Math-Net.Ru

Общероссийский математический портал

А. И. Макосий, А. В. Тимофеев, О мазуровских тройках спорадической группы B и гамильтоновых циклах графа Кэли, *Дискрет. матем.*, 2008, том 20, выпуск 1, 87–93

DOI: <https://doi.org/10.4213/dm992>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением

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

Параметры загрузки:

IP: 54.196.121.252

26 апреля 2023 г., 13:29:41

О мазуровских тройках спорадической группы B и гамильтоновых циклах графа Кэли

© 2008 г. А. И. Макосий, А. В. Тимофеев

Систему образующих группы, состоящую из трех инволюций, две из которых перестановочны, будем называть мазуровской тройкой. Излагаются алгоритмы нахождения в явном виде мазуровских троек одного из спорадических монстров, конечной простой группы B , и построения гамильтонова цикла в графе Кэли конечной группы с мазуровской тройкой. Приведены примеры гамильтоновых циклов в графах Кэли некоторых групп.

Работа выполнена при поддержке Российского фонда фундаментальных исследований, проект 05-01-00576.

1. Введение

Напомним, что диэдральной называется группа, порожденная двумя инволюциями, то есть элементами второго порядка. Очевидно, что группа диэдра является полупрямым произведением циклической подгруппы, порожденной произведением этих инволюций, и подгруппы, порожденной одной из них. Если порядок указанной циклической подгруппы равен натуральному числу n , то группу диэдра можно интерпретировать как группу поворотов, совмещающих с собой в трехмерном пространстве правильный n -угольник.

Список групп, порожденных тремя инволюциями, пока малообозрим. Например, тремя инволюциями порождена каждая (известная) конечная простая группа за исключением группы $PSU_3(9)$ [1, 2]. С другой стороны, описаны группы, порожденные тремя инволюциями, порядки произведений каждых двух из которых невелики. Например, если эти порядки равны 2, 3, 5, то соответствующая группа является либо знакопеременной группой A_5 , либо прямым произведением группы A_5 и группы порядка два. Систему образующих группы, состоящую из трех инволюций, две из которых перестановочны, будем называть мазуровской тройкой этой группы [4].

Более четверти века назад объявлено [3] о классификации конечных простых групп, которые разделены сегодня на бесконечные серии циклических групп (простого порядка), знакопеременных групп, групп лиева типа и серию из 26 спорадических (исключительных) групп. Несколько лет назад было выяснено, какие конечные простые группы обладают мазуровской тройкой, а в каких любые три инволюции, две из которых перестановочны, порождают собственную подгруппу. Не углубляясь в историю этого вопроса, изложенную в работе В. Д. Мазурова [4], отметим только, что Я. Н. Нудин доказал отсутствие мазуровских троек в некоторых линейных группах размерностей, не превосходящих 4, и в знакопеременных группах A_6 , A_7 , A_8 , а в других простых знакопеременных группах и группах лиева типа указал явно мазуровские тройки.

В работе [4] по одной схеме с применением теории характеров доказано, что среди спорадических групп, только группы Матье M_{11} , M_{22} , M_{23} и группа Маклафлина McL не обладают мазуровскими тройками. В явном виде такие тройки в других спорадических группах, кроме Монстров B и M , найдены при помощи компьютерных вычислений в работах [5, 6]. В настоящей работе (теорема 1) найдены мазуровские тройки группы Бэби B . Алгоритм поиска инволюций, использованный при доказательстве теоремы 1, реализован в системе компьютерной алгебры GAP (см. <http://www.gap-system.org>).

Найденные в явном виде мазуровские тройки группы находят приложения. Одним из них является построение гамильтоновых циклов в графе, то есть таких замкнутых путей, путешествуя по которым попадаешь в каждую вершину только один раз. Этому посвящена вторая часть работы.

По одной мазуровской тройке в каждой (за исключением группы Монстр) спорадической группе, в которой такие тройки существуют, размещено на сайте ИВМ СО РАН (<http://icm.krasn.ru>). Там же находятся программы поиска указанных троек и программа построения гамильтоновых циклов в графе Кэли группы, обладающей мазуровской тройкой. В работе использована теоретико-групповая терминология из [7].

Авторы благодарят Р. Вилсона (R. Wilson) за консультации по использованию Атласа представлений конечных групп (см. <http://brauer.maths.qmul.ac.uk/Atlas/>).

2. Мазуровские тройки группы Бэби

Напомним (см. [3]), что строение централизатора инволюции стало основой открытия в середине семидесятых годов прошлого века спорадических групп Бэби B и Монстр M (тогда их обозначали F_2 и F_1 соответственно), заметно превышающих другие спорадические группы по числу элементов. Эти две группы близки друг другу не только по порядку. Централизатор одной из инволюций группы M является расширением группы B с помощью группы второго порядка. Доказательство существования группы M и построение ее линейных представлений совпало по времени с объявлением о завершении классификации конечных простых групп в начале восьмидесятых годов. Порядки групп B , M и известные степени их линейных представлений не позволяют стандартными (помещенными в системы компьютерной алгебры) алгоритмами проверить, порождают ли данные элементы группы ее собственную подгруппу, либо саму группу.

Алгоритм, приводящий к мазуровской тройке в группе B , как и в спорадических группах Янко J_4 , Лайенса Ly и Томпсона Th , [6], опирается на описание ее максимальных подгрупп. А именно, если G — одна из этих групп, то в некоторой из ее максимальных подгрупп так выбираются инволюции i, j , что в максимальных подгруппах группы G , содержащих элементы порядка $|ij|$, нет элементов некоторого порядка n . Ищем теперь такую инволюцию k , что группа $\langle i, j, k \rangle$, порожденная элементами i, j, k , обладает элементом порядка n . Следовательно, $\langle i, j, k \rangle = G$, и если $ki = ik$ или $jk = kj$, то (i, j, k) — мазуровская тройка группы G .

При исследовании группы B изложенная выше схема алгоритма построения мазуровских троек нуждается в принципиальном дополнении, вызванном тем, что на умножение даже двух элементов этой группы уходит много времени. Поэтому произведения матриц группы B в большинстве случаев заменены произведениями абстрактных символов и основным инструментом поиска требуемых инволюций группы B стало построение групповых слов. Такого рода техника вычислений лишь эпизодически применялась для групп J_4 , Ly , Th . Таким образом, элементы группы B представлялись и как матрицы

Теорема 1. Пусть a, b — указанные в Атласе порождающие элементы группы B , $i = a,$

$$j = ((ababbabababbababababbababb)^6)^{babbabbababb}$$

$$j = ((bababababbababbababababbababbabbabb)^{12})ababbabababb.$$

тогда тройка инволюций (i, j, k) — мазуровская для всех $k \in \{x, y(xy^2)^2(xy)^2(xy^2)^3xy(xy^2)^3(xy)^3xy^2(xy)^2xy^2(xy)^2xy^2(xy)^4xy^2(xy)^2xy^2xy(xy^2)^2x, (xy)^2(xy^2)^2(xy)^2xy^2xyxy^2(xy)^2xy^2(xy)^2(xy^2)^5xy(xy^2)^3xyxy^2xyxy^2(xy)^4(xy^2)^2xyxy^2(xy)^4xy^2xy, xy^2(xy)^4xy^2xy(xy^2)^2xy(xy^2)^5xy(xy^2)^2xyxy^2xy(xy^2)^2(xy)^2(xy^2)^2xy(xy^2)^3xyxy^2(xy)^3(xy^2)^2(xy)^2(xy^2)^2(xy)^2(xy^2)^3xy(xy^2)^4xy, y(xy^2)^2(xy)^2(xy^2)^3xy(xy^2)^3(xy^2)xy^2(xy)^4xy^2xy(xy^2)^2xyxy^2(xy)^2(xy^2)^3(xy)^3(xy^2)^2(xy)^2xy^2xy(xy^2)^2xyxy^2(xy)^2xy^2, (xy^2)^3xyxy^2(xy)^2(xy^2)^2yxyxy^2xy(xy^2)^3xyxy^2(xy)^2(xy^2)^2xy, y(xy^2)^2(xy)^2xy^2xyxy^2(xy)^2xy^2(xy)^5xy^2(xy)^2xy^2xy(xy^2)^3xy(xy^2)^3xyxy^2(xy)^2(xy^2)^3(xy)^3(xy^2)^3xyxy^2xy(xy^2)^4, (xy^2)^2xy^2xyxy^2(xy)^2xy^2(xy)^5xy^2(xy)^2xy^2xy(xy^2)^3xy(xy^2)^2xyxy^2(xy^2)xy^2(xy)^2xy^2xyxy^2xy(xy^2)^4xy(xy^2)^5, y^2(xy^2)^2(xy)^2(xy^2)^3xy(xy^2)^3(xy)^4(xy^2xy)^3(xy^2)^2xyxy^2(xy)^2(xy^2)^2(xyxy^2)^4xy(xy^2)^2(xy)^2(xy^2)^2(xy)^2(xy^2)^3xyxy^2, y^2(xy^2)^3(xy)^3xy^2(xy)^3(xy^2)^2xy(xy^2)^3xy(xy^2)^2xy(xy^2)^4(xy)^2(xy^2)^2xy(xy^2)^2(xy)^2\}$, где

$$x = (ab)^{-13}(abababb)^{10}(ab)^{13}, \quad y = b^{(abb)^{17}}xb^{(abb)^{17}}x(bb)^{(abb)^{17}}.$$

В Атласе для группы B приведены порождающие ее матрицы a, b размерности 4370 над полем $GF(2)$. Они имеют порядки 2 и 3 соответственно. Группа B содержит четыре класса сопряженных инволюций, обозначенных в Атласе $2A, 2B, 2C, 2D$. Порождающий элемент a лежит в классе $2C$. В качестве инволюции i возьмем матрицу a .

В классе $2D$ сопряженных инволюций существует такая инволюция j , что $|ij| = 38$. Элемент j может быть найден так. Представителем класса $2D$ является произведение $(ababbabababbababababbababbabb)^6$. Далее строим слова в алфавите $\{a, b\}$, сопрягая которыми указанный представитель, получаем элементы класса $2D$ до тех пор, пока порядок произведения полученного элемента и инволюции i не будет равен 38. Строим в алфавите $\{a, b\}$ слова с учетом правил сокращения $aa = bbb = 1$ и находим требуемое слово $babbabbababb$ длины 12. Таким образом, $j = ((ababbabababbababababbababbabb)^6)^{babbabbababb}$. Аналогичные действия приводят к другому элементу, который можно взять в качестве j , если представителем класса

2D взять инволюцию $(bababababbababbababababbababbabb)^{12}$. Тогда элемент j принимает вид $((bababababbababbababababbababbabb)^{12})^{ababbabababb}$. Следовательно, указанная в теореме инволюция j построена.

Третью инволюцию мазуровской тройки, обозначенную в теореме k , ищем в централизаторе $C_B(i)$. Построение централизатора группы B в каком-либо виде стандартными средствами системы GAP при современном состоянии средств вычислительной техники и самой системы невозможно. Поэтому будем строить подмножество централизатора инволюции i по некоторой подгруппе группы B . Эту подгруппу выбираем так, чтобы ее инволюции могли быть выражены через порождающие группы B . Для этого в максимальной подгруппе группы B , изоморфной группе Th , возьмем максимальную подгруппу $U_3(8) : 6$, являющуюся расширением группы $PSU_3(64)$ с помощью группы порядка 6. Построим, с точностью до сопряженности, все ее инволюции. Оказалось, что все произведения id , где d — инволюция из построенного множества, имеют четный порядок, а значит, элементы вида $(id)^{|id|/2}$ суть инволюции, принадлежащие централизатору $C_B(i)$.

Если для полученной инволюции $k \in C_B(i)$ найдется такой элемент группы $\langle i, j, k \rangle$, что в каноническом разложении порядка этого элемента либо показатели m_1, m_2, m_3 при основаниях 2, 3, 5 соответственно удовлетворяют одному из условий $m_1 > 36, m_2 > 9, m_3 > 2$, либо есть числа 23, 31, 47, то группа $\langle i, j, k \rangle$ совпадает с B , и k — указанная в теореме инволюция. Проверка такого условия для первых одиннадцати найденных в $C_B(i)$ инволюций показала, что такой элемент найдется. Поиск элемента осуществлялся построением слов в алфавите $\{i, j, k\}$ с учетом правил сокращения $ii = jj = kk = jk = (ij)^{38} = 1$ и проверкой указанного выше условия.

Очевидно, что если (i, j, k) — мазуровская тройка, то тройки $(ik, j, k), (ik, j, i)$ также являются мазуровскими. Это позволяет расширить построенное множество мазуровских троек и завершить доказательство теоремы.

Следствие 1. Пусть a, b — указанные в Атласе порождающие элементы группы B . Тогда B порождена инволюциями $a, ((ababbababbabababababbababb)^6)^{bababbababb}, (ab)^{-13}(abababb)^{10}(ab)^{13}$, первая и третья из которых перестановочны.

Следствие 2. Пусть G — группа и $C_2(G)$ — множество упорядоченных пар порядков произведений непериодических инволюций мазуровских троек группы G . Тогда $C_2(B) \supseteq \{(6, 38), (6, 56), (8, 34), (8, 38), (8, 40), (8, 56), (10, 38), (10, 42), (10, 56), (10, 66), (12, 16), (12, 22), (12, 24), (12, 28), (12, 38), (12, 42), (12, 60), (12, 70), (16, 38), (18, 34), (18, 36), (18, 38), (20, 30), (20, 34), (20, 38), (21, 36), (21, 38), (22, 30), (22, 38), (24, 38), (28, 38), (30, 34), (30, 38), (34, 34), (34, 38), (36, 38), (38, 40), (38, 42), (38, 56), (38, 60), (38, 66), (38, 70)\}$.

3. Гамильтоновы циклы графа Кэли

Мазуровские тройки интересны тем, что при наличии в группе такой тройки граф Кэли группы относительно этой тройки содержит гамильтонов цикл. Напомним, что графом Кэли группы G относительно ее системы образующих M называется орграф $\Gamma(G, M)$, вершинами которого являются все элементы группы G , и вершины u, v соединены ребром от u к v , помеченным элементом $m \in M$, в том и только том случае, когда, $v = um$. Гамильтонов цикл графа — это замкнутый путь, проходящий по одному разу через все вершины графа. В нашем случае, когда M состоит из инволюций равенство $v = um$ влечет равенство $u = vm$, и потому граф $\Gamma(G, M)$ можно считать неориентированным.

3.1. Нахождение гамильтонова цикла

Опишем процесс нахождения гамильтонова цикла в графе Γ конечной группы $G = \langle i, j, k \rangle$, порожденной мазуровской тройкой инволюций i, j, k . При этом мы, как правило, без ссылок будем пользоваться соотношениями

$$i^2 = j^2 = k^2 = e, \quad ij = ji, \quad (ij)^2 = (jk)^l = e,$$

где l — порядок элемента jk в группе G , а также их следствиями

$$(jk)^s = (kj)^{l-s}, \quad k(jk)^s = j(kj)^{l-s-1},$$

где e — единица группы G . Обозначим еще через D_1 группу $\langle j, k \rangle$, и пусть d — индекс подгруппы D_1 в группе G .

Шаг 1. Выделим в Γ цикл C_1 , состоящий из всех вершин подгруппы $D_1 = \langle j, k \rangle$. Очевидно, что D_1 есть группа диэдра порядка $2l$ и каждый ее элемент однозначно представляется в виде $(kj)^s$ или $j(kj)^s$ при $0 \leq s \leq l-1$. Следовательно, граф Γ содержит цикл $e - j - kj - j(kj) - (kj)^2 - j(kj)^2 - \dots - (kj)^{l-1} - j(kj)^{l-1} - e$, проходящий по одному разу все вершины из D_1 .

Если $G = D_1$, то процесс закончен и C_1 — искомый гамильтонов цикл. В противном случае выполняем следующий шаг.

Шаг 2. Выделим в графе Γ цикл C_2 , состоящий из всех вершин множества $D_2 = D_1 \cup D_1 y_1$, где $y_1 = ax_1$, $x_1 = (kj)^s$, $s \in \{0, 1, \dots, l-1\}$. Так как $i \notin D_1$, множество $D_1 y_1$ есть смежный класс, отличный от D_1 , и $D_1 \cap D_1 y_1 = \emptyset$. Для получения цикла C_2 заменим в цикле C_1 звено $x_1 - jx_1$ цепью $x - y_1 - ky_1 - (jk)y_1 - k(jk)y_1 - (jk)^2 y_1 - \dots - (jk)^{l-1} y_1 - k(jk)^{l-1} y_1 - jx_1$. Так как i, j, k — инволюции и $ji = ij$, в G выполняются равенства

$$k(jk)^{l-1} y_1 = j^2 k(jk)^{l-1} y_1 = j(jk)^l y_1 = jy_1, \quad i(jy_1) = j(iy_1) = jx_1.$$

Поэтому полученный в итоге цикл C_2 содержится в графе Γ . А так как множество $\{e, k, jk, k(jk), (jk)^2, \dots, k(jk)^{l-1}\}$ совпадает с D_1 , цикл C_2 проходит по одному разу все вершины из D_2 .

Допустим, что мы на шаге с номером $m \geq 2$ найдем в графе Γ цикл C_m , проходящий по одному разу все вершины множества D_m , состоящего из m смежных классов группы G по подгруппе D_1 , $D_m = D_1 \cup D_1 y_1 \cup \dots \cup D_1 y_{m-1}$. Если $D_m = G$, то процесс закончен, и C_m — гамильтонов цикл графа Γ . Пусть $D_m \neq G$. Тогда выполняем следующий шаг.

Шаг $m+1$. Находим в G элемент x , удовлетворяющий условиям

$$x \in D_m, \quad y = ix \notin D_m. \quad (1)$$

Такой элемент x найдется, поскольку в противном случае D_m было бы инвариантным относительно умножения слева на элементы i, j, k , и потому совпадало бы с G , вопреки условию. Введем обозначение $D_{m+1} = D_m \cup D_1 y$ и найдем в Γ цикл C_{m+1} , проходящий по одному разу через все вершины из D_{m+1} . Так как $x \in D_m$, в цикле C_m есть звено $x - tx$, где $t \in \{i, j, k\}$. В действительности $t \neq i$, так как $tx \in D_m$, $ix \notin D_m$. Поэтому остается две возможности, $t = j$ и $t = k$. Рассмотрим их.

В первом случае цикл C_{m+1} строится из C_m точно так же, как на шаге 2 строился цикл C_2 из C_1 , с заменой лишь x_1 и y_1 соответственно на x и y .

Второй случай сводится к первому следующим образом. В цикле C_m есть звено $x' - x$ и подцепь $x' - x - kx$. Из определения графа Кэли следует, что $x = ux'$ при некотором $u \in \{i, j, k\}$. Здесь $u \neq i$, так как $ix \in D_m$, $ix \notin D_m$, и $u \neq k$, так как C_m — цикл длины, большей 1. Следовательно, $u = j$, и для звена $x' - jx'$ выполняется условие первого случая. Для замены x на x' и y на $y' = ix'$ остается лишь показать, что $ix' \notin D_m$. Допустим, что $ix' \in D_m$. Тогда $ix' \in D_1 y_r$ при некотором $r \in \{0, 1, \dots, m-1\}$, и мы получаем, что $ix = i(jx') = j(ix') \in jD_1 y_r = D_1 y_r$. Следовательно, $ix \in D_m$, что противоречит условию.

Таким образом, в обоих случаях искомым цикл C_{m+1} в графе Γ найден. Ясно, что при $m+1 = d$ мы получим гамильтонов цикл графа Кэли группы G .

3.2. Гамильтоновы циклы в графах Кэли некоторых групп

Описанный выше процесс не является алгоритмом в строгом смысле, поскольку он не удовлетворяет свойству детерминированности. На шаге m при $m > 0$, мы выбираем любой элемент x , удовлетворяющий условию (1). В общем случае таких элементов может быть много, и выбирая различные x , мы будем получать различные гамильтоновы циклы.

В построенных ниже примерах единица e принята за начало всех строящихся циклов и при переходе от цикла C_m к C_{m+1} в качестве элемента x с условием (1) выбран самый первый из таких элементов цикла C_m . Так получен алгоритм построения вполне определенного гамильтонова цикла C . Он запрограммирован в системе компьютерной алгебры GAP.

Пример 1. Гамильтонов цикл графа $\Gamma(A_5, \{i, j, k\})$ знакопеременной группы A_5 с мазуровской тройкой подстановок $i = (1, 4)(2, 3)$, $j = (1, 3)(2, 4)$, $k = (1, 5)(2, 3)$ имеет вид $e - i - ki - iki - (ki)^2 - j(ki)^2 - kj(ki)^2 - ikj(ki)^2 - kikj(ki)^2 - jkikj(ki)^2 - (kjki)^2 ki - i(kjki)^2 ki - (kikj)^2 (ki)^2 - j(kikj)^2 (ki)^2 - (kjki)^3 ki - i(kjki)^3 ki - (kikj)^3 (ki)^2 - j(kikj)^3 (ki)^2 - (kjki)^4 ki - (jk)^2 i(kjki)^3 ki - k(jk)^2 i(kjki)^3 ki - (kj)^2 i(kjki)^3 ki - jkji(kjki)^3 ki - kji(kjki)^3 ki - ji(kjki)^3 ki - (jk)^2 i(kjki)^2 ki - k(jk)^2 i(kjki)^2 ki - (kj)^2 i(kjki)^2 ki - jkji(kjki)^2 ki - kji(kjki)^2 ki - ji(kjki)^2 ki - (jk)^2 ikj(ki)^2 - k(jk)^2 ikj(ki)^2 - (kj)^2 ikj(ki)^2 - jkjikj(ki)^2 - kjikj(ki)^2 - jikj(ki)^2 - (jk)^2 iki - k(jk)^2 iki - (kj)^2 iki - jkiki - kjiki - jiki - jki - kjki - (jk)^2 i - k(jk)^2 i - (kj)^2 i - jkji - kji - ji - j - kj - jkj - (kj)^2 - j(kj)^2 - (jk)^2 - kjk - jk - k - e.$

Пример 2. Для симметрической группы S_4 гамильтоновым циклом ее графа Кэли $\Gamma(S_4, \{i, j, k\})$ является цикл $e - i - ki - iki - (ki)^2 - i(ki)^2 - (ki)^3 - j(ki)^3 - kj(ki)^3 - (jk)^2 i(ki)^2 - k(jk)^2 i(ki)^2 - j(ki)^2 - kj(ki)^2 - (jk)^2 iki - k(jk)^2 iki - jki - kjki - (jk)^2 i - k(jk)^2 i - j - kj - jkj - (kj)^2 - j(kj)^2 - e$, где $i = (1, 3)(2, 4)$, $j = (2, 4)$, $k = (1, 2)$.

Пример 3. Порядок группы Матве M_{12} равен 95040, и ясно, что приводить здесь гамильтонов цикл для этой группы нет смысла. Отметим только, что на его построение ушла 21 мин. машинного времени (на компьютере с процессором Intel Celeron 1,5 ГГц, GAP 4.4.9 с рабочим пространством 400 Мб под Windows XP).

Список литературы

1. Di Martino L., Tamburini M. C., 2-generation of finite simple groups and some related topics. In: *Generators and relations in groups and geometries* (Barlotti A., Ellers E. W., Plaumann P., Strambach K., eds.). Kluwer, Dordrecht, 1991, pp. 195–233.
2. Маковский А. И., Порождающие четверки инволюций группы $PSU_3(9)$. В сб.: *Избранные докл. междунар. конф. по математике и механике*. Изд-во Томского госунив., Томск, 2003, с. 28–30.
3. Горенштейн Д., *Конечные простые группы. Введение в их классификацию*. Мир, Москва, 1985.
4. Мазуров В. Д., О порождении спорадических простых групп тремя инволюциями, две из которых перестановочны. *Сибирский матем. журнал* (2003) **44**, №1, 193–198.
5. Тимофеев А. В., *О порождающих тройках инволюций в спорадических группах*, Деп. ВИНТИ, 19.03.01 №693–В2001.
6. Тимофеев А. В., О порождающих тройках инволюций больших спорадических групп. *Дискретная математика* (2003) **15**, №2, 103–112.
7. Каргаполов М. И., Мерзляков Ю. И., *Основы теории групп*. Наука, Москва, 1996.

Статья поступила 15.06.2007.

Переработанный вариант поступил 24.10.2007.