

РОССИЙСКАЯ АКАДЕМИЯ НАУК

Сибирское отделение

Редколлегия

“Сибирского математического журнала”

РАЗРЕШАЮ
НА ДЕПОНИРОВАНИЕ

УДК 512.54

А.В. Тимофеев

О ПОРОЖДАЮЩИХ ТРОЙКАХ ИНВОЛЮЦИЙ
В СПОРАДИЧЕСКИХ ГРУППАХ

Автор

(Тимофеев А.В.)

Новосибирск 2001

За исключением группы $PSU_3(9)$, каждая (известная) конечная простая группа порождается тремя инволюциями [1]. *Какие конечные простые группы порождаются тремя инволюциями, две из которых перестановочны?* Ответ на этот вопрос В.Д. Мазурова 7.30 из [2] для знакопеременных групп и групп лиева типа удалось найти Я.Н. Нужину в серии работ [3, 4, 5, 6]. Оказалось, что среди перечисленных групп только знакопеременные группы A_6, A_7, A_8 и некоторые линейные группы размерностей ≤ 4 не имеют порождающих троек инволюций, две из которых коммутируют.

В отличие от бесконечных серий конечных простых групп, все известные автору ответы на вопрос 7.30 для sporadicических групп, кроме групп J_1, J_4, Ly , опираются на компьютерные вычисления. Так, например, Я.Н. Нужин доказал [7] без компьютера, что порождающими тройками инволюций, две из которых перестановочны, обладают sporadicические группы Янко J_1, J_2 и группа Матье M_{24} . Однако, его рассуждения опираются на генетический код этих групп, который был построен [8] в системе компьютерной алгебры. Различными алгоритмами, но с помощью одной системы GAP (Группы, алгоритмы, программирование) [9, 10], студенты красноярских вузов Т.Е. Колесникова, А.В. Ершов и Н.С. Невмержицкая доказали, что в любой порождающей группу Матье M_{11} тройке инволюций нет перестановочных элементов. Двое последних нашли вместе с автором для группы M_{12} порождающие ее три инволюции, две из которых перестановочны. Алгоритмы поиска всех порождающих троек инволюций с точностью до порядков произведений их неперестановочных элементов были применены автором [7] в решении задачи В.Д.Мазурова 7.30 для sporadicических групп:

$$M_{11}, M_{12}, M_{22}, M_{23}, M_{24}, HS, McL, J_1. \quad (1)$$

В настоящей работе доказана

Теорема. *Тремя инволюциями, две из которых перестановочны, порождаются группы Янко J_1, J_2, J_3, J_4 , группы Конвея Co_2 и Co_3 , Фишера F_{22} и F_{23} , Матье M_{12} и M_{24} , группа Хигмана-Симса HS , группа Хельда He , группа Рудвалиса Ru , группа Сузуки Suz , группа О'Нэна ON и группа Лайонса Ly . Группа Маклафлина McL и группы Матье M_{11}, M_{22} и M_{23} не обладают этим*

свойством.

Таким образом, для 18 sporadicических групп из 20, имеющих в электронном атласе [11] точное подстановочное представление, проблема В.Д. Мазурова 7.30 закрыта.

На самом деле доказано больше, чем сказано теоремой. А именно, если G – группа,

$$C_3(G) = \{(|ij|, |jk|, |ik|) \mid |i| = |j| = |k| = 2, \text{гр}(i, j, k) = G\},$$

$$C_2(G) = \{(|ik|, |kj|) \mid G = \text{гр}(i, j, k), |i| = |j| = |k| = |ij| = 2\},$$

то для каждой группы G из множества $\{M_{11}, M_{22}, M_{23}, McL\}$ построено множество $C_3(G)$, причем каждая его тройка не содержит число 2. Для любой другой группы G из теоремы построено непустое множество $C_2(G)$, либо его непустое подмножество, либо найдено число в некоторой паре из $C_2(G)$. Кроме того, построены множества $C_2(A_9)$, $C_2(A_{10})$, $C_2(A_{11})$ и подмножество из $C_2(A_{12})$. Следовательно, для перечисленных групп получен ответ на вопрос Я.Н. Нужина: “Какие конечные простые группы являются гомоморфными образами группы Коксетера

$$\text{гр}(a, b, c \mid a^2, b^2, c^2, (ac)^2, (ab)^p, (bc)^q)$$

при фиксированных p и q ?”

Необходимо отметить, что после построения множества $C_2(G)$ для каждой группы G из списка (1), успеху в решении проблем В.Д. Мазурова и Я.Н. Нужина способствовала

Гипотеза (Я.Н. Нужин). *Из sporadicических групп только группы Матье M_{11}, M_{22}, M_{23} и группа Маклафлина McL не порождаются тремя инволюциями, две из которых перестановочны.*

1 Группы и графы Коксетера

Напомним, что *группой Коксетера* называют группу

$$\text{гр}(x_1, x_2, \dots, x_n \mid (x_i x_j)^{m_{i,j}} = 1, m_{i,i} = 1, 1 \leq i \leq j \leq n),$$

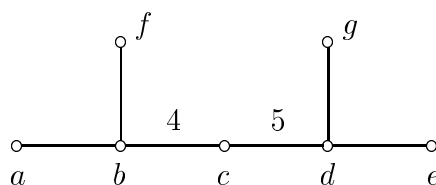
а ее гомоморфный образ – группой типа Коксетера.

Порождающие группу типа Коксетера инволюции иногда изображают точками и если $m_{ij} > 2$, то элементы x_i и x_j связывают ребром. В свою очередь, если $m_{ij} > 3$, то над ребром принято писать число $m_{ij}(= |x_i x_j|)$. Построенный граф тоже носит имя Г.С.М. Коксетера.

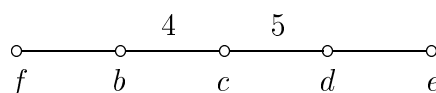
Следующие два предложения демонстрируют “немашинные” подходы к проблеме 7.30.

Предложение 1. Для некоторого числа q пара $(6, q) \in C_2(M_{24})$.

Доказательство. В силу [8] группа M_{24} является группой типа Коксетера с графом



и $g(abc)^3 = a(cde)^5 = 1$. Из этих соотношений легко следует что группа M_{24} является группой типа Коксетера с графом



Рассмотрим подгруппу M , порожденную тремя инволюциями fc, e, bd , первые две из которых перестановочны. Так как $(bde)^3 = b$, то $b, d \in M$. Далее, $(fcd)^5 = f$. Отсюда и $f, c \in M$. Следовательно, $M = M_{24}$. Сейчас, учитывая, что $(bde)^6 = 1$, получаем $(6, q) \in C_2(M_{24})$. Что и требовалось.

Доказательство любезно предоставил автору Я.Н. Нужин. Его же доказательство теоремы для группы J_1 проходит и для групп J_4 и Lu .

Предложение 2. Для некоторого делителя q периода группы J_4 пара $(q, 43) \in C_2(J_4)$ и для делителей r, s периода группы Lu справедливо включение $C_2(Lu) \supset \{(r, 37), (s, 67)\}$.

Доказательство опирается на описание максимальных подгрупп спорадических простых конечных групп Ly и J_4 (см., например, [11]). Действительно, группа J_4 содержит максимальную подгруппу Фробениуса $F_{602} = (a) \rtimes (b)$, причем $|a| = 43$, $|b| = 14$, а другие максимальные подгруппы не содержат циклических подгрупп порядка 43. В группе F_{602} выберем элементы i, j порядков 2. Пусть $i = (1, b^7)$, $j = (a, b^7)$ и k – инволюция четверной подгруппы Клейна централизатора $C_{J_4}(i)$, причем $k \neq i$. Тогда $\text{gr}(i, j)$ – группа диэдра порядка 86 и $J_4 = \text{gr}(i, j, k)$. Точно также подгруппы F_{666} и F_{1474} группы Ly применяются для доказательства оставшейся части предложения.

2 Схема доказательства теоремы

Теорема доказывается для каждой ее группы G построением множества $C_2(G)$, либо его подмножества. За исключением групп J_4 и Ly элементы из $C_2(G)$ находит компьютер по GAP-программе.

Примененные алгоритмы основаны на переборе всех, либо достаточного числа троек инволюций, две из которых перестановочны. Прежде всего, строятся все классы сопряженных инволюций группы (в спорадических группах их не больше трех). Представители этих классов (по которым система GAP строит сам класс) можно найти либо в электронном атласе [11], либо среди инволюций силовской 2-подгруппы, которую тоже строит система GAP одним из своих операторов.

Двадцать групп теоремы разбиваем на следующие множества.

а) $\{M_{11}, M_{12}, M_{22}, M_{23}, M_{24}, McL, HS, J_1, J_2\}$. В этом случае удастся построить все элементы множества $C_2(G)$.

б) $\{J_3\}$. В третьей группе Янко все инволюции сопряжены. Поэтому, выбрав две перестановочные инволюции, третий элемент второго порядка выбираем в классе сопряженных инволюций случайным образом до тех пор, пока три эти инволюции не породят группу J_3 . Проверка на порождаемость группы J_3 найденной тройкой инволюций происходит без участия теоретико-вероятностных алгоритмов. Вычислив порядки произведений непорочных инволюций в

этой тройке, получаем элемент множества $C_2(J_3)$.

в) $\{Co_3, He, Ru^1, Suz\}$. В этих группах по два класса сопряженных инволюций, Поэтому организованы два цикла в соответствии с расположением трех инволюций подгруппы Клейна в этих классах: 1) все три инволюции в одном классе, 2) две в одном, третья – в другом классе.

г) $\{Co_2, F_{22}\}$. Поскольку в группах Co_2 и F_{22} по три класса сопряженных инволюций, то к случаям 1) и 2) из в) добавляется еще один – 3) инволюции подгруппы Клейна расположены по одной в каждом классе сопряженных инволюций.

д) $\{F_{23}, ON\}$. Указанные группы имеют самые высокие степени подстановочных представлений. Эффективным оказался выбор клейновской подгруппы в одной из максимальных подгрупп каждой из групп F_{23} и ON . Третью инволюцию находили тоже оператором Random в классе сопряженных инволюций.

е) $\{J_4, Ly\}$. Автор знает только некомпьютерное построение – см. предложение 2.

Ситуации б) и в) можно рассматривать как частные случаи г), а построение клейновской подгруппы в максимальных подгруппах из д) аналогично построению подгруппы Клейна в г). Поэтому в следующих подпараграфах подробнее опишем алгоритм для случаев а) и г), т.е. когда строится множество $C_2(G)$ и подмножество этого множества.

2.1 Построение множества $C_2(G)$

Как известно, простая группа G из множества $\{M_{11}, M_{12}, M_{22}, M_{23}, M_{24}, McL, HS, J_1, J_2\}$ имеет не более двух классов сопряженных инволюций. Обозначим их символами $s_l, l = 1, 2$. Следовательно, три инволюции могут находиться при $l = 1, 2$:

- 1) либо в одном классе s_l ,
- 2) либо две в классе s_l , одна в классе $s_{l'}$, где $l' \in \{1, 2\} \setminus \{l\}$.

Разберем отдельные случаи. Причем вместо класса s_l будем этим же символом обозначать список всех его инволюций.

¹В построении множества $C_2(Ru)$ принимал участие Е.И. Кузнецов.

1) В списке s_l зафиксируем инволюцию i . Пусть (j, k) пробегает множество всех (неупорядоченных) пар инволюций из s_l . Тогда если существует порождающая группу G тройка инволюций, в которой два элемента перестановочны, то она будет либо тройкой (i, j, k) , либо ей сопряженной. Действительно, $s_l = i^G$. Поэтому произвольную тройку инволюций из s_l можно представить в виде $(i^{u^{-1}}, i^v, i^w)$ для некоторых $u, v, w \in G$. В свою очередь,

$$\{i^{u^{-1}}, i^v, i^w\}^u = \{i, j, k\}, \text{ где } j = i^{vu}, k = i^{wu}, \quad (2)$$

что и требовалось.

Заметим, что с каждой тройкой (i, i^v, i^w) сопряжены тройки инволюций $(i, i^{v^{-1}}, i^{wv^{-1}})$ и $(i, i^{vw^{-1}}, i^{w^{-1}})$. Однако, опыт показал, что учет этого обстоятельства не приводит к увеличению скорости вычислений при изучении групп Матье.

2) для каждого $l = 1, 2$ в списке s_l выберем инволюцию i . Затем организуем перебор всевозможных пар (j, k) , где $j \in s'_1, k \in s'_2$, где s'_l – список всех элементов из s_l кроме i , $l = 1, 2$. На каждом шаге проверяем порождает ли тройка (i, j, k) группу G . Как показано в (2) любую тройку с условием 2) можно перевести сопряжением в тройку (i, j, k) .

Таким образом, с точностью до сопряженности мы можем получить все порождающие группу G тройки инволюций. В частности, несколько часов потребовалось для перебора всех (с точностью до сопряженности) троек инволюций группы Маклафлина McL .

2.2 Подмножество множества $C_2(G)$

Понятно, что две любые инволюции порождают либо 4-группу Клейна, либо группу диэдра. Поэтому для поиска тройки порождающих группу G инволюций надо взять диэдральную подгруппу и проверять порождают ли она и некоторая инволюция группу G , либо взять четверную подгруппу Клейна и делать тоже самое.

Случай г) из п. 2 рассмотрим на примере группы Конвея Co_2 . Прежде всего, построим силовскую 2-подгруппу S группы Co_2 . Затем повторяем случайный выбор в S неединичного элемента h до тех пор, пока список порядков классов

сопряженных с инволюцией $h^{|h|/2}$ элементов не будет состоять из трех чисел. Некоторые из этих чисел превышают 100000 – верхнюю границу размера списка в системе GAP344. Поэтому инволюции придется не перебирать одна за другой из списка (как в случае а)), а случайным образом выбирать каждую из класса сопряженных инволюций. Эту инволюцию будем добавлять к двум инволюциям подгруппы Клейна и проверять будут ли три эти элемента порождать группу Co_2 .

Гипотеза Я.Н. Нужина (из введения) ориентирует автора на поиск положительного ответа на вопрос В.Д. Мазурова 7.30. Рассматривая варианты 1)–3) расположения инволюций в подгруппе Клейна (см. случаи в) и г) в начале параграфа) и выбирая еще одну инволюцию в каждом из трех классов сопряженных элементов второго порядка группы Co_2 , действительно удастся построить непустое подмножество множества $C_2(Co_2)$.

3 Результаты вычислений

Для каждой группы G из теоремы ниже размещены сведения о ее множестве $C_2(G)$, либо множестве $C_3(G)$. Аналогичная информация дана и о четырех знакопеременных группах.

В квадратных скобках указаны порядки классов сопряженных инволюций.

Для групп, степень подстановочного представления которых не превышает ста, опубликуем порождающие их тройки инволюций, две из которых перестановочны. Порождающие тройки инволюций других групп лежат на сайте Красноярского алгебраического семинара [12].

3.1 Группа Матье M_{12}

$$C_2(M_{12}) = \{(5, 6), (5, 8), (6, 6), (6, 8), (6, 10), (8, 8), (8, 10), (10, 10)\}.$$

$$[495, 396]$$

$$M_{12} = \text{гр}((1, 2) (3, 4) (5, 6) (7, 11) (8, 12) (9, 10), (1, 2) (3, 4) (5, 11) (6, 7) (8, 10) (9, 12), (1, 3) (2, 5) (4, 8) (6, 11) (7, 12) (9, 10)).$$

3.2 Группа Матъе M_{24}

$C_2(M_{24})=\{(4,8), (4,10), (4,11), (4,12), (5,6), (5,10), (5,11), (5,12), (6,6), (6,8), (6,10), (6,11), (6,12), (8,8), (8,10), (8,11), (8,12), (10,10), (10,11), (10,12), (11,11), (11,12), (12,12)\}$.

[11385,31878]

$M_{24} = \text{gp}((1,2) (3,4) (5,6) (7,10) (8,18) (9,21) (11,24) (12,23) (13,15) (14,16) (17,19) (20,22), (1,2) (3,4) (5,7) (6,9) (8,12) (10,11) (13,23) (14,19) (15,17) (16,18) (20,24) (21,22), (1,5) (2,6) (3,11) (4,24) (7,8) (9,17) (10,18) (12,13) (14,20) (15,23) (16,22) (19,21))$.

3.3 Группа Хигмана-Симпса HS

$C_2(HS)=\{(3,15), (4,7), (4,10), (4,15), (5,7), (5,8), (5,12), (5,15), (6,6), (6,7), (6,8), (6,10), (6,12), (6,15), (7,7), (7,8), (7,10), (7,12), (7,15), (8,8), (8,10), (8,12), (8,15), (10,10), (10,12), (10,15), (12,12), (12,15), (15,15)\}$.

[5775,15400]

$HS = \text{gp}((1,2) (3,6) (4,55) (5,21) (7,34) (8,31) (9,58) (10,47) (11,79) (12,53) (13,43) (14,77) (15,30) (16,97) (17,78) (18,27) (19,42) (20,89) (22,69) (23,80) (24,32) (25,45) (26,96) (28,37) (29,70) (33,50) (35,82) (36,41) (38,40) (39,51) (44,91) (46,99) (48,83) (49,86) (52,66) (54,65) (56,72) (57,64) (59,98) (60,68) (61,87) (62,92) (63,95) (67,75) (71,84) (73,90) (74,81) (76,93) (85,88) (94,100), (1,100) (2,76) (3,62) (4,37) (5,95) (6,88) (7,57) (8,85) (10,65) (11,39) (12,63) (13,58) (15,33) (19,68) (20,78) (21,29) (23,56) (24,72) (25,98) (26,90) (27,46) (28,48) (34,96) (36,61) (38,51) (41,43) (44,74) (45,86) (47,91) (49,52) (50,55) (54,75) (60,93) (66,71) (69,73) (70,77) (79,99) (80,89) (82,87) (92,97), (1,3) (2,6) (4,95) (5,48) (7,40) (8,70) (9,39) (10,50) (11,25) (12,35) (13,52) (14,57) (15,75) (16,60) (17,65) (18,99) (19,69) (20,100) (21,83) (22,42) (23,49) (24,91) (26,62) (27,46) (28,41) (29,31) (30,67) (32,44) (33,47) (34,38) (36,37) (43,66) (45,79) (51,58) (53,82) (54,78) (55,63) (56,73) (59,81) (61,88) (64,77) (68,97) (71,76) (72,90) (74,98) (80,86) (84,93) (85,87) (89,94) (92,96))$.

3.4 Группа Янко J_1

$C_2(J_1)=\{(3,7), (3,10), (3,11), (3,15), (3,19), (5,5), (5,7), (5,10), (5,15), (5,19), (6,7), (6,10), (6,11), (6,15), (6,19), (7,7), (7,10), (7,11), (7,15), (7,19), (10,10), (10,11), (10,15), (10,19), (11,11), (11,15), (11,19), (15,15), (15,19), (19,19)\}.$

[1463]

3.5 Группа Янко J_2

$C_2(J_2)=\{(3,12), (3,15), (4,7), (4,15), (5,6), (5,7), (5,8), (5,10), (5,12), (5,15), (6,6), (6,7), (6,8), (6,10), (6,12), (6,15), (8,8), (8,10), (8,15), (10,10), (10,12), (10,15), (12,12), (12,15), (15,15)\}.$

[315,2520]

$J_2 = \text{gp}((1, 2) (3, 5) (4, 6) (7,69) (8,54) (9,59) (10,43) (11,20) (12,55) (13,25) (14,90) (15,68) (16,47) (17,42) (18,26) (19,40) (21,86) (22,33) (23,35) (24,34) (27,31) (28,63) (29,97) (30,99) (32,51) (36,79) (37,77) (38,39) (41,71) (44,76) (45,81) (46,78) (48,58) (49,96) (50,85) (52,60) (53,91) (56,65) (57,61) (62,80) (64,84) (66,70) (67,89) (72,88) (73,74) (75,93) (82,95) (83,87) (92,98) (94,100), (3,16) (4,36) (5,21) (6,34) (7,98) (9,26) (10,63) (11,85) (12,62) (13,87) (14,95) (15,67) (17,49) (18,89) (19,61) (22,47) (23,90) (25,46) (28,44) (30,99) (31,57) (32,40) (33,75) (35,78) (37,39) (38,70) (41,43) (48,74) (50,96) (54,60) (56,79) (58,82) (59,71) (64,91) (66,93) (68,76) (73,83) (77,86) (84,92) (94,97), (1,11) (2,20) (3,48) (4,63) (5,58) (6,28) (7,55) (8,73) (9,29) (10,62) (12,69) (13,49) (14,23) (15,85) (16,76) (17,71) (18,89) (19,87) (21,39) (22,94) (24,57) (25,96) (26,67) (27,81) (30,95) (31,45) (32,93) (33,100) (34,61) (35,90) (36,53) (37,92) (38,86) (40,83) (41,42) (43,80) (44,47) (46,64) (50,68) (51,75) (52,65) (54,74) (56,60) (59,97) (66,88) (70,72) (77,98) (78,84) (79,91) (82,99)).$

3.6 Группа Янко J_3

$C_2(J_3) \supseteq \{ (3, 10), (3, 12), (3, 15), (3, 17), (4, 9), (4, 10), (4, 15), (5, 6), (5, 8), (5, 9), (5, 10), (5, 12), (5, 15), (5, 17), (6, 6), (6, 8), (6, 9), (6, 10), (6, 12), (6, 15), (6, 17), (8, 9), (8, 10), (8, 12), (8, 15), (8, 17), (9, 9), (9, 10), (9, 12), (9, 15), (9, 17), (10, 10), (10, 12), (10, 15), (10, 17), (12, 12), (12, 15), (12, 17), (15, 15), (15, 17), (17, 17)\}.$

[26163]

3.7 Группа Янко J_4

$C_2(J_4) \ni (?, 43)$.

3.8 Группа Фишера F_{22}

$C_2(F_{22}) \supseteq \{ (5, 18), (5, 30), (6, 6), (6, 8), (6, 9), (6, 10), (6, 12), (6, 13), (6, 14), (6, 15), (6, 18), (6, 20), (6, 21), (6, 24), (6, 30), (7, 8), (7, 10), (7, 12), (7, 13), (7, 18), (7, 21), (7, 24), (7, 30), (8, 8), (8, 9), (8, 10), (8, 12), (8, 13), (8, 14), (8, 15), (8, 18), (8, 20), (8, 21), (8, 24), (8, 30), (9, 9), (9, 10), (9, 12), (9, 13), (9, 14), (9, 15), (9, 18), (9, 20), (9, 21), (9, 24), (9, 30), (10, 10), (10, 12), (10, 13), (10, 14), (10, 15), (10, 18), (10, 20), (10, 21), (10, 24), (10, 30), (12, 12), (12, 13), (12, 14), (12, 15), (12, 18), (12, 20), (12, 21), (12, 24), (12, 30), (13, 13), (13, 14), (13, 15), (13, 18), (13, 20), (13, 21), (13, 24), (13, 30), (14, 14), (14, 15), (14, 18), (14, 20), (14, 21), (14, 24), (14, 30), (15, 15), (15, 18), (15, 20), (15, 21), (15, 24), (15, 30), (18, 18), (18, 20), (18, 21), (18, 24), (18, 30), (20, 20), (20, 21), (20, 24), (20, 30), (21, 21), (21, 24), (21, 30), (24, 24), (24, 30), (30, 30) \}.$

[3510,1216215,36486450]

3.9 Группа Фишера F_{23}

$C_2(F_{23}) \supseteq \{ (3, 12), (3, 13), (3, 14), (3, 17), (3, 26), (3, 27), (3, 36), (3, 42), (4, 7), (4, 8), (4, 12), (4, 13), (4, 14), (4, 15), (4, 17), (4, 18), (4, 20), (4, 21), (4, 24), (4, 26), (4, 27), (4, 30), (4, 35), (4, 36), (4, 39), (4, 42), (4, 60), (5, 6), (5, 7), (5, 8), (5, 9), (5, 12), (5, 13), (5, 14), (5, 15), (5, 17), (5, 18), (5, 20), (5, 21), (5, 22), (5, 24), (5, 26), (5, 27), (5, 28), (5, 30), (5, 35), (5, 36), (5, 39), (5, 42), (5, 60), (6, 6), (6, 7), (6, 8), (6, 9), (6, 10), (6, 11), (6, 12), (6, 13), (6, 14), (6, 15), (6, 17), (6, 18), (6, 20), (6, 21), (6, 22), (6, 24), (6, 26), (6, 27), (6, 28), (6, 30), (6, 35), (6, 36), (6, 39), (6, 42), (6, 60), (7, 8), (7, 9), (7, 10), (7, 11), (7, 12), (7, 13), (7, 14), (7, 15), (7, 17), (7, 18), (7, 20), (7, 21), (7, 22), (7, 24), (7, 26), (7, 27), (7, 28), (7, 30), (7, 35), (7, 36), (7, 39), (7, 42), (7, 60), (8, 8), (8, 9), (8, 10), (8, 11), (8, 12), (8, 13), (8, 14), (8, 15), (8, 17), (8, 18), (8, 20), (8, 21), (8, 22), (8, 24), (8, 26), (8, 27), (8, 28), (8, 30), (8, 35), (8, 36), (8, 39), (8, 42), (8, 60), (9, 9), (9, 10), (9, 11), (9, 12), (9, 13), (9, 14), (9, 15), (9, 17), (9, 18),$

$(9, 20), (9, 21), (9, 22), (9, 24), (9, 26), (9, 27), (9, 28), (9, 30), (9, 35), (9, 36), (9, 39),$
 $(9, 42), (9, 60), (10, 10), (10, 11), (10, 12), (10, 13), (10, 14), (10, 15), (10, 17), (10, 18),$
 $(10, 20), (10, 21), (10, 22), (10, 24), (10, 26), (10, 27), (10, 28), (10, 30), (10, 35), (10, 36),$
 $(10, 39), (10, 42), (10, 60), (11, 11), (11, 12), (11, 13), (11, 14), (11, 15), (11, 17), (11, 18),$
 $(11, 20), (11, 21), (11, 22), (11, 24), (11, 26), (11, 27), (11, 28), (11, 30), (11, 35), (11, 36),$
 $(11, 39), (11, 42), (11, 60), (12, 12), (12, 13), (12, 14), (12, 15), (12, 17), (12, 18), (12, 20),$
 $(12, 21), (12, 22), (12, 24), (12, 26), (12, 27), (12, 28), (12, 30), (12, 35), (12, 36), (12, 39),$
 $(12, 42), (12, 60), (13, 13), (13, 14), (13, 15), (13, 17), (13, 18), (13, 20), (13, 21), (13, 22),$
 $(13, 24), (13, 26), (13, 27), (13, 28), (13, 30), (13, 35), (13, 36), (13, 39), (13, 42), (13, 60),$
 $(14, 14), (14, 15), (14, 17), (14, 18), (14, 20), (14, 21), (14, 22), (14, 24), (14, 26), (14, 27),$
 $(14, 28), (14, 30), (14, 35), (14, 36), (14, 39), (14, 42), (14, 60), (15, 15), (15, 17), (15, 18),$
 $(15, 20), (15, 21), (15, 22), (15, 24), (15, 26), (15, 27), (15, 28), (15, 30), (15, 35), (15, 36),$
 $(15, 39), (15, 42), (15, 60), (17, 17), (17, 18), (17, 20), (17, 21), (17, 22), (17, 24), (17, 26),$
 $(17, 27), (17, 28), (17, 30), (17, 35), (17, 36), (17, 39), (17, 42), (17, 60), (18, 18), (18, 20),$
 $(18, 21), (18, 22), (18, 24), (18, 26), (18, 27), (18, 28), (18, 30), (18, 35), (18, 36), (18, 39),$
 $(18, 42), (18, 60), (20, 20), (20, 21), (20, 22), (20, 24), (20, 26), (20, 27), (20, 28), (20, 30),$
 $(20, 35), (20, 36), (20, 39), (20, 42), (20, 60), (21, 21), (21, 22), (21, 24), (21, 26), (21, 27),$
 $(21, 28), (21, 30), (21, 35), (21, 36), (21, 39), (21, 42), (21, 60), (22, 22), (22, 24), (22, 26),$
 $(22, 27), (22, 28), (22, 30), (22, 35), (22, 36), (22, 39), (22, 42), (22, 60), (24, 24), (24, 26),$
 $(24, 27), (24, 28), (24, 30), (24, 35), (24, 36), (24, 39), (24, 42), (24, 60), (26, 26), (26, 27),$
 $(26, 28), (26, 30), (26, 35), (26, 36), (26, 39), (26, 42), (26, 60), (27, 27), (27, 28), (27, 30),$
 $(27, 35), (27, 36), (27, 39), (27, 42), (27, 60), (28, 28), (28, 30), (28, 35), (28, 36), (28, 39),$
 $(28, 42), (28, 60), (30, 30), (30, 35), (30, 36), (30, 39), (30, 42), (30, 60), (35, 35), (35, 36),$
 $(35, 39), (35, 42), (35, 60), (36, 36), (36, 39), (36, 42), (36, 60), (39, 39), (39, 42), (39, 60),$
 $(42, 42), (42, 60), (60, 60)\}.$

[55582605]

3.10 Группа Рудвалиса Ru

$C_2(Ru) \supseteq \{ (3, 7), (3, 8), (3, 10), (3, 12), (3, 13), (3, 14), (3, 15), (3, 20), (3, 24),$
 $(3, 26), (3, 29), (4, 5), (4, 6), (4, 7), (4, 8), (4, 10), (4, 12), (4, 13), (4, 14), (4, 15),$
 $(4, 20), (4, 24), (4, 26), (4, 29), (5, 5), (5, 6), (5, 7), (5, 8), (5, 10), (5, 12), (5, 13),$

(5, 14), (5, 15), (5, 20), (5, 24), (5, 26), (5, 29), (6, 6), (6, 7), (6, 8), (6, 10), (6, 12), (6, 13), (6, 14), (6, 15), (6, 20), (6, 24), (6, 26), (6, 29), (7, 7), (7, 8), (7, 10), (7, 12), (7, 13), (7, 14), (7, 15), (7, 20), (7, 24), (7, 26), (7, 29), (8, 8), (8, 10), (8, 12), (8, 13), (8, 14), (8, 15), (8, 20), (8, 24), (8, 26), (8, 29), (10, 10), (10, 12), (10, 13), (10, 14), (10, 15), (10, 20), (10, 24), (10, 26), (10, 29), (12, 12), (12, 13), (12, 14), (12, 15), (12, 20), (12, 24), (12, 26), (12, 29), (13, 13), (13, 14), (13, 15), (13, 20), (13, 24), (13, 26), (13, 29), (14, 14), (14, 15), (14, 20), (14, 24), (14, 26), (14, 29), (15, 15), (15, 20), (15, 24), (15, 26), (15, 29), (20, 20), (20, 24), (20, 26), (20, 29), (24, 24), (24, 26), (24, 29), (26, 26), (26, 29), (29, 29)).

[1252800,593775]

3.11 Группа О'Нэна ON

$C_2(ON) \supseteq \{ (4, 16), (5, 11), (5, 14), (5, 15), (5, 16), (5, 28), (6, 8), (6, 10), (6, 11), (6, 12), (6, 15), (6, 16), (6, 19), (6, 28), (7, 10), (7, 15), (7, 16), (8, 8), (8, 10), (8, 11), (8, 12), (8, 14), (8, 15), (8, 16), (8, 19), (8, 28), (10, 11), (10, 14), (10, 15), (10, 16), (10, 19), (10, 28), (11, 11), (11, 12), (11, 14), (11, 15), (11, 16), (11, 19), (11, 28), (12, 16), (12, 19), (12, 28), (14, 14), (14, 15), (14, 16), (14, 19), (14, 28), (15, 15), (15, 16), (15, 19), (15, 28), (16, 16), (16, 19), (16, 28), (19, 19), (19, 28), (28, 28) \}.$

[2857239]

3.12 Группа Хельда He

$C_2(He) \supseteq \{ (3, 12), (3, 17), (3, 21), (4, 8), (4, 10), (4, 12), (4, 15), (4, 17), (4, 21), (5, 8), (5, 12), (5, 15), (5, 17), (5, 21), (6, 6), (6, 7), (6, 8), (6, 10), (6, 12), (6, 15), (6, 17), (6, 21), (7, 8), (7, 10), (7, 12), (7, 15), (7, 17), (7, 21), (8, 8), (8, 10), (8, 12), (8, 15), (8, 17), (8, 21), (10, 10), (10, 12), (10, 15), (10, 17), (10, 21), (12, 12), (12, 15), (12, 17), (12, 21), (15, 15), (15, 17), (15, 21), (17, 17), (17, 21), (21, 21) \}.$

[24990,187425]

3.13 Группа Сузуки Suz

$C_2(Suz) \supseteq \{ (3, 10), (3, 11), (3, 12), (3, 13), (3, 14), (3, 15), (3, 20), (3, 21), (3, 24), (4, 8), (4, 10), (4, 11), (4, 12), (4, 13), (4, 14), (4, 15), (4, 20), (4, 21), (4, 24), (5, 6),$

(5, 7), (5, 8), (5, 10), (5, 11), (5, 12), (5, 13), (5, 14), (5, 15), (5, 20), (5, 21), (5, 24),
(6, 6), (6, 7), (6, 8), (6, 10), (6, 11), (6, 12), (6, 13), (6, 14), (6, 15), (6, 20), (6, 21),
(6, 24), (7, 7), (7, 8), (7, 10), (7, 11), (7, 12), (7, 13), (7, 14), (7, 15), (7, 20), (7, 21),
(7, 24), (8, 8), (8, 10), (8, 11), (8, 12), (8, 13), (8, 14), (8, 15), (8, 20), (8, 21), (8, 24),
(10, 10), (10, 11), (10, 12), (10, 13), (10, 14), (10, 15), (10, 20), (10, 21), (10, 24), (11, 11),
(11, 12), (11, 13), (11, 14), (11, 15), (11, 20), (11, 21), (11, 24), (12, 12), (12, 13), (12, 14),
(12, 15), (12, 20), (12, 21), (12, 24), (13, 13), (13, 14), (13, 15), (13, 20), (13, 21), (13, 24),
(14, 14), (14, 15), (14, 20), (14, 21), (14, 24), (15, 15), (15, 20), (15, 21), (15, 24), (20, 20),
(20, 21), (20, 24), (21, 21), (21, 24), (24, 24)}.

[2779920,135135]

3.14 Группа Конвея Co_2

$C_2(Co_2) \supseteq \{ (4, 7), (4, 8), (4, 9), (4, 10), (4, 11), (4, 12), (4, 14), (4, 15), (4, 16), (4, 18),$
 $(4, 20), (4, 24), (4, 28), (4, 30), (5, 5), (5, 6), (5, 7), (5, 8), (5, 9), (5, 10), (5, 11), (5, 12),$
 $(5, 14), (5, 15), (5, 16), (5, 18), (5, 20), (5, 24), (5, 28), (5, 30), (6, 6), (6, 7), (6, 8),$
 $(6, 9), (6, 10), (6, 11), (6, 12), (6, 14), (6, 15), (6, 16), (6, 18), (6, 20), (6, 24), (6, 28),$
 $(6, 30), (7, 7), (7, 8), (7, 9), (7, 10), (7, 11), (7, 12), (7, 14), (7, 15), (7, 16), (7, 18),$
 $(7, 20), (7, 24), (7, 28), (7, 30), (8, 8), (8, 9), (8, 10), (8, 11), (8, 12), (8, 14), (8, 15),$
 $(8, 16), (8, 18), (8, 20), (8, 24), (8, 28), (8, 30), (9, 9), (9, 10), (9, 11), (9, 12), (9, 14),$
 $(9, 15), (9, 16), (9, 18), (9, 20), (9, 24), (9, 28), (9, 30), (10, 10), (10, 11), (10, 12),$
 $(10, 14), (10, 15), (10, 16), (10, 18), (10, 20), (10, 24), (10, 28), (10, 30), (11, 11), (11, 12),$
 $(11, 14), (11, 15), (11, 16), (11, 18), (11, 20), (11, 24), (11, 28), (11, 30), (12, 12), (12, 14),$
 $(12, 15), (12, 16), (12, 18), (12, 20), (12, 24), (12, 28), (12, 30), (14, 14), (14, 15), (14, 16),$
 $(14, 18), (14, 20), (14, 24), (14, 28), (14, 30), (15, 15), (15, 16), (15, 18), (15, 20), (15, 24),$
 $(15, 28), (15, 30), (16, 16), (16, 18), (16, 20), (16, 24), (16, 28), (16, 30), (18, 18), (18, 20),$
 $(18, 24), (18, 28), (18, 30), (20, 20), (20, 24), (20, 28), (20, 30), (24, 24), (24, 28), (24, 30),$
 $(28, 28), (28, 30), (30, 30)}.$

[56925,1024650,28690200]

3.15 Группа Конвея Co_3

$C_2(Co_3) \supseteq \{ (3, 9), (3, 10), (3, 12), (3, 14), (3, 15), (3, 18), (3, 21), (3, 24), (3, 30), (4, 9), (4, 10), (4, 12), (4, 14), (4, 15), (4, 18), (4, 21), (4, 24), (4, 30), (5, 6), (5, 7), (5, 8), (5, 9), (5, 10), (5, 12), (5, 14), (5, 15), (5, 18), (5, 21), (5, 24), (5, 30), (6, 6), (6, 7), (6, 8), (6, 9), (6, 10), (6, 12), (6, 14), (6, 15), (6, 18), (6, 21), (6, 24), (6, 30), (7, 7), (7, 8), (7, 9), (7, 10), (7, 12), (7, 14), (7, 15), (7, 18), (7, 21), (7, 24), (7, 30), (8, 8), (8, 9), (8, 10), (8, 12), (8, 14), (8, 15), (8, 18), (8, 21), (8, 24), (8, 30), (9, 9), (9, 10), (9, 12), (9, 14), (9, 15), (9, 18), (9, 21), (9, 24), (9, 30), (10, 10), (10, 12), (10, 14), (10, 15), (10, 18), (10, 21), (10, 24), (10, 30), (12, 12), (12, 14), (12, 15), (12, 18), (12, 21), (12, 24), (12, 30), (14, 14), (14, 15), (14, 18), (14, 21), (14, 24), (14, 30), (15, 15), (15, 18), (15, 21), (15, 24), (15, 30), (18, 18), (18, 21), (18, 24), (18, 30), (21, 21), (21, 24), (21, 30), (24, 24), (24, 30), (30, 30) \}.$

[170775,2608200]

3.16 Группа Лайонса Ly

$C_2(Ly) \supseteq \{ (?, 37), (?, 67) \}.$

3.17 Группы Матье M_{11}, M_{22}, M_{23} и группа Маклафлина McL

На числа p, q, r , расположенные у ребер следующего графа Коксетера



можно смотреть как на меру удаления от тройки инволюций, в которой два элемента перестановочны. Если в GAP-программе для групп Матье не требовать перестановочности порождающих группу инволюций, то итогом вычислений по этой программе будут порождающие группы Матье тройки инволюций и соответствующие им числа p, q, r . Собранный таким образом информация занесена в следующие множества:

$$C_3(M_{11}) = \{ (3, 4, 5), (3, 4, 6), (3, 5, 6), (3, 6, 6), (4, 4, 5), (4, 4, 6), (4, 5, 5), (4, 5, 6), (4, 6, 6), (5, 5, 6), (5, 6, 6), (6, 6, 6) \},$$

$$C_3(M_{22}) = \{ (3, 4, 5), (3, 4, 6), (3, 5, 5), (3, 5, 6), (3, 6, 6), (4, 4, 4), (4, 4, 5), (4, 4, 6), (4, 5, 5), (4, 5, 6), (4, 6, 6), (5, 5, 5), (5, 5, 6), (5, 6, 6) \},$$

$$C_3(M_{23}) = \{ (3, 5, 6), (3, 6, 6), (4, 4, 5), (4, 4, 6), (4, 5, 5), (4, 5, 6), (4, 6, 6), (5, 5, 6), (5, 6, 6), (6, 6, 6) \},$$

$$C_3(McL) = \{ (3, 5, 5), (3, 5, 6), (3, 6, 6), (4, 4, 5), (4, 4, 6), (4, 5, 5), (4, 5, 6), (4, 6, 6), (5, 5, 5), (5, 5, 6), (5, 6, 6) \}.$$

3.18 Знакопеременные группы $A_9, A_{10}, A_{11}, A_{12}$

GAP-программы для групп Маттье были использованы для вычисления множества

$C_2(A_i), i = 9, 10, 11, 12$. Оказалось, что

$$C_2(A_9) = \{ (4, 9), (4, 10), (4, 12), (5, 9), (6, 7), (6, 9), (6, 10), (6, 12), (7, 9), (7, 10), (9, 9), (9, 10), (9, 12), (10, 10), (10, 12), (12, 12) \},$$

$$C_2(A_{10}) = \{ (3, 21), (4, 21), (5, 6), (5, 7), (5, 8), (5, 9), (5, 10), (5, 12), (5, 15), (5, 21), (6, 8), (6, 9), (6, 21), (7, 9), (7, 21), (8, 15), (8, 21), (9, 9), (9, 10), (9, 12), (9, 15), (9, 21), (10, 21), (12, 12), (12, 15), (12, 21), (15, 21), (21, 21) \},$$

$$C_2(A_{11}) = \{ (5, 5), (5, 12), (5, 14), (5, 15), (5, 20), (5, 21), (6, 8), (6, 12), (6, 14), (6, 15), (6, 20), (6, 21), (8, 12), (8, 15), (8, 20), (12, 12), (12, 14), (12, 15), (12, 20), (12, 21), (14, 15), (14, 20), (14, 21), (15, 15), (15, 20), (15, 21), (20, 20), (20, 21), (21, 21) \},$$

$$C_2(A_{12}) \supset \{ (5, 12), (5, 15), (6, 6), (6, 12), (6, 14), (6, 15), (6, 21), (6, 30), (8, 12), (12, 12), (12, 15), (12, 20), (12, 21), (14, 15), (14, 30), (15, 15), (15, 20), (15, 21), (20, 20), (20, 21), (21, 30) \}.$$

4 Заключение

Автор рассчитывает, что доказательство теоремы пригодится и для поиска порождающих троек инволюций в тех спорадических группах, для которых порождающие тройки инволюций (в том числе с дополнительными условиями) еще не найдены. Укажем на препятствия, не позволившие закрыть проблему

В.Д. Мазурова 7.30 для 6 спорадических групп:

$$Fi_{24}, Co_1, Th, BM, M \text{ и } HN. \quad (3)$$

Прежде всего, степени подстановок, порождающих группы Фишера Fi'_{24} и Харады-Нортонна HN , оказалась слишком высокими), чтобы оперативная память (128 Мбайт) имеющейся в распоряжении автора вычислительной техники быстро справилась с предложенным ей объемом информации.

Для групп Co_1 , Th и BM списка (3) в атласе [11] расположены порождающие их матрицы. Хотя система GAP и находит подстановочные представления линейных групп, степени этих представлений остаются слишком высокими для результативной работы в GAP344. Видимо, здесь придется из максимальных подгрупп добывать информацию путем углубления рассуждений, доказывающих предложение 2, и применения компьютерных вычислений к подгруппам только небольшого порядка.

Что касается вопросов “чистого” программирования, то, очевидно, следующий шаг за UNIX и UNIX-подобными операционными системами. Дело не только в том, что система GAP развивается под такие системы, а, в первую очередь, потому, что станет возможным загрузить на многие недели и месяцы вычислительные мощности учебных заведений и предприятий, компьютеры которых простаивают в ночные часы и выходные дни, либо организовать вычисления в Интернет подобно тому как энтузиасты ищут числа Ферма на 2500 машинах.

Работа выполнена при финансовой поддержке РФФИ (грант 99-01-00432).

Автор благодарит рецензента за ценные замечания и предложения.

ЛИТЕРАТУРА

1. Di Martino L., Tamburini M.C. *2-generation of finite simple groups and some related topics*. – Netherlands: Kluwer Academic Publishers, 1991. – P.195–233.
2. Коуровская тетрадь. – Новосибирск: Институт математики СО РАН, 1999. – 134 с.
3. Нужин Я.Н. *Порождающие тройки инволюций групп Шевалле над конечным полем характеристики 2*// Алгебра и логика – 1990. – Т.29.– 2.– С.192–206.

4. Нужин Я.Н. *Порождающие тройки инволюций знакопеременных групп*// Математические заметки – 1990. – Т.51.– 4. –С.91–95.
5. Нужин Я.Н. *Порождающие тройки инволюций групп лиева типа над конечным полем нечетной характеристики. I*// Алгебра и логика – 1997. – Т.36.– 1.–С.77–96.
6. Нужин Я.Н. *Порождающие тройки инволюций групп лиева типа над конечным полем нечетной характеристики. II*// Алгебра и логика – 1997. – Т.36.– 4.–С.422–440.
7. Нужин Я.Н., Тимофеев А.В. *Порождающие тройки инволюций некоторых спорадических групп*. – Красноярск, ИВМ СО РАН, 1999. –20 с. (Препринт N 13–99).
8. Dokovic D.Z. *Presentations of some finite simple groups*// J.Austral. Math. Soc. (Series A) – 1986. – Vol. 45.–P.143–168.
9. <http://www-gap.dcs.st-and.ac.uk/gap>.
10. Schonert M. together with ..., *GAP Groups, Algorithms and Programming, v3r4p4*. – manual, 1997.
11. Wilson R. <http://www.mat.bham.ac.uk/atlas/>.
12. Тимофеев А.В. <http://icm.krasn.ru/seminar1.html>, 22 августа 2000 г.

Статья поступила

г.Красноярск

Институт вычислительного моделирования СО РАН

timofeen@edk.krasnoyarsk.su,timofeen@icm.krasn.ru

О порождающих тройках инволюций в спорадических группах. Тимофеев-ко А.В. Ред. “Сиб. мат. журн.” РАН. Сиб. отд-ние. Новосибирск, 2001, 18 с., библиогр. 12 назв. (Рукопись деп. в ВИНТИ 19.03.01 N 693–В2001).

С помощью системы компьютерной алгебры GAP доказано, что тремя инволюциями, две из которых перестановочны, порождаются четыре группы Ян-ко, группы Конвея Co_2 и Co_3 , Фишера F_{22} и F_{23} , Матъе M_{12} и M_{24} ; группа Хигмана-Симса HS , группа Хельда He , группа Рудвалиса Ru , группа Сузу-ки Suz , группа О’Нэна ON и группа Лайонса Ly . Группа Маклафлина McL и группы Матъе M_{11} , M_{22} и M_{23} не обладают этим свойством. Таким образом, для 20 (из 26) спорадических групп найден ответ на вопрос В.Д. Мазурова 7.30 из “Коуровской тетради”.

Если G – одна из перечисленных выше групп, либо знакопеременная группа A_9 , A_{10} , A_{11} или A_{12} , то построено либо множество

$$C_3(G) = \{(|ij|, |jk|, |ik|) \mid |i| = |j| = |k| = 2, \text{гр}(i, j, k) = G\},$$

$$\text{либо } C_2(G) = \{(|ik|, |kj|) \mid G = \text{гр}(i, j, k), |i| = |j| = |k| = |ij| = 2\},$$

либо непустое подмножество последнего, причем для двух групп без компью-тера установлено, что $C_2(Ly) \supset \{(r, 37), (s, 67)\}$ и $(q, 43) \in C_2(J_4)$, где q, r, s – некоторые делители периода соответствующей группы.

Автор

(Тимофеев А.В.)

А.В. Тимофеев

О ПОРОЖДАЮЩИХ ТРОЙКАХ ИНВОЛЮЦИЙ
В СПОРАДИЧЕСКИХ ГРУППАХ

С помощью системы компьютерной алгебры GAP доказано, что тремя инволюциями, две из которых перестановочны, порождаются четыре группы Янко, группы Конвея Co_2 и Co_3 , Фишера F_{22} и F_{23} , Матъе M_{12} и M_{24} ; группа Хигмана-Симса HS , группа Хельда He , группа Рудвалиса Ru , группа Сузуки Suz , группа О'Нэна ON и группа Лайонса Ly . Группа Маклафлина McL и группы Матъе M_{11} , M_{22} и M_{23} не обладают этим свойством. Таким образом, для 20 (из 26) спорадических групп найден ответ на вопрос В.Д. Мазурова 7.30 из "Коуровской тетради".

Если G – одна из перечисленных выше групп, либо знакопеременная группа A_9 , A_{10} , A_{11} или A_{12} , то построено либо множество

$$C_3(G) = \{(|ij|, |jk|, |ik|) \mid |i| = |j| = |k| = 2, \text{гр}(i, j, k) = G\},$$

$$\text{либо } C_2(G) = \{(|ik|, |kj|) \mid G = \text{гр}(i, j, k), |i| = |j| = |k| = |ij| = 2\},$$

либо непустое подмножество последнего, причем для двух групп без компьютера установлено, что $C_2(Ly) \supset \{(r, 37), (s, 67)\}$ и $(q, 43) \in C_2(J_4)$, где q, r, s – некоторые делители периода соответствующей группы.

Работа выполнена при финансовой поддержке РФФИ (грант 99-01-00432).

Библиогр. 12.