2008 Теоретические основы прикладной дискретной математики № 2(2)
DOI 10.17223/20710410/2/6
УДК 519.7

О С-ШИРИНЕ КОНЕЧНЫХ АЦИКЛИЧЕСКИХ ГРУПП

В.М. Фомичев

Московский инженерно-физический институт (*государственный университет*)

E-mail: fomichev@nm.ru

Даны начальные результаты исследования представления конечной группы в виде покрытия максимальными циклическими подгруппами. Указан способ построения групп линейных подстановок множества V_n, у которых c-ширина не меньше 2^n.

***Ключевые слова*:** *циклическая группа*, *с-ширина группы.*

Конечная группа G имеет единственное несократимое представление в виде канонического c-покрытия, то есть в виде объединения максимальных циклических подгрупп [1,3]:

$$G = \bigcup_{g \in B_G} \langle g \rangle,$$

где B_G есть c-базис группы G, представляющий собой систему элементов группы G, порождающих все максимальные в G циклические подгруппы. Порядок множества B_G называется c-шириной группы G (обозначается $h_c(G)$).

Величина c-ширины группы G характеризует сложность определения наследственного признака H в группе G в рамках подхода [4, 5], предполагающего определение признака H во всех максимальных циклических подгруппах группы G.

Для c-ширины произвольной ациклической группы G верны оценки:

$$1 < h_c(G) \le |G| - 1, \tag{1}$$

где $h_c(G) = 1$ тогда и только тогда, когда G – циклическая группа. Верхняя оценка (1) достигается, в частности, когда G – прямая сумма нескольких циклических групп порядка 2. Если Σ_r – группа сдвигов пространства V_r двоичных r-мерных векторов, то $h_c(\Sigma_r)=2^r - 1$, так как c-базис группы Σ_r образуют все ненулевые векторы пространства V_r.

1. Свойства канонического *c*-покрытия конечной группы

Обозначим через N множество натуральных чисел. Далее считаем, что G – конечная ациклическая группа и её каноническое c-покрытие имеет вид

$$G = \bigcup_{i=1}^{h} \langle g_i \rangle, \tag{2}$$

где $\{g_1, \ldots, g_h\}$ есть c-базис группы G и $h = h_c(G) > 1$.

Обозначим через $\mathrm{Gen}\langle g \rangle$ множество элементов, порождающих циклическую подгруппу $\langle g \rangle$ группы G. Известно [2], что если $\mathrm{ord}\, g = n$, то $\mathrm{Gen}\langle g \rangle$ состоит из всех элементов вида g^t, где $(t, n) = 1$.

Утверждение 1. Если $(g_i)^t \in \mathrm{Gen}\langle g_i \rangle$, то при любом $\tau = 1, \ldots, \mathrm{ord} g_j$ элементы $(g_i)^t(g_j)^\tau$ и $(g_j)^\tau(g_i)^t$ группы G не принадлежат группе $\langle g_j \rangle$, где $i, j \in \{1, \ldots, h\}$ и $i \ne j$.

Доказательство. Если $(g_i)^t(g_j)^\tau \in \langle g_j \rangle$, то $(g_i)^t = (g_j)^k$ при некотором натуральном k. Следовательно, $\langle g_i \rangle$ – подгруппа группы $\langle g_j \rangle$, что невозможно в силу максимальности циклической подгруппы $\langle g_i \rangle$ в группе G. Для элемента $(g_j)^\tau(g_i)^t$ утверждение доказывается аналогично.

Следствие 1. Если $(g_i)^t \in \mathrm{Gen}\langle g_i \rangle$ и $(g_j)^\tau \in \mathrm{Gen}\langle g_j \rangle$, то элементы $(g_i)^t(g_j)^\tau$ и $(g_j)^\tau(g_i)^t$ группы G не принадлежат множеству $\langle g_i \rangle \cup \langle g_j \rangle$, где $i, j \in \{1, \ldots, h\}$ и $i \ne j$.

Теперь нижнюю из оценок (1) можно уточнить для ациклических групп.

Следствие 2. $h_c(G) > 2$.

Доказательство. В силу ацикличности группы G в ней имеется не менее двух максимальных циклических подгрупп. Пусть эти подгруппы порождаются элементами g_1 и g_2 соответственно. По следствию 1 утверждения 1 элемент $g_1 g_2 \notin \langle g_1 \rangle \cup \langle g_2 \rangle$. Следовательно, $h_c(G) > 2$.

Оценим c-ширину группы G через её порядок и порядки элементов её c-базиса. Обозначим: $\omega(G) = \max\limits_{g \in G} \mathrm{ord} g$. Заметим, что $\omega(G)$ совпадает с наибольшим из порядков максимальных циклических подгрупп группы G.

Утверждение 2. Если G – конечная ациклическая группа, то $h_c(G) \geq \dfrac{|G|-1}{\omega(G)-1}$.

Доказательство. Из равенства (2) следует, что $G\setminus\{e\} = \bigcup\limits_{i=1}^{h}(\langle g_i\rangle \setminus \{e\})$, так как единичный элемент e группы G является единичным элементом любой её подгруппы. Отсюда

$$|G| - 1 \leq \sum_{i=1}^{h} (\mathrm{ord} g_i - 1). \tag{3}$$

По определению $\mathrm{ord}\, g_i \leq \omega(G)$, $i = 1, \ldots, h$, поэтому из (3) получаем

$$|G| - 1 \leq h(\omega(G) - 1),$$

откуда следует требуемое неравенство.

Для циклической группы $\langle g\rangle$ порядка $n > 1$ назовём Gen-комплексом всякое её подмножество X порядка $r > 1$, удовлетворяющее условиям: $X \cap \mathrm{Gen}\langle g\rangle \neq \varnothing$ и $g^{t-\tau} \in \mathrm{Gen}\langle g\rangle$ для всех g^t, g^τ из X при $t > \tau$. Заметим, что при $g \neq e$ пара элементов $\{e, g\}$ является Gen-комплексом группы $\langle g\rangle$. Обозначим через $\mu(n)$ наибольший из порядков всех Gen-комплексов циклической группы порядка $n > 1$.

Утверждение 3. Величина $\mu(n)$ равна наименьшему простому делителю числа n.

Доказательство. Пусть p – наименьший простой делитель числа n, где $n > 1$. Тогда множество $\{e, g, \ldots, g^{p-1}\}$ содержит элемент g, порождающий группу $\langle g\rangle$ и $g^{t-\tau} \in \mathrm{Gen}\langle g\rangle$ для всех t, τ из $\{0, 1, \ldots, p-1\}$ при $t \neq \tau$, так как $(t - \tau, p) = 1$ в силу простоты числа p. Отсюда, раз натуральное число $t - \tau$ взаимно просто с p и меньше n, то $t - \tau$ взаимно просто и с любым другим делителем числа n. Следовательно, $(t - \tau, n) = 1$. Значит, множество $\{e, g, \ldots, g^{p-1}\}$ является Gen-комплексом группы $\langle g\rangle$.

Вместе с тем, если подмножество X (порядка $r > 1$) группы $\langle g\rangle$ содержит элементы g^t и g^τ, где $t \equiv \tau \pmod p$, то X не является Gen-комплексом группы $\langle g\rangle$, так как $g^{t-\tau} \notin \mathrm{Gen}\langle g\rangle$. Действительно, в этом случае $(t - \tau, p) = p$, откуда получаем, что $(t - \tau, n) \geq p > 1$. Следовательно, Gen-комплекс группы $\langle g\rangle$ содержит не более p элементов. Таким образом, $\mu(n) = p$.

Gen-комплекс $\{e, g, \ldots, g^{p-1}\}$ нетривиальной группы $\langle g\rangle$ порядка n, где p – наименьший простой делитель числа n, обозначим через $\mathrm{Gen}^*\langle g\rangle$. Установим соотношения между характеристиками элементов c-базиса ациклической группы G порядка n, определяемой представлением (2). Так как $h_c(G) \geq 3$, то число n – не простое. Следовательно, корректными являются следующие обозначения: $\mu_I = \mu(\mathrm{ord} g_i)$, $\eta_I = \max\limits_{j\in\{1,\ldots,h\}\setminus\{i\}} \mu_j$, $i = 1, \ldots, h$.

Теорема 1. Для ациклической группы G, определяемой представлением (2), при любом $i = 1, \ldots, h$ выполнено

$$|G| \geq \mathrm{ord} g_i \cdot \eta_i.$$

Если $\langle g_i\rangle \cap \langle g_j\rangle = \{e\}$ для $i, j \in \{1, \ldots, h\}$, $i \neq j$, то $|G| \geq \mathrm{ord} g_i \cdot \mathrm{ord} g_j$.

Доказательство. Пусть M – подмножество элементов группы G вида

$$M = \{(g_i)^t \cdot (g_j)^\tau\},$$

где $t = 0, 1, \ldots, \mathrm{ord}\, g_i - 1$, $\tau = 0, 1, \ldots, \theta - 1$ при некотором натуральном θ.

Так как $|G| \geq |M|$, то для доказательства теоремы достаточно показать, что множество M не содержит одинаковых элементов группы G при любом из двух условий: *а*) $\theta = \mu_j$; *б*) $\theta = \mathrm{ord}\, g_j$, если $\langle g_i\rangle \cap \langle g_j\rangle = \{e\}$. Предположим противное – пусть

$$(g_i)^t \cdot (g_j)^\tau = (g_i)^v \cdot (g_j)^w \tag{4}$$

при $t, v \in \{0, 1, \ldots, \mathrm{ord}\, g_i - 1\}$ и $\tau, w \in \{0, 1, \ldots, \theta - 1\}$, где $(t, \tau) \neq (v, w)$, тогда равенство (4) равносильно следующему равенству:

$$(g_i)^{t-v} = (g_j)^{w-\tau}. \tag{5}$$

В случае (*а*) $\langle (g_j)^{w-\tau}\rangle = \langle g_j\rangle$ при $w \neq \tau$, так как по утверждению 3 $(g_j)^w$, $(g_j)^\tau \in \mathrm{Gen}^*\langle g_j\rangle$ при $\theta = \mu_j$. Отсюда и из (5) следует включение $\langle g_j\rangle \subseteq \langle g_i\rangle$, противоречащее равенству (2) в силу максимальности подгруппы $\langle g_j\rangle$ в группе G. Следовательно, в случае (*а*) множество M не содержит одинаковых элементов группы G.

Рассмотрим случай (*б*). Если $t = v$ при $w \neq \tau$, то из (5) получаем равенство $(g_j)^{w-\tau} = e$, которое невозможно при любых различных $\tau, w \in \{0, 1, \ldots, \mathrm{ord}\, g_j - 1\}$.

Если $t \neq v$ при $w = \tau$, то из (5) получаем равенство $(g_i)^{t-v} = e$, которое невозможно при любых различных $t, v \in \{0, 1, \ldots, \mathrm{ord}\, g_i - 1\}$.

Если $t \neq v$ и $w \neq \tau$, то элементы $(g_i)^{t-v}$ и $(g_j)^{w-\tau}$ отличны от e и из (5) следует, что оба они принадлежат $\langle g_i\rangle \cap \langle g_j\rangle$, что противоречит условию случая (*б*).

Следовательно, и в случае (*б*) множество M не содержит одинаковых элементов группы G.

Следствие 1. Если $\mathrm{ord} g_i = \omega(G)$, то $h_c(G) > \eta_i$.

Доказательство. По теореме 1 $|G| \geq \mathrm{ord}\, g_i \cdot \eta_i$ для ациклической группы G при любом $i = 1, \ldots, h$. Отсюда получаем равносильное неравенство:

$$|G| - 1 \geq \mathrm{ord} g_i \cdot \eta_i - \eta_i + \eta_i - 1.$$

По определению $\eta_i > 1$ при любом $i = 1, \ldots, h$, поэтому из последнего неравенства следует:

$$|G| - 1 > (\mathrm{ord}\, g_i - 1)\eta_i.$$

Разделив обе части неравенства на натуральное число $\mathrm{ord}\, g_i - 1$, имеем

$$\frac{|G|-1}{\mathrm{ord} g_i - 1} > \eta_i,\ i = 1, \ldots, h.$$

В частности, при $\mathrm{ord}\, g_i = \omega(G)$ по утверждению 2 имеем, что $h_c(G) > \eta_i$.

Следствие 2. Если при некоторых $i, j \in \{1, \ldots, h\}$, где $i \neq j$, $\mathrm{ord}\, g_j$ – простое число и $\mathrm{ord}\, g_i \geq \mathrm{ord}\, g_j$, то $h_c(G) > \mathrm{ord}\, g_j$.

Доказательство. Пусть $\omega(G) = \mathrm{ord}\, g_k$, где $k \in \{1, \ldots, h\} \setminus \{j\}$, при указанном j такое k найдётся, так как $\mathrm{ord} g_i \geq \mathrm{ord} g_j$. Тогда по следствию 1 теоремы 1 $h_c(G) > \eta_k$, где $\eta_k \geq \mathrm{ord}\, g_j$ при простом $\mathrm{ord}\, g_j$.

Таким образом, c-ширина любой конечной ациклической группы G не меньше 3. Более точная нижняя оценка может быть получена с помощью числовых характеристик, определяемых порядками элементов c-базиса группы G.

2. Строение конечных ациклических групп c-ширины 3

Опишем строение ациклических групп, c-ширина которых равна 3.

Теорема 2. Если каноническое c-покрытие группы G есть $\langle g_1\rangle \cup \langle g_2\rangle \cup \langle g_3\rangle$, то $|G| = 4m$ при некотором $m \in N$, $\mathrm{ord} g_1 = \mathrm{ord} g_2 = \mathrm{ord} g_3 = 2m$ и $\langle (g_1)^2\rangle = \langle (g_2)^2\rangle = \langle (g_3)^2\rangle$. Для любого $m \in N$ имеется ациклическая группа G порядка $4m$, c-ширина которой равна 3.

Доказательство. 1) Пусть порядок одной из максимальных циклических подгрупп группы G равен 2. Например, $\mathrm{ord} g_1 = 2$. Тогда $\langle g_1\rangle \setminus \{e\} = \{g_1\}$ и по следствию 1 утверждения 1 получаем, что $g_2 g_3 = g_1 = g_3 g_2$. Докажем, что в этом случае $\mathrm{ord} g_2 = \mathrm{ord} g_3 = 2$.

Действительно, $g_2, (g_2)^{-1} \in \mathrm{Gen}\, \langle g_2\rangle$, откуда по следствию 1 утверждения 1 получаем, что $g_2 g_3 = g_1$ и $(g_2)^{-1} g_3 = g_1$. Следовательно, $g_2 = (g_2)^{-1}$ и $\mathrm{ord} g_2 = 2$. Равенство $\mathrm{ord} g_3 = 2$ доказывается аналогично.

Следовательно, если порядок одной из максимальных циклических подгрупп группы G равен 2, то теорема верна ($m = 1$).

2) Пусть $\min\{\mathrm{ord}\, g_1, \mathrm{ord}\, g_2, \mathrm{ord}\, g_3\} > 2$. Тогда $g_1 \neq (g_1)^{-1}$ и $(g_1)^2 \neq e$.

Обозначим $a = g_1 g_2$, $b = (g_1)^{-1} g_2$. Так как $g_1, (g_1)^{-1} \in \mathrm{Gen}\langle g_1\rangle$, то по следствию 1 утверждения 2 $a, b \in \langle g_3\rangle \setminus \{e\}$. Следовательно, $b^{-1} \in \langle g_3\rangle \setminus \{e\}$ и $ab^{-1} \in \langle g_3\rangle \setminus \{e\}$, где $ab^{-1} = (g_1)^2$.

Отсюда получаем, что

$$\langle (g_1)^2\rangle < \langle g_3\rangle, \tag{6}$$

где $\mathrm{ord}\, g_1$ – чётное число. Действительно, в случае нечётности числа $\mathrm{ord}\, g_1$ имеем $(g_1)^2 \in \mathrm{Gen}\langle g_1\rangle$, и, следовательно, $\langle g_1\rangle < \langle g_3\rangle$, что противоречит максимальности циклической подгруппы $\langle g_1\rangle$ в группе G. Заметим, что группа $\langle g_3\rangle$ не содержит нечётных степеней элемента g_1, так как в противном случае из включения (6) следовало бы включение $\langle g_1\rangle < \langle g_3\rangle$.

Аналогично доказываются другие включения типа (6), а именно: $\langle (g_i)^2\rangle < \langle g_j\rangle$, где группа $\langle g_j\rangle$ не содержит нечётных степеней элемента g_i, $i, j \in \{1, 2, 3\}$, $i \neq j$. Совокупность этих условий означает, что $\langle (g_i)^2\rangle < \langle (g_j)^2\rangle$, $i, j \in \{1, 2, 3\}$, $i \neq j$. Следовательно, $\langle (g_1)^2\rangle = \langle (g_2)^2\rangle = \langle (g_3)^2\rangle$ и множества $\langle g_1\rangle \setminus \langle (g_1)^2\rangle$, $\langle g_2\rangle \setminus \langle (g_2)^2\rangle$, $\langle g_3\rangle \setminus \langle (g_3)^2\rangle$ попарно не пересекаются. Таким образом, из канонического c-покрытия группы G вытекает разбиение группы G:

$$G = \langle (g_1)^2\rangle \cup (\langle g_1\rangle \setminus \langle (g_1)^2\rangle) \cup (\langle g_2\rangle \setminus \langle (g_2)^2\rangle) \cup (\langle g_3\rangle \setminus \langle (g_3)^2\rangle).$$

Так как $\mathrm{ord}\, g_i$ – чётное число (пусть оно равно $2m$ при некотором $m \in N$), то $|\langle g_i\rangle \setminus \langle (g_i)^2\rangle| = \mathrm{ord}\, \langle (g_i)^2\rangle = m$, $i = 1, 2, 3$. Следовательно, в указанном разбиении каждый блок имеет мощность m, откуда получаем, что $|G| = 4m$.

Существование для любого $m \in N$ ациклической группы G порядка $4m$, c-ширина которой равна 3, обеспечивается следующим построением. Пусть $G = \langle g_1, g_2, g_3\rangle$, где g_1, g_2, g_3 – попарно различные элементы порядка $2m$, $(g_1)^2 = (g_2)^2 = (g_3)^2$ и при любой перестановке (i, j, k) номеров 1, 2, 3 выполнено равенство множеств

$$\langle (g_i)^2\rangle \cdot g_j = \langle g_k\rangle \setminus \langle (g_k)^2\rangle.$$

Следствие 1. Если порядок группы G не делится на 4, то $h_c(G) > 3$.

Следствие 2. Если $|G| = 4$, то $h_c(G) = 3$ и группа G изоморфна группе сдвигов Σ_2.

Доказательство. Если группа G ациклическая и $|G| = 4$, то G состоит из нейтрального элемента и трех элементов порядка 2. Изоморфизм φ задается биекцией между элементами порядка 2 группы G и ненулевыми векторами группы Σ_2.

3. *c*-Ширина ациклических групп порядка *pq* при простых *p* и *q*

Пусть $|G| = pq$, где p и q – простые числа и $p \geq q \geq 2$. Заметим, что если $p = q = 2$, то $h_c(G) = 3$ по следствию 2 теоремы 2. В противном случае $h_c(G) > 3$ по следствию 1 теоремы 2. Уточним оценку величины $h_c(G)$ при $p + q > 4$.

Лемма 1. Пусть c-базис группы G состоит из n_1 элементов порядка p_1, …, n_k элементов порядка p_k, где $k \in N$ и p_1, …, p_k – простые числа. Тогда

$$h_c(G) = n_1 + \ldots + n_k,$$

$$|G| = 1 + n_1(p_1 - 1) + \ldots + n_k(p_k - 1).$$

Доказательство. Первое равенство следует из определения чисел n_1, …, n_k.

Для доказательства второго равенства заметим, что каноническое c-покрытие (2) группы G есть объединение $n_1 + \ldots + n_k$ циклических групп порядков p_1, …, p_k, где в силу простоты чисел p_1, …, p_k пересечение любых двух циклических групп из канонического c-покрытия состоит лишь из нейтрального элемента. Следовательно, множество $G\backslash\{e\}$ разбивается на $n_1 + \ldots + n_k$ блоков, мощности которых есть мощности циклических групп из канонического c-покрытия за вычетом нейтрального элемента.

Утверждение 4. Пусть $|G| = p^2$, тогда $h_c(G) = p + 1$.

Доказательство. В условиях утверждения группа G состоит из нейтрального элемента и элементов порядка p. Каноническое c-покрытие (2) группы G есть объединение $h_c(G)$ циклических групп порядка p. Отсюда по лемме 1 $|G| = 1 + h_c(G)(p - 1)$. Следовательно, $h_c(G) = \dfrac{p^2 - 1}{p - 1} = p + 1$.

Теорема 3. Пусть $|G| = pq$, где $p > q \geq 2$, тогда

1) $q + 1 \leq h_c(G) \leq p + \dfrac{p-1}{q-1}$;

2) $n_q > 0$;

3) если $n_p = 0$, то $q - 1$ делит $p - 1$ и достигается верхняя оценка, то есть $h_c(G) = p + \dfrac{p-1}{q-1}$.

Доказательство. Пусть теперь $p > q \geq 2$, в этом случае ациклическая группа G порядка pq состоит из нейтрального элемента и некоторого числа элементов порядков p и q. Обозначим через n_p и n_q соответственно числа элементов порядков p и q в c-базисе группы G. По лемме 1 $h_c(G) = n_p + n_q$ и

$$pq = 1 + n_p(p - 1) + n_q(q - 1). \tag{7}$$

1) Так как $p > q$, то из равенства (7) получаем

$$(n_p + n_q)(q - 1) \leq pq - 1 \leq (n_p + n_q)(p - 1).$$

Отсюда с учетом леммы 1 следует:

$$q + \frac{q-1}{p-1} \leq h_c(G) \leq p + \frac{p-1}{q-1}.$$

Так как $h_c(G)$ – целое число, то нижнюю оценку можно уточнить, заменив на 1 положительную дробь $\dfrac{q-1}{p-1}$, которая меньше единицы.

2) Если $n_q = 0$, то из (7) получаем, что $h_c(G) = \dfrac{pq-1}{p-1} = q + \dfrac{q-1}{p-1}$. Имеем противоречие, так как $h_c(G)$ – целое число, в то время как $\dfrac{q-1}{p-1}$ не целое. Значит, $n_q > 0$.

3) Если $n_p = 0$, то из (7) получаем, что

$$h_c(G) = \frac{pq-1}{q-1} = p + \frac{p-1}{q-1}. \tag{8}$$

Отсюда, если $q - 1$ не делит $p - 1$, то имеем противоречие, так как $h_c(G)$ – целое число, в то время как $\dfrac{p-1}{q-1}$ не целое. Значит, если $n_p = 0$, то $q - 1$ делит $p - 1$ и выполнено (8), то есть достигается верхняя оценка для $h_c(G)$.

4. О построении класса конечных перестановочных автоматов, группы которых имеют *c*-ширину, превышающую заданную величину

Пусть $A = (V_1, V_n, h)$ – конечный автомат Мили без выходов со входным алфавитом $V_1 = \{0, 1\}$, с множеством состояний $V_n = \{(v_1, \ldots, v_n)\}$ (двоичные n-мерные векторы) и с функцией переходов $h: V_n \to V_n$, определяемой при входном двоичном символе x формулой

$$h(x, v_1, \ldots, v_n) = x \cdot g_1(v_1, \ldots, v_n) \oplus \bar{x} \cdot g_2(v_1, \ldots, v_n),$$

где g_1, g_2 – подстановки множества V_n. Группа G_A автомата A есть $\langle g_1, g_2 \rangle$.

Укажем условия, при которых группа G_A автомата A имеет c-ширину не меньше 2^n.

Утверждение 5. Пусть число $2^n - 1$ – простое и g_1, g_2 – линейные подстановки максимального периода, где $\langle g_1 \rangle \neq \langle g_2 \rangle$. Тогда $h_c(G_A) \geq 2^n$.

Доказательство. Каждый из элементов g_1 и g_2, порождающих группу G_A, порождает максимальную циклическую подгруппу группы G_A. Действительно, по условию G_A – группа линейных преобразований множества V_n, поэтому всякая ее циклическая подгруппа порядка $2^n - 1$, в том числе группа $\langle g_1 \rangle$ и группа $\langle g_2 \rangle$, является максимальной в группе G_A. Следовательно, с учетом неравенства $\langle g_1 \rangle \neq \langle g_2 \rangle$ получаем по теореме 1, что в группе G_A имеется c-базис, включающий и элемент g_1, и элемент g_2. Отсюда, учитывая простоту числа $\operatorname{ord} g_2 = 2^n - 1$, по следствию 2 теоремы 1 получаем оценку: $h_c(G_A) > \operatorname{ord} g_2 = 2^n - 1$. Следовательно, $h_c(G_A) \geq 2^n$.

Выводы. Для конечных ациклических групп получены следующие результаты:

1) показано, что c-ширина любой группы не меньше 3, если порядок группы не делится на 4, то ее c-ширина больше 3;

2) описано строение групп, c-ширина которых равна 3;

3) показано, что c-ширина любой группы G не меньше $\dfrac{|G|-1}{\omega(G)-1}$, где $\omega(G)$ – наибольший из порядков элементов группы G;

4) c-ширина группы оценена снизу через числовые характеристики, определяемые порядками некоторых элементов c-базиса группы;

5) оценена c-ширина групп порядка pq, где p и q – простые числа, $p \leq q$, через числа p и q:

$$q + 1 \leq h_c(G) \leq p + \frac{p-1}{q-1},$$

в частности, при $p = q$ c-ширина группы в точности равна $p + 1$;

6) указан способ построения групп линейных подстановок множества V_n, у которых c-ширина не меньше 2^n.

ЛИТЕРАТУРА

1. *Биркгоф Г.* Теория решёток. М.: Наука, 1984. 567 с.
2. *Глухов М.М.*, *Елизаров В.П.*, *Нечаев А.А.* Алгебра. Т. 1. М.: Гелиос-АРВ, 2003. 336 с.
3. *Гретцер Г.* Общая теория решёток. М.: Мир, 1982. 454 с.
4. *Фомичёв В.М.* Исследование признаков в конечных группах и в группах подстановок // Математические вопросы кибернетики. Вып. 14: Сб. статей / Под ред. О.Б. Лупанова. М.: Физматлит, 2005. С. 161 – 260.
5. *Фомичёв В.М.* О вычислительной сложности определения характеристик наследственного подмножества группы с заданным признаком // Безопасность информационных технологий. М.: МИФИ, 2006. №2. С. 82 – 85.