Сибирский математический журнал
Январь—февраль, 2013. Том 54, № 1

УДК 512.542

О НЕАБЕЛЕВЫХ ПРОСТЫХ ГРУППАХ С ГРАФОМ ПРОСТЫХ ЧИСЕЛ КАК У ЗНАКОПЕРЕМЕННОЙ ГРУППЫ

М. А. Звездина

Аннотация. Найдены все случаи совпадения графов простых чисел неизоморфных конечных неабелевых простых групп G и S, где G — знакопеременная группа подстановок степени $n \geq 5$, а S — конечная неабелева простая группа. Получена точная оценка максимального числа попарно не изоморфных неабелевых простых групп, одна из которых является знакопеременной, таких, что их графы простых чисел совпадают.

Ключевые слова: конечная простая группа, знакопеременная группа подстановок, граф простых чисел.

1. Введение

Пусть G — конечная группа и $\pi(G)$ — множество всех простых делителей ее порядка. *Графом простых чисел* группы G называется граф, множество вершин которого совпадает с $\pi(G)$, а различные вершины r и s смежны тогда и только тогда, когда в G существует элемент порядка rs. Понятие графа простых чисел введено Грюнбергом и Кегелем, поэтому граф также называют *графом Грюнберга — Кегеля*.

Многие исследования в современной теории конечных групп связаны с распознаваемостью группы по некоторому набору параметров, например по спектру группы. Напомним, что *спектром* группы называется множество порядков ее элементов. Группа G называется *распознаваемой по набору параметров*, если любая группа S с тем же набором параметров изоморфна G. Очевидно, что из распознаваемости группы по графу простых чисел следует ее распознаваемость по спектру.

Первые примеры конечных групп, распознаваемых по графу простых чисел, приведены Хаги в [1], где доказана распознаваемость некоторых спорадических групп. Другие примеры распознаваемых групп приведены в [2–10].

Предположим, что граф простых чисел конечной группы G совпадает с графом простых чисел некоторой конечной простой группы. Что можно сказать о группе G в этом случае? Ответа на этот вопрос пока нет даже в предположении, что сама группа G является конечной простой группой.

В [11] А. В. Васильевым был сформулирован

Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (код проекта 12–01–33102) и программы СО РАН проектов партнерских исследований на 2012–2014 гг. (проект № 14).

Вопрос 16.26. Существует ли такое натуральное k, что никакие k попарно не изоморфных конечных неабелевых простых групп не могут иметь один и тот же граф простых чисел? *Гипотеза*: $k = 5$.

В данной работе этот вопрос рассматривается в том случае, когда одна из рассматриваемых попарно не изоморфных групп является знакопеременной. В этом случае гипотеза верна. Более того, верна следующая

Теорема. *Пусть G — знакопеременная группа A_n, $n \geq 5$, а S — конечная простая группа. Графы простых чисел групп G и S совпадают тогда и только тогда, когда выполняется одно из следующих утверждений:*

(а) $(G, S) \in \{(A_5, A_6), (A_7, L_2(49)), (A_7, U_4(3)), (A_9, J_2), (A_9, S_6(2)), (A_9, O_8^+(2))\}$;

(б) $S = A_{n-1}$, *n нечетно и числа n, $n-4$ составные.*

П. (б) теоремы получен по модулю гипотезы Гольдбаха в следующей формулировке: для любого четного числа $n > 6$ найдется пара различных простых чисел, сумма которых равна n. Подтверждение гипотезы о том, что $k = 5$, является следствием основной теоремы.

Следствие. *Если G — знакопеременная группа A_n, $n \geq 5$, то существует не более трех попарно не изоморфных неабелевых простых групп, отличных от G, граф простых чисел которых совпадает с $GK(G)$.*

1. Свойства графа знакопеременной группы

В этом разделе перечислены основные свойства и особенности графа простых чисел знакопеременной группы.

Прежде всего необходимо сформулировать критерий смежности вершин в $GK(A_n)$, который легко проверить непосредственно.

Лемма 1. *Пусть $G = A_n$, $n \geq 5$, — знакопеременная группа.*

(1) *Если $r, s \in \pi(G)$ — нечетные числа, то r и s несмежны тогда и только тогда, когда $r + s > n$.*

(2) *Если $r \in \pi(G)$ — нечетное число, то 2 и r несмежны тогда и только тогда, когда $r + 4 > n$.*

Этот критерий можно сформулировать, используя следующие обозначения. Для любого простого числа r положим $e(r) = r$, если r нечетно, и $e(r) = 4$, если $r = 2$. Отметим, что функция $e(r)$ является биекцией.

Лемма 1$'$. *Пусть $G = A_n$ — знакопеременная группа степени n и числа r, s содержатся в $\pi(G)$. Тогда r и s несмежны в том и только в том случае, если $e(r) + e(s) > n$.*

Очевидным следствием этой леммы является следующее свойство: если p и r — простые числа, $e(r) < e(p)$ и $p \in \pi(A_n)$, то $r \in \pi(A_n)$.

Критерий совпадения графов Грюнберга — Кегеля двух различных простых знакопеременных групп, указанный в утверждении (б) теоремы, получен по модулю гипотезы Гольдбаха.

Гипотеза Гольдбаха. *Для любого четного числа $n > 6$ найдется пара простых чисел p и q таких, что $n = p + q$.*

На июль 2008 г. бинарная гипотеза Гольдбаха была проверена (см., например, [12]) для всех четных чисел, не превосходящих $1.2 \cdot 10^{18}$. В [13, 14] также доказано, что доля непредставимых чисел, если они существуют, стремится к нулю с ростом n. Нам требуется более сильное предположение, что любое четное число $n > 6$ является суммой двух различных простых чисел. Это верно для непосредственно проверенных четных чисел, и нижняя оценка числа различных представлений числа n в виде суммы двух простых растет с ростом n.

Множество вершин графа называется *кокликой*, если вершины, принадлежащие этому множеству, попарно не смежны. Обозначим через $t(G)$ число вершин, входящих в коклику максимального размера в $GK(G)$. Это число называется *неплотностью* графа. По аналогии для произвольной вершины r обозначим через $t(r, G)$ мощность наибольшей коклики, содержащей вершину r.

Чтобы описать структуру максимальных коклик в $GK(G)$, введем два множества $\Theta(G)$ и $\Theta'(G)$, элементами которых являются подмножества $\pi(G)$. Каждая коклика максимального размера в $GK(G)$ представляется в виде $\rho(G) = \theta(G) \cup \theta'(G)$, где $\theta(G) \in \Theta(G)$ и $\theta'(G) \in \Theta'(G)$.

Обозначим через $\theta(G)$ пересечение всех коклик максимального размера в $GK(G)$. Тогда $\Theta(G) = \{\theta(G)\}$. Множество $\theta'(G)$, являющееся подмножеством $\pi(G) \setminus \theta(G)$, будет элементом $\Theta'(G)$ тогда и только тогда, когда $\rho(G) = \theta(G) \cup \theta'(G)$ — коклика максимального размера в $GK(G)$.

Пусть $G = A_n$, $n \geq 5$, — знакопеременная группа. Обозначим через $\tau(n)$ множество простых чисел r таких, что $\frac{n}{2} \leq r \leq n$, а через s_n и s'_n — наименьшие элементы из $\tau(n)$ и $\tau(n) \setminus s_n$ соответственно. Пусть $\tau'(n)$ — множество простых чисел r таких, что $e(r) < \frac{n}{2}$ и $e(r) + e(s_n) > n$, а $\tau''(n)$ — множество простых чисел r таких, что $e(r) < \frac{n}{2}$ и $e(r) + e(s'_n) > n$.

Лемма 2. *Пусть $G = A_n$, $n \geq 5$ — знакопеременная группа.*

1. *Если $\tau'(n) = \tau''(n) = \varnothing$, то $\theta(G) = \tau(n)$ и $\Theta'(G) = \varnothing$.*
2. *Если $\tau'(n) = \varnothing$, $\tau''(n) \neq \varnothing$, то $\theta(G) = \tau(n) \setminus \{s_n\}$ и $\Theta'(G) = \{\{r\} | r \in \tau''(n) \cup \{s_n\}\}$.*
3. *Если $|\tau'(n)| = 1$, то $\theta(G) = \tau(n) \cup \tau'(n)$ и $\Theta'(G) = \varnothing$.*
4. *Если $|\tau'(n)| \geq 2$, то $\theta(G) = \tau(n)$ и $\Theta'(G) = \{\{r\} | r \in \tau'(n)\}$.*

Доказательство следует из критерия смежности вершин.

Лемма 3. *Для графа простых чисел знакопеременной группы A_n выполняется: $t(A_n) > 3$ тогда и только тогда, когда $n = 17$ или $n \geq 19$.*

Доказательство. Легко убедиться, что $t(G) \leq 4$, если $n < 17$ или $n = 18$, и $t(G) = 4$, если $n \in \{17, 27, 28\}$. Если $19 \leq n \leq 26$ или $29 \leq n \leq 37$, то в промежутке $\left[\frac{n}{2}, n\right]$ находится не менее четырех простых чисел, которые согласно лемме 2 входят в коклику максимального размера графа $GK(G)$, а значит, выполняется неравенство $t(G) \geq 4$. Если $n > 37$, то существует по меньшей мере четыре простых числа p_i таких, что $\frac{n+1}{2} < p_i < n$ (этот факт сформулирован в [15, лемма 1], его доказательство опирается на результат, полученный в [16]). Лемма доказана.

Для дальнейших рассуждений достаточно утверждения леммы, однако выполняется и более общее свойство: для любого заданного натурального числа k существует такое натуральное n, что для любой знакопеременной группы A_m, степень m которой больше, чем n, выполнено $t(G) > k$.

Лемма 4. *Для любого натурального n не существует четырех различных простых чисел $v_1, v_2, w_1, w_2 \in \pi(A_n)$ таких, что в графе $GK(A_n)$ есть ребра (v_1, w_1) и (v_2, w_2) и нет ребер (v_1, w_2) и (v_2, w_1).*

Доказательство. Пусть в $GK(A_n)$ вершина v_1 смежна с w_1 и не смежна с w_2. Из критерия смежности следует, что $e(w_2) > e(w_1)$. Если при этом существует вершина v_2, смежная с w_2 и не смежная с w_1, то $e(w_1) > e(w_2)$; мы пришли к противоречию.

2. Знакопеременные и спорадические группы

Предложение 1. *Пусть m и n — натуральные числа, $5 \leq m < n$. Графы простых чисел знакопеременных групп A_n и A_m совпадают тогда и только тогда, когда $m = n - 1$ и выполняется одно из следующих утверждений:*

(1) *n нечетно и оба числа n, $n-4$ составные;*

(2) *$n = 6$.*

Доказательство. Предположим, что $m \leq n-2$. Одно из чисел n и $n-1$ четно. Так как $n \geq m+2 \geq 7$, согласно гипотезе Гольдбаха существуют два различных простых числа r и s таких, что $m \leq n-2 < r+s \leq n$. Следовательно, в графе $GK(A_n)$ есть ребро (r,s), а в графе $GK(A_m)$ такого ребра нет, и эти графы различны.

Пусть теперь $m = n-1$. Прямая проверка показывает, что графы $GK(A_6)$ и $GK(A_5)$ совпадают. Предположим, что $n > 6$. Если число $n > 6$ четно, то в силу гипотезы Гольдбаха оно может быть представлено в виде суммы двух различных простых чисел. Пусть $n = r + s$. Тогда $GK(A_n)$ содержит ребро (r,s) и не совпадает с графом $GK(A_{n-1})$. Пусть n нечетно. Предположим, что графы $GK(A_n)$ и $GK(A_{n-1})$ различны. Множества вершин этих графов различаются тогда и только тогда, когда n является простым числом. Если n — составное число, то множества вершин совпадают и множества ребер графов должны различаться. Тогда существуют простые числа $r, s \in \pi(A_n)$ такие, что $n-1 < e(r)+e(s) \leq n$. Очевидно, что $e(r)+e(s) = n$, но n — нечетное число. Это возможно тогда и только тогда, когда $\{r,s\} = \{2, n-4\}$. Следовательно, $n-4 \in \pi(A_n)$, и $n-4$ является простым числом.

Предложение 2. *Пусть $G = A_n$ — простая знакопеременная группа, $n \geq 5$, S — спорадическая группа. Тогда $GK(G) = GK(S)$ в том и только в том случае, если $(G,S) = (A_9, J_2)$.*

Доказательство. Отметим, что если p и q — различные простые числа, $q < p$ и $p \in \pi(A_n)$, то $q \in \pi(A_n)$. Можно непосредственно проверить наличие этого свойства у графа простых чисел любой спорадической группы S, используя информацию об их спектрах из [17]. Свойство не выполняется, если S — одна из групп Co_1, Co_2, Co_3, F_1, F_2, F_3, Fi_{23}, Fi_{24}, He, HN, J_1, J_3, J_4, Ly, M_{11}, M_{23}, M_{24}, $O'N$, Ru. Проверка оставшихся шести групп показывает, что графы простых чисел групп Fi_{22}, HS, M_{22}, McL, Suz не могут совпадать с графом знакопеременной группы. Граф группы J_2 с множеством вершин $\{2,3,5,7\}$ и множеством ребер $\{(2,3),(2,5),(3,5)\}$ совпадает с графом знакопеременной группы A_9.

3. Предварительные сведения о группах лиева типа

Для ненулевого целого числа q и простого числа r через q_r обозначается r-часть числа q, т. е. наибольшая степень числа r, делящая q. Если q — ненулевое целое число, r — нечетное простое число и $(q,r) = 1$, то *мультипликативным порядком* $e(r,q)$ числа q по модулю r называется минимальное натуральное число m, удовлетворяющее условию $q^m \equiv 1 \pmod r$. Для нечетного q положим $e(2,q) = 1$, если $q \equiv 1 \pmod 4$, и $e(2,q) = 2$, если $q \equiv 3 \pmod 4$.

Простое число r, удовлетворяющее условию $e(r,q)=m$, называется *примитивным простым делителем* числа q^m-1. Для данного q обозначим через $R_m(q)$ множество всех примитивных простых делителей числа q^m-1. Если q фиксировано, обозначим через r_m некоторый примитивный простой делитель числа q^m-1, если таковой существует (в этом случае по определению $r_m \in R_m(q)$, при этом мощность множества $R_m(q)$ может быть, вообще говоря, любой). Через $k_m(q)$ обозначается произведение всех примитивных простых делителей числа q^m-1. Пусть q — целое число, по модулю большее 1. Почти всегда множество $R_m(q)$ непусто, поскольку существование примитивных делителей почти для всех пар (q,m) установлено Жигмонди в [18].

Лемма 5 (следствие теоремы Жигмонди [18]). *Пусть q — целое число, по модулю большее* 1. *Тогда для каждого натурального числа m найдется простое число r такое, что $e(r,q)=m$, за исключением случаев, когда*

$$(q,m) \in \{(2,1),(2,6),(-2,2),(-2,3),(3,1),(-3,2)\}.$$

Лемма 6. *Пусть i, k, q — различные натуральные числа, большие* 1, $(i,k)=1$ *и множества $R_i(q)$ и $R_{ik}(q)$ непусты. Тогда $|R_i(q^k)|>1$.*

Доказательство см. в [19, лемма 6].

Число компонент связности графа $GK(G)$ обозначается через $s(G)$, а сами компоненты связности — через $\pi_i(G)$, где $1 \le i \le s(G)$. Если порядок $|G|$ четен, то считаем, что $2 \in \pi_1(G)$. Напомним, что через $t(G)$ обозначается неплотность графа $GK(G)$. Через $\rho(G)$ обозначаем коклику максимального размера в графе $GK(G)$.

Далее удобно использовать n в качестве индекса в обозначениях групп лиева типа. Степень знакопеременной группы будем обозначать через m.

Чтобы в удобном виде сформулировать критерии смежности вершин в графе простых чисел групп лиева типа, введем следующие обозначения: $L_n^\varepsilon(q)$, $O_{2n}^\varepsilon(q)$, где $\varepsilon \in \{+,-\}$, и $L_n^+(q)=L_n(q)$, $n \ge 2$, — проективная специальная линейная группа, $L_n^-(q)=U_n(q)$, $n \ge 3$, — проективная специальная унитарная группа, $O_{2n}^+(q)$ и $O_{2n}^-(q)$, $n \ge 4$, — простые ортогональные группы четной размерности в обозначениях [17]. В тех же обозначениях $S_{2n}(q)$, $n \ge 2$, — простая симплектическая группа, $O_{2n+1}(q)$, $n \ge 3$, — простая ортогональная группа нечетной размерности.

В [20] в удобном для нас виде переформулированы следующие утверждения, доказанные в [21], являющиеся критериями смежности вершин в графах простых чисел групп $L_n(q)$ и $U_n(q)$.

Лемма 7 [20, лемма 2.1]. *Пусть $G=L_n^\varepsilon(q)$ — простая группа над полем характеристики p. Пусть r,s — нечетные простые числа из $\pi(G)$, отличные от p. Положим $k=e(r,\varepsilon q)$, $l=e(s,\varepsilon q)$ и предположим, что $2 \le k \le l$. Тогда r и s несмежны в $GK(G)$ в том и только в том случае, если $k+l>n$ и k не делит l.*

Лемма 8 [20, лемма 2.2]. *Пусть $G=L_n^\varepsilon(q)$ — простая группа над полем характеристики p. Пусть $r \in \pi(G)$ и $r \ne p$. Тогда r и p несмежны в $GK(G)$ в том и только в том случае, если выполняется одно из следующих утверждений:*

(1) *r нечетно и $e(r,\varepsilon q)>n-2$;*

(2) *$G=L_2(q)$ и $r=2$;*

(3) *$G=L_3^\varepsilon(q)$, $r=3$ и $(\varepsilon q-1)_3=3$.*

Критерии смежности вершин в графах простых чисел простых симплектических и ортогональных групп найдены в [21, 22].

Лемма 9 [22, предложение 2.4]. *Пусть G — одна из конечных простых групп лиева типа $S_{2n}(q)$ или $O_{2n+1}(q)$ над полем характеристики p. Определим функцию*

$$\eta(m) = \begin{cases} m, & \text{если } m \text{ нечетно,} \\ \frac{m}{2}, & \text{если } m \text{ четно.} \end{cases}$$

Пусть r, s — нечетные простые числа и $r, s \in \pi(G) \setminus \{p\}$. Обозначим $k = e(r, q)$, $l = e(s, q)$ и предположим, что $1 \leq \eta(k) \leq \eta(l)$. Тогда r и s несмежны в том и только в том случае, если $\eta(k) + \eta(l) > n$ и $\frac{l}{k}$ не является нечетным натуральным числом.

Лемма 10 [22, предложение 2.5]. *Пусть $G = O^{\varepsilon}_{2n}(q)$ — конечная простая группа лиева типа над полем характеристики p и функция $\eta(m)$ определена в лемме 9. Пусть r, s — нечетные простые числа и $r, s \in \pi(O^{\varepsilon}_{2n}(q)) \setminus \{p\}$. Обозначим $k = e(r, q)$, $l = e(s, q)$ и предположим, что $1 \leq \eta(k) \leq \eta(l)$. Тогда r и s несмежны в том и только в том случае, когда $2 \cdot \eta(k) + 2 \cdot \eta(l) > 2n - (1 - \varepsilon(-1)^{k+l})$, $\frac{l}{k}$ не является нечетным натуральным числом, и если $\varepsilon = +$, то не выполняется цепочка равенств*

$$n = l = 2 \cdot \eta(l) = 2 \cdot \eta(k) = 2 \cdot k$$

Лемма 11 [21, предложение 3.1]. *Пусть G — простая симплектическая или ортогональная группа над полем характеристики p и $r \in \pi(G) \setminus \{p\}$. Тогда r и p несмежны в том и только в том случае, если выполняется одно из следующих условий:*

(1) $G = S_{2n}(q)$, $\eta(e(r, q)) > n - 1$ (*функция $\eta(m)$ определена в лемме* 9);
(2) $G = O_{2n+1}(q)$, $\eta(e(r, q)) > n - 1$;
(3) $G = O^{\varepsilon}_{2n}(q)$, $\eta(e(r, q)) > n - 2$.

Критерии смежности вершин в графах простых чисел исключительных групп лиева типа также приведены в [21, 22]. Одним из следствий перечисленных критериев является следующее важное свойство графа простых чисел произвольной простой группы лиева типа.

Лемма 12. *Пусть G — простая группа лиева типа. Тогда для любого числа $r \in \pi(G)$ существует число $s \in \pi(G)$ такое, что r и s несмежны в графе $GK(G)$.*

Лемма 13. *Если S — простая группа лиева типа, $G = A_m$, $m \geq 5$, — знакопеременная группа и их графы простых чисел совпадают, то граф $GK(S) = GK(G)$ несвязен.*

Доказательство. Согласно лемме 12 для любого числа $r \in \pi(S) = \pi(G)$ существует число $s \in \pi(G)$ такое, что r и s несмежны в графе $GK(G)$. В частности, в $GK(G)$ найдется вершина r, не смежная с вершиной 3. Но тогда для любого числа $s \in \pi(G)$ числа r и s несмежны в графе $GK(G)$, т. е. r — изолированная вершина. Значит, граф $GK(G) = GK(S)$ несвязен.

4. Линейные и унитарные группы

Пусть S — проективная специальная линейная (унитарная) группа, которую далее будем обозначать через $L_n(q)$, $n \geq 2$ (соответственно $U_n(q)$, $n \geq 3$). Отметим, что группы $U_3(2)$, $L_2(2)$ и $L_2(3)$ не являются простыми; кроме того, имеют место изоморфизмы

$$L_2(4) \cong L_2(5) \cong A_5; \quad L_2(9) \cong A_6; \quad L_4(2) \cong A_8; \quad L_2(q) \cong U_2(q).$$

Будем рассматривать случаи совпадения графов простых чисел не изоморфных между собой групп.

Предложение 3. *Пусть $G = A_m$ — простая знакопеременная группа, $m \geq 5$, S — простая линейная или унитарная группа, не изоморфная G. Тогда $GK(G) = GK(S)$ в том и только в том случае, если $G = A_7$ и $S \in \{U_4(3), L_2(49)\}$.*

Доказательство. Пусть $G = A_m$ — знакопеременная группа, и пусть $t(G) \leq 3$. Тогда $m < 19$ (по лемме 3) и $\pi(G)$ является подмножеством множества $\{2, 3, 5, 7, 11, 13, 17\}$. Нужно найти все простые линейные и унитарные группы S такие, что $\pi(S)$ содержится в множестве $\{2, 3, 5, 7, 11, 13, 17\}$ и выполняется условие: если $r \in \pi(S)$, то любое простое число $r_1 < r$ также содержится в $\pi(S)$.

Все неабелевы простые группы, простые делители порядка которых не превосходят 1000, приведены в [23, табл. 1], где также указаны порядки этих групп. Используя эти данные, получаем, что при выполнении указанных выше условий S изоморфна одной из следующих групп: $L_2(49)$, $L_3(4)$, $L_6(3)$, $U_3(5)$, $U_4(2)$, $U_4(3)$, $U_6(2)$. Графы простых чисел групп $U_4(3)$ и $L_2(49)$ совпадают с графом знакопеременной группы $GK(A_7)$, состоящим из вершин $\{2, 3, 5, 7\}$ и ребра $(2, 3)$. Графы остальных перечисленных групп не могут совпадать с графом знакопеременной группы.

Пусть теперь $t(S) \geq 4$. Если S — линейная или унитарная группа и $t(S) \geq 4$, то из [21, табл. 8] вытекают ограничения на размерность группы S. Рассмотрим все возможные случаи.

Пусть $n = 3$ и $(q - \varepsilon 1)_3 = 3$, $q + \varepsilon 1 \neq 2^k$. В этом случае $t(S) = 4$ и любая коклика максимального размера в $GK(S)$ содержит вершину 3, а значит, граф $GK(S)$ не может совпадать с графом знакопеременной группы. Действительно, если A_m — знакопеременная группа, то обозначим через $\rho(A_m)$ некоторую коклику максимального размера в графе $GK(A_m)$ и предположим, что вершина 3 содержится в $\rho(A_m)$. Обозначим через s_1 и s_2 два наибольших простых числа в $\pi(A_m)$. По лемме 2 коклика $\rho(A_m)$ содержит вершины s_1 и s_2. Из леммы 1 следует, что $s_1 > m - 3$ и $s_2 > m - 3$. Значит, среди чисел $m, m-1, m-2$ два являются простыми. Это возможно в единственном случае: $s_1 = m$, $s_2 = m - 2$. Не существует еще одной вершины $s_3 \in \pi(A_m)$ такой, что $s_3 > m - 3$. Следовательно, $\rho(A_m)$ содержит не более трех вершин.

Пусть $n \geq 7$, $S \neq L_7(2)$, $S \neq L_8(2)$. Воспользуемся леммой 4, чтобы показать, что $GK(S)$ не может совпадать с графом знакопеременной группы. Необходимо предъявить четыре вершины $v_1, v_2, w_1, w_2 \in \pi(S)$ такие, что в графе $GK(S)$ есть ребра (v_1, w_1), (v_2, w_2) и нет ребер (v_1, w_2), (v_2, w_1). Опираясь на критерий смежности вершин (леммы 7, 8), выбираем искомую четверку вершин следующим образом.

Если n — четное число, то

$$v_1 = p, \quad v_2 \in R_{\frac{n}{2}}(\varepsilon q), \quad w_2 \in R_n(\varepsilon q), \quad w_1 \in R_{n-2}(\varepsilon q).$$

Если n — нечетное число, то

$$v_1 = p, \quad v_2 \in R_{\frac{n-1}{2}}(\varepsilon q), \quad w_2 \in R_{n-1}(\varepsilon q), \quad w_1 \in R_{n-2}(\varepsilon q).$$

Предложение доказано.

5. Симплектические и ортогональные группы

Отметим, что при любых n и q выполнено равенство

$$GK(S_{2n}(q)) = GK(O_{2n+1}(q)).$$

Кроме того, имеют место изоморфизмы

$$S_{2n}(2^k) \cong O_{2n+1}(2^k), \quad S_4(q) \cong O_5(q).$$

Пусть $G = A_m$, $m \geq 5$, — знакопеременная группа, S — простая симплектическая или ортогональная группа. Предположим, что G и S неизоморфны и их графы простых чисел совпадают. По лемме 13 граф $GK(G) = GK(S)$ несвязен. Отметим, что $s(G) \leq 3$, поскольку граф знакопеременной группы содержит не более двух изолированных вершин, а остальные вершины являются связной частью графа. Все неабелевы простые группы с несвязным графом простых чисел описаны в [24, 25]. В [15, табл. 1] суммированы необходимые нам результаты этих работ. В следующей лемме перечислены те группы, которые рассматриваются в данном разделе, а именно простые симплектические и ортогональные группы S, удовлетворяющие условию $s(S) \in \{2, 3\}$.

Лемма 14. *Все простые симплектические и ортогональные группы S такие, что $s(S) \in \{2, 3\}$, перечислены в таблице. Через t обозначено простое число.*

Таблица

№	S	Условия на S	$s(S)$
1	$O_{2t}^+(q)$	$t \geqslant 5$, $q = 2, 3, 5$	2
2	$O_{2n}^-(2)$	$n = 2^k + 1 \geqslant 5$	2
3	$S_{2t}(q)$	$q = 2, 3$	2
4	$O_{2t+1}(3)$		2
5	$O_{2(t+1)}^+(q)$	$q = 2, 3$	2
6	$O_{2t}^-(3)$	$5 \leq t = 2^k + 1$	3
7	$O_{2n}^-(3)$	$n = 2^k + 1 \neq t$	2
8	$O_{2t}^-(3)$	$7 \leqslant t \neq 2^k + 1$	2
9	$O_{2n}^-(q)$	$n = 2^k \geqslant 4$	2
10	$S_{2n}(q)$	$n = 2^k \geqslant 2$	2
11	$O_{2n+1}(q)$	$n = 2^k \geqslant 4$, q нечетно	2

Таким образом, если S — простая симплектическая или ортогональная группа такая, что $GK(S) = GK(G)$, то S содержится в таблице.

Предложение 4. *Пусть $G = A_m$, $m \geq 5$, — знакопеременная группа, S — простая симплектическая или ортогональная группа, не изоморфная группе G. Тогда $GK(G) = GK(S)$ в том и только в том случае, если $(G, S) \in \{(A_9, S_6(2)), (A_9, O_8^+(2))\}$.*

Доказательство. Далее в тексте доказательства цифра (цифры) в начале абзаца указывает на номер строки таблицы, группы из которой рассматриваются в этом абзаце.

1–8. Сначала рассмотрим группы малых размерностей. Необходимая информация о графах простых чисел этих групп может быть получена из [17] или с помощью [26]. Непосредственная проверка графов простых чисел групп $S_{2t}(2)$ $(t = 3, 5)$, $S_{2t}(3)$ $(t = 2, 3, 5, 7)$, $O_{2l}^+(2)$ $(l = 4, 5, 6, 7)$, $O_{2l}^+(3)$ $(l \in \{4, 5, 6, 7, 8\})$, $O_{10}^-(2)$, $O_{2l}^-(3)$ $(l = 5, 7, 9)$ показывает, что они не могут совпадать с графом знакопеременной группы, за исключением случаев $GK(S_6(2)) = GK(O_8^+(2)) = GK(A_9)$.

Теперь рассмотрим группы из пп. 1–8 по отдельности, опуская случаи малых размерностей, перечисленные выше.

1. Пусть $q = 2$. Поскольку случаи $t = 5, 7$ уже рассмотрены, можно считать, что $t > 7$. Тогда в графе $GK(S)$ вершина $r_{2(t-4)}(2)$ смежна с $r_8(2) = 17$ и не смежна с $r_{12}(2) = 13$. Из критерия смежности вершин в графе знакопеременной группы G (лемма 1) следует, что если для чисел $v, w_1, w_2 \in \pi(G)$ выполнено неравенство $w_1 > w_2$ и вершина v смежна с w_1 в графе $GK(G)$, то она смежна и с w_2. Однако для $GK(S)$ это неверно, поэтому $GK(S)$ не может совпадать с графом знакопеременной группы. Далее в доказательстве аналогичное рассуждение не будет приводиться в развернутом виде.

Пусть $q = 3$. Поскольку $t \geq 11$, из чисел $\{t-8, t-6\}$ можно выбрать нечетное число, не кратное 11. Обозначим это число через s. Тогда в графе $GK(S)$ число $r_s(3)$ смежно с $r_8(3) = 41$ и не смежно с $r_{11}(3) = 23$.

Пусть $q = 5$. Здесь можно не рассматривать отдельно группы малых размерностей, так как рассуждение верно при $t \geq 5$. Множества $R_1(5)$ и $R_2(5)$ непусты. В графе $GK(S)$ есть ребра $(r_1(5), r_t(5))$, $(r_2(5), r_{2t}(5))$ и нет ребер $(r_1(5), r_{2t}(5))$, $(r_2(5), r_t(5))$. Это противоречит лемме 4, поэтому $GK(S)$ не может совпадать с графом знакопеременной группы.

2. Пусть $S = O_{2n}^-(2)$ и $(n = 2^k + 1 > 5)$. Тогда в графе $GK(S)$ вершина $r_{n-4}(2)$ смежна с $r_8(2) = 17$ и не смежна с $r_{12}(2) = 13$; противоречие.

3. Пусть $S = S_{2t}(2)$ и $t > 5$. Тогда в графе $GK(S)$ вершина $r_{t-4}(2)$ смежна с $r_8(2) = 17$ и не смежна с $r_{10}(2) = 11$, что невозможно.

Пусть $S = S_{2t}(3)$ и $t > 7$. Тогда если число $t-4$ не кратно 5, то в графе $GK(S)$ вершина $r_{t-4}(3)$ смежна с $r_3(3) = 13$ и не смежна с $r_5(3) = 11$. Если $t-4$ делится на 5, то вершина $r_{t-3}(3)$ смежна с $r_3(3) = 13$ и не смежна с $r_5(3) = 11$.

4. Пусть $S = O_{2t+1}(3)$ и $t > 7$. Выполнено равенство $GK(O_{2t+1}(3)) = GK(S_{2t}(3))$. Эти симплектические группы рассмотрены в п. 3.

5. Пусть $S = O_{2(t+1)}^+(2)$ и $t > 5$. Тогда в графе $GK(S)$ вершина $r_{t-4}(2)$ смежна с $r_5(2) = 31$ и не смежна с $r_{12}(2) = 13$.

Пусть $S = O_{2(t+1)}^+(3)$ и $t > 7$. Из чисел $\{t-6, t-4\}$ можно выбрать число s, не кратное 11. Тогда в графе $GK(S)$ вершина $r_s(3)$ смежна с $r_8(3) = 41$ и не смежна с $r_{11}(3) = 23$.

6, 7, 8. Эти пункты можно объединить, поскольку рассуждение верно для всех трех случаев. Пусть $S = O_{2k}^-(3)$, где k —нечетное число, не меньшее 11. Среди чисел $\{n-6, n-4\}$ можно выбрать число s, не кратное 11. Тогда в графе $GK(S)$ вершина $r_s(3)$ смежна с $r_8(3) = 41$ и не смежна с $r_{11}(3) = 23$.

9–11. Пусть S — одна из групп $O_{2n+1}(q)$, $S_{2n}(q)$ $(n = 2^k \geq 2)$, $O_{2n}^-(q)$ $(n = 2^k \geq 4)$ над полем порядка $q = p^a$.

Рассмотрим сначала группы небольших размерностей.

Пусть $S = S_4(q)$. Тогда $t(S) = 2$. Среди неабелевых простых знакопеременных групп только для $G = A_9, A_{10}, A_{12}$ выполнено $t(G) = 2$. Используя [23, табл. 1], несложно убедиться, что $GK(S)$ не может совпадать с графом знакопеременной группы.

Пусть $S = S_8(q)$, $S = O_9(q)$ или $O_8^-(q)$. Тогда $t(S) \leq 4$ и в графе $GK(S)$ существует изолированная вершина $r_8(q)$. Это число является простым делителем числа $\frac{q^4+1}{2}$. С другой стороны, если $GK(S)$ совпадает с графом знакопеременной группы G, то $t(G) \leq 4$, следовательно, $\pi(G) \subseteq \{2, 3, \ldots, 37\}$. Тогда

$r_8(q) \leq \frac{q^4+1}{2} \leq 37$, значит, $q = 2$. Графы простых чисел групп $S_8(2)$, $O_9(2)$, $O_8^-(2)$ не могут совпадать с графом знакопеременной группы.

Осталось рассмотреть группы из пп. 9–11 таблицы при $n \geq 8$.

9. Пусть S — группа $O_{2n}^-(q)$ ($n = 2^k \geq 8$) и ее граф простых чисел совпадает с графом знакопеременной группы. Прямая проверка показывает, что граф группы $O_{16}^-(2)$ не может совпадать с графом знакопеременной группы. Поскольку $n-5$ — нечетное число, не кратное пяти, и множество $R_{2(n-5)}(q)$ непусто при $(q,n) \neq (2,8)$, в $GK(S)$ есть ребра $(r_5(q), r_{2(n-5)}(q))$, $(r_{10}(q), r_{n-5}(q))$ и нет ребер $(r_5(q), r_{n-5}(q))$, $(r_{10}(q), r_{2(n-5)}(q))$, что противоречит лемме 4.

10, 11. Если число $q = p^a$ составное, то, обозначив через a_0 некоторый простой делитель числа a, получаем $q = p^a = q_0^{a_0}$, где $q_0 = p^{\frac{a}{a_0}}$ и a_0 — простое число. По лемме 6 имеем $|R_i(q)| = \left|R_i\left(q_0^{a_0}\right)\right| > 1$, если $(i, a_0) = 1$ и множества $R_i(q_0)$, $R_{ia_0}(q_0)$ непусты. При $n \geq 8$ для любого $a \geq 2$ найдутся по крайней мере два различных множества $R_i(q)$, $R_j(q)$ такие, что $R_i(q) \cup R_j(q) \subset \pi(S)$ и множества $R_i(q_0)$, $R_j(q_0)$, $R_{ia_0}(q_0)$, $R_{ja_0}(q_0)$ непусты. Согласно лемме 6 выполнены неравенства $|R_i(q)| > 1$ и $|R_j(q)| > 1$. Более того, при указанных ограничениях эти два множества можно выбрать таким образом, чтобы любые две вершины $v_1 \in R_i(q)$, $v_2 \in R_j(q)$ были не смежны в графе $GK(S)$. Но тогда совпадение графа $GK(S)$ с графом знакопеременной группы невозможно. Выбрав вершины $v_1, w_1 \in R_i(q)$, $v_2, w_2 \in R_j(q)$, получим противоречие с леммой 4. Значит, рассматривая случаи, когда $n \geq 8$, можно считать, что S — группа над полем простого порядка $q = p$.

Исключим случаи $q = 2, 3$.

Если $S = S_{2n}(2)$ или $S = O_{2n+1}(2)$ и $8 < n = 2^k$, то в графе $GK(S)$ вершина $r_{n-5}(2)$ смежна с $r_5(2) = 31$ и не смежна с $r_{12}(2) = 13$. Если $n = 8$, то непосредственная проверка показывает, что граф $GK(S_{16}(2)) = GK(O_{17}(2))$ не совпадает с графом знакопеременной группы.

Если $S = S_{2n}(3)$ или $S = O_{2n+1}(3)$ и $8 \leq n = 2^k$, то в графе $GK(S)$ вершина $r_{n-5}(3)$ смежна с $r_{10}(3) = 61$ и не смежна с $r_{16}(3) = 17$, поэтому $GK(S)$ не совпадает с графом знакопеременной группы.

Пусть $p \geq 5$ — простое число и S — группа $S_{2n}(p)$ или $O_{2n+1}(p)$, $n = 2^k \geq 8$, и ее граф простых чисел совпадает с графом знакопеременной группы.

Пусть k четно, тогда $n \equiv 1 \pmod 3$. В этом случае в $GK(S)$ есть ребра $(r_3(p), r_{n-1}(p))$, $(r_6(p), r_{2(n-1)}(p))$ и нет ребер $(r_3(p), r_{2(n-1)}(p))$, $(r_6(p), r_{n-1}(p))$, что противоречит лемме 4.

Если k нечетно, то $n \equiv -1 \pmod 3$. Обозначим через $r_0(p)$ число $r_3(p)$, если $p \equiv 1 \pmod 3$, и $r_6(p)$, если $p \equiv -1 \pmod 3$. Рассмотрим числа $r_4(p)$ и $r_0(p)$. Число $r_4(p)$ является делителем числа $k_4(p) = \frac{p^2+1}{2}$. Покажем, что при сделанных предположениях $k_4(p)$ — простое число. Если оно составное, то существует его простой делитель $r \in R_4(p)$ такой, что $r \leq \sqrt{\frac{p^2+1}{2}} < p$. Но в $GK(S)$ вершина $s = r_{n-2}(p)$ смежна с p и не смежна с r. Это противоречит тому, что $GK(S)$ совпадает с графом знакопеременной группы. Значит, $r_4(p) = \frac{p^2+1}{2}$. Если $p \equiv 1 \pmod 3$, то $r_0(p) = r_3(p)$ — простой делитель числа $k_3(p) = \frac{p^2+p+1}{3}$; если $p \equiv -1 \pmod 3$, то $r_0(p) = r_6(p)$ — простой делитель числа $k_6(p) = \frac{p^2-p+1}{3}$. В любом случае $r_4(p) = \frac{p^2+1}{2} > \frac{p^2+p+1}{3} \geq r_0(p)$, но в графе $GK(S)$ вершина $r_4(p)$ смежна с $r_{2(n-2)}(p)$, а вершина $r_0(p)$ не смежна; противоречие. Значит, $GK(S)$ не может совпадать с графом знакопеременной группы. Предложение доказано.

6. Исключительные группы лиева типа

Предложение 5. *Пусть $G = A_m$ — простая знакопеременная группа, $m \geq 5$, S — исключительная группа лиева типа. Тогда $GK(G)$ не совпадает с $GK(S)$.*

Доказательство. Если $S \in \{G_2(q), {}^3D_4(q), {}^2F_4(2)'\}$, то $t(S) \leq 3$. Поэтому если $GK(S) = GK(A_m)$, то $\pi(S) \in \{2, 3, 5, 7, 11, 13, 17\}$. Из [23, табл. 1] следует, что в этом случае совпадений нет.

Теперь предположим, что $t(S) \geq 4$. Если $S \in \{E_6^\varepsilon(q),\ E_7(q),\ E_8(q)\}$, то по лемме 4 граф $GK(S)$ не совпадает с графом знакопеременной группы. Компактные формы графов простых чисел этих исключительных групп приведены в [22]. Перечислим наборы вершин $v_1, v_2,\ w_1, w_2$ такие, что в $GK(S)$ есть ребра (v_1, w_1), (v_2, w_2) и нет ребер (v_1, w_2), (v_2, w_1):

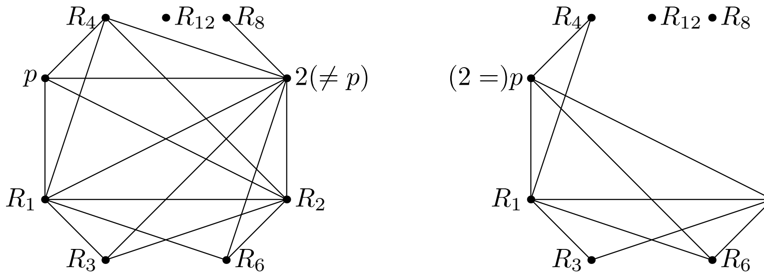
если $S = E_6^\varepsilon(q)$, то $v_1 \in R_4$, $v_2 \in R_{12}$, $w_1 \in R_{\nu_\varepsilon(6)}$, $w_2 \in R_{\nu_\varepsilon(3)}$;

если $S = E_7(q)$, то $v_1 \in R_8$, $v_2 \in R_{10}$, $w_1 \in R_4$, $w_2 \in R_6$;

если $S = E_8(q)$, то $v_1 \in R_9$, $v_2 \in R_{10}$, $w_1 \in R_3$, $w_2 \in R_4$.

Пусть теперь $S = F_4(q)$.

Приведем компактную форму для $GK(S)$ (см. [22]):



Пусть $p \neq 2$. Тогда либо $p = 3$, либо $3 \in R_1(q)$, либо $3 \in R_2(q)$. В любом случае вершина r_8 смежна с 2 и не смежна с 3, что невозможно в графе знакопеременной группы.

Пусть $p = 2$. Тогда $t(S) = 4$ и r_8, r_{12} — изолированные вершины. Если $GK(S) = GK(A_m)$, то $t(A_m) = 4$ и оба числа m, $m-2$ простые. Единственная знакопеременная группа, удовлетворяющая этим условиям, — это группа A_{19}. Ее граф простых чисел не совпадает с $GK(S)$.

Осталось рассмотреть группы Сузуки и Ри. Поскольку порядки простых групп Сузуки $S = {}^2B_2(2^{2n+1})$ не делятся на 3, то $GK(S) \neq GK(S)$ в этом случае. Заметим, наконец, что если $G = A_m$ — знакопеременная группа, то $t(2, G) \leq 3$ и $t(3, G) \leq 3$. Это не так для простых групп Ри: в графе $GK({}^2G_2(3^{2n+1}))$ вершина 3 входит в коклику максимального размера 5; в графе $GK({}^2F_4(2^{2n+1}))$ вершина 2 входит в коклику максимального размера 4. Предложение и теорема доказаны.

ЛИТЕРАТУРА

1. *Hagie M.* The prime graph of a sporadic simple group // Comm. Algebra. 2003. V. 31, N 9. P. 4405–4424.
2. *Заварницин А. В.* О распознавании конечных групп по графу простых чисел // Алгебра и логика. 2006. Т. 45, № 4. С. 390–408.
3. *Хосрави А., Хосрави Б.* Квазираспознавание простой группы ${}^2G_2(q)$ по графу простых чисел // Сиб. мат. журн. 2007. Т. 48, № 3. С. 707–715.

4. *Хосрави А., Хосрави Б.* 2-распознаваемость $PSL(2, p^2)$ по графу простых чисел // Сиб. мат. журн. 2008. Т. 49, № 4. С. 934–944.
5. *Khosravi B.* n-Recognition by prime graph of the simple group $PSL(2, q)$ // J. Algebra Appl. 2008. V. 7, N 6. P. 735–748.
6. *Khosravi B., Amiri S. S.* Groups with the same prime graph as $L_2(q)$ where $q = p^a < 100$ // Hadronic J. 2007. V. 30, N 3. P. 343–354.
7. *Khosravi Bahman, Khosravi Behnam, Khosravi B.* On the prime graph of $PSL(2, p)$ where $p > 3$ is a prime number // Acta Math. Hungar. 2007. V. 116, N 4. P. 295–307.
8. *Khosravi Bahnam, Khosravi Behnam, Khosravi B.* Groups with the same prime graph as a CIT simple group // Houston J. Math. 2007. V. 33, N 4. P. 967–977. (electronic).
9. *Khosravi Bahnam, Khosravi Behnam, Khosravi B.* A characterization of the finite simple group $L_{16}(2)$ by its prime graph // Manuscripta Math. 2008. V. 126. P. 49–58.
10. *Zavarnitsine A. V.* Uniqueness of the prime graph of $L_{16}(2)$ // Сиб. электрон. мат. изв. 2010. V. 7. P. 119–121.
11. *Нерешенные вопросы теории групп.* Коуровская тетрадь. 16-е изд. Новосибирск: Ин-т математики, 2006.
12. *Weisstein E. W.* Goldbach conjecture. From Mathworld-AWolfram Web Resourse (http://mathworld.wolfram.com/GoldbachConjecture.html).
13. *Vinogradov I. M.* Some theorems concerning the theory of primes // Recueil Math. 1937. V. 2. P. 179–195.
14. *Estermann T.* On Goldbach's problem: proof that almost all even positive integers are sums of two primes // Proc. London Math. Soc. Ser. 2. 1938. V. 44. P. 307–314.
15. *Кондратьев А. С., Мазуров В. Д.* Распознавание знакопеременных групп простой степени по порядкам их элементов // Сиб. мат. журн. 2000. Т. 41, № 2. С. 359–369.
16. *Rohrbach H., Weis J.* Zum finiten Fall des Bertrandschen Postulates // J. Reine Angew. Math. 1964. V. 214, N 5. P. 432–440.
17. *Conway J. H., Curtis R. T., Norton S. P., Parker R. A., Wilson R. A.* Atlas of finite groups. Oxford: Clarendon Press, 1985.
18. *Zsigmondy K.* Zur Theorie der Potenzreste // Monatsh. Math. Phys. 1892. Bd 3. S. 265–284.
19. *Гречкосеева М. А., Лыткин Д. В.* Почти распознаваемость по спектру конечных простых линейных групп простой размерности // Сиб. мат. журн. 2012. Т. 53, № 4. С. 805–818.
20. *Васильев А. В., Гречкосеева М. А., Старолетов А. М.* О конечных группах, изоспектральных простым линейным и унитарным группам // Сиб. мат. журн. 2011. Т. 52, № 1. С. 39–53.
21. *Васильев А. В., Вдовин Е. П.* Критерий смежности в графе простых чисел конечной простой группы // Алгебра и логика. 2005. Т. 44, № 6. С. 682–725.
22. *Васильев А. В., Вдовин Е. П.* Коклики максимального размера в графе простых чисел конечной простой группы // Алгебра и логика. 2011. Т. 50, № 4. С. 425–470.
23. *Zavarnitsine A. V.* Finite simple groups with narrow prime spectrum // SEMR. 2009. V. 6. P. 1–12.
24. *Williams J. S.* Prime graph components of finite groups // J. Algebra. 1981. V. 69, N 2. P. 487–513.
25. *Кондратьев А. С.* О компонентах графа простых чисел для конечных простых групп // Мат. сб. 1989. Т. 180, № 6. С. 787–797.
26. *The GAP Group.* GAP — Groups, Algorithms, and Programming. Version 4.4, 2004. (http://www.gap-system.org).

Статья поступила 31 октября 2012 г.

Звездина Мария Анатольевна
Новосибирский гос. университет,
ул. Пирогова, 2, Новосибирск 630090
suslo118@gmail.com