Сибирский математический журнал
Март—апрель, 2009. Том 50, № 2

УДК 512.542

О РАСПОЗНАВАНИИ КОНЕЧНЫХ ПРОСТЫХ ГРУПП СО СВЯЗНЫМ ГРАФОМ ПРОСТЫХ ЧИСЕЛ

А. В. Васильев, И. Б. Горшков

Аннотация. *Спектром конечной группы* называется множество порядков ее элементов. Доказана структурная теорема о строении конечной группы, спектр которой совпадает со спектром конечной неабелевой простой группы. Эта теорема может быть использована для решения проблемы распознаваемости конечных простых групп по спектру.

Ключевые слова: конечная группа, конечная простая группа, спектр группы, граф простых чисел группы.

Введение

Пусть G — конечная группа, $\pi(G)$ — множество простых делителей ее порядка и $\omega(G)$ — спектр группы G, т. е. множество порядков ее элементов. *Граф простых чисел* $GK(G)$ группы G определяется следующим образом. Множество вершин графа $GK(G)$ есть $\pi(G)$, и два простых числа $r, s \in \pi(G)$, рассматриваемые как вершины графа, смежны (соединены ребром) тогда и только тогда, когда $rs \in \omega(G)$. Грюнберг и Кегель ввели понятие графа простых чисел (он также называется *графом Грюнберга — Кегеля*) в середине 70-х гг. прошлого века и дали характеризацию конечных групп с несвязным графом простых чисел (мы будем обозначать число несвязных компонент графа $GK(G)$ через $s(G)$). Этот глубокий результат, а также классификация конечных простых групп с условием $s(G) > 1$, полученная Вильямсом и А. С. Кондратьевым (см. [1, 2]), повлекли целый ряд важных следствий.

Доказательство теоремы Грюнберга — Кегеля существенно опиралось на тот факт, что $\pi(G)$ содержит нечетное простое число, не связанное в $GK(G)$ путем с числом 2. Оказалось, что условие несвязности может быть успешно заменено более слабым условием несмежности числа 2 с хотя бы одним нечетным простым числом.

Обозначим через $t(G)$ наибольшее число простых чисел в $\pi(G)$, попарно не смежных в $GK(G)$. Другими словами, $t(G)$ — это наибольшее число вершин в кокликах, т. е. независимых множествах вершин, графа $GK(G)$. В теории графов это число принято называть *числом вершинной независимости* или *неплотностью графа.* По аналогии обозначим через $t(r, G)$ наибольшее число вершин в кокликах графа $GK(G)$, содержащих простое число r. Назовем это число *r-неплотностью.* Недавно в [3] была дана характеризация конечных

Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (проекты 08–01–00322 и 06–01–39001), Президиума СО РАН (интеграционный проект 2006.1.2), а также Совета по грантам Президента РФ для поддержки ведущих научных школ (НШ–344.2008.1) и молодых докторов наук (МД–2848.2007.1).

групп G, для которых $t(G) \geq 3$ и $t(2, G) \geq 2$, а в [4] было доказано, что все конечные неабелевы простые группы, за исключением знакопеременных групп подстановок, удовлетворяют условию $t(2, G) \geq 2$. В этой работе получено усиление основной теоремы из [3].

Теорема 1. *Пусть G — конечная группа, удовлетворяющая условиям $t(G) \geq 3$ и $t(2, G) \geq 2$. Тогда выполняются следующие утверждения.*

(1) *Существует конечная неабелева простая группа S такая, что $S \leq \overline{G} = G/K \leq \mathrm{Aut}(S)$ для максимальной нормальной разрешимой подгруппы K группы G.*

(2) *Для каждого независимого подмножества ρ множества $\pi(G)$ такого, что $|\rho| \geq 3$, не более чем одно простое число из ρ делит произведение $|K| \cdot |\overline{G}/S|$. В частности, $t(S) \geq t(G) - 1$.*

(3) *Выполняется одно из двух утверждений:*

(а) *каждое простое число $r \in \pi(G)$, не смежное в $GK(G)$ с числом 2, не делит произведение $|K| \cdot |\overline{G}/S|$; в частности, $t(2, S) \geq t(2, G)$;*

(б) *существует простое число $r \in \pi(K)$, не смежное в $GK(G)$ с числом 2; в этом случае $t(G) = 3$, $t(2, G) = 2$, и $S \simeq \mathrm{Alt}_7$ или $A_1(q)$ для некоторого нечетного числа q.*

Вышеупомянутая характеризация вместе с описанием графа простых чисел каждой конечной неабелевой простой группы (см. [4]) может быть применена к так называемой проблеме распознаваемости. Для данной конечной группы G обозначим через $h(G)$ число попарно не изоморфных конечных групп H с условием $\omega(H) = \omega(G)$. Группа G называется *распознаваемой* (по спектру), если $h(G) = 1$, *почти распознаваемой*, если $1 < h(G) < \infty$, и *нераспознаваемой*, если $h(G) = \infty$. Будем говорить, что для данной конечной группы G *проблема распознаваемости решена*, если известно значение $h(G)$. Поскольку каждая конечная группа с нетривиальной нормальной разрешимой подгруппой нераспознаваема, каждая распознаваемая группа или почти распознаваемая группа является расширением прямого произведения M неабелевых простых групп с помощью некоторой подгруппы из $\mathrm{Out}(M)$. Таким образом, наибольший интерес проблема распознаваемости имеет для простых и почти простых групп. Пусть L — конечная неабелева простая группа и G — конечная группа с условием $\omega(G) = \omega(L)$. Ясно, что равенство $\omega(G) = \omega(L)$ влечет совпадение простых графов групп G и L. Таким образом, если L удовлетворяет условиям теоремы 1, им удовлетворяет и группа G. Утверждение (1) заключения теоремы влечет, что G имеет единственный неабелев композиционный фактор S. С другой стороны, утверждения (2) и (3) помогают доказать, что этот фактор S изоморфен L. Если этот факт установлен, мы говорим, что L *квазираспознаваема*. Очевидно, что доказательство квазираспознаваемости группы L является существенным шагом на пути доказательства распознаваемости или почти распознаваемости группы L.

Описание графа простых чисел [4] показывает, что условие $t(2, L) \geq 2$ выполняется для всех конечных неабелевых простых групп, исключая знакопеременные группы Alt_n, где n таково, что числа $n, n-1, n-2, n-3$ не являются простыми. С другой стороны, для каждой конечной простой группы L с условием $t(L) < 3$ проблема распознаваемости уже решена.

Следующий результат показывает, что мы можем опустить исключительный случай (б) утверждения (3) теоремы 1, когда применяем теорему к проблеме распознавания конечных неабелевых простых групп.

Теорема 2. *Пусть L — конечная неабелева простая группа, для которой*

$t(L) \geq 3$ и $t(2, L) \geq 2$, а G — конечная группа, удовлетворяющая условию $\omega(G) = \omega(L)$. Тогда выполняются следующие утверждения.

(1) *Существует конечная неабелева простая группа S такая, что $S \leq \overline{G} = G/K \leq \mathrm{Aut}(S)$ для максимальной нормальной разрешимой подгруппы K группы G.*

(2) *Для каждого независимого подмножества ρ множества $\pi(G)$ такого, что $|\rho| \geq 3$, не более чем одно простое число из ρ делит произведение $|K| \cdot |\overline{G}/S|$. В частности, $t(S) \geq t(G) - 1$.*

(3) *Каждое простое число $r \in \pi(G)$, не смежное в $GK(G)$ с числом 2, не делит произведение $|K| \cdot |\overline{G}/S|$. В частности, $t(2, S) \geq t(2, G)$.*

§ 1. Предварительные результаты

Мы начинаем с основного результата из [3]. Заметим, что мы обозначаем конечные простые группы лиева типа в соответствии с лиевой нотацией, даже если они являются классическими группами.

Лемма 1 [3]. *Пусть G — конечная группа, удовлетворяющая условиям $t(G) \geq 3$ и $t(2, G) \geq 2$. Тогда существует конечная неабелева простая группа S такая, что $S \leq \overline{G} = G/K \leq \mathrm{Aut}(S)$ для максимальной нормальной разрешимой подгруппы K группы G. Кроме того, $t(S) \geq t(G) - 1$, и выполняется одно из следующих утверждений.*

(1) *$S \simeq \mathrm{Alt}_7$ или $A_1(q)$ для некоторого нечетного q, и $t(S) = t(2, S) = 3$.*

(2) *Для каждого простого числа $p \in \pi(G)$, не смежного с числом 2 в $GK(G)$, силовская p-подгруппа группы G изоморфна силовской p-подгруппе группы S. В частности, $t(2, S) \geq t(2, G)$.*

На самом деле неравенство $t(S) \geq t(G) - 1$ в приведенной выше теореме получено с использованием следующего предложения.

Лемма 2 [3, предложение 3]. *Пусть G — конечная группа, удовлетворяющая условиям леммы 1, и группы K, S, $\overline{G}$ такие же, как в заключении леммы 1. Тогда $t(S) \geq t(G) - 1$. Более того, для каждого независимого подмножества ρ множества $\pi(G)$ такого, что $|\rho| \geq 3$, не более чем одно простое число из ρ делит произведение $|K| \cdot |\overline{G}/S|$.*

Лемма 3 [5, лемма 1]. *Пусть G — конечная группа, K — ее нормальная подгруппа и G/K — группа Фробениуса с ядром F и циклическим дополнением C. Если $(|F|, |K|) = 1$ и F не лежит в $KC_G(K)/K$, то $r \cdot |C| \in \omega(G)$ для некоторого простого делителя r числа $|K|$.*

Лемма 4 [6]. *Пусть r, s — два различных простых числа, $H\langle x \rangle$ — полупрямое произведение нормальной $\{2, r, s\}'$-подгруппы H и группы $\langle x \rangle$ порядка s такой, что $[H, x] \neq 1$. Если $H\langle x \rangle$ действует точно на векторном пространстве V над полем порядка r, то $C_V(x) \neq 0$.*

Теперь, следуя [4], определим понятие примитивного простого делителя, которое восходит к известной теореме Жигмонди. Если q — натуральное число, r — нечетное простое число и $(r, q) = 1$, то через $e(r, q)$ обозначим наименьшее натуральное число n, для которого $q^n \equiv 1 (\mathrm{mod}\, r)$. Если q нечетно, положим $e(2, q) = 1$, если $q \equiv 1 (\mathrm{mod}\, 4)$, и $e(2, q) = 2$, если $q \equiv -1 (\mathrm{mod}\, 4)$.

Лемма 5 (теорема Жигмонди [7]). *Пусть q — натуральное число, большее 1. Тогда для каждого $n \in \mathbb{N}$ найдется простое число r такое, что $e(r, q) = n$, исключая случаи $q = 2$ и $n = 1$, $q = 3$ и $n = 1$, $q = 2$ и $n = 6$.*

Простое число r с условием $e(r,q)=i$ называется *примитивным простым делителем* числа q^i-1. По теореме Жигмонди такое число существует, исключая указанные выше случаи. Если q фиксировано, обозначим через r_i любой примитивный простой делитель числа q^i-1 (очевидно, что q^i-1 может иметь более одного такого делителя). Заметим, что в соответствии с определением каждый простой делитель числа $q-1$ является примитивным простым делителем, за единственным исключением: 2 не является примитивным простым делителем числа $q-1$, если $e(2,q)=2$. В последнем случае 2 — примитивный простой делитель числа q^2-1. Если q фиксировано, обозначим через k_i наибольший делитель числа q^i-1 такой, что множество простых делителей числа k_i является множеством всех примитивных простых делителей числа q^i-1. Число k_i называется *наибольшим примитивным делителем* числа q^i-1.

§ 2. Доказательство теоремы 1

Пусть G — конечная группа, удовлетворяющая условиям теоремы 1. По лемме 1 утверждение (1) заключения теоремы выполняется, а по лемме 2 выполняется и утверждение (2). Если п. (a) утверждения (3) неверен, то по лемме 1 неабелев композиционный фактор S группы G изоморфен группе Alt_7 или $A_1(q)$ для нечетного q. Таким образом, в дальнейшем мы полагаем, что п. (a) утверждения (3) неверен для G, и доказываем, что в этом случае $t(G)=3$ и $t(2,G)=2$.

Начнем с доказательства того, что $t(2,G)=2$. На самом деле мы докажем следующее утверждение.

Лемма 6. *Если п.* (a) *утверждения* (3) *теоремы* 1 *неверен, то разрешимый радикал K группы G содержит нетривиальную нормальную $2'$-подгруппу N индекса* 2 *такую, что силовская* 2*-подгруппа группы G/N является обобщенной группой кватернионов, G/N имеет центр порядка* 2*, все нечетные простые числа из $\pi(G)$, не смежные с* 2 *в $GK(G)$, смежны между собой, делят порядок K и не делят порядок G/K; в частности, $t(2,G)=2$.*

Доказательство. По нашему предположению существует простое число $r\in\pi(G)$ такое, что r не смежно с числом 2 в $GK(G)$ и r делит произведение $|K|\cdot|\overline{G}/S|$. По [3, лемма 1.2] число r не может делить $|\overline{G}/S|$, поэтому оно принадлежит $\pi(K)$. Пусть T — силовская 2-подгруппа группы G и H — холлова $\{2,r\}$-подгруппа группы KT. Поскольку силовская r-подгруппа R группы H является силовской r-подгруппой группы K, фактор-группа ее нормализатора $N=N_G(R)$ по подгруппе $N\cap K$ изоморфна группе $\overline{G}$ и содержит подгруппу, изоморфную группе S. Если R является циклической, то $C_G(R)K/K$ должен содержать S и тем самым $2r\in\omega(G)$; противоречие. Таким образом, R не является циклической. Поэтому $O_2(H)=1$. Следовательно, H — группа Фробениуса с ядром R и дополнением T. Поскольку силовская 2-подгруппа неабелевой простой группы S не может быть циклической, группа T как силовская 2-подгруппа группы G также не является циклической. Значит, T — обобщенная группа кватернионов. Если $M=O_{2'}(G)=O_{2'}(K)$, то по теореме Брауэра — Сузуки [8] фактор-группа G/M имеет центр Z/M порядка 2. Легко видеть, что $Z=K$ и число 2 смежно с любым нечетным простым делителем числа $|G/K|$. Предположим, что существует простое число $s\in\pi(K)$ такое, что $s\neq r$ и s не смежно с числом 2 в $GK(G)$. Холлова $\{2,r,s\}$-подгруппа группы K является группой Фробениуса с дополнением порядка 2. Поскольку холлова $\{r,s\}$-подгруппа группы K есть ядро этой группы Фробениуса, она абелева. Следовательно, r смежно с s, и $t(2,G)=2$. Лемма доказана.

Рассмотрим теперь величину $t(G)$. Поскольку $t(S) = 3$, неравенство $t(S) \geq t(G) - 1$ из леммы 1 влечет, что $t(G) \leq 4$. Предположим, что $t(G) = 4$, т. е. максимальное независимое множество ρ вершин графа $GK(G)$ содержит четыре простых числа. Из леммы 2 и равенства $t(S) = 3$ следует, что ровно одно из этих чисел делит произведение $|K| \cdot |\overline{G}/S|$. Обозначим это число через r. Заметим, что r нечетно, так как $t(2, G) = 2$. Предположим, что r делит число $|\overline{G}/S|$. Если $S \simeq \mathrm{Alt}_7$, то r не может делить $|\overline{G}/S| \leq 2$. Пусть $S \simeq A_1(q)$ и $q = p^m$, где p — характеристика поля определения. Поскольку каждая максимальная коклика из $GK(S)$ имеет вид $\{p, r_1, r_2\}$, где r_i — примитивный простой делитель числа $q^i - 1$ для $i = 1, 2$, число p должно быть одним из трех простых чисел из $\rho \cap \pi(S)$. С другой стороны, поскольку $\overline{G}/S$ изоморфна подгруппе группы $\mathrm{Out}\, S$, найдется элемент x нечетного порядка r из $\overline{G} \setminus S$, который сопряжен полевому автоморфизму группы S. Тогда $pr \in \omega(G)$; противоречие. Таким образом, мы можем полагать, что r делит порядок группы K.

Если $S \simeq \mathrm{Alt}_7$, то $\rho = \{3, 5, 7, r\}$. Пусть T — силовская 3-подгруппа группы G и H — холлова $\{3, r\}$-подгруппа группы KT. Поскольку силовская r-подгруппа группы H является силовской r-подгруппой группы K, она не циклическая. Таким образом, $O_3(H) = 1$, и H — группа Фробениуса с дополнением T. Следовательно, T должна быть циклической, что невозможно, так как силовская 3-подгруппа группы S не является циклической.

Предположим, что $S \simeq A_1(q)$, где $q = p^m$ и p — нечетное простое число. Тогда $\rho = \{r, p, s, t\}$, где все числа нечетны, s делит $q - 1$ и t делит $q + 1$. Заметим, что по лемме 2 (или по утверждению (2) теоремы) порядок группы K взаимно прост с произведением pst. Пусть R — силовская r-подгруппа группы K и $N = N_G(R)$ — ее нормализатор в G. В силу аргумента Фраттини $G/K \simeq N/N \cap K$, поэтому можно без потери общности полагать, что R — нормальная подгруппа группы G. Группа S содержит подгруппу F, которая является группой Фробениуса с ядром порядка q и дополнением порядка s. Поскольку $(|K|, |F|) = 1$, по теореме Шура — Цассенхауса фактор-группа G/R содержит подгруппу, изоморфную группе F. Из леммы 3 вытекает, что G содержит элемент порядка rs; противоречие. Теорема 1 доказана.

§ 3. Доказательство теоремы 2

Пусть L — конечная неабелева простая группа, G — конечная группа с условием $\omega(G) = \omega(L)$. Из теоремы 1 следует, что $S \leq \overline{G} = G/K \leq \mathrm{Aut}(S)$, где K — разрешимый радикал группы G, а S — конечная неабелева простая группа. Более того, если мы предположим, что для группы G п. (a) утверждения (3) теоремы 1 не выполняется, то S изоморфна группе Alt_7 или $A_1(q)$ для нечетного q; $t(L) = t(G) = 3$, $t(2, L) = t(2, G) = 2$. По [9] группа S не может быть изоморфна группе Alt_7 (в этом случае $L \simeq \mathrm{Alt}_7$ и $K = 1$), поэтому мы можем полагать, что $S \simeq A_1(q)$. Из леммы 6 следует, что каждое простое число r, не смежное с числом 2 в $GK(G)$, делит только порядок подгруппы K. Поскольку в [4] значения неплотности и 2-неплотности были определены для всех конечных неабелевых простых групп, мы можем перечислить все такие группы L, удовлетворяющие условиям $t(L) = 3$ и $t(2, L) = 2$. Используя [4], можно проверить, что любая максимальная коклика $\rho(L)$ графа $GK(L)$ содержит некоторое простое число r, не смежное с числом 2 в $GK(L)$. Поскольку r делит порядок группы K, любое другое число из $\rho(L)$ делит только порядок фактора S.

Пусть $S \simeq A_1(q)$, где $q = p^m$ для нечетного простого числа p. Как уже говорилось, каждая максимальная коклика в $GK(S)$ имеет вид $\{p, r_1, r_2\}$, где r_i —

примитивный простой делитель числа q^i-1 при $i=1,2$. Пусть $\rho(G)=\rho(L)=\{r,s,t\}$ — максимальная коклика, а $\rho(2,G)=\rho(2,L)=\{2,r\}$ — максимальная коклика, содержащая 2, в $GK(L)$, а значит, и в $GK(G)$. Тогда $s,t\in\{p,r_1,r_2\}$.

Предположим, что $s=r_1$ — нечетный простой делитель числа $q-1$. Переходя к фактор-группе группы G по $O_{r'}(K)$, а затем к фактор-группе группы $G/O_{r'}(K)$ по подгруппе Фраттини ее максимальной нормальной r-подгруппы, мы можем полагать, что $O_{r'}(K)=1$, $V=O_r(K)$ является нетривиальной нормальной элементарной абелевой r-подгруппой группы G и $C_G(V)=V$. Обозначим через $\widetilde{G}$ и $\widetilde{K}$ фактор-группы групп G и K по подгруппе V. Пусть $\widetilde{S}$ — прообраз группы S в $\widetilde{G}$ и P — силовская p-подгруппа группы $\widetilde{S}$. Положим $\widetilde{P}=P\cap\widetilde{K}$ и $N=N_{\widetilde{S}}(\widetilde{P})$. Поскольку в силу аргумента Фраттини $N/N\cap\widetilde{K}\simeq\widetilde{S}/\widetilde{K}$, мы можем полагать, что подгруппа $\widetilde{P}$ нормальна в $\widetilde{S}$ и, следовательно, $N_{\widetilde{S}}(P)/\widetilde{K}=N_S(U)$, где $U=P/\widetilde{P}$ — силовская p-подгруппа группы S. Нормализатор $N_S(U)$ содержит элемент y порядка s, и $U\langle y\rangle$ является группой Фробениуса с ядром U и дополнением $\langle y\rangle$; в частности $[U,y]\neq 1$. Следовательно, $N_{\widetilde{S}}(P)$ содержит элемент x порядка s, и $[P,x]\neq 1$. Поскольку $C_G(V)=V$, группа $P\langle x\rangle$ действует точно на группе V, которую мы можем рассматривать как векторное пространство над полем порядка r. Из леммы 4 вытекает, что $C_V(x)\neq 1$. Значит, $sr\in\omega(G)$; противоречие.

Таким образом, $s,t\in\{p,r_2\}$. Пусть $s=p$, а $t=r_2$ является нечетным простым делителем числа $q+1$. Если $q>p$, то абелева силовская p-подгруппа U группы S не является циклической. Рассматривая действие группы U на нормальной r-подгруппе из K, получаем, что группа G содержит элемент порядка pr, что невозможно, так как $pr\notin\omega(L)$. Следовательно, $q=p$, и $S\simeq A_1(p)$ для некоторого нечетного простого числа p.

Если граф простых чисел группы L несвязен, то несвязен и граф простых чисел группы G, а ее разрешимый радикал K нильпотентен (по теореме Томпсона о нильпотентности группы, допускающей регулярный автоморфизм простого порядка). С другой стороны, по лемме 6 в подгруппе K лежит элемент порядка 2. Следовательно, в этом случае простое число r, не смежное с числом 2 в $GK(G)$, не может делить порядок группы K, что противоречит нашему предположению. Таким образом, граф простых чисел группы L должен быть связен.

Поскольку все спорадические простые группы имеют несвязные графы простых чисел, ни одна из них не может быть контрпримером к утверждению теоремы. Среди знакопеременных групп, удовлетворяющих условиям $t(L)=3$ и $t(2,L)=2$, только группа Alt_{16} имеет связный граф простых чисел. Однако эта группа распознаваема по спектру [10]. Все исключительные группы лиева типа, кроме групп типа E_7, также имеют несвязный граф простых чисел. Поскольку для $L\simeq E_7(q)$ выполняется $t(L)=8$, мы можем полагать, что L — классическая группа лиева типа. Используя условие связности графа простых чисел вместе с равенствами $t(L)=3$ и $t(2,L)=2$, получаем, что группы, которые мы должны рассмотреть, содержатся среди следующих групп: $A_3(u)$, $A_5(u)$, ${}^2A_3(u)$, ${}^2A_5(u)$, $B_3(u)$, $C_3(u)$, $D_4(u)$, $B_4(2)$ и $C_4(2)$.

Пусть L изоморфна $B_4(2)$ или $C_4(2)$. Граф простых чисел $GK(L)=GK(G)$ имеет максимальную коклику $\rho(L)=\{5,7,17\}$ и максимальную коклику $\rho(2,L)=\{2,17\}$, содержащую число 2. Поскольку 17 делит только порядок разрешимого радикала K, простые числа $5,7$ делят только порядок $S\simeq A_1(p)$, а значит, $5,7\in\{p,r_2\}$. Если $p=5$, то 7 должно делить $p+1=6$. Если $p=7$, то 5 должно делить $p+1=8$. Оба случая невозможны.

Пусть L изоморфна одной из групп $A_3(u)$, $A_5(u)$, ${}^2A_3(u)$, ${}^2A_5(u)$, $B_3(u)$, $C_3(u)$, $D_4(u)$, где $u = v^m$ и v — простое число. Мы можем полагать, что v нечетно, так как иначе $t(2, L) = 3$. Пусть w_i — примитивный простой делитель числа $u^i - 1$, а k_i — максимальный примитивный делитель числа $u^i - 1$.

Лемма 7. *Пусть v — нечетное простое число и $u = v^m$. Тогда имеют место следующие утверждения.*

(1) *Если $L \simeq A_3(u)$, то для произвольных w_3 и w_4 множество $\{v, w_3, w_4\}$ является максимальной кокликой в $GK(L)$.*

(2) *Если $L \simeq {}^2A_3(u)$, то для произвольных w_4 и w_6 множество $\{v, w_4, w_6\}$ является максимальной кокликой в $GK(L)$.*

(3) *Если $L \simeq A_5(u)$, то для произвольных w_4, w_5 и w_6 множества $\{v, w_5, w_6\}$ и $\{w_4, w_5, w_6\}$ являются максимальными кокликами в $GK(L)$.*

(4) *Если $L \simeq {}^2A_5(u)$, то для произвольных w_3, w_4 и w_{10} множества $\{v, w_3, w_{10}\}$ и $\{w_4, w_3, w_{10}\}$ являются максимальными кокликами в $GK(L)$.*

(5) *Если $L \simeq B_3(u)$, $C_3(u)$ или $D_4(u)$, то для произвольных w_3 и w_6 множество $\{v, w_3, w_6\}$ является максимальной кокликой в $GK(L)$.*

(6) $k_3 = (u^2+u+1)/(3, u-1)$, $k_4 = (u^2+1)/2$, $k_5 = (u^4+u^3+u^2+u+1)/(5, u-1)$, $k_6 = (u^2 - u + 1)/(3, u + 1)$, $k_{10} = (u^4 - u^3 + u^2 - u + 1)/(5, u + 1)$.

Доказательство. Величины k_i могут быть вычислены непосредственно. Остальное следует из [4]. Лемма доказана.

Граф простых чисел каждой из наших групп L имеет максимальную коклику ρ вида $\{v, w_i, w_j\}$ из леммы 7. Выше отмечено, что коклика ρ содержит ровно одно простое число r, не смежное с числом 2, и это число не является характеристикой v, которая смежна с 2. Для определенности положим, что w_j смежно, а w_i не смежно с числом 2. По нашему предположению w_j делит порядок K и $(w_j, |G/K|) = 1$. С другой стороны, w_i и v делят порядок S и $(w_i v, |K| \cdot |G/S|) = 1$. Как было доказано, $S \simeq A_1(p)$ для некоторого нечетного простого числа p, и простые числа w_i, v принадлежат $\{p, r_2\}$, где r_2 — нечетный простой делитель числа $p + 1$.

Предположим, что $v = p$. Тогда w_i должен делить $p + 1$. С другой стороны, w_i является примитивным простым делителем числа $u^i - 1 = p^{mi} - 1$, что невозможно, так как $i > 2$ по лемме 7. Таким образом, v делит $p + 1$ и $w_i = p$. Рассмотрим наибольший примитивный делитель k_i числа $u^i - 1$. Поскольку в группе L есть элемент порядка k_i, элемент такого порядка есть и в группе G. С другой стороны, $(k_i, |K|\cdot|G/S|) = 1$. Поэтому и в группе S есть элемент порядка k_i. Поскольку по лемме 7 равенство $w_i = p$ должно выполняться для произвольного примитивного делителя w_i числа $u^i - 1$, наибольший примитивный делитель k_i равен p.

Пусть L изоморфна $B_3(u)$, $C_3(u)$ или $D_4(u)$. Тогда p равно k_3 или k_6 по лемме 7.

Предположим, что $p = k_3 = (u^2 + u + 1)/(3, u - 1)$. Поскольку v делит $p + 1$, число v делит $u^2 + u + 2$ при $(3, u - 1) = 1$ и v делит $u^2 + u + 4$ при $(3, u - 1) = 3$. В обоих случаях $v = 2$; противоречие.

Предположим, что $p = k_6 = (u^2 - u + 1)/(3, u + 1)$. Тогда v делит $u^2 - u + 2$, если $(3, u + 1) = 1$, и v делит $u^2 - u + 4$, если $(3, u + 1) = 3$. Вновь $v = 2$; противоречие.

Пусть L изоморфна $A_3(u)$ или ${}^2A_3(u)$. Поскольку равенства $p = k_3$ и $p = k_6$ приводят к противоречию, мы можем полагать, что $p = k_4 = (u^2 + 1)/2$. Следовательно, v делит $p + 1 = (u^2 + 3)/2$, поэтому $v = 3$. Группа L содержит элемент порядка 9. С другой стороны, $v = 3$ делит только порядок группы S. Значит, 9 делит $p + 1 = (u^2 + 3)/2 = (3^{2m} + 3)/2$; противоречие.

Пусть $L \simeq A_5(u)$. Если $p = k_5 = u^4+u^3+u^2+u+1$, то $v = 2$, что невозможно. Если $p = k_5 = (u^4 + u^3 + u^2 + u + 1)/5$, то v делит $u^4 + u^3 + u^2 + u + 6$, а значит, $v = 3$. По лемме 7 граф $GK(L)$ содержит коклику $\{w_4, w_5, w_6\}$, которая также является максимальной. Поскольку $w_5 = p$ и $w_6 \in \pi(K)$, все примитивные простые делители w_4 числа $u^4 - 1$ должны делить $p + 1$. В группе L есть элемент порядка k_4, следовательно, элемент такого порядка есть и в S, а значит, $k_4 = (u^2 + 1)/2$ делит $p + 1 = u^4 + u^3 + u^2 + u + 6$. Значит, $u^2 + 1$ делит $2(u^4 + u^3 + u^2 + u + 6)$. Поэтому $u^2 + 1$ делит 12; противоречие.

Пусть $L \simeq {}^2A_5(u)$. Если $p = k_{10} = u^4 - u^3 + u^2 - u + 1$, то $v = 2$, что невозможно. Если $p = k_5 = (u^4-u^3+u^2-u+1)/5$, то v делит $u^4-u^3+u^2-u+6$, а значит, $v = 3$. По лемме 7 граф $GK(L)$ содержит коклику $\{w_4, w_{10}, w_3\}$, которая также является максимальной. Поскольку $w_{10} = p$ и $w_3 \in \pi(K)$, все примитивные простые делители w_4 числа $u^4 - 1$ делят $p + 1$ и, значит, как и в предыдущем случае, $k_4 = (u^2 + 1)/2$ делит $p + 1 = u^4 - u^3 + u^2 - u + 6$. Следовательно, $u^2 + 1$ делит $2(u^4 - u^3 + u^2 - u + 6)$. Поэтому $u^2 + 1$ делит 12; противоречие.

Теорема доказана.

ЛИТЕРАТУРА

1. *Williams J. S.* Prime graph components of finite groups // J. Algebra. 1981. V. 69, N 2. P. 487–513.
2. *Кондратьев А. С.* О компонентах графа простых чисел конечных простых групп // Мат. сб. 1989. Т. 180, № 6. С. 787–797.
3. *Васильев А. В.* О связи между строением конечной группы и свойствами ее графа простых чисел // Сиб. мат. журн. 2005. Т. 46, № 3. С. 511–522.
4. *Васильев А. В., Вдовин Е. П.* Критерий смежности для графа простых чисел конечной простой группы // Алгебра и логика. 2005. Т. 44, № 6. С. 682–725.
5. *Мазуров В. Д.* Характеризация конечных групп множествами порядков их элементов // Алгебра и логика. 1997. Т. 36, № 1. С. 37–53.
6. *Khukhro E. I., Mazurov V. D.* Finite groups with an automorphism of prime order whose centralizer has small rank // J. Algebra. 2006. V. 301, N 2. P. 474–492.
7. *Zsigmondy K.* Zur Theorie der Potenzreste // Monatsh. Math. Phys. 1892. Bd 3. S. 265–284.
8. *Brauer R., Suzuki M.* On finite groups of even order whose 2-Sylow group is a quaternion group // Proc. Nat. Acad. Sci. USA. 1959. V. 45. P. 1757–1759.
9. *Горшков И. Б.* О группах с композиционным фактором, изоморфным знакопеременной группе степени 7 // Algebra and model theory. Collection of papers. NSTU. Новосибирск, 2007. P. 21–37.
10. *Заварницин А. В.* Распознавание знакопеременных групп степени $r + 1$ и $r + 2$ для простого r и группы степени 16 по их множествам порядков элементов // Алгебра и логика. 2000. Т. 39, № 6. С. 648–662.

Статья поступила 30 октября 2007 г.

Васильев Андрей Викторович
Институт математики им. С. Л. Соболева СО РАН,
пр. Академика Коптюга, 4, Новосибирск 630090
vasand@math.nsc.ru

Горшков Илья Борисович
Новосибирский гос. университет, ул. Пирогова, 2, Новосибирск 630090
ilygor@ngs.ru