ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ
Январь—март 1996. Том 3, № 1, 43–51

УДК 519.71

О СЛОЖНОСТИ ВЫЧИСЛЕНИЙ В КОНЕЧНЫХ НИЛЬПОТЕНТНЫХ ГРУППАХ*)

В. В. Кочергин

Рассматривается вопрос о сложности вычислений элементов конечных нильпотентных групп. При вычислении элемента конечной группы над заданным порождающим множеством разрешается многократное использование промежуточных результатов, т. е. в качестве вычислительной модели используются схемы из функциональных элементов умножения. На входы схем подаются элементы из некоторого порождающего (конечную) группу G множества элементов M_G этой группы, а сами схемы состоят из двувходовых элементов, которые реализуют произведение элемента группы, поступившего на первый вход, и элемента, поступившего на второй вход (подразумевается, что входы элемента схемы упорядочены). Кроме того, выходы некоторых элементов схемы помечены — это выходы схемы. Такие схемы будем называть схемами над порождающим множеством M_G.

Пусть G — конечная группа, а M_G — порождающее множество этой группы. Обозначим через $L(g, M_G)$ наименьшее число операций умножения (считаем, что операция в группе — умножение), достаточное для вычисления элемента g группы G, исходя из элементов множества M_G (допускается многократное использование промежуточных элементов). Например, пусть абелева группа $\langle g_1\rangle_7 \times \langle g_2\rangle_{19}$ задана порождающим множеством $\{g_1, g_2\}$ (порядки элементов g_1, g_2 соответственно равны 7 и 19). Тогда для элемента $g_1^5 g_2^{12}$ справедливо равенство $L(g_1^5 g_2^{12}, \{g_1, g_2\}) = 5$, так как, исходя из элементов g_1 и g_2, элемент $g_1^5 g_2^{12}$ можно получить, использовав 5 операций умножения следующим образом:

$$g_1 \times g_2 = g_1 g_2, \quad g_1 g_2 \times g_1 g_2 = (g_1 g_2)^2, \quad (g_1 g_2)^2 \times (g_1 g_2)^2 = (g_1 g_2)^4,$$

$$(g_1 g_2)^4 \times (g_1 g_2)^4 = (g_1 g_2)^8, \quad (g_1 g_2)^4 \times (g_1 g_2)^8 = g_1^5 g_2^{12},$$

в то время как с использованием только четырех операций умножения элемент $g_1^5 g_2^{12}$ получить нельзя.

*) Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (код проекта 93-01-01527).

Положим $L(G, M_G) = \max L(g, M_G)$, где максимум берется по всем элементам группы G. Для произвольного класса $\mathbf{K}_n$ групп порядка n положим $L(\mathbf{K}_n) = \max L(G, M_G)$, где максимум берется по всем парам (G, M_G) для всех групп G из класса $\mathbf{K}_n$.

В работах [1–3] изучались некоторые вопросы сложности вычислений элементов конечных абелевых, нильпотентных и разрешимых групп. В частности, было доказано, что

$$L(\mathbf{A}_n) = \log n + \frac{\log n}{\log\log n}(1 + o(1)),$$

$$L(\mathbf{MA}_n) \sim \log n, \quad L(\mathbf{N}_n) \asymp \log n,$$

$$\log n \lesssim L(\mathbf{R}_n) \leqslant \log n \log\log n,$$

где $\mathbf{A}_n$ — класс всех абелевых групп порядка n, $\mathbf{MA}_n$ — класс метабелевых (двуступенно нильпотентных) групп порядка n, $\mathbf{N}_n$ — класс нильпотентных групп порядка n и $\mathbf{R}_n$ — класс разрешимых групп порядка n, а $\log x$ обозначает $\log_2 x$.

Кроме того, было показано, что если $G = \langle g_1\rangle_{k_1} \times \langle g_2\rangle_{k_2} \times \cdots \times \langle g_q\rangle_{k_q}$, то

$$L(G, \{g_1, g_2, \ldots, g_q\}) = \log \max_{1\leqslant i\leqslant q} k_i + \frac{\log|G|}{\log\log|G|}(1 + o(1)) + O(q).$$

В данной работе по сравнению с доказательством из [3] дано более конструктивное доказательство (и с меньшей константой) верхней оценки сложности вычислений в конечных нильпотентных группах. В отличие от доказательства из [3] предлагаемое доказательство можно пытаться распространить на более широкие классы конечных групп.

Прежде чем перейти к содержательной части работы, напомним некоторые определения (см., например, [4]).

Если x и y — элементы группы G, то элемент $[x, y] = x^{-1}y^{-1}xy$ группы G называется *коммутатором* этих элементов. Если X и Y — подгруппы группы G, то $[X, Y]$ — подгруппа, порожденная всеми коммутаторами $[x, y]$ при $x \in X$, $y \in Y$.

Нижний центральный ряд

$$G = \gamma_1(G) \supseteq \gamma_2(G) \supseteq \ldots$$

группы G определяется по правилу $\gamma_{i+1}(G) = [\gamma_i(G), G]$. В частности, группа $\gamma_2(G) = [G, G]$ есть *коммутант* группы G, иначе обозначаемый через G'.

Группа G называется *нильпотентной*, если найдется такое k, что $\gamma_{k+1}(G) = e$. Наименьшее значение k, удовлетворяющее этому условию, называется *ступенью* нильпотентности группы G.

Замечание 1. Для любой группы G справедливо включение $[\gamma_i(G), \gamma_j(G)] \subseteq \gamma_{i+j}(G)$ (см. [4, упр. 14.4.2]).

Теперь, аналогично М. Холлу [5], для произвольной группы G, заданной порождающим множеством $M_G = \{g_1, g_2, \ldots, g_q\}$, определим *порождающие коммутаторы* (у М. Холла — базисные коммутаторы) c_j и их *веса* $w(c_j)$ следующим образом.

1. Положим $c_i = g_i, i = 1, \ldots, q$, — порождающие коммутаторы веса один, т. е. $w(g_i) = 1$.

2. Пусть порождающие коммутаторы, имеющие вес меньше m, уже определены. Тогда порождающими коммутаторами веса m являются коммутаторы $c_r = [c_i, c_j]$, где c_i и c_j — порождающие коммутаторы, причем $i > j$ и $w(c_i) + w(c_j) = m$.

3. Коммутаторы веса m следуют за коммутаторами веса меньшего m, а между собой они упорядочены так, чтобы выполнялись следующие условия:

а) если $[c_s, c_j]$ и $[c_t, c_j]$ — порождающие коммутаторы и $s < t$, то порождающий коммутатор $[c_s, c_j]$ предшествует порождающему коммутатору $[c_t, c_j]$;

б) если $[c_i, c_s]$ и $[c_i, c_t]$ — порождающие коммутаторы и $s < t$, то порождающий коммутатор $[c_i, c_s]$ предшествует порождающему коммутатору $[c_i, c_t]$.

Порождающие коммутаторы считаем занумерованными так, что они упорядочены по индексам.

Замечание 2. Вес порождающего коммутатора характеризует не элемент группы, а некоторую его запись.

Замечание 3. Согласно определению порождающих коммутаторов существует только конечное число порождающих коммутаторов веса не больше m.

Лемма 1. *Пусть G — нильпотентная группа ступени k, заданная порождающим множеством $M_G = \{g_1, \ldots, g_q\}$. Тогда любой порождающий коммутатор веса $k + 1$ является записью единичного элемента группы.*

Доказательство. Индукцией по весу m порождающего коммутатора c_i докажем, что как элемент группы G коммутатор c_i содержится в подгруппе $\gamma_m(G)$.

При $m = 1$ это очевидно.

Пусть этот факт верен для всех порождающих коммутаторов веса меньше m. Докажем его для произвольного порождающего коммутатора c_i веса m. В силу определения порождающий коммутатор c_i можно представить в виде $c_i = [c_s, c_t]$, причем $w(c_s) + w(c_t) = m$. Так как

$w(c_s) < m$ и $w(c_t) < m$, то по предположению индукции порождающие коммутаторы c_s и c_t как элементы группы G принадлежат соответственно подгруппам $\gamma_{w(c_s)}(G)$ и $\gamma_{w(c_t)}(G)$. Но тогда в силу замечания 1 $[c_s, c_t] \in \gamma_m(G)$. Таким образом, произвольный порождающий коммутатор веса $k+1$ является записью некоторого элемента из $\gamma_{k+1}(G)$. Но $\gamma_{k+1}(G) = e$. Лемма 1 доказана.

Для произвольного порождающего коммутатора c обозначим через $I(c)$ индекс (номер) этого порождающего коммутатора. Очевидно, что $c_{I(c)} = c$.

Лемма 2. *Пусть G — конечная нильпотентная группа ступени k, заданная порождающим множеством M_G, а $c_1, \ldots, c_u$ — все порождающие коммутаторы веса не больше k. Тогда для любого s, $1 \leqslant s \leqslant u$, и произвольного элемента $g \in G$, если $g \in \langle c_i \mid s \leqslant i \leqslant u \rangle$, то для каждого t, $1 \leqslant t \leqslant u$, справедливо включение $[g, c_t] \in \langle c_i \mid r \leqslant i \leqslant u \rangle$, где*

$$r = \begin{cases} I([c_s, c_t]), & \text{если } s > t; \\ I([c_t, c_s]), & \text{если } t > s; \\ I([c_{s+1}, c_s]), & \text{если } s = t. \end{cases}$$

Доказательство будем проводить индукцией по s от u до 1, а при фиксированном s — по наименьшей возможной длине j слова в алфавите $c_s, \ldots, c_u$, являющегося записью данного элемента g.

Основание индукции. Для случая $s = u$ утверждение леммы справедливо, так как в этом случае согласно лемме 1 $[g, c_t] \in \langle c_i \mid i > u \rangle = \langle e \rangle$. Для произвольного $s = u, \ldots, 1$, если минимальная длина слова, представляющего элемент g в алфавите $c_s, \ldots, c_u$, равна 1, то в силу п. 3 определения порождающих коммутаторов утверждение леммы также выполняется.

Пусть утверждение леммы справедливо для всех $s' = u, \ldots, s+1$, а при $s' = s$ — для всех элементов, допускающих представление в алфавите $c_s, \ldots, c_u$ словами длины меньше j. Докажем справедливость леммы в том случае, когда наименьшая длина слова в алфавите $c_s, \ldots, c_u$, представляющего элемент g, равна j.

Пусть $g = c_{i_1} \ldots c_{i_{j-1}} c_{i_j}$, где $s \leqslant i_1, \ldots, i_j \leqslant u$. Для произвольного t, $1 \leqslant t \leqslant u$, имеем

$$[g, c_t] = [c_{i_1} \ldots c_{i_{j-1}} c_{i_j}, c_t] = [c_{i_1} \ldots c_{i_{j-1}}, c_t]\,[[c_{i_1} \ldots c_{i_{j-1}}, c_t], c_{i_j}]\,[c_{i_j}, c_t].$$

Очевидно, что $[c_{i_j}, c_t] \in \langle c_i \mid r \leqslant i \leqslant u \rangle$. По предположению индукции $[c_{i_1} \ldots c_{i_{j-1}}, c_t] \in \langle c_i \mid r \leqslant i \leqslant u \rangle$. Так как $r > s$, то, применяя еще раз предположение индукции, получаем, что $[[c_{i_1} \ldots c_{i_{j-1}}, c_t], c_{i_j}] \in \langle c_i \mid r' \leqslant i \leqslant u \rangle$ для некоторого $r' > r$.

Следовательно, $[g, c_t] \in \langle c_i \mid r \leqslant i \leqslant u \rangle$. Лемма 2 доказана.

Лемма 3. *Пусть G — конечная нильпотентная группа ступени k, заданная порождающим множеством M_G, а $c_1, \ldots, c_u$ — все порождающие коммутаторы веса не больше k. Тогда для любых σ $(1 \leqslant \sigma \leqslant u)$, τ $(1 \leqslant \tau \leqslant u)$, $\sigma \neq \tau$, и элемента $g \in G$, если $g \in \langle c_i \mid \sigma + 1 \leqslant i \leqslant u \rangle$, то*

а) *при $\sigma > \tau$ справедливо включение $[g, c_\tau] \in \langle c_i \mid I([c_\sigma, c_\tau]) + 1 \leqslant i \leqslant u \rangle$;*

б) *при $\tau > \sigma$ справедливо включение $[c_\tau, g] \in \langle c_i \mid I([c_\tau, c_\sigma]) + 1 \leqslant i \leqslant u \rangle$.*

Доказательство. Применим лемму 2, положив $s = \sigma + 1$, $t = \tau$. Отдельно рассмотрим три случая.

Случай 1. $\sigma + 1 > \tau$. Тогда $[g, c_\tau] \in \langle c_i \mid I([c_{\sigma+1}, c_\tau]) \leqslant i \leqslant u \rangle$. Но $I([c_{\sigma+1}, c_\tau]) \geqslant I([c_\sigma, c_\tau]) + 1$. Следовательно, $[g, c_\tau] \in \langle c_i \mid I([c_\sigma, c_\tau]) + 1 \leqslant i \leqslant u \rangle$.

Случай 2. $\sigma + 1 = \tau$. Тогда $s = t$, и поэтому

$$[g, c_\tau] \in \langle c_i \mid I([c_{\tau+1}, c_{\sigma+1}]) \leqslant i \leqslant u \rangle \subseteq \langle c_i \mid I([c_\tau, c_\sigma]) + 1 \leqslant i \leqslant u \rangle.$$

Случай 3. $\sigma + 1 < \tau$. Тогда

$$[g, c_\tau] \in \langle c_i \mid I([c_\tau, c_{\sigma+1}]) \leqslant i \leqslant u \rangle \subseteq \langle c_i \mid I([c_\tau, c_\sigma]) + 1 \leqslant i \leqslant u \rangle.$$

Для завершения доказательства осталось отметить, что $[c_\tau, g] = [g, c_\tau]^{-1}$. Лемма 3 доказана.

Лемма 4. *Пусть G — конечная нильпотентная группа ступени k, заданная порождающим множеством M_G, а $c_1, \ldots, c_u$ — все порождающие коммутаторы веса не больше k. Тогда числа $l_1, \ldots, l_u$, определяемые равенствами*

$$l_i = \frac{|\langle c_j \mid j \geqslant i \rangle|}{|\langle c_j \mid j \geqslant i + 1 \rangle|}, i = 1, \ldots, u,$$

удовлетворяют условиям:

1) *если $l_k > 1$ и $c_k = [c_s, c_t]$ для некоторых s и t, то $\min(l_s, l_t) > 1$,*

2) $l_1 \ldots l_u = |G|$,

3) *каждый элемент $g \in G$ можно представить в виде*

$$g = c_1^{\alpha_1} \ldots c_u^{\alpha_u},$$

где $0 \leqslant \alpha_i < l_i$, $i = 1, \ldots, u$.

Доказательство. Обозначим через C_i, $i = 1, 2, \ldots$, подгруппу группы G, определяемую порождающими коммутаторами c_i, c_{i+1}, $c_{i+2}, \ldots$ Тогда справедливы равенства $l_i = |C_i| / |C_{i+1}|$, $i = 1, \ldots, u$.

Покажем, что числа $l_1, \ldots, l_u$ удовлетворяют условию 1.

Допустим, найдется такое $l_k > 1$, что $c_k = [c_s, c_t]$, но $\min(l_s, l_t) = 1$. Если $l_s = 1$, то $c_s \in \langle c_i \mid s + 1 \leqslant i \leqslant u \rangle$, а если $l_t = 1$, то $c_t \in \langle c_i \mid t + 1 \leqslant$

$i \leqslant u\rangle$; в обоих случаях в силу леммы 3 справедливо включение $[c_s, c_t] \in \langle c_i \mid I([c_s, c_t]) + 1 \leqslant i \leqslant u\rangle$. Следовательно, $l_k = 1$, что противоречит предположению.

В силу равенств

$$l_1 l_2 \dots l_u = \frac{|C_1|}{|C_2|}\frac{|C_2|}{|C_3|} \dots \frac{|C_u|}{|C_{u+1}|} = |G|$$

выполняется условие 2 леммы.

Покажем, что любой элемент $h \in G$ можно представить в виде

$$h = c_1^{\alpha_1} \dots c_u^{\alpha_u},$$

где $0 \leqslant \alpha_i < l_i$, $i = 1, \dots, u$.

Для этого достаточно показать, что произвольный элемент $h_m \in C_m$, $m = 1, \dots, u$, можно представить в виде $h_m = c_m^{\alpha_m} h_{m+1}$, где $0 \leqslant \alpha_m < l_m$, $h_{m+1} \in C_{m+1}$.

Так как $h_m \in C_m$, то элемент h_m можно представить в виде

$$h_m = c_{i_1} c_{i_2} \dots c_{i_s},$$

где $i_1, i_2, \dots, i_s \geqslant m$. Пусть $c_{i_j} = c_m$ — первое вхождение порождающего коммутатора c_m в данное представление элемента h_m. Тогда представление $h_m = c_{i_1} \dots c_{i_{j-1}} c_{i_j} \dots c_{i_s}$ заменим на следующее:

$$h_m = c_{i_1} \dots c_{i_j} c_{i_{j-1}} [c_{i_{j-1}}, c_{i_j}] \dots c_{i_s},$$

где $[c_{i_{j-1}}, c_{i_j}]$ — порождающий коммутатор (так как $i_{j-1} > m$, а $i_j = m$), причем $I([c_{i_{j-1}}, c_{i_j}]) > m$. При этом переходе от одной записи к другой порождающий коммутатор c_{i_j} сдвинулся на одно место влево и появился новый порождающий коммутатор $[c_{i_{j-1}}, c_{i_j}]$ из подгруппы C_{m+1}. После конечного числа таких шагов коммутатор c_{i_j} переместится на первое место в представлении элемента h_m. Проделав аналогичные операции с остальными вхождениями коммутатора c_{i_j}, для элемента h_m получим представление вида $h_m = c_m^{\alpha'_m} h'_{m+1}$, где $h'_{m+1} \in C_{m+1}$. Учитывая, что $c_m^{l_m} \in C_{m+1}$, получаем нужное представление элемента h_m. Лемма 4 доказана.

Обозначим $\mathfrak{C} = \{ c_i \mid (1 \leqslant i \leqslant u) \& (l_i > 1)\}$.

Теорема. *Для величины $L(\mathrm{N}_n)$ справедливы оценки*

$$(1 + o(1)) \log n < L(\mathrm{N}_n) \underset{\frown}{<} \log n.$$

Доказательство. Нижняя оценка. В силу введенных определений справедливы неравенства

$$L(\mathrm{N}_n) \geqslant L(\langle g \rangle_n, \{g\}) \geqslant L(g^{n-1}, \{g\}).$$

С другой стороны, если $L(g^a, \{g\}) = b$, то $a \leqslant 2^b$ (этот факт легко устанавливается по индукции). Поэтому

$$L(\mathrm{N}_n) \geqslant \log(n-1) \geqslant (1 + o(1)) \log n.$$

Верхняя оценка. Пусть G — конечная нильпотентная группа порядка n и ступени k, заданная порождающим множеством $M_G = \{g_1, g_2, \ldots, g_q\}$, а $c_1, \ldots, c_u$ — все порождающие коммутаторы веса не больше k. Пусть, кроме того, выполняется равенство $L(G, M_G) = L(\mathrm{N}_n)$. Тогда найдется такой элемент $g \in G$, что выполняется равенство $L(g, M_G) = L(\mathrm{N}_n)$. Без ограничения общности можно считать, что M_G — неприводимое порождающее множество, т. е. никакое его собственное подмножество не является порождающим множеством для группы G. Оценим сверху величину $L(g, M_G)$, предложив конкретную схему вычисления элемента g, состоящую из трех частей.

Часть 1. Получение по элементам $g_1, g_2, \ldots, g_q$ элементов $(g_1)^{-1}$, $(g_2)^{-1}, \ldots, (g_q)^{-1}$.

Сначала, используя $q-1$ раз операцию умножения, последовательно вычисляем элементы $g_1g_2, g_1g_2g_3, \ldots, g_1g_2\ldots g_q$. Затем элемент $g_1g_2\ldots g_q$ возводим в степень $O(g_1g_2\ldots g_q) - 1$, где $O(g_1g_2\ldots g_q)$ — порядок элемента $g_1g_2\ldots g_q$, тем самым получая элемент $(g_1g_2\ldots g_q)^{-1}$. В силу [6] для этого потребуется не более $(\log n + \log n/\log\log n)(1 + o(1))$ умножений. После этого, используя $2q-2$ раз операцию умножения, проводим следующие вычисления:

$$(g_1g_2\ldots g_q)^{-1} \times (g_1g_2\ldots g_{q-1}) = g_q^{-1}; g_q \times (g_1g_2\ldots g_q)^{-1} = (g_1g_2\ldots g_{q-1})^{-1};$$

$$(g_1g_2\ldots g_{q-1})^{-1} \times (g_1g_2\ldots g_{q-2}) = g_{q-1}^{-1}; g_{q-1} \times (g_1g_2\ldots g_q)^{-1} = (g_1g_2\ldots g_{q-2})^{-1};$$

$$\ldots\ldots\ldots\ldots$$

$$(g_1g_2g_3)^{-1} \times (g_1g_2) = g_3^{-1}; g_3 \times (g_1g_2g_3)^{-1} = (g_1g_2)^{-1};$$

$$(g_1g_2)^{-1} \times g_1 = g_2^{-1}; g_2 \times (g_1g_2)^{-1} = g_1^{-1}.$$

Таким образом, получены элементы $(g_1)^{-1}, (g_2)^{-1}, \ldots, (g_q)^{-1}$.

Часть 2. Получение элементов из множества $\mathfrak{C}$ и обратных к ним.

Элементы $c_1^{-1} = g_1^{-1}$, $c_2^{-1} = g_2^{-1}$, $\ldots$, $c_q^{-1} = g_q^{-1}$ уже реализованы в первой части. Отметим, что в силу неприводимости порождающего множества M_G и леммы 4 элементы c_1, c_2, $\ldots$, c_q принадлежат множеству $\mathfrak{C}$. Вычислим в порядке возрастания индексов оставшиеся элементы из множества $\mathfrak{C}$ и обратные к ним следующим образом. Пусть $c_i = [c_s, c_t]$ — порождающий коммутатор из множества $\mathfrak{C}$, имеющий наименьший индекс среди еще не полученных порождающих коммутаторов из множества $\mathfrak{C}$. Тогда элементы c_s, c_s^{-1}, c_t и c_t^{-1} группы G в силу

леммы 4 уже вычислены (так как $l_s > 1$ и $l_t > 1$). Поэтому порождающий коммутатор c_i и элемент, обратный к нему, вычисляются по формулам $c_i = c_s^{-1}c_t^{-1}c_sc_t$ и $c_i^{-1} = c_t^{-1}c_s^{-1}c_tc_s$ с использованием шести операций умножения.

Часть 3. Вычисление элемента g.

Все элементы из множества $\mathfrak{C}$ уже реализованы. Поэтому, учитывая лемму 12 из [3], элемент g можно вычислить по представлению из леммы 4 с использованием не более

$$\sum_{i=1}^{u}(2\log(\alpha_i + 1) - 2) + |\mathfrak{C}|$$

операций умножения.

Таким образом, суммируя оценки числа операций умножения, используемых в каждой из трех частей схемы, получаем

$$L(g, M_G) \leqslant (3q + \log n + \frac{\log n}{\log\log n}(1 + o(1)) + 6(|\mathfrak{C}| - q) + \left(\sum_{i=1}^{u}(2\log(\alpha_i + 1) - 2) + |\mathfrak{C}|\right).$$

Учитывая неравенства $q \leqslant |\mathfrak{C}| \leqslant \log n$ и $|\mathfrak{C}| \leqslant u$, окончательно имеем

$$L(g, M_G) \leqslant 3\log n(1 + o(1)) + 7|\mathfrak{C}| - 2u \leqslant 8(1 + o(1))\log n$$

и, следовательно,

$$L(\mathrm{N}_n) \leqslant \log n.$$

Теорема доказана.

ЛИТЕРАТУРА

1. **Кочергин В. В.** О сложности вычислений в конечных абелевых группах // Докл. АН СССР. 1991. Т. 317, № 2. С. 291–294.
2. **Кочергин В. В.** О сложности вычислений в конечных абелевых группах // Математические вопросы кибернетики. М.: Наука, 1992. Вып. 4. С. 178–217.
3. **Кочергин В. В.** О сложности вычислений в конечных абелевых, нильпотентных и разрешимых группах // Дискретная математика. 1993. Т. 5, вып. 1. С. 91–111.

4. **Каргаполов М. И., Мерзляков Ю. И.** Основы теории групп. М.: Наука, 1982.
5. **Холл М.** Теория групп. М.: Изд-во иностр. лит., 1962.
6. **Brauer A.** On addition chains // Bull. Amer. Math. Soc. 1939. V. 45. P. 736–739.

Адрес автора:

Россия,
119899 Москва,
Воробьевы горы,
МГУ, мех.-мат. факультет

Статья поступила

15 января 1996 г.