Общероссийский математический портал

И. А. Круглов, О слоях в системе образующих элементов подпрямого произведения подгрупп конечной группы, *Дискрет. матем.*, 2009, том 21, выпуск 1, 52–65

DOI: <https://doi.org/10.4213/dm1038>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 54.224.60.19

26 апреля 2023 г., 09:14:47

О слоях в системе образующих элементов подпрямого произведения подгрупп конечной группы

© 2009 г. И. А. Круглов

В статье дано описание слоев в системе образующих элементов для подпрямого произведения подгрупп конечной группы, а также доказана формула для соответствующей ширины покрытия в терминах подгрупп этой конечной группы. На основе данных результатов описано предельное поведение распределений случайных величин в некоторых частных случаях схемы линейной авторегрессии со случайным управлением на конечной группе.

Работа выполнена при поддержке программой Президента Российской Федерации поддержки ведущих научных школ, грант НШ-4.2008.10.

Пусть $(G, *)$ — конечная группа, $G \times G$ — прямое произведение группы G на себя, групповую операцию в группе $G \times G$ будем также обозначать символом $*$.

Пусть M — произвольное непустое подмножество в $G \times G$, $\mathcal{G}$ — подгруппа группы $G \times G$, порожденная множеством образующих элементов M . Определим индуктивно множества

$$M^1 = M, \quad M^{N+1} = M^N * M, \quad N \geq 1.$$

В соответствии с [2], множества M^N называются слоями группы $\mathcal{G}$ в системе образующих элементов M .

Зафиксируем произвольный элемент $(a_1, \sigma_1) \in M$. Известно [2], что существуют такие натуральные числа N_0, m , что множество $\mathfrak{M} = M^{N_0}$ есть нормальный делитель группы $\mathcal{G}$, фактор-группа $\mathcal{G}/\mathfrak{M}$ — циклическая, порожденная смежным классом $(a_1, \sigma_1) * \mathfrak{M}$, и верны равенства:

$$\begin{aligned} \mathcal{G} &= \mathfrak{M} \cup (a_1, \sigma_1) * \mathfrak{M} \cup \dots \cup (a_1, \sigma_1)^{m-1} * \mathfrak{M}, \\ (a_1, \sigma_1)^k * \mathfrak{M} &= M^{N_0+k}, \quad k \geq 1, \end{aligned} \quad (1)$$

где $m = |\mathcal{G} : \mathfrak{M}|$ — индекс $\mathfrak{M}$ в $\mathcal{G}$, $\mathfrak{M}$ — минимальный нормальный делитель среди всех нормальных делителей L группы $\mathcal{G}$, удовлетворяющих соотношению $M \subset (a_1, \sigma_1) * L$.

В настоящей работе мы опишем множества из разложения (1) в терминах подгрупп исходной группы G . Аналогичная задача решалась ранее автором в работе [4] в несколько иной постановке. А именно, множество M можно рассматривать как носитель распределения некоторой случайной величины со значениями в группе $G \times G$. В работе [4] без ограничения общности в качестве данной случайной величины рассматривалась пара вида $(\zeta, \xi * \zeta)$, где ζ и ξ — некоторые (зависимые) случайные величины со значениями в

группе G . Для произвольной случайной величины η со значениями в некоторой конечной группе будем обозначать через $\Omega(\eta)$ носитель распределения η . Тогда

$$M = \Omega(\zeta, \xi * \zeta), \quad M^N = \Omega(\chi^{(N)}, \omega^{(N)}), \quad N \geq 1, \quad (2)$$

где

$$\begin{aligned} (\chi^{(N)}, \omega^{(N)}) &= (\zeta_1, \xi_1 * \zeta_1) * (\zeta_2, \xi_2 * \zeta_2) * \dots * (\zeta_N, \xi_N * \zeta_N) \\ &= (\zeta_1 * \dots * \zeta_N, \xi_1 * \zeta_1 * \dots * \xi_N * \zeta_N) \end{aligned} \quad (3)$$

— произведение независимых одинаково распределенных случайных величин $(\zeta_j, \xi_j * \zeta_j)$, $j \in \{1, \dots, N\}$, распределение которых совпадает с распределением случайной величины $(\zeta, \xi * \zeta)$. Для элемента $a \in G$, удовлетворяющего условию $\mathbf{P}(\chi^{(N)} = a) > 0$, обозначим через $\omega_a^{(N)}$ случайную величину со значениями в группе G , распределение которой совпадает с условным распределением случайной величины $\omega^{(N)}$ при условии $\chi^{(N)} = a$.

Согласно (2), (3),

$$M^N = \bigcup_{a \in \Omega(\chi^{(N)})} \{a\} \times \Omega(\omega_a^{(N)}), \quad N \geq 1. \quad (4)$$

В [4] было дано описание носителей распределений случайных величин $\omega_a^{(N)}$, $a \in G$, $\mathbf{P}(\chi^{(N)} = a) > 0$. Воспользуемся этим описанием для исследования множеств (4) и введем необходимые обозначения, соответствующие обозначениям из [4].

Пусть

$$\{a_1, \dots, a_s\} = \{a \in G \mid \exists g \in G: (a, g) \in M\}, \quad s \geq 1,$$

$a_i \neq a_j$ для всех $i \neq j$, и $\mathfrak{A} = \langle a_1, \dots, a_s \rangle$ — подгруппа группы G , порожденная множеством $\{a_1, \dots, a_s\}$, $\mathfrak{N}$ — минимальный нормальный делитель группы $\mathfrak{A}$ среди ее нормальных делителей L , удовлетворяющих условию $\{a_1, \dots, a_s\} \subset a_1 L$; обозначим также через $d = |\mathfrak{A} : \mathfrak{N}|$ индекс $\mathfrak{N}$ в $\mathfrak{A}$.

Для всех $k \in \{1, \dots, s\}$ пусть

$$M_k = \{\sigma \in G \mid (a_k, \sigma) \in M\}.$$

Для всех $k \in \{1, \dots, s\}$ зафиксируем произвольный элемент $\sigma_k \in M_k$. Тогда $(a_k, \sigma_k) \in M$ для всех $k \in \{1, \dots, s\}$.

Словом в алфавите $\{a_1, \dots, a_s\}$ назовем последовательность

$$z = (a_{k_1}^{\varepsilon_1}, \dots, a_{k_N}^{\varepsilon_N}), \quad k_1, \dots, k_N \in \{1, \dots, s\}, \quad \varepsilon_1, \dots, \varepsilon_N \in \{-1, 1\}. \quad (5)$$

Обозначим через C множество всех слов в алфавите $\{a_1, \dots, a_s\}$.

Для каждого слова $z \in C$ вида (5) определим элемент $a(z)$ группы $\mathfrak{A}$, полагая для всех $z \in C$

$$a(z) = a_{k_1}^{\varepsilon_1} * \dots * a_{k_N}^{\varepsilon_N}, \quad (6)$$

элемент группы G , полагая для всех $z \in C$

$$g(z) = (\sigma_{k_1})^{\varepsilon_1} * \dots * (\sigma_{k_N})^{\varepsilon_N}, \quad (7)$$

а также множество элементов $\Omega(z)$ группы G , полагая для всех $z \in C$

$$\Omega(z) = M_{k_1}^{\varepsilon_1} * \dots * M_{k_N}^{\varepsilon_N}. \quad (8)$$

Тогда $g(z) \in \Omega(z)$ для всех $z \in C$.

Будем говорить, что слово z вида (5) представляет элемент $a \in \mathfrak{A}$, если $a(z) = a$, в частности, z — единичное слово, если $a(z) = e_G$ — единичный элемент G . Пусть C_0 — множество всех единичных слов в алфавите $\{a_1, \dots, a_s\}$, положим для всех $z \in C_0$ вида (5)

$$l(z) = \frac{1}{d}(\varepsilon_1 + \dots + \varepsilon_N). \quad (9)$$

Согласно следствию 1 к теореме 1 работы [2], для всех $z \in C_0$ число $l(z)$ целое и существует единичное слово z_0 , для которого $l(z_0) = 1$. Зафиксируем произвольное такое слово z_0 и определим элемент

$$x = g(z_0). \quad (10)$$

Так как группа $\mathfrak{A}$ конечна, существует конечная совокупность единичных слов $z_1, \dots, z_p$ в алфавите $\{a_1, \dots, a_s\}$ такая, что равенства $z_i = e_G, i \in \{1, \dots, p\}$, образуют систему определяющих соотношений группы $\mathfrak{A}$ относительно ее системы образующих $\{a_1, \dots, a_s\}$. Зафиксируем произвольную такую совокупность.

Обозначим через H минимальную подгруппу среди подгрупп L группы G , одновременно удовлетворяющих соотношениям

$$M_k \subset L * \sigma_k, \quad (11)$$

$$\sigma_k * (L * x) = (L * x) * \sigma_k, \quad (12)$$

$$g(z_i) \in L * x^{l(z_i)} \quad (13)$$

для всех $k \in \{1, \dots, s\}$ и всех $i \in \{1, \dots, p\}$.

Пусть

$$r = \min\{l \geq 1 \mid x^l \in H\}.$$

Каждому элементу $a \in \mathfrak{A}$ поставим в соответствие элемент $g(a) \in G$ следующим образом. Согласно [2], однозначно определено число $v \in \{0, 1, \dots, d-1\}$, для которого $a \in \mathfrak{A}a_1^v$, и существует слово $z_a \in C$ вида (5), представляющее a и удовлетворяющее равенству $\varepsilon_1 + \dots + \varepsilon_N = v$. Зафиксируем произвольно такое слово z_a и положим $g(a) = g(z_a)$. Далее, пусть $\Omega = M_1 \cup \dots \cup M_s$, $\Omega = \Omega(\xi * \zeta)$, и $T = \langle \Omega \rangle$ — подгруппа группы G , порожденная множеством Ω . Согласно (8), $\Omega(z) \subset T$ для всех $z \in C$.

Докажем вспомогательное утверждение.

Лемма 1. Подгруппа H есть нормальный делитель группы T , а отображение $\alpha: \mathfrak{A} \rightarrow T/H$ такое, что $\alpha(b) = H * g(b)$ для любого $b \in \mathfrak{A}$, есть гомоморфизм групп.

Доказательство. Условия (11), (12), (13) выполнены при $L = T$. Следовательно, $H \subset T$. Условия (11), (12) выполняются при $L = H$, поэтому $\sigma * H = H * \sigma$ для всех $\sigma \in \Omega$. Следовательно, $H \triangleleft T$.

При доказательстве леммы 2 в [4] доказано, что для всех $z \in C_0$

$$\Omega(z) \subset x^{l(z)} * H. \quad (14)$$

Пусть $a, b \in \mathfrak{A}$ — произвольные элементы, тогда $a * b \in \mathfrak{A}$. По определению элементов $g(a), g(b), g(a * b)$

$$g(a) = g(z_a), \quad g(b) = g(z_b), \quad g(a * b) = g(z_{ab}), \quad z_a, z_b, z_{ab} \in C, \quad (15)$$

и для каждого из слов z_1, z_b, z_{ab} в представлении (5) выполнено равенство

$$\varepsilon_1 + \varepsilon_2 + \dots + \varepsilon_N = 0. \quad (16)$$

Для произвольных слов v, w в образующих $\{a_1, \dots, a_s\}$ обозначим через (v, w) слово, полученное приписыванием w справа от v . Из соотношений (6)–(9) следует, что

$$\begin{aligned} a((v, w)) &= a(v) * a(w), \\ g((v, w)) &= g(v) * g(w), \\ \Omega((v, w)) &= \Omega(v) * \Omega(w), \quad v, w \in C, \\ l((v, w)) &= l(v) + l(w), \quad v, w \in C_0. \end{aligned} \quad (17)$$

Слову $z \in C$ вида (5) соответствует слово $z^{-1} = (a_{k_N}^{-\varepsilon_N}, a_{k_{N-1}}^{-\varepsilon_{N-1}}, \dots, a_{k_2}^{-\varepsilon_2}, a_{k_1}^{-\varepsilon_1})$, $z^{-1} \in C$, и из (6), (7), (8), (9) следует, что

$$\begin{aligned} g(z^{-1}) &= g(z)^{-1}, \quad a(z^{-1}) = a(z)^{-1}, \quad \Omega(z^{-1}) = \Omega(z)^{-1}, \quad z \in C, \\ l(z^{-1}) &= -l(z), \quad z \in C_0. \end{aligned} \quad (18)$$

Для слова $z = (z_{ab}^{-1}, z_a, z_b)$ согласно (17), (18), (16) справедливы соотношения

$$z \in C_0, \quad l(z) = 0. \quad (19)$$

Из соотношений (14), (15), (17), (18), (19) следует, что $g(a * b)^{-1} * g(a) * g(b) \in H$, таким образом,

$$H * g(a * b) = H * g(a) * H * g(b)$$

для всех $a, b \in \mathfrak{N}$.

Лемма 1 доказана.

Введем обозначение

$$\mathfrak{H} = \ker \alpha = \{a \in \mathfrak{N} \mid g(a) \in H\}.$$

Пусть $\mathfrak{B}$ — произвольная фиксированная система представителей смежных классов группы $\mathfrak{N}$ по подгруппе $\mathfrak{H}$.

Теорема 1. *Справедливы равенства*

$$\mathfrak{M} = \bigcup_{b \in \mathfrak{B}} (\mathfrak{H} * b) \times (H * g(b)), \quad (20)$$

$$m = dr, \quad (21)$$

и существует $N_1 \geq 1$, для которого для чисел s вида

$$s = Nrd + ld + v \quad (22)$$

при произвольных $v \in \{0, 1, \dots, d-1\}$, $l \in \{0, 1, \dots, r-1\}$ и $N \geq N_1$ справедливо равенство

$$M^s = (e_G, x^l) * (a_1^v, \sigma_1^v) * \mathfrak{M}. \quad (23)$$

Доказательство. Из следствия 1 работы [4] и равенства (4) вытекает, что существует $N_1 \geq 1$, для которого при выполнении (22) верно равенство

$$M^s = \bigcup_{a \in \mathfrak{N} * a_1^v} \{a\} \times (x^l * H * g(a)). \quad (24)$$

Из (24) следует, что $|M^s| = |\mathfrak{N}| |H|$ для всех $s \geq N_1 r d$. Таким образом (см. [2]), множества M^s , $s \geq N_1 r d$, суть смежные классы группы $\mathfrak{G}$ по нормальному делителю $\mathfrak{M}$. Кроме того,

$$M^{N_1 r d} = \bigcup_{b \in \mathfrak{N}} \{b\} \times (H * g(b)).$$

Так как α — гомоморфизм, справедливо равенство $Hg(e_G) = H$, таким образом, слой $M^{N_1 r d}$ содержит единичный элемент (e_G, e_G) группы $\mathfrak{G}$ и поэтому совпадает с $\mathfrak{M}$. Следовательно,

$$\mathfrak{M} = \bigcup_{b \in \mathfrak{N}} \{b\} \times (H * g(b)). \quad (25)$$

В силу леммы 1, для всех $b_1, b_2 \in \mathfrak{N}$ равенство $H * g(b_1) = H * g(b_2)$ справедливо тогда и только тогда, когда $\mathfrak{H} * b_1 = \mathfrak{H} * b_2$. Поэтому из (25) следует равенство (20).

Зафиксируем в (22) и (24) числа $v \in \{0, 1, \dots, d-1\}$ и $l \in \{0, 1, \dots, r-1\}$. Если $a = a_1^v * b \in \mathfrak{N} * a_1^v$, $b \in \mathfrak{N}$, то аналогично доказательству леммы 1 можно показать, что для всех $a \in \mathfrak{N} * a_1^v$

$$H * g(a) = H * g(a_1^v) * g(b) = \sigma_1^v * H * g(b). \quad (26)$$

Подставив (26) в (24), с учетом (25), (20) получим равенство (23). Заметим, что множество в правой части (23) содержит пару (e_G, e_G) тогда и только тогда, когда $v = l = 0$. Из этого замечания следует равенство (21). Теорема 1 доказана.

Отметим, что равенство (20) соответствует описанию подпрямых произведений из теоремы 5.5.1 книги [5].

Основная трудность в применении теоремы 1 заключается в необходимости построения системы определяющих соотношений $z_1, \dots, z_p$ группы $\mathfrak{A}$, а также слов z_a , $a \in \mathfrak{N}$, для определения элементов $g(a)$, $a \in \mathfrak{N}$. Представляют интерес условия на множество M , при выполнении которых указанных трудностей можно избежать.

Во-первых, мы будем предполагать, что

$$\mathfrak{N} = \langle \{a_1^{-1} * a_2, \dots, a_1^{-1} * a_s\} \rangle. \quad (27)$$

Условие (27) означает, что минимальная подгруппа группы $\mathfrak{A}$ среди всех ее подгрупп L , для которых $a_i \in a_1 * L$ для всех $i \in \{1, \dots, s\}$, является нормальным делителем $\mathfrak{A}$. Данное условие заведомо выполнено, если $\{a_1, \dots, a_s\} \ni e_G$, либо в случае коммутативности группы $\mathfrak{A}$, то есть когда $a_i * a_j = a_j * a_i$ для всех $i, j \in \{1, \dots, s\}$.

Во-вторых, будем предполагать, что существует элемент $h_1 \in G$, для которого для всех $k \in \{1, \dots, s\}$

$$(a_k, h_1 * a_k) \in M, \quad (28)$$

В этом случае будем считать выполненным соотношение $\sigma_k = h_1 * a_k$ для всех $k \in \{1, \dots, s\}$. Заметим, что из (27), (28) следует включение $\mathfrak{N} \subset T$.

Следствие 1. Пусть выполнены условия (27) и (28), тогда справедливы следующие утверждения.

Подгруппа H совпадает с минимальной подгруппой среди всех подгрупп L группы G , для которых выполнено условие (11), а также справедливы соотношения

$$\sigma_k * L = L * \sigma_k, \quad (29)$$

$$L * h_1 * a_1^{-1} * a_k = L * a_1^{-1} * a_k * h_1 \quad (30)$$

для всех $k \in \{1, \dots, s\}$. Кроме того,

$$H * x = H * \sigma_1^d * a_1^{-d}, \quad (31)$$

$$r = \min\{l \geq 1 \mid (\sigma_1^d * a_1^{-d})^l \in H\}, \quad (32)$$

$$\mathfrak{H} = \mathfrak{N} \cap H, \quad (33)$$

$$\mathfrak{M} = \bigcup_{b \in \mathfrak{B}} ((\mathfrak{N} \cap H) * b) \times (H * b), \quad (34)$$

где $\mathfrak{B}$ — произвольная система представителей смежных классов группы $\mathfrak{N}$ по подгруппе $\mathfrak{N} \cap H$,

$$M^s = (e_G, (\sigma_1^d * a_1^{-d})^l) \times (a_1^v, \sigma_1^v) \times \mathfrak{M}, \quad s = v + d(l + rN) \quad (35)$$

для всех $N \geq N_1$, $v \in \{0, 1, \dots, d-1\}$ и $l \in \{0, 1, \dots, r-1\}$.

Доказательство. Обозначим через H^* минимальную подгруппу среди всех подгрупп L группы G , удовлетворяющих соотношениям (11), (29) и (30). Докажем, что

$$H^* \subset H. \quad (36)$$

Условие (12) выполнено при $L = H$, так что и (29) выполняется при $L = H$. Следовательно, для доказательства (36) достаточно показать, что соотношение (30) выполняется при $L = H$.

Из леммы 2 работы [4] следует, что подгруппа H является минимальной подгруппой среди всех подгрупп L группы G при всех $z \in C_0$ таких, что $l(z) = 0$, удовлетворяющих соотношению

$$\Omega(z) \subset L. \quad (37)$$

В частности, (37) верно и при $L = H$, то есть при всех $z \in C_0$ таких, что $l(z) = 0$,

$$\Omega(z) \subset H. \quad (38)$$

Из условия (28) следует равенство (см. (7))

$$g(a_1^{-1} * a_k) = \sigma_1^{-1} * \sigma_k = a_1^{-1} * a_k \quad (39)$$

для всех $k \in \{1, \dots, s\}$.

Из (39) и определения гомоморфизма $\alpha: \mathfrak{N} \rightarrow T/H$ следует, что

$$\alpha(a_1^{-1} * a_k) = H * g(a_1^{-1} * a_k) = H * a_1^{-1} * a_k.$$

Но тогда, так как α — гомоморфизм, из (27) следует, что $\alpha(b) = H * b$ для всех $b \in \mathfrak{N}$, то есть для всех $b \in \mathfrak{N}$

$$H * g(b) = H * b. \quad (40)$$

Зафиксируем $k \in \{1, \dots, s\}$ и пусть

$$b = a_1^{-1} * a_k, \quad b' = a_1^{-1} * b^{-1} * a_1, \quad b, b' \in \mathfrak{N}.$$

Рассмотрим слово $z = (z_b, a_1, z_{b'}, a_1^{-1})$, тогда (см. (7))

$$g(z) = g(z_b) * \sigma_1 * g(z_{b'}) \sigma_1^{-1}. \quad (41)$$

Поскольку $H \triangleleft T$, согласно (40) и (41)

$$\begin{aligned} H * g(z) &= H * g(z_b) * H * \sigma_1 * H * g(z_{b'}) * H * \sigma_1^{-1} \\ &= H * g(b) * H * \sigma_1 * H * g(b') * H * \sigma_1^{-1} \\ &= H * b * H * \sigma_1 * H * b' * H * \sigma_1^{-1} \\ &= H * (a_1^{-1} * a_k) * h_1 * (a_1^{-1} * a_k)^{-1} * h_1^{-1}. \end{aligned} \quad (42)$$

С другой стороны, ввиду (6), при $z \in C_0$ таких, что $l(z) = 0$,

$$a(z) = b * a_1 * b' * a_1^{-1} = a_1^{-1} * a_k * a_1 * a_1^{-1} * a_k^{-1} * a_1^2 * a_1^{-1} = e_G.$$

Согласно (38), отсюда следует, что $g(z) \in H$, то есть, с учетом (42),

$$H * (a_1^{-1} * a_k) * h_1 = H * h_1 * (a_1^{-1} * a_k).$$

Таким образом, соотношение (30) при $L = H$, а с ним и включение (36) доказано.

Докажем обратное включение

$$H \subset H^*. \quad (43)$$

Для доказательства (43) достаточно показать, что соотношение (37) выполняется при $L = H^*$.

Соотношения (11), (29) и (30) выполняются при $L = H^*$, таким образом, $H^* \triangleleft T$ и при всех $k \in \{1, \dots, s\}$

$$M_k \subset H^* * \sigma_k, \quad (44)$$

$$H^* * h_1 * a_1^{-1} * a_k = H^* * a_1^{-1} * a_k * h_1. \quad (45)$$

Для элементов группы G

$$g_0 = e_G, \quad g_\nu = \sigma_1^\nu * a_1^{-\nu}, \quad \nu \in \{1, \dots, d\},$$

докажем, что при всех $\nu \in \{1, \dots, d\}$, $b \in \mathfrak{N} * a_1^{\nu-1}$ и $k \in \{1, \dots, s\}$

$$b * M_k * (ba_k)^{-1} \subset g_{\nu-1}^{-1} * H^* * g_\nu. \quad (46)$$

Сначала рассмотрим случай $\nu = 1$, зафиксируем произвольно $k \in \{1, \dots, s\}$. Так как $g_1 = \sigma_1 * a_1^{-1} = h_1$, в силу (44) включение (46) при $\nu = 1$ эквивалентно соотношению

$$b * H^* * h_1 * b^{-1} = H^* * h_1, \quad b \in \mathfrak{N}. \quad (47)$$

Так как $H^* \triangleleft T$, $T \supset \mathfrak{N}$, согласно (45),

$$(a_1^{-1} * a_q) * H^* * h_1 * (a_1^{-1} * a_q)^{-1} = H^* * h_1, \quad q \in \{1, \dots, s\}. \quad (48)$$

Из (27) и (48) следует (47), то есть (46) при $\nu = 1$ доказано.

Пусть $d \geq 2$, $k \in \{1, \dots, s\}$, $\nu \in \{2, \dots, d\}$, $b \in \mathfrak{N} * a_1^{\nu-1}$, $b = a_1^{\nu-1} * b'$, $b' \in \mathfrak{N}$. Как было показано (случай $\nu = 1$), $b' * M_k * (b' * a_k)^{-1} \subset H^* * h_1$, следовательно, так как $\sigma_1 * H^* = H^* * \sigma_1$,

$$\begin{aligned} b * M_k * (b * a_k)^{-1} &= a_1^{\nu-1} * b' * M_k * (b' * a_k)^{-1} * a_1^{1-\nu} \\ &\subset a_1^{\nu-1} * H^* * h_1 * a_1^{1-\nu} = a_1^{\nu-1} * \sigma_1^{1-\nu} * H^* * \sigma^\nu * a_1^{-\nu} = g_{\nu-1}^{-1} * H^* * g_\nu, \end{aligned}$$

и соотношение (46) доказано полностью.

Рассмотрим теперь произвольное слово $z \in C$ вида (5), пусть

$$\varepsilon_1 + \varepsilon_2 + \dots + \varepsilon_N = \nu + sd,$$

где $s \in \mathbf{Z}$, $\nu \in \{1, \dots, d\}$. Докажем включение

$$\Omega(z) \subset H^* * (g_d)^s * g_\nu * a(z). \quad (49)$$

Применим индукцию по N .

Пусть $N = 1$, $\varepsilon_1 = 1$, $z = a_{k_1}$, $a(z) = a_{k_1}$, $\nu = 1$, $s = 0$. Тогда с учетом (44), (8)

$$\Omega(z) = M_{k_1} \subset H^* * \sigma_{k_1} = H^* * g_1 * a(z),$$

и (49) выполнено.

Пусть $N = 1$, $\varepsilon_1 = -1$, $z = a_{k_1}^{-1}$, $a(z) = a_{k_1}^{-1}$, $\nu = d - 1$, $s = -1$. Возьмем в соотношении (46) $k = k_1$, $b = a_{k_1}^{-1}$, тогда $b \in \mathfrak{N} * a_1^{d-1}$ и

$$a_{k_1}^{-1} * M_{k_1} \subset g_{d-1}^{-1} * H^* * g_d. \quad (50)$$

Заметим, что $g_d \in T$, следовательно,

$$g_d * H^* = H^* * g_d. \quad (51)$$

Из соотношений (50), (51) следует, что $M_{k_1}^{-1} \subset H^* * g_d^{-1} * g_{d-1} * a(z)$, то есть (49) выполнено.

Предположим, что для некоторого $N \geq 1$ соотношение (49) выполняется для всех слов z вида (5). Пусть слово $z \in C$ имеет вид

$$\begin{aligned} z &= (a_{k_1}^{\varepsilon_1}, a_{k_2}^{\varepsilon_2}, \dots, a_{k_{N+1}}^{\varepsilon_{N+1}}), \\ \varepsilon_1 + \dots + \varepsilon_{N+1} &= \nu + sd, \quad \nu \in \{1, \dots, d\}, \quad s \in \mathbf{Z}; \end{aligned} \quad (52)$$

докажем, что и для слова z вида (52) верно соотношение (49). Введем обозначение

$$v = (a_{k_1}^{\varepsilon_1}, a_{k_2}^{\varepsilon_2}, \dots, a_{k_N}^{\varepsilon_N}),$$

тогда $z = (v, a_{k_{N+1}}^{\varepsilon_{N+1}})$ и в силу (8)

$$\Omega(z) = \Omega(v) * M_{k_{N+1}}^{\varepsilon_{N+1}}. \quad (53)$$

Рассмотрим случай, когда в (52) $\varepsilon_{N+1} = 1$. Здесь имеют место представления $\varepsilon_1 + \dots + \varepsilon_N = \nu - 1 + sd$ при $\nu \in \{2, \dots, d\}$ и $\varepsilon_1 + \dots + \varepsilon_N = d + (s - 1)d$ при $\nu = 1$. Так как (49) верно по предположению индукции для слова v , в обоих случаях

$$\Omega(v) \subset H^* * (g_d)^s * g_{\nu-1} * a(v). \quad (54)$$

Пусть в соотношении (46) $k = k_{N+1}$, $b = a(v)$, тогда $b \in \mathfrak{N} * a_1^{v-1}$, $b * a_{k_{N+1}} = a(z)$ и $a(v) * M_{k_{N+1}} * a(z)^{-1} \subset g_{v-1}^{-1} * H^* * g_v$, то есть

$$M_{k_{N+1}} \subset a(v)^{-1} * g_{v-1}^{-1} * H^* * g_v * a(z). \quad (55)$$

Подставив (54), (55) в (53) и используя (51), получим, что (49) выполняется для слова z .

Рассмотрим случай, когда в (52) $\varepsilon_{N+1} = -1$ и $v \in \{1, \dots, d-1\}$. Здесь справедливо равенство

$$\varepsilon_1 + \dots + \varepsilon_N = v + 1 + sd.$$

По предположению индукции (49) верно для слова v , поэтому

$$\Omega(v) \subset H^* * (gd)^s * g_{v+1} * a(v). \quad (56)$$

Пусть в соотношении (46) $k = k_{N+1}$, $b = a(z)$, тогда $b * a_k = a(v)$, $b \in \mathfrak{N} * a_1^v$ и

$$a(z) * M_{k_{N+1}} * a(v)^{-1} \subset g_v^{-1} * H^* * g_{v+1}, \quad (57)$$

то есть

$$M_{k_{N+1}}^{-1} \subset a(v)^{-1} * g_{v+1}^{-1} * H^* * g_v * a(z). \quad (58)$$

Подставив (56) и (58) в (53) и воспользовавшись (51), получим, что (49) верно для z .

Рассмотрим случай, когда в (52) $\varepsilon_{N+1} = -1$, $v = d$. Здесь

$$\varepsilon_1 + \dots + \varepsilon_N = 1 + (s+1)d.$$

По предположению индукции (49) верно для слова v , поэтому

$$\Omega(v) \subset H^* * (gd)^{s+1} * g_1 * a(v). \quad (59)$$

Пусть в соотношении (46) $k = k_{N+1}$, $b = a(z)$, тогда $b * a_k = a(v)$, $b \in \mathfrak{N}$ и

$$a(z) * M_{k_{N+1}} * a(v)^{-1} \subset H^* * g_1,$$

то есть

$$M_{k_{N+1}}^{-1} \subset a(v)^{-1} * g_1^{-1} * H^* * a(z). \quad (60)$$

Подставив (59) и (60) в (53) и используя (51), получим, что (49) верно для z вида (52) и в этом случае.

Итак соотношение (49) доказано полностью.

Пусть $z \in C_0$, $l(z) = 0$, тогда в представлении z в виде (5)

$$\varepsilon_1 + \dots + \varepsilon_N = d + d(-1).$$

Из соотношения (49) при $v = d$, $s = -1$, $a(z) = e_G$ следует, что $\Omega(z) \subset H^*$ для всех $z \in C_0$, $l(z) = 0$, таким образом, (37) верно при $L = H^*$, соотношение (43), а с ним и равенство $H = H^*$, полностью доказано.

Для доказательства (31) воспользуемся равенством (10). В представлении слова z_0 в виде (5) верны равенства

$$\varepsilon_1 + \dots + \varepsilon_N = d, \quad a(z_0) = e_G.$$

Но тогда из (49) следует, что

$$x = g(z_0) \in \Omega(z_0) \subset H^* * g_d = H^* * \sigma_1^d * a_1^{-d},$$

и (31) доказано.

Равенство (33) следует из определения $\mathfrak{H}$ и равенства (40), (32) следует из (31) и определения r , (34) и (35) следуют из (20), (23), (33) и (40). Следствие 1 доказано.

В случае $d = 1$ формулировка следствия 1 упрощается.

Следствие 2. Пусть множество $a_1, \dots, a_s$ не содержится в одном смежном классе группы $\mathfrak{A} = \langle a_1, \dots, a_s \rangle$ по ее собственной подгруппе и выполнено условие (28). Тогда подгруппа H есть минимальная подгруппа среди всех подгрупп L группы G , удовлетворяющих соотношениям (11), (29) и условию

$$L * a_k * h_1 = L * h_1 * a_k, \quad k \in \{1, \dots, s\};$$

верны равенства

$$r = \min \left\{ l \geq 1 \mod h_1^l \in H \right\},$$

$$\mathfrak{M} = \bigcup_{b \in \mathfrak{B}} ((\mathfrak{A} \cap H) * b) \times (H * b),$$

где $\mathfrak{B}$ — произвольная система представителей смежных классов группы $\mathfrak{A}$ по ее подгруппе $\mathfrak{A} \cap H$; и равенства

$$M^s = (e_G, h_1^l) * \mathfrak{M}, \quad s = l + rN,$$

для всех $N \geq N_1$, $l \in \{0, 1, \dots, r-1\}$.

Следствия 1 и 2 представляют интерес при исследовании линейной авторегрессии со случайным управлением на конечной группе (см. [1]).

Пусть $(F, \cdot)$ — некоторая конечная группа, $(\text{Aut } F, \circ)$ — группа автоморфизмов F . Образ элемента $g \in F$ при преобразовании $A \in \text{Aut } F$ будем обозначать через g^A . Значок $\circ$ обозначает композицию отображений, таким образом, $g^{(A \circ B)} = (g^B)^A$ для всех $g \in F$ и всех $A, B \in \text{Aut } F$.

Пусть $\mu^{(0)}$ — некоторая случайная величина со значениями в F , (ξ_N, ζ_N) , $N \geq 1$, — последовательность одинаково распределенных случайных величин, принимающих значения в декартовом произведении $F \times \text{Aut } F$. Будем предполагать, что случайные величины $\mu^{(0)}$, (ξ_N, ζ_N) , $N \geq 1$, независимы, ξ_N и ζ_N , вообще говоря, зависимы при каждом $N \geq 1$. Построим по индукции последовательность случайных величин со значениями в группе F

$$\mu^{(N)} = \xi_N(\mu^{(N-1)})^{\zeta_N}, \quad N \geq 1.$$

Далее, если не оговорено противное, будем предполагать, что $\mu^{(0)} = e_F$.

Для всех $N \in \mathbb{N}$ и $A \in \text{Aut } G$ таких, что $\mathbf{P}(\zeta_N \circ \zeta_{N-1} \circ \dots \circ \zeta_1 = A) > 0$, введем случайную величину $\mu_A^{(N)}$ на группе G , распределение которой совпадает с условным распределением случайной величины $\mu^{(N)}$ при условии

$$\zeta_N \circ \zeta_{N-1} \circ \dots \circ \zeta_1 = A, \mu^{(0)} = e_F.$$

Предельное поведение последовательностей распределений случайных величин $\mu_A^{(N)}$, $N \geq 1$, $A \in \text{Aut } F$, $\mathbf{P}(\xi_N \circ \dots \circ \xi_1 = A) > 0$, при $N \rightarrow \infty$ описано в [1]. На основе этих результатов и формулы полной вероятности

$$\mathbf{P}(\mu^{(N)} = \sigma) = \sum_{A \in \text{Aut } F} \mathbf{P}(\xi_N \circ \dots \circ \xi_1 = A) \mathbf{P}(\mu_A^{(N)} = \sigma), \quad \sigma \in F, \quad (61)$$

может быть исследовано предельное поведение последовательности распределений случайных величин $\mu^{(N)}$, $N \geq 1$.

Однако применение данного подхода даже в части определения условий предельной равновероятности на группе F для распределений $\mu^{(N)}$ при $N \rightarrow \infty$ вызывает значительные трудности (см. [3]). Доказанные выше следствия 1 и 2 позволяют упростить исследование в некоторых довольно широких частных случаях.

Приведенным выше обозначениям соответствуют следующие:

$$\begin{aligned} \Omega(\xi) &= \{A_1, A_2, \dots, A_s\} \subset \text{Aut } F, \\ \mathfrak{A} &= \langle A_1, A_2, \dots, A_s \rangle \subset \text{Aut } F, \end{aligned}$$

$\mathfrak{N}$ — минимальный нормальный делитель группы $\mathfrak{A}$ среди всех ее нормальных делителей L , для которых $\Omega(\xi) \subset A_1 \circ L$, $d = |\mathfrak{A} : \mathfrak{N}|$.

Для $k \in \{1, \dots, s\}$ пусть $\xi^{(k)}$ — случайная величина со значениями в F , распределение которой есть условное распределение ξ при условии $\xi = A_k$.

Пусть выполнены условия

$$\langle A_1^{-1} \circ A_2, \dots, A_1^{-1} \circ A_s \rangle = \mathfrak{N}, \quad (62)$$

$$\bigcap_{k=1}^s \Omega(\xi^{(k)}) \neq \emptyset. \quad (63)$$

Зафиксируем произвольный элемент

$$h_1 \in \bigcap_{k=1}^s \Omega(\xi^{(k)}).$$

Пусть H — минимальная подгруппа среди всех подгрупп L группы F , удовлетворяющих соотношениям

$$\Omega(\xi) \subset Lh_1, \quad (64)$$

$$L^{A_k} = h_1^{-1} Lh_1, \quad (65)$$

$$(Lh_1)^{A_1} = (Lh_1)^{A_k} \quad (66)$$

для всех $k \in \{1, \dots, s\}$. Пусть

$$x = h_1 h_1^{A_1} \dots h_1^{(A_1)^{d-1}}, \quad r = \min\{l \geq 1 : x^l \in H\}.$$

Следствие 3. Если выполнены условия (62), (63), то для всех $v \in \{0, 1, \dots, d-1\}$ и всех $l \in \{0, 1, \dots, r-1\}$ последовательность распределений случайных величин $\mu^{(sN)}$, $s_N = v + d(l + N)$, $N \geq 1$, имеет своим пределом равномерное распределение на множестве

$$x^l H h_1 h_1^{A_1} \dots h_1^{(A_1)^v}. \quad (67)$$

Последовательность распределений случайных величин $\mu^{(N)}$, $N \geq 1$, имеет при $N \rightarrow \infty$ предельное равномерное распределение на группе F при произвольном распределении $\mu^{(0)}$ тогда и только тогда, когда группа F не содержит собственной подгруппы L , удовлетворяющей соотношениям (64), (65), (66).

Доказательство. Покажем сначала, что исследование предельного поведения распределений случайных величин $\mu_A^{(N)}$ при $N \rightarrow \infty$ можно свести к изучению предельного поведения распределений случайных величин $\omega_a^{(N)}$ в специально выбранной схеме произведений со сдвигом независимых случайных величин.

На множестве $F \times \text{Aut } F$ определим бинарную операцию $*$, полагая

$$(g_1, A_1) * (g_2, A_2) = (g_1 g_2^{A_1}, A_1 \circ A_2)$$

для всех $g_1, g_2 \in F$ и всех $A_1, A_2 \in \text{Aut } F$.

Множество $G = F \times \text{Aut } F$ относительно операции $*$ является группой, $(G, *)$ — голоморф группы F , или полупрямое произведение F на $\text{Aut } F$. Пусть E — единичный автоморфизм, отождествим элементы $g \in F$ с элементами вида $(g, E) \in G$, элементы $A \in \text{Aut } F$ с элементами вида (e_F, A) . Таким образом, можно считать, что F и $\text{Aut } F$ — подгруппы группы G , $(g, A) = g * A$ для всех $g \in F$ и $A \in \text{Aut } F$, $\xi_N, \zeta_N, \mu^{(N)}$, $N \geq 1$, — случайные величины со значениями в G . Индукцией по $N \geq 1$ можно показать, что верно равенство

$$\xi_N * \zeta_N * \dots * \xi_1 * \zeta_1 = \mu^{(N)} * \zeta_N * \dots * \zeta_1 = (\mu^{(N)}, \zeta_N \circ \dots \circ \zeta_1). \quad (68)$$

Рассмотрим случайные величины со значениями в G

$$\begin{aligned} \omega^{(N)} &= \xi_1 * \zeta_1 * \dots * \xi_N * \zeta_N, \\ \chi^{(N)} &= \zeta_1 * \dots * \zeta_N. \end{aligned}$$

Как и в (68), случайная величина $\omega^{(N)} * \chi^{(N)-1}$ принимает значения в подгруппе F группы G , случайная величина $\zeta_1 * \dots * \zeta_N$ — в подгруппе $\text{Aut } F$ группы G , таким образом,

$$\omega^{(N)} = (\omega^{(N)} * \chi^{(N)-1}, \chi^{(N)}). \quad (69)$$

Так как случайные пары (ξ_t, ζ_t) , $t \in \{1, \dots, N\}$, независимы и одинаково распределены, распределения случайных величин (68) и $\omega^{(N)}$ совпадают. Следовательно, согласно (69), для любого $A \in \text{Aut } F$ такого, что $\mathbf{P}(\zeta_N \circ \dots \circ \zeta_1 = A) > 0$, распределение случайной величины $\mu_A^{(N)}$ совпадает с условным распределением $\omega^{(N)} * \chi^{(N)-1}$ при условии $\chi^{(N)} = A$, то есть с распределением случайной величины $\omega_A^{(N)} * A^{-1}$. Таким образом,

$$\mathbf{P}(\mu_A^{(N)} = \sigma) = \mathbf{P}(\omega_A^{(N)} * A^{-1} = \sigma), \quad \mathbf{P}(\zeta_N \circ \dots \circ \zeta_1 = A) > 0, \quad (70)$$

для всех $\sigma \in F$, $A \in \text{Aut } F$, $N \geq 1$.

Из соотношений (62) и (63) следует, что выполнены условия (27) и (28). Согласно следствию 1, подгруппа H есть минимальная подгруппа среди всех подгрупп L группы G , удовлетворяющих соотношениям

$$\Omega(\xi) \subset L * h_1, \quad (71)$$

$$L * g = g * L, \quad g \in \Omega(\xi * \zeta), \quad (72)$$

$$(L * h_1) * (A_1^{-1} * A_k) = (A_1^{-1} * A_k) * L * h_1, \quad k \in \{1, \dots, s\}. \quad (73)$$

Число

$$r = \min\{l \geq 1 \mid ((h_1 * A_1)^d * A_1^{-d})^l \in H\}.$$

Для любых $v \in \{0, 1, \dots, d-1\}$, $A \in A_1^v * \mathfrak{N}$, $l \in \{0, 1, \dots, r-1\}$ последовательность распределений случайных величин $\omega_A^{(s_N)}$, $s_N = v + d(l + Nr)$, $A \in \Omega(\zeta)^{s_N}$, $N \geq 1$, имеет своим пределом равномерное распределение на множестве

$$H * ((h_1 * A_1)^d * A_1^{-d})^l * (h_1 * A_1)^v * A_1^{-v} * A. \quad (74)$$

Условия (64), (65) и (66) на подгруппу H суть переформулировка соотношений (71), (72), (73) для полупрямого произведения группы F на ее группу автоморфизмов. Наконец, множество (67) есть множество (74), умноженное справа на A^{-1} .

Таким образом, из следствия 1 и соотношения (70) получаем, что для всех $v \in \{0, 1, \dots, d-1\}$, всех $A \in \mathfrak{N} \circ A_1^v$ и всех $l \in \{0, 1, \dots, r-1\}$ последовательность распределений случайных величин $\mu_A^{(s_N)}$, $s_N = v + d(l + Nr)$, $\mathbf{P}(\zeta_{s_N} \circ \dots \circ \zeta_1 = A) > 0$, $N \geq 1$, имеет своим пределом при $N \rightarrow \infty$ равномерное распределение на множестве (67). Так как множество (67) не зависит от выбора $A \in \mathfrak{N} \circ A_1^v$, отсюда и из (61) следует доказываемое утверждение.

Частным случаем следствия 3 является следующее утверждение.

Пусть выполнено соотношение (63), а также верно равенство

$$\langle A_1^{-1} \circ A_2, \dots, A_1^{-1} \circ A_s \rangle = \mathfrak{A}. \quad (75)$$

Обозначим через H минимальную подгруппу среди всех подгрупп L группы F , удовлетворяющих соотношениям

$$\Omega(\xi) \subset Lh_1, \quad (76)$$

$$Lh_1 = h_1L, \quad (77)$$

$$(Lh_1)^{A_k} = Lh_1, \quad k \in \{1, \dots, s\}. \quad (78)$$

Пусть

$$r = \min\{l \geq 1 \mid h_1^l \in H\}.$$

Следствие 4. При выполнении (63), (75) для всех $l \in \{0, 1, \dots, r-1\}$ последовательность распределений случайных величин $\mu^{(s_N)}$, $s_N = l + Nr$, $N \geq 1$, имеет своим пределом при $N \rightarrow \infty$ равномерное распределение на множестве Hh_1^l .

Последовательность распределений случайных величин $\mu^{(N)}$, $N \geq 1$, имеет при $N \rightarrow \infty$ предельное равномерное распределение на группе F при произвольном распределении $\mu^{(0)}$ тогда и только тогда, когда группа F не содержит собственной подгруппы L , удовлетворяющей соотношениям (76), (77), (78).

Следствия 3 и 4 в частных случаях, когда автоморфизмы $A_1, A_2, \dots, A_s$ попарно перестановочны, либо когда множество $\Omega(\zeta)$ содержит единичный автоморфизм, доказаны другим методом Б. В. Евтеевым в 1976.

Список литературы

1. Горчинский Ю. Н., Круглов И. А., Капитонов В. М., Вопросы теории распределений на конечных группах. *Труды по дискретной математике* (1997) **1**, 85–112.
2. Глухов М. М., О числовых параметрах, связанных с заданием конечных групп системами образующих элементов. *Труды по дискретной математике* (1997) **1**, 43–66.
3. Круглов И. А., Условия предельной равновероятности распределений в схеме линейной авторегрессии со случайным управлением на конечной группе. *Дискретная математика* (2005) **17**, №3, 12–18.
4. Круглов И. А., Произведения со сдвигом независимых случайных величин со значениями в конечных группах. *Дискретная математика* (2007) **19**, №1, 40–49.
5. Холл М., *Теория групп*. ИЛ, Москва, 1962.

Статья поступила 15.12.2008.