необходимые сведения из теории таких схем приведены в §2). Группа автоморфизмов $\mathrm{Aut}\,(\mathcal{C})$ схемы $\mathcal{C}$ совпадает с пересечением групп автоморфизмов этих подграфов. Эта группа нормальна в группе $\mathrm{Iso}\,(\mathcal{C})$ всех изоморфизмов этой схемы, т.е. в наибольшей подгруппе симметрической группы $\mathrm{Sym}\,(V)$, сохраняющей указанное выше разбиение. Ассоциативная схема называется *циркулянтной*, если её группа автоморфизмов содержит регулярную циклическую подгруппу.

Теорема 1.1. *Группа автоморфизмов и группа изоморфизмов циркулянтной схемы на n точках могут быть найдены за время $n^{O(1)}$.*

Доказательство. Первое утверждение следует из теоремы 4.5, в доказательстве которой существенно использованы идеи и результаты работы [2]. Для доказательства второго утверждения предположим, что $\mathcal{C} = (V, \mathcal{R})$ – циркулянтная ассоциативная схема на n точках. Тогда из результатов работы [11] следует, что существует множество $P \subset \mathrm{Sym}\,(V)$ мощности, не превосходящей n^2 такое, что

$$\forall f \in \mathrm{Iso}\,(\mathcal{C}) \quad \exists g_f \in P \quad \forall R \in \mathcal{R}: \quad R^f = R^{g_f}.$$

Положим $P_0 = \{g_f :\ f \in \mathrm{Iso}\,(\mathcal{C})\}$ и обозначим через $\pi : \mathrm{Iso}\,(\mathcal{C}) \to \mathrm{Sym}\,(\mathcal{R})$ естественный гомоморфизм, индуцированный действием группы $\mathrm{Iso}\,(\mathcal{C})$ на множестве $\mathcal{R}$. Тогда $\mathrm{Im}(\pi) = \{\pi(g) :\ g \in P_0\}$. Поскольку, очевидно, $\ker(\pi) = \mathrm{Aut}\,(\mathcal{C})$, отсюда следует, что $\mathrm{Iso}\,(\mathcal{C}) = \langle \mathrm{Aut}\,(\mathcal{C}), P_0\rangle$. Для завершения доказательства достаточно заметить, что в силу [2] за время $n^{O(1)}$ можно найти регулярную циклическую подгруппу группы $\mathrm{Aut}\,(\mathcal{C})$, а в силу [11] по любой такой подгруппе можно найти множество P за то же время. $\square$

Из равенства (1) следует, что граф $\mathfrak{G}$ является циркулянтным в том и только в том случае, когда циркулянтна ассоциативная схема $\mathcal{C}(\mathfrak{G})$. Поэтому из теоремы 1.1 вытекает следующее утверждение.

Следствие 1.2. *Группа автоморфизмов циркулянтного графа на n вершинах может быть найдена за время $n^{O(1)}$.* $\square$

Анализ основного алгоритма (п. 4.3), лежащего в основе доказательства теоремы 1.1, базируется на изучении секций группы автоморфизмов циркулянтной схемы. Под *секцией* транзитивной группы перестановок Γ понимается любая группа перестановок

$$\Gamma_{X/E} = \{\gamma_{X/E} : \ \gamma \in \Gamma, \ X^\gamma = X\},$$

где X – блок группы Γ, E – Γ-инвариантная эквивалентность и $\gamma_{X/E}$ – перестановка классов этой эквивалентности, содержащихся в X, индуцированная перестановкой γ. В случае, когда Γ – группа автоморфизмов циркулянтной схемы, существенная информация о секциях этой группы получается из знания структуры флагов ассоциативной схемы $\mathrm{Inv}(\Gamma)$, определяемой как схема, базисными отношениями которой являются 2-орбиты группы Γ. Структура флагов произвольной циркулянтной схемы была детально изучена в работе [2]. Используя содержащиеся там результаты мы получаем следующее явное описание примитивных секций группы автоморфизмов циркулянтной схемы.

Теорема 1.3. *Пусть Γ – группа автоморфизмов некоторой циркулянтной схемы. Тогда каждая примитивная секция группы Γ изоморфна как группа перестановок либо симметрической группе $\mathrm{Sym}(d)$ для $d \geqslant 4$, либо некоторой подгруппе аффинной группы $\mathrm{AGL}_1(p)$ для простого числа p.*

Доказательство. Для примитивной секции $\Gamma_{X/E}$ группы Γ через E' обозначим Γ-инвариантную эквивалентность, одним из классов которой является X. Тогда $F = E'/E$ – примитивный флаг ассоциативной схемы $\mathcal{C} = \mathrm{Inv}(\Gamma)$. Поскольку эта схема, очевидно, является циркулянтной, из теоремы 3.3 следует, что флаг F либо разрешимый, либо симметрический. В первом случае число $p = |X/E|$ является простым, а группа $\mathrm{Aut}(\mathcal{C})_{X/E}$ изоморфна подгруппе группы $\mathrm{Hol}(G_p) \cong \mathrm{AGL}_1(p)$, где G_p – циклическая группа порядка p и $\mathrm{Hol}(G_p)$ – её голоморф (см. (4)). Во втором случае $\mathrm{Aut}(\mathcal{C})_{X/E} = \mathrm{Sym}(X/E)$ (см. (2)), и при $|X/E| \leqslant 3$ он сводится к первому. Поскольку $\Gamma = \mathrm{Aut}(\mathcal{C})$, теорема доказана. $\square$

Группа перестановок Γ называется 2-замкнутой, если она совпадает со своим 2-замыканием $\mathrm{Aut}(\mathrm{Inv}(\Gamma))$ (см. [5]). Очевидно, что 2-замыкание любой 2-транзитивной группы совпадает с симметрической группой. С другой стороны, согласно теореме Бернсайда–Шура каждая примитивная группа перестановок, содержащая регулярную циклическую подгруппу, либо 2-транзитивна, либо изоморфна как группа перестановок некоторой подгруппе аффинной группы $\mathrm{AGL}_1(p)$ для простого числа p. Поэтому теорема 1.3 может рассматриваться как обобщение теоремы Бернсайда–Шура в классе всех 2-замкнутых групп перестановок. Следующее утверждение характеризует разрешимые группы автоморфизмов циркулянтных схем в терминах их примитивных секций.

Теорема 1.4. *Группа автоморфизмов циркулянтной схемы разрешима тогда и только тогда, когда ни одна примитивная секция этой группы не изоморфна как группа перестановок симметрической группе* $\mathrm{Sym}(d)$ *для* $d \geqslant 5$.

Доказательство. Необходимость утверждения очевидна. Для доказательства достаточности обозначим через Γ группу автоморфизмов некоторой циркулянтной схемы. Предположим, что ни одна примитивная секция этой группы не изоморфна как группа перестановок симметрической группе $\mathrm{Sym}(d)$ для $d \geqslant 5$. Тогда по теореме 1.3 схема $\mathcal{C} = \mathrm{Inv}(\Gamma)$ не имеет симметрических флагов степени по крайней мере 5. Поэтому группа $\Gamma = \mathrm{Aut}(\mathcal{C})$ разрешима по первой части теоремы 4.3. □

Все используемые в данной работе понятия и результаты, касающиеся групп перестановок, могут быть найдены в [5, 14]. В §2 приводятся необходимые сведения об ассоциативных схемах; этот же параграф содержит некоторые замечания по поводу алгоритмов для них и для групп перестановок. В §3 доказывается теорема 3.3, используемая для анализа основного алгоритма. Сам алгоритм приводится в §4.

Обозначения. На протяжении всей работы V обозначает конечное множество. Под эквивалентностью E на V всегда понимается обычное отношение эквивалентности на множестве V. Множество всех классов эквивалентности E обозначается через V/E, и для $X \subset V$ мы полагаем $X/E = X/(E \cap X^2)$. Если E совпадает с $\Delta(V) = \{(v,v) : v \in V\}$, то множество X/E отождествляется с X.

Для (бинарного) отношения R на V, множества $X \subset V$ и эквивалентности E на V мы полагаем

$$R_{X/E} = \{(Y,Z) \in (X/E)^2 : (Y \times Z) \cap R \neq \emptyset\}$$

и рассматриваем это множество как отношение на X/E.

Группа всех перестановок множества V обозначается через $\mathrm{Sym}(V)$; при $V = \{1, \dots, d\}$ мы пишем $\mathrm{Sym}(d)$ вместо $\mathrm{Sym}(V)$. Множество всех полных циклов на V обозначается через $\mathrm{Cyc}(V)$.

Каждая биекция $f : V \to V'$ $(v \mapsto v^f)$ определяет естественные биекцию $R \mapsto R^f$ из множества всех отношений на V на множество всех отношений на V' и групповой изоморфизм $g \mapsto g^f$ из $\mathrm{Sym}(V)$ на $\mathrm{Sym}(V')$. Для множества $X \subset V$ и эквивалентности E на V биекция f индуцирует биекцию $f_{X/E} : X/E \to X'/E'$, где $X' = X^f$ и $E' = E^f$.

2. Ассоциативные схемы

2.1. Пусть V – конечное множество и $\mathcal{R}$ – множество непустых бинарных отношений на V. Пара $\mathcal{C} = (V, \mathcal{R})$ называется *ассоциативной схемой* или *схемой* на V, если выполнены следующие условия:

(1) множество $\mathcal{R}$ образует разбиение множества V^2,

(2) диагональ $\Delta(V)$ множества V^2 принадлежит $\mathcal{R}$,

(3) множество $\mathcal{R}$ замкнуто относительно перестановки координат,

(4) если $R, S, T \in \mathcal{R}$, то число $|\{v \in V : (u,v) \in R, \ (v,w) \in S\}|$ не зависит от выбора $(u,w) \in T$.

Элементы множеств V и $\mathcal{R} = \mathcal{R}(\mathcal{C})$ называются *точками* и *базисными отношениями* схемы $\mathcal{C}$, соответственно; числа $\deg(\mathcal{C}) = |V|$ и $\mathrm{rk}(\mathcal{C}) = |\mathcal{R}|$ называются её *степенью* и *рангом*.

Схемы $\mathcal{C}$ на V и $\mathcal{C}'$ на V' называются *изоморфными*, если $(\mathcal{R}(\mathcal{C}))^f = \mathcal{R}(\mathcal{C}')$ для некоторой биекции $f : V \to V'$, называемой *изоморфизмом* схемы $\mathcal{C}$ на схему $\mathcal{C}'$. Если $\mathcal{C} = \mathcal{C}'$, то группа $\mathrm{Iso}(\mathcal{C})$ всех таких изоморфизмов имеет нормальную подгруппу

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

называемую *группой автоморфизмов* схемы $\mathcal{C}$.

Данное выше определение схемы эквивалентно определению однородной когерентной конфигурации из [7][1]. С другой стороны, имеется естественное взаимно однозначное соответствие ме-

[1] В определении когерентной конфигурации условие (2) заменяется более слабым: отношение $\Delta(V)$ является объединением элементов из $\mathcal{R}$.

жду когерентными конфигурациями и клеточными кольцами, введёнными в [13]. Это соответствие таково, что схема и отвечающее ей однородное клеточное кольцо оказываются с точностью до языка одним и тем же объектом (см., например, [6]). Имея это в виду, мы будем свободно использовать для схем результаты, полученные в [2] для однородных клеточных колец.

2.2. Множество всех эквивалентностей на V, являющихся объединениями базисных отношений схемы $\mathcal{C}$, обозначается через $\mathcal{E}(\mathcal{C})$, а его элементы называются *эквивалентностями* этой схемы. Мощность класса такой эквивалентности не зависит от выбора этого класса. Легко видеть, что $\Delta(V), V^2 \in \mathcal{E}(\mathcal{C})$; схема $\mathcal{C}$ степени > 1 называется *примитивной*, если каждая её непустая эквивалентность совпадает с $\Delta(V)$ или V^2. Можно показать, что если $E_1, E_2 \in \mathcal{E}(\mathcal{C})$, то

$$E_1 \cap E_2,\ \langle E_1 \cup E_2 \rangle \in \mathcal{E}(\mathcal{C}),$$

где эквивалентность $\langle E_1 \cup E_2 \rangle$ определяется как пересечение всех эквивалентностей на V, содержащих E_1 и E_2. Любая пара $\mathcal{C}_{X/E} = (X/E, \mathcal{R}_{X/E})$, где X – класс некоторой эквивалентности схемы $\mathcal{C}$, $E \in \mathcal{E}(\mathcal{C})$ и $\mathcal{R}_{X/E} = \{R_{X/E} :\ R \in \mathcal{R}\}$, является схемой на множестве X/E.

В следующей лемме, используемой в § 3, предполагается, что $\mathcal{C}$ – схема на V и для эквивалентностей $E, E' \in \mathcal{E}(\mathcal{C})$ выполнены равенства

$$E \cap E' = \Delta(V), \quad \langle E \cup E' \rangle = V^2.$$

Мы опускаем доказательство этой леммы, поскольку она является частным случаем леммы 2.1 и следствия 2.3 из работы [2].

Лемма 2.1. *Если G – регулярная абелева подгруппа группы* $\mathrm{Aut}(\mathcal{C})$, *то отображение*

$$f : V \to V/E \times V/E',\ v \mapsto (Y, Y'),$$

где Y и Y' – классы эквивалентностей E и E', содержащие v, является биекцией. Более того, эти эквивалентности G-инвариантны и для каждого множества $X \in V/E$ имеют место следующие утверждения:

(1) *отображение $t_X : X \to V/E'$, переводящее элемент из X в содержащий его класс эквивалентности E', является биекцией,*
(2) $(G_X)^{t_X} = G_{V/E'}$. □

2.3. Сделаем несколько замечаний по поводу алгоритмов, используемых в этой работе. Схема $\mathcal{C}$ всегда будет задаваться множеством своих базисных отношений. В этом представлении проверка примитивности и построение схем $\mathcal{C}_{X/E}$ для всех подходящих X и E могут быть осуществлены за время $n^{O(1)}$, где $n = \deg(\mathcal{C})$.

Группа перестановок Γ степени n всегда будет задаваться сильным множеством образующих (из не более чем n^2 перестановок, см. [9]). В этом представлении за время $n^{O(1)}$ можно проверить принадлежность к Γ. Более того, за то же время можно построить секцию группы Γ и стабилизатор любого её блока. Следующее утверждение, используемое в доказательстве теоремы 4.3, является частным случаем следствия 3.6 из [3].

Теорема 2.2. *Пусть* $\Gamma \leqslant \mathrm{Sym}(V)$ *– разрешимая группа. Тогда для любой схемы* $\mathcal{C}$ *на* V *группа* $\mathrm{Aut}(\mathcal{C}) \cap \Gamma$ *может быть найдена за время* $n^{O(1)}$, *где* $n = |V|$. □

3. Флаги в циркулянтных схемах

3.1. Схема называется *циркулянтной*, если её группа автоморфизмов содержит регулярную циклическую подгруппу. В этом пункте, используя обозначения и результаты работы [2], мы устанавливаем некоторые свойства циркулянтных схем. На протяжении всего параграфа $\mathcal{C}$ обозначает циркулянтную схему на множестве V. Положим

$$\mathcal{F}(\mathcal{C}) = \{F = (E_0, E_1) : \ E_0, E_1 \in \mathcal{E}(\mathcal{C}), \ E_0 \subset E_1\}.$$

Каждый элемент F множества $\mathcal{F}(\mathcal{C})$ называется *флагом* схемы $\mathcal{C}$ и будет обозначаться ниже через E_1/E_0. Числа $|X/E_0|$ и $\mathrm{rk}\,(\mathcal{C}_{X/E_0})$ не зависят от выбора множества $X \in V/E_1$; они называются *степенью* и *рангом* флага F и обозначаются соответственно через $|F|$ и $\mathrm{rk}\,(\mathcal{C}_F)$. Верно также, что все схемы $\mathcal{C}_{X/E_0}$ примитивны или нет одновременно. В первом случае флаг F называется *примитивным*.

Говорят, что флаг E_3/E_2 схемы $\mathcal{C}$ *кратен* флагу E_1/E_0 той же схемы, если $E_0 = E_1 \cap E_2$ и $E_3 = \langle E_1 \cup E_2 \rangle$. Обозначим через $\sim$ наименьшую эквивалентность на множестве $\mathcal{F}(\mathcal{C})$, содержащую отношение “быть кратным”. Пусть C – класс этой эквивалентности. Флаг $F \in C$ называется *наименьшим* (соответственно *наибольшим*) в C, если каждый флаг из этого класса кратен флагу F

(соответственно флаг F кратен каждому флагу этого класса). По лемме 5.2 из работы [2] каждый класс C содержит наименьший и наибольший элементы. Следующее утверждение суммирует свойства $\sim$-эквивалентных флагов, вытекающие из теоремы 2.2 той же работы.

Лемма 3.1. *Пусть $\mathcal{C}$ – циркулянтная схема. Тогда для каждого класса $\sim$-эквивалентности числа $|F|$, $\mathrm{rk}\,(\mathcal{C}_F)$ и свойство флага F "быть примитивным" не зависят от выбора флага F в этом классе.* □

3.2. Из теоремы Бернсайда–Шура следует, что у каждой примитивной циркулянтной схемы либо ранг равен 2, либо степень является простым числом (см. теорему 2.10.5 из [4]). В п. 3.3 мы обобщим это утверждение на примитивные флаги произвольной циркулянтной схемы. С этой целью рассмотрим флаг $F = E_1/E_0$ схемы $\mathcal{C}$. Назовём этот флаг *симметрическим*, если

$$\mathrm{Aut}\,(\mathcal{C})_{X/E_0} = \mathrm{Sym}\,(X/E_0), \quad X \in V/E_1. \tag{2}$$

В этом случае, очевидно, $\mathrm{rk}\,(\mathcal{C}_F) = 2$ и, в частности, флаг F является примитивным. Если он удовлетворяет более сильному условию

$$\mathrm{Aut}\,(\mathcal{C})_{V/E_0} \geqslant \mathrm{Sym}\,(F), \quad \text{где} \quad \mathrm{Sym}\,(F) = \prod_{X \in V/E_1} \mathrm{Sym}\,(X/E_0), \tag{3}$$

назовём его *суперсимметрическим* флагом. Наконец, F называется *разрешимым*, если он является примитивным флагом простой степени и

$$\mathrm{Aut}\,(\mathcal{C})_{X/E_0} \leqslant \mathrm{Hol}(G_{X/E_0}), \quad X \in V/E_1, \tag{4}$$

для каждой регулярной циклической группы $G \leqslant \mathrm{Aut}\,(\mathcal{C})$, где $\mathrm{Hol}(G_{X/E_0})$ – нормализатор группы G_{X/E_0} в группе $\mathrm{Sym}\,(X/E_0)$. (Легко видеть, что группа $\mathrm{Hol}(G_{X/E_0})$ изоморфна голоморфу группы G_{X/E_0}.) Отметим, что любой флаг степени не выше 3 является разрешимым. Кроме того, поскольку группа в правой части включения (4) является разрешимой, флаг F может быть одновременно разрешимым и симметрическим, только когда $|F| \leqslant 4$.

Теорема 3.2. *Пусть $\mathcal{C}$ – циркулянтная схема и C – класс $\sim$-эквивалентности, содержащий какой-нибудь её примитивный флаг. Тогда C содержит либо разрешимый, либо суперсимметрический флаг. В последнем случае наименьший элемент класса C является симметрическим.*

Доказательство. Выведем теорему из результатов работы [2], сохраняя используемую в ней терминологию и нумерацию утверждений. Предположим, что класс C не содержит разрешимых флагов. Поскольку каждый субнормальный флаг является разрешимым, а каждый квазинормальный флаг $\sim$-эквивалентен субнормальному, наше предположение влечет, что C не содержит квазинормальных флагов. В силу утверждения 5.3 отсюда следует, что схема $\mathcal{C}$ имеет сингулярность степени $d \geqslant 4$ в паре (F, F') её флагов, где F и F' – соответственно наименьший и наибольший элементы класса C. Пусть $F = E_1/E_0$ и $F' = E_3/E_2$. Поскольку схема $\mathcal{C}$ циркулянтна и F' кратен F, условия леммы 2.1 этой работы выполнены для $\mathcal{C} = \mathcal{C}_{X/E_0}$, $V = X/E_0$, $E = (E_1)_{X/E_0}$ и $E' = (E_2)_{X/E_0}$, где $X \in V/E_3$. Поэтому множества X/E_0 и $X/E_1 \times X/E_2$ можно отождествить с помощью биекции f, определённой в этой лемме. Тогда из доказательства теоремы 4.2 и леммы 4.3 следует, что

$$\mathrm{Aut}\,(\mathcal{C})_{V/E_0} \geqslant \prod_{X \in V/E_3} \{\mathrm{id}_{\,X/E_1}\} \times \mathrm{Sym}\,(X/E_2).$$

Отсюда следует, что флаг F симметрический, а флаг F' суперсимметрический, что доказывает первую часть теоремы. Вторая часть следует из того, что F – наименьший элемент в C. $\square$

3.3. Основным результатом этого пункта является следующее утверждение, из которого в действительности и следует теорема 1.3.

Теорема 3.3. *Пусть $\mathcal{C}$ – циркулянтная схема на V и C – класс $\sim$-эквивалентности, содержащий какой-нибудь её примитивный флаг. Тогда либо каждый флаг из C разрешимый, либо каждый флаг из C симметрический. В частности, каждый примитивный флаг схемы $\mathcal{C}$ разрешимый или симметрический.*

Доказательство. Пусть $G \leqslant \mathrm{Aut}\,(\mathcal{C})$ – регулярная циклическая группа. Докажем две вспомогательные леммы.

Лемма 3.4. *Если F и F' – примитивные флаги схемы $\mathcal{C}$, причём F' кратен F, то имеют место следующие утверждения:*

(1) *F разрешимый, если F' разрешимый,*

(2) *F' симметрический, если F симметрический.*

Доказательство. Пусть $F = E_1/E_0$ и $F' = E_3/E_2$. Тогда по условию леммы $E_0 = E_1 \cap E_2$ и $E_3 = \langle E_1 \cup E_2 \rangle$. Поэтому для каждого множества $Y \in V/E_3$ условия леммы 2.1 выполнены для $\mathcal{C} = \mathcal{C}_{Y/E_0}$, $V = Y/E_0$, $G = G_{Y/E_0}$ и $E = (E_1)_{Y/E_0}$, $E' = (E_2)_{Y/E_0}$. В силу утверждения (1) этой леммы для каждого множества $X \in Y/E_1$ отображение $t : X/E_0 \to Y/E_2$, переводящее класс эквивалентности $(E_0)_X$ в содержащий его класс эквивалентности $(E_2)_Y$, является биекцией. Отсюда следует, что

$$(G_{X/E_0})^t = G_{Y/E_2}, \quad (\mathrm{Aut}\,(\mathcal{C})_{X/E_0})^t \leqslant \mathrm{Aut}\,(\mathcal{C})_{Y/E_2}. \tag{5}$$

Действительно, равенство и включение здесь являются следствиями соответственно утверждения (2) леммы 2.1 и очевидного равенства $g_{X/E_0} \circ t = g_{Y/E_2}$, где $g \in \mathrm{Aut}\,(\mathcal{C})$.

Предположим, что флаг F' – разрешимый. Тогда его степень является простым числом и $\mathrm{Aut}\,(\mathcal{C})_{Y/E_2} \leqslant \mathrm{Hol}(G_{Y/E_2})$ (см. (4)). Поэтому в силу леммы 3.1 степень флага F проста, и из (5) следует, что

$$\begin{aligned} \mathrm{Aut}\,(\mathcal{C})_{X/E_0} &\leqslant (\mathrm{Aut}\,(\mathcal{C})_{Y/E_2})^{t^{-1}} \leqslant \mathrm{Hol}(G_{Y/E_2})^{t^{-1}} \\ &= \mathrm{Hol}((G_{Y/E_2})^{t^{-1}}) = \mathrm{Hol}(G_{X/E_0}), \end{aligned}$$

т.е. флаг F – разрешимый. Это доказывает утверждение (1) леммы. Для доказательства утверждения (2) предположим, что флаг F – симметрический. Тогда из формул (2) и (5) следует, что

$$\mathrm{Aut}\,(\mathcal{C})_{Y/E_2} \geqslant (\mathrm{Aut}\,(\mathcal{C})_{X/E_0})^t = \mathrm{Sym}\,(X/E_0)^t = \mathrm{Sym}\,(Y/E_2),$$

т.е. флаг F' – симметрический. □

Лемма 3.5. *Пусть $G \leqslant \Gamma \leqslant \mathrm{Sym}\,(V)$, где G – регулярная циклическая группа. Предположим, что E и E' – Γ-инвариантные эквивалентности на V такие, что*

(1) *$E \cap E' = \Delta(V)$, $\langle E \cup E' \rangle = V^2$,*

(2) *$|V/E|$ – простое число,*

(3) *группа Γ_X разрешима для некоторого множества $X \in V/E'$.*

Тогда $\Gamma_{V/E} \leqslant \mathrm{Hol}(G_{V/E})$.

Доказательство. Положим

$$K = \{\gamma \in \Gamma \colon \gamma_{V/E'} = \mathrm{id}_{V/E'}\}.$$

Тогда из условия (1) следует, что $G_{V/E}$ – регулярная циклическая подгруппа группы $K_{V/E}$, и что группа K действует на множестве X точно. Поскольку, очевидно, $K_X \leqslant \Gamma_X$, последнее в силу условия (3) влечёт, что группа K, а потому и группа $K_{V/E}$, разрешима. Таким образом, $K_{V/E}$ – транзитивная разрешимая группа простой степени (здесь мы воспользовались условием (2) и тем, что группа $K_{V/E}$ содержит транзитивную подгруппу $G_{V/E}$). Отсюда следует, что $G_{V/E}$ – нормальная, а потому и характеристическая, подгруппа группы $K_{V/E}$ (см. [5, с. 91]). Принимая во внимание, что последняя группа нормальна в группе $\Gamma_{V/E}$, мы заключаем, что $G_{V/E}$ – нормальная подгруппа группы $\Gamma_{V/E}$. Поэтому $\Gamma_{V/E} \leqslant \mathrm{Hol}(G_{V/E})$, что и требовалось доказать. □

Вернёмся к доказательству теоремы 3.3. Заметим, что по теореме 3.2 класс C содержит либо разрешимый, либо суперсимметрический флаг. В последнем случае вторая часть той же теоремы влечёт, что наименьшим элементом в C является симметрический флаг. Поэтому каждый флаг в C кратен симметрическому флагу и потому сам является симметрическим по утверждению (2) леммы 3.4. Таким образом, не умаляя общности, можно считать, что класс C содержит разрешимый флаг и, следовательно, по утверждению (1) леммы 3.4 наименьший флаг в классе C является разрешимым. Обозначим его через $F = E_1/E_0$.

Пусть $F' = E_3/E_2$ – произвольный флаг из C. Тогда $F' \sim F$, и по лемме 3.1 он является примитивным флагом простой степени. Заметим далее, что для каждого множества $X \in V/E_3$ условия леммы 3.5 выполнены для $V = X/E_0$, $\Gamma = \mathrm{Aut}\,(\mathcal{C})_{X/E_0}$, $G = G_{X/E_0}$ и $E = (E_2)_{X/E_0}$, $E' = (E_1)_{X/E_0}$. Действительно, условие (1) выполнено, поскольку флаг F' кратен флагу F, условие (2) выполнено, поскольку число $|(X/E_0)/(E_2)_{X/E_0}| = |X/E_2| = |F'|$ простое, и, наконец, условие (3) следует из разрешимости флага F. Поэтому из утверждения этой леммы следует, что $\mathrm{Aut}\,(\mathcal{C})_{X/E_2} \leqslant \mathrm{Hol}(G_{X/E_2})$. Таким образом, флаг F' является разрешимым. □

4. Нахождение группы автоморфизмов циркулянтной схемы

4.1. В этом пункте мы опишем алгоритмическую технику для работы с суперсимметрическими флагами, основанную на методах §4 работы [2]. Пусть $F = E_1/E_0$ – флаг циркулянтной схемы $\mathcal{C}$ на V. Схема $\mathcal{C}'$ на том же множестве называется *F-расширением* схемы $\mathcal{C}$, если $\mathrm{rk}\,(\mathcal{C}') > \mathrm{rk}\,(\mathcal{C})$ и существует семейство $\mathfrak{F} = \{f_X\}_{X \in V/E_1}$ перестановок $f_X \in \mathrm{Cyc}(X/E_0)$ такое, что

$$\mathrm{Aut}\,(\mathcal{C}') = \{g \in \mathrm{Aut}\,(\mathcal{C}) :\ R(\mathfrak{F})^g = R(\mathfrak{F})\}, \tag{6}$$

где $R(\mathfrak{F})$ – отношение на множестве V, определяемое следующим образом:

$$R(\mathfrak{F}) = \bigcup_{X \in V/E_1} \bigcup_{Y \in X/E_0} Y \times Y^{f_X}. \tag{7}$$

Ниже мы говорим, что группа $\Gamma \leqslant \mathrm{Sym}\,(V)$ является *суперсимметрической в F*, если $\Gamma_{V/E_0} = \mathrm{Sym}(F)$ (см. (3)).

Лемма 4.1. *Во введённых выше обозначениях предположим, что Γ – суперсимметрическая в F подгруппа группы* $\mathrm{Aut}\,(\mathcal{C})$*. Тогда* $\mathrm{Aut}\,(\mathcal{C}) = \langle \mathrm{Aut}\,(\mathcal{C}'), \Gamma\rangle$.

Доказательство. Поскольку, очевидно, $\langle \mathrm{Aut}\,(\mathcal{C}'), \Gamma\rangle \leqslant \mathrm{Aut}\,(\mathcal{C})$, достаточно доказать, что $\mathrm{Aut}\,(\mathcal{C}) \leqslant \langle \mathrm{Aut}\,(\mathcal{C}'), \Gamma\rangle$. Пусть $g \in \mathrm{Aut}\,(\mathcal{C})$. Тогда $E_0^g = E_0$ и $E_1^g = E_1$, и потому

$$(Y^{f_X})^g = ((Y^{gg^{-1}})^{f_X})^g = (Y^g)^{(g_{X/E_0})^{-1} f_X g_{X/E_0}} = (Y^g)^{f'_{X^g}}$$

для всех $X \in V/E_1$ и $Y \in X/E_0$, где $f'_{X^g} = (g_{X/E_0})^{-1} f_X g_{X/E_0}$. (В частности, $f'_X \in \mathrm{Cyc}(X/E_0)$ для всех X.) В силу (7) отсюда следует, что

$$\begin{aligned}(R(\mathfrak{F}))^g &= \bigcup_{X \in V/E_1} \bigcup_{Y \in X/E_0} Y^g \times (Y^{f_X})^g \\ &= \bigcup_{X \in V/E_1} \bigcup_{Y \in X/E_0} Y^g \times (Y^g)^{f'_{X^g}} = R(\mathfrak{F}'),\end{aligned}$$

где $\mathfrak{F}' = \{f'_X\}_{X \in V/E_1}$ и $f'_X \in \mathrm{Cyc}(X/E_0)$. С другой стороны, для каждого множества $X \in V/E_1$ существует перестановка $h_X \in \mathrm{Sym}\,(X/E_0)$ такая, что $(h_X)^{-1} f'_X h_X = f_X$. Группа Γ, будучи суперсимметрической в F, содержит элемент $\gamma \in \Gamma$, для которого

$\gamma_{X/E_0} = h_X$ при всех X. Повторяя проведённое выше вычисление с заменой g на $g\gamma^{-1}$, мы получим равенство $(R(\mathfrak{F}))^{g\gamma^{-1}} = R(\mathfrak{F})$. Поскольку $g, \gamma \in \mathrm{Aut}\,(\mathcal{C})$, отсюда следует, что $g\gamma^{-1} \in \mathrm{Aut}\,(\mathcal{C}')$ (см. (6)). Таким образом, $g \in \langle \mathrm{Aut}\,(\mathcal{C}'), \Gamma \rangle$. □

Теорема 4.2. *Для циркулянтной схемы $\mathcal{C}$ на n точках за время $n^{O(1)}$ можно проверить имеет ли она суперсимметрический флаг степени по крайней мере 4, и (если это так) найти такой флаг F и циркулянтное F-расширение схемы $\mathcal{C}$. Более того, в последнем случае по заданной регулярной циклической подгруппе группы* $\mathrm{Aut}\,(\mathcal{C})$ *за то же время можно найти суперсимметрическую в F подгруппу группы* $\mathrm{Aut}\,(\mathcal{C})$.

Доказательство. Выведем теорему из результатов работы [2], сохраняя используемую в ней терминологию и нумерацию утверждений. Пусть $\mathcal{C}$ – циркулянтная схема. Применяя алгоритм A2, проверим, является ли схема $\mathcal{C}$ сингулярной, и (если это так) найдём пару флагов (F, F') этой схемы, в которой она имеет сингулярность, и соответствующее этой паре её допустимое расширение $\mathcal{C}'$. По теореме 4.4 это можно сделать за время $(mn)^{O(1)}$, где $m = |\mathcal{E}(\mathcal{C})|$. В силу неравенства $m \leqslant n$, справедливого для произвольной циркулянтной схемы, время работы алгоритма не превосходит $n^{O(1)}$. Поскольку схема $\mathcal{C}$ циркулянтна, из леммы 4.3 и теоремы 4.2 следует, что в случае, когда эта схема сингулярна, флаг F является суперсимметрическим, а схема $\mathcal{C}'$ – циркулянтным F-расширением схемы $\mathcal{C}$. Таким образом, для завершения доказательства первой части теоремы достаточно проверить, что если схема $\mathcal{C}$ не сингулярна, то у неё нет суперсимметрических флагов степени по крайней мере 4. Однако, в этом случае из теоремы 5.1 следует, что схема $\mathcal{C}$ квазинормальна, и потому каждый её примитивный флаг $\sim$-эквивалентен субнормальному флагу. Поскольку любой субнормальный флаг является разрешимым, из теоремы 3.3 этой работы следует, что каждый примитивный флаг схемы $\mathcal{C}$ – разрешимый. Поэтому в $\mathcal{C}$ нет суперсимметрических флагов степени по крайней мере 4, что завершает доказательство первой части теоремы. Вторая часть легко следует из последнего абзаца на стр. 17 и леммы 4.3. □

4.2. Теорема 3.3 из работы [2] показывает, что подгруппа группы автоморфизмов квазинормальной схемы (не обязательно циркулянтной), порождённая всеми её регулярными циклическими подгруппами, разрешима. В силу теоремы 3.3 этой работы в квазинормальной циркулянтной схеме нет симметрических флагов степени по крайней мере 4. Поэтому следующее утверждение усиливает упомянутый выше результат для случая, когда рассматриваемая схема циркулянтна.

Теорема 4.3. *Пусть $\mathcal{C}$ – циркулянтная схема на V без симметрических флагов степени по крайней мере 5. Тогда группа $\mathrm{Aut}\,(\mathcal{C})$ разрешима и может быть найдена за время $n^{O(1)}$, где $n = |V|$.*

Доказательство. Пусть G – регулярная циклическая подгруппа группы $\mathrm{Aut}\,(\mathcal{C})$, и

$$\Delta(V) = E_0 \subset E_1 \subset \cdots \subset E_s = V^2$$

– последовательность эквивалентностей схемы $\mathcal{C}$ такая, что E_i/E_{i-1} – примитивный флаг этой схемы для всех $i = 1, \dots, s$. Каждому такому флагу поставим в соответствие некоторое множество V_i мощности $|E_i/E_{i-1}|$, регулярную циклическую группу $G_i \leqslant \mathrm{Sym}\,(V_i)$ и семейство биекций $f_X : X/E_{i-1} \to V_i$, $X \in V/E_i$, таких, что $(G_{X/E_{i-1}})^{f_X} = G_i$. Заметим, что по теореме 3.3 каждый флаг E_i/E_{i-1} является разрешимым или симметрическим. Однако, поскольку у схемы $\mathcal{C}$ нет симметрических флагов степени по крайней мере 5, отсюда следует, что либо число $|V_i|$ – простое, либо $|V_i| = 4$. В первом случае положим $\Gamma_i = \mathrm{Hol}(G_i)$, а во втором – $\Gamma_i = \mathrm{Sym}\,(V_i)$. Тогда

$$(\mathrm{Aut}\,(\mathcal{C})_{X/E_{i-1}})^{f_X} \leqslant \Gamma_i, \quad i = 1, \dots, s, \quad X \in V/E_i.$$

Определим группу перестановок $\mathrm{wr}(\Gamma_1, \dots, \Gamma_s)$, равной $\{1\}$, если $s = 0$, равной Γ_1, если $s = 1$, равной сплетению групп Γ_1 и Γ_2 (в импримитивном действии), если $s = 2$, и равной $\mathrm{wr}(\mathrm{wr}(\Gamma_1, \dots, \Gamma_{s-1}), \Gamma_s)$, если $s \geqslant 3$. Тогда по лемме 3.4 из работы [2] отображение

$$\mathfrak{f} : V \to \prod_{i=1}^{s} V_i, \quad v \mapsto (\dots, f_{X_i}(X_{i-1}), \dots), \tag{8}$$

где X_i – класс эквивалентности E_i, содержащий точку v, является биекцией и $\mathrm{Aut}\,(\mathcal{C})^{\mathfrak{f}} \leqslant \mathrm{wr}(\Gamma_1, \dots, \Gamma_s)$. Поскольку группа Γ_i разрешима для всех i, таковой же будет и группа $\mathrm{wr}(\Gamma_1, \dots, \Gamma_s)$, а потому и группа $\mathrm{Aut}\,(\mathcal{C})$. Первая часть теоремы полностью доказана.

Для доказательства второй части теоремы заметим, что по теореме 4.4, формулируемой ниже, за время $n^{O(1)}$ можно найти некоторую регулярную циклическую группу $G \leqslant \mathrm{Aut}\,(\mathcal{C})$. Поэтому отображение (8) и группа $\Gamma = \mathrm{wr}(\Gamma_1, \ldots, \Gamma_s)$ также могут быть найдены за то же время. Поскольку эта группа разрешима, группа $\mathrm{Aut}\,(\mathcal{C}) = \Gamma^{\mathfrak{f}^{-1}} \cap \mathrm{Aut}\,(\mathcal{C})$ можно найти за время $n^{O(1)}$ по теореме 2.2. □

4.3. В этом пункте мы опишем эффективный алгоритм для нахождения группы автоморфизмов произвольной циркулянтной схемы. Следующее утверждение, используемое в его описании, является прямым следствием теоремы 7.1 из работы [2].

Теорема 4.4. *Для циркулянтной схемы $\mathcal{C}$ на n точках за время $n^{O(1)}$ можно найти некоторую регулярную циклическую подгруппу группы* $\mathrm{Aut}\,(\mathcal{C})$. □

Основной алгоритм
Вход: циркулянтная схема $\mathcal{C}$.
Выход: группа $\mathrm{Aut}\,(\mathcal{C})$.

Шаг 1. Найти регулярную циклическую группу $G \leqslant \mathrm{Aut}\,(\mathcal{C})$ (теорема 4.4).

Шаг 2. Проверить имеет ли схема $\mathcal{C}$ суперсимметрический флаг степени по крайней мере 4 (теорема 4.2). Если таких флагов нет, то подать на выход группу $\mathrm{Aut}\,(\mathcal{C})$ (теорема 4.3).

Шаг 3. Найти суперсимметрический флаг F схемы $\mathcal{C}$, её циркулянтное F-расширение $\mathcal{C}'$ и суперсимметрическую в F группу $\Gamma \leqslant \mathrm{Aut}\,(\mathcal{C})$ (теорема 4.2).

Шаг 4. Рекурсивно найти группу $\mathrm{Aut}\,(\mathcal{C}')$ и подать на выход группу $\mathrm{Aut}\,(\mathcal{C}) = \langle \mathrm{Aut}\,(\mathcal{C}'), \Gamma \rangle$. □

Теорема 4.5. *Для циркулянтной схемы $\mathcal{C}$ на n точках основной алгоритм корректно находит группу* $\mathrm{Aut}\,(\mathcal{C})$ *за время* $n^{O(1)}$.

Доказательство. Докажем корректность алгоритма. Если он завершает работу на шаге 2, то по теореме 4.2 у схемы $\mathcal{C}$ нет суперсимметрических флагов степени по крайней мере 4. Тогда в силу теоремы 3.2 каждый флаг этой схемы $\sim$-эквивалентен разрешимому флагу или суперсимметрическому флагу степени не превосходящей 3. Поэтому из теоремы 3.3 следует, что у схемы $\mathcal{C}$ нет симметрических флагов степени по крайней мере 4 и, следовательно, корректность алгоритма вытекает из теоремы 4.3. Предположим, что алгоритм не завершает работу на шаге 2. Тогда по определению F-расширения для циркулянтной схемы $\mathcal{C}'$, найденной на шаге 3, выполнено неравенство $\mathrm{rk}\,(\mathcal{C}') > \mathrm{rk}\,(\mathcal{C})$. Используя индукцию по $n-\mathrm{rk}\,(\mathcal{C})$ предположим, что на шаге 4 группа $\mathrm{Aut}\,(\mathcal{C}')$ найдена корректно. Тогда алгоритм корректно завершает работу по лемме 4.1. Для оценки времени его работы заметим, что в силу неравенства $n > \mathrm{rk}\,(\mathcal{C}') > \mathrm{rk}\,(\mathcal{C})$ общее число рекурсивных вызовов на шаге 4 не превосходит n. Поэтому требуемая оценка следует из теорем 4.4, 4.2 и 4.3. $\square$

Литература

1. Б. Ю. Вейсфейлер, А. А. Леман, *Приведение графа к каноническому виду и возникающая при этом алгебра.* — НТИ, сер. 2, 9 (1968), 12–16.
2. С. Евдокимов, И. Пономаренко, *Распознавание и проверка изоморфизма циркулянтных графов за полиномиальное время.* — Алгебра и анализ, **15** (2003), 6, 1–34.
3. L. Babai, E. M. Luks, *Canonical labeling of graphs.* — In: Proc. 15th ACM STOC, (1983), pp. 171–183.
4. A. E. Brouwer, A. M. Cohen, A. Neumaier, *Distance-regular graphs.* — Springer, Berlin (1989).
5. J. D. Dixon, B. Mortimer, *Permutation groups.* — Graduate Texts in Mathematics, No. 163, Springer-Verlag, New York (1996).
6. S. Evdokimov, I. Ponomarenko, *Separability number and schurity number of coherent configurations.* — Electronic Journal of Combinatorics, **7** (2000), #R31.
7. D. G. Higman, *Coherent configurations* 1. — Rend. Mat. Sem. Padova, **44** (1970), 1–25.
8. M. Klin, M. Muzychuk, R. Pöschel, *The isomorphism problem for circulant graphs via Schur rings theory.* — DIMACS Series in Discrete Mathematics and Theoretical Computer Science, **56** (2001), 241–265.
9. E. M. Luks, *Permutation groups and polynomial-time computation.* — DIMACS Series in Discrete Mathematics and Theoretical Computer Science, **11** (1993), 139–175.
10. R. Mathon, *A note on the graph isomorphism counting problem,* — Inform. Process. Lett., **8** (1979), 131–132.
11. M. Muzychuk, *A solution of the isomorphism problem for circulant graphs.* — Proc. London Math. Soc., **88** (2004), 1–41.
12. I. Ponomarenko, *Polynomial-time algorithms for recognizing and isomorphism testing of cyclic tournaments.* — Acta Appl. Math., **29** (1992), 139–160.

13. B. Weisfeiler (editor), *On construction and identification of graphs.* — Springer Lecture Notes, **558** (1976).
14. H. Wielandt, *Finite permutation groups.* — Academic press, New York-London (1964).

Ponomarenko I. N. Finding the automorphism group of a circulant association scheme in polynomial time.

We construct a polynomial-time algorithm for finding the automorphism group of a circulant association scheme. The correctness of the algorithm is based on a new result generalizing the Burnside–Schur theorem (on permutation groups having a regular cyclic subgroup) in the class of the automorphism groups of association schemes.

Санкт-Петербургское отделение
Математичекого института
им. В. А. Стеклова РАН

E-mail: inp@pdmi.ras.ru

Поступило 25 ноября 2004 г.