Math-Net.Ru

Общероссийский математический портал

И. А. Круглов, Произведения со сдвигом независимых случайных величин со значениями в конечных группах, *Дискрет. матем.*, 2007, том 19, выпуск 1, 40–49

DOI: <https://doi.org/10.4213/dm6>

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: 34.227.88.159

26 апреля 2023 г., 15:26:30

Произведения со сдвигом независимых случайных величин со значениями в конечных группах

© 2007 г. И. А. Круглов

Рассматриваются последовательности случайных величин

$$\chi^{(N)} = \zeta_1 \zeta_2 \dots \zeta_N, \quad \omega^{(N)} = \xi_1 \zeta_1 \xi_2 \zeta_2 \dots \xi_N \zeta_N, \quad N \geq 1,$$

где (ξ_N, ζ_N) , $N \geq 1$, — последовательность независимых одинаково распределенных случайных величин, принимающих значения в декартовом произведении $G \times G$, $(G; \cdot)$ — конечная группа. Изучается степень зависимости случайных величин $\chi^{(N)}$ и $\omega^{(N)}$, такая задача возникает при исследовании свойств одного класса алгоритмов защиты информации. В связи с этой задачей изучается случайная величина $\omega_a^{(N)}$ со значениями в G , распределение которой совпадает с условным распределением случайной величины $\omega^{(N)}$ при условии, что $\chi^{(N)} = a$, где $a \in G$ таково, что $\mathbf{P}\{\chi^{(N)} = a\} > 0$. В работе указаны условия сходимости и найдены предельные распределения при $N \rightarrow \infty$ для $\omega_a^{(s_N)}$, где s_N — последовательность целых чисел, стремящаяся к бесконечности, такая, что $\mathbf{P}\{\chi^{(s_N)} = a\} > 0$.

Работа выполнена при поддержке программой Президента Российской Федерации поддержки ведущих научных школ, грант НШ 8564.2006.10.

Пусть $(G; \cdot)$ — конечная группа, (ξ_N, ζ_N) , $N \geq 1$, — последовательность независимых одинаково распределенных случайных величин, принимающих значения в декартовом произведении $G \times G$. Положим

$$\chi^{(N)} = \zeta_1 \zeta_2 \dots \zeta_N, \quad \omega^{(N)} = \xi_1 \zeta_1 \xi_2 \zeta_2 \dots \xi_N \zeta_N, \quad N \geq 1.$$

Для каждого N случайную величину $\omega^{(N)}$ можно рассматривать как произведение сомножителей, каждый из которых получен сдвигом ξ_k сомножителя ζ_k из произведения $\chi^{(N)}$; при этом сдвиг ξ_k случаен, и его значение, вообще говоря, зависит от значения сдвигаемого сомножителя ζ_k . Случайные величины $\omega^{(N)}$ и $\chi^{(N)}$ являются зависимыми, в целом эта зависимость ослабевает с ростом N . Задача оценки степени зависимости между случайными величинами $\chi^{(N)}$ и $\omega^{(N)}$ возникает в связи с исследованием свойств одного класса алгоритмов защиты информации.

Для $a \in G$ и натурального числа N таких, что вероятность $\mathbf{P}(\chi^{(N)} = a) > 0$, обозначим через $\omega_a^{(N)}$ случайную величину со значениями в группе G , распределение которой совпадает с условным распределением случайной величины $\omega^{(N)}$ при условии $\chi^{(N)} = a$.

В работе указаны условия сходимости и найдены предельные распределения для последовательностей случайных величин $\omega_a^{(s_N)}$, где a — некоторый фиксированный элемент G и s_N , $N \geq 1$, — последовательность натуральных чисел такие, что $s_N \rightarrow \infty$ при $N \rightarrow \infty$ и $\mathbf{P}(\chi^{(s_N)} = a) > 0$ для всех $N \geq 1$.

Введем обозначения, необходимые для формулировки основной теоремы. Для произвольной случайной величины η со значениями в G пусть

$$\Omega(\eta) = \{g \in G \mid \mathbf{P}(\eta = g) > 0\}$$

— носитель распределения случайной величины η . Пусть

$$\Omega(\zeta_1) = \{a_1, a_2, \dots, a_s\},$$

где $a_i \neq a_j$, если $i \neq j$.

Пусть $\mathfrak{A}$ — подгруппа группы G , порожденная множеством $\Omega(\zeta_1)$, $\mathfrak{N}$ — минимальный нормальный делитель группы $\mathfrak{A}$ среди ее нормальных делителей L , удовлетворяющих условию $\Omega(\zeta_1) \subset a_1 L$, обозначим через $d = |\mathfrak{A} : \mathfrak{N}|$ индекс $\mathfrak{N}$ в $\mathfrak{A}$.

Для $k = 1, 2, \dots, s$ пусть

$$\Omega_k = \{g \in G \mid \mathbf{P}(\xi_1 = g, \zeta_1 = a_k) > 0\}, \quad M_k = \Omega_k a_k.$$

Тогда

$$\Omega(\xi_1 \zeta_1) = M_1 \cup M_2 \cup \dots \cup M_s.$$

Для $k = 1, 2, \dots, s$ зафиксируем произвольный элемент $g_k \in \Omega_k$. Словом в образующих $\Omega(\zeta_1)$ назовем последовательность

$$z = a_{k_1}^{\varepsilon_1} a_{k_2}^{\varepsilon_2} \dots a_{k_N}^{\varepsilon_N}, \quad k_1, k_2, \dots, k_N \in \{1, 2, \dots, s\}, \quad \varepsilon_1, \varepsilon_2, \dots, \varepsilon_N \in \{-1, 1\}. \quad (1)$$

Обозначим через C множество всех слов в алфавите $\{a_1, a_2, \dots, a_s\}$.

Для произвольных подмножеств $L_1, L_2 \subset G$ положим

$$\begin{aligned} L_1 L_2 &= \{\sigma_1 \sigma_2 \mid \sigma_1 \in L_1, \sigma_2 \in L_2\}, \\ L_1^{-1} &= \{\sigma^{-1} \mid \sigma \in L_1\}. \end{aligned}$$

Для каждого слова $z \in C$ вида (1) определим элемент группы $\mathfrak{A}$

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

элемент группы G

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

а также множество элементов группы G

$$\Omega(z) = M_{k_1}^{\varepsilon_1} M_{k_2}^{\varepsilon_2} \dots M_{k_N}^{\varepsilon_N} a(z)^{-1}. \quad (2)$$

Будем говорить, что слово z вида (1) 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 $\{a_1, \dots, a_s\}$, для всех $z \in C_0$ положим

$$l(z) = \frac{1}{d}(\varepsilon_1 + \varepsilon_2 + \dots + \varepsilon_N).$$

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

Так как группа $\mathfrak{A}$ конечна, существует конечная совокупность единичных слов $z_1, z_2, \dots, z_p$ в алфавите $\Omega(\zeta_1)$ такая, что система равенств

$$z_i = e_G, \quad i = 1, 2, \dots, p,$$

есть система определяющих соотношений группы $\mathfrak{A}$ относительно ее системы образующих $\Omega(\zeta_1)$ (см. [3]).

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

$$\Omega_k \subset Lg_k, \quad k = 1, 2, \dots, s, \quad (3)$$

$$(g_k a_k)(Lx) = (Lx)(g_k a_k), \quad k = 1, 2, \dots, s, \quad (4)$$

$$\Omega(z_i) \subset Lx^{l(z_i)}, \quad i = 1, 2, \dots, p. \quad (5)$$

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 раздела 2 в [1] однозначно определено число $v \in \{0, 1, \dots, d-1\}$, для которого $a \in \mathfrak{A}_1^v$, и существует слово $z_a \in C$ вида (1), представляющее a и удовлетворяющее равенству $\varepsilon_1 + \varepsilon_2 + \dots + \varepsilon_N = v$. Зафиксируем произвольно такое слово z_a и положим $g(a) = g(z_a)$. Кроме того, заметим, что распределения случайных величин $\omega_a^{(N)}$ не определены, если $N \not\equiv v \pmod{d}$ и определены для всех достаточно больших N таких, что $N \equiv v \pmod{d}$.

Теорема 1. Пусть $a \in \mathfrak{A}_1^v$, $v \in \{0, 1, \dots, d-1\}$, m_N , $N \geq 1$, — последовательность натуральных чисел, $m_N \rightarrow \infty$ при $N \rightarrow \infty$. Тогда последовательность распределений случайных величин

$$\omega_a^{(s_N)}, \quad s_N = v + m_N d, \quad N \geq 1 \quad (6)$$

имеет предел при $N \rightarrow \infty$ тогда и только тогда, когда существует такое $l \in \{0, 1, \dots, r-1\}$, что

$$m_N \equiv l \pmod{r}$$

при всех достаточно больших N . При выполнении этого условия предел последовательности распределений случайных величин (6) есть равновероятное распределение на множестве $Hx^l g(a)$.

Доказательство. Определим случайную величину со значениями в G , полагая

$$\mu_a^{(N)} = \omega_a^{(N)} a^{-1},$$

где $a \in \mathfrak{A}$ и $N \geq 1$ таковы, что выполняется условие $\mathbf{P}(x^{(N)} = a) > 0$. Покажем, что случайные величины $\mu_a^{(N)}$ можно рассматривать как произведения случайных величин, распределения которых определяются некоторой конечной простой однородной цепью

Маркова (см. раздел 3 в [2]). Пусть $\{b_1, b_2, \dots, b_n\}$ — множество элементов группы $\mathfrak{A}$, занумерованных в некотором порядке, $b_1 = e_G$. Рассмотрим конечную простую однородную цепь Маркова $\mathfrak{Z}$, множество состояний которой есть $\{b_1, b_2, \dots, b_n\}$, начальное состояние с вероятностью единица есть b_1 , и переходные вероятности для всех $i, j = 1, 2, \dots, n$ определяются равенством

$$p(i, j) = \mathbf{P}(\zeta_1 = b_i^{-1}b_j), \quad (7)$$

Из результатов раздела 2 работы [1] следует, что цепь Маркова $\mathfrak{Z}$ неразложима и множество $\mathfrak{A}$ ее состояний разбивается на d циклических классов $\mathfrak{N}, a_1\mathfrak{N}, \dots, a_1^{d-1}\mathfrak{N}$.

Для $k = 1, 2, \dots, s$ определим случайную величину $\xi^{(k)}$ как случайную величину со значениями в G , распределение которой совпадает с условным распределением случайной величины ξ_1 при условии $\zeta_1 = a_k$. Пары состояний $b_i, b_j, i, j \in \{1, \dots, n\}$, такой, что $p(i, j) > 0$, поставим в соответствие случайную величину $\xi_{i,j}$ со значениями в G , распределение которой определяется следующим образом: если $b_i^{-1}b_j = a_k$, где $k \in \{1, 2, \dots, s\}$ (см. (7)), то распределение $\xi_{i,j}$ есть распределение случайной величины $b_i\xi^{(k)}b_i^{-1}$.

Обозначим через $p^{(N)}(i, j)$, $i, j \in \{1, 2, \dots, n\}$, $n \geq 1$, вероятность перехода за N шагов цепи Маркова $\mathfrak{Z}$ из состояния a_i в состояние a_j . В соответствии с разделом 3 работы [2] можно считать, что заданы произведения $\eta_{i,j}^{(N)}$, $i, j \in \{1, 2, \dots, n\}$, $N \geq 1$, $p^{(N)}(i, j) > 0$, случайных величин со значениями в G , распределения которых определяются цепью Маркова $\mathfrak{Z}$ и исходными распределениями $\xi_{i,j}$, $i, j \in \{1, 2, \dots, n\}$, $p(i, j) > 0$.

Лемма 1. Для любых $j \in \{1, 2, \dots, n\}$ и $N \geq 1$

$$p^{(N)}(1, j) = \mathbf{P}(\kappa^{(N)} = b_j),$$

и если $p^{(N)}(1, j) > 0$, то распределения случайных величин $\mu_{b_j}^{(N)}$ и $\eta_{1,j}^{(N)}$ совпадают.

Доказательство. Обозначим через $b_{\alpha_1}, b_{\alpha_2}, \dots, b_{\alpha_{N+1}}$ случайную реализацию цепочки состояний цепи Маркова $\mathfrak{Z}$ в первых $N+1$ испытаниях. С вероятностью единица $b_{\alpha_1} = e_G$, поэтому для всех $j \in \{1, 2, \dots, n\}$

$$p^{(N)}(1, j) = \mathbf{P}(b_{\alpha_{N+1}} = b_j).$$

Каждой цепочке состояний $b_{i_2}, b_{i_3}, \dots, b_{i_N}$, удовлетворяющей условию

$$\mathbf{P}(b_{\alpha_2} = b_{i_2}, \dots, b_{\alpha_N} = b_{i_N}, b_{\alpha_{N+1}} = b_j) > 0, \quad (8)$$

взаимно однозначно соответствует последовательность элементов множества $\Omega(\zeta_1)$

$$a_{k_1} = b_{i_2}, a_{k_2} = b_{i_2}^{-1}b_{i_3}, \dots, a_{k_N} = b_{i_N}^{-1}b_j, \quad (9)$$

где $k_1, k_2, \dots, k_N \in \{1, 2, \dots, s\}$, при этом, согласно (7) и в силу независимости случайных величин $\zeta_1, \zeta_2, \dots, \zeta_N$ выполняются равенства

$$\begin{aligned} \mathbf{P}(b_{\alpha_2} = b_{i_2}, \dots, b_{\alpha_N} = b_{i_N}, b_{\alpha_{N+1}} = b_j) &= p(1, i_2)p(i_2, i_3) \dots p(i_{N-1}, i_N)p(i_N, j) \\ &= \mathbf{P}(\zeta_1 = a_{k_1})\mathbf{P}(\zeta_2 = a_{k_2}) \dots \mathbf{P}(\zeta_N = a_{k_N}), \end{aligned} \quad (10)$$

а также

$$\begin{aligned} p^{(N)}(1, j) &= \sum_{i_2=1}^n \dots \sum_{i_N=1}^n p(1, i_2) p(i_2, i_3) \dots p(i_N, j) \\ &= \sum_{k_1, \dots, k_N, a_{k_1} \dots a_{k_N} = b_j} \mathbf{P}(\xi_1 = a_{k_1}) \dots \mathbf{P}(\xi_N = a_{k_N}) = \mathbf{P}(x^{(N)} = b_j), \end{aligned}$$

и первое утверждение леммы доказано.

Для каждой цепочки состояний $b_{i_2}, b_{i_3}, \dots, b_{i_N}$ цепи Маркова $\mathfrak{Z}$, удовлетворяющей условию (8), условное распределение случайной величины $\eta_{1,j}^{(N)}$ при условии

$$b_{\alpha_1} = e_G, b_{\alpha_2} = b_{i_2}, \dots, b_{\alpha_N} = b_{i_N}, b_{\alpha_{N+1}} = b_j,$$

совпадает с распределением случайной величины

$$\varphi_1 b_{i_2} \varphi_2 b_{i_2}^{-1} b_{i_3} \varphi_3 \dots \varphi_{N-1} b_{i_{N-1}}^{-1} b_{i_N} \varphi_N b_{i_N}^{-1}, \quad (11)$$

где случайные величины $\varphi_1, \varphi_2, \dots, \varphi_N$ независимы и для каждого $l \in \{1, 2, \dots, N\}$ распределение случайной величины φ_l совпадает с распределением случайной величины $\xi^{(k_l)}$, а числа $k_1, \dots, k_N$, в свою очередь, определяются равенствами (9). Но тогда

$$b_{i_N} = a_{k_1} a_{k_2} \dots a_{k_{N-1}}, \quad b_j = a_{k_1} a_{k_2} \dots a_{k_N},$$

и случайная величина (11) совпадает со случайной величиной

$$\varphi_1 a_{k_1} \varphi_2 a_{k_2} \dots \varphi_N a_{k_N} b_j^{-1}. \quad (12)$$

Однако распределение случайной величины (12) совпадает с условным распределением случайной величины $\omega^{(N)}(x^{(N)})^{-1}$ при условии

$$\xi_1 = a_{k_1}, \xi_2 = a_{k_2}, \dots, \xi_N = a_{k_N}, \quad (13)$$

то есть с условным распределением случайной величины $\mu_{b_j}^{(N)}$ при условии (13). Учитывая равенства (10) и (7), по формуле полной вероятности получаем, что распределения случайных величин $\eta_{1,j}^{(N)}$ и $\mu_{b_j}^{(N)}$ совпадают.

Лемма 1 доказана.

Таким образом, для исследования предельного поведения последовательностей распределений случайных величин $\mu_a^{(N)}$, $a \in \mathfrak{A}$, можно воспользоваться результатами раздела 3 работы [2]. Графу Γ переходов цепи Маркова $\mathfrak{Z}$ соответствует граф Кэли правого регулярного представления группы $\mathfrak{A}$ относительно системы образующих $\{a_1, a_2, \dots, a_s\}$.

Каждому слову $z \in C$ вида (1) с числом букв N взаимно однозначно соответствует путь v в графе Γ с началом $b_1 = e_G$ и концом $b_j = a(z)$. При этом индукцией по N можно показать, что для множества $\Omega(v)$, определенного согласно обозначениям раздела 3 работы [2], верно равенство $\Omega(v) = \Omega(z)$. Отсюда следует, что каждому единичному слову z взаимно однозначно соответствует цикл v в графе Γ с концом b_1 , причем для всех $z \in C_0$ верны равенства

$$\Omega(v) = \Omega(z), \quad l(v) = l(z) \quad (14)$$

(в левых частях равенств (14) используются обозначения раздела 3 работы [2]). Из (14) следует, что в качестве введенного в разделе 3 статьи [2] элемента $x_1 \in G$ можно взять выбранный выше элемент x , а также, что введенная там же подгруппа H_1 группы G в нашем случае есть минимальная подгруппа среди таких подгрупп L группы G , что для всех $z \in C_0$

$$\Omega(z) \subset Lx^{l(z)}. \quad (15)$$

Заметим, что соотношение (15) выполняется при $L = H_1$, то есть для всех $z \in C_0$

$$\Omega(z) \subset H_1x^{l(z)}. \quad (16)$$

Кроме того, как следует из результатов раздела 3 статьи [2], для любого $h \in H_1$ существует такое единичное слово $z \in C_0$ в образующих $\Omega(\zeta_1)$, что $h \in \Omega(z)$ и $l(z) \neq 0$.

Лемма 2. *Справедливо равенство*

$$H_1 = H. \quad (17)$$

Доказательство. Для слов v, w в образующих $\Omega(\zeta_1)$ обозначим через (v, w) слово, полученное приписыванием w справа от v . Из соотношения (2) следует, что для всех $v, w \in C$

$$\Omega((v, w)) = \Omega(v)a(v)\Omega(w)a(v)^{-1}. \quad (18)$$

Слову $z \in C$ вида (1) соответствует слово

$$z^{-1} = (a_{k_N}^{(-\varepsilon_N)}, a_{k_{N-1}}^{(-\varepsilon_{N-1})}, \dots, a_{k_2}^{(-\varepsilon_2)}, a_{k_1}^{(-\varepsilon_1)}),$$

и из (2) следует, что для всех $z \in C$

$$a(z^{-1}) = a(z)^{-1}, \quad \Omega(z^{-1}) = a(z)^{-1}\Omega(z)^{-1}a(z). \quad (19)$$

Для любого единичного слова $z \in C_0$ пусть для всех $N \geq 2$

$$z^N = (z^{N-1}, z), \quad z^{-N} = (z^{-1})^N,$$

тогда из (18) и (19) следует, что для всех $N \in \mathbf{Z}$, $N \neq 0$, и всех $z \in C_0$

$$\Omega(z^N) = \Omega(z)^N. \quad (20)$$

Кроме того,

$$\begin{aligned} l((v, z)) &= l(v) + l(z), \quad z, v \in C_0, \\ l(z^N) &= Nl(z), \quad N \in \mathbf{Z}, \quad N \neq 0, \quad z \in C_0. \end{aligned} \quad (21)$$

Докажем включение $H \subset H_1$, по определению H для этого достаточно показать, что соотношения (3), (4), (5) выполняются при $L = H_1$.

Соотношение (5) есть частный случай (16) при $z = z_i$, $i \in \{1, 2, \dots, p\}$.

Для доказательства (3) положим в (16) $z = (a_k, a_k^{-1})$, $k \in \{1, \dots, s\}$, тогда

$$\Omega(a_k, a_k^{-1}) \subset H_1, \quad k \in \{1, \dots, s\}. \quad (22)$$

Из (18) и (19) следует, что

$$\Omega(a_k, a_k^{-1}) = \Omega_k \Omega_k^{-1}, \quad k \in \{1, \dots, s\}. \quad (23)$$

Согласно (22) и (23), соотношение (3) при $L = H_1$ доказано.

Докажем, что верны равенства

$$(g_k a_k) H_1 = H_1 (g_k a_k), \quad k \in \{1, \dots, s\}. \quad (24)$$

Зафиксируем $k \in \{1, \dots, s\}$ и $h \in H_1$. Как уже отмечалось после соотношения (16), существует единичное слово z такое, что $h \in \Omega(z)$ и $l(z) \neq 0$. Пусть $v = (a_k, z, a_k^{-1}, z_0^{-l(z)})$, тогда $v \in C_0$, и используя (18), (19), (20), можно получить равенство

$$\Omega(v) = \Omega_k a_k \Omega(z) (\Omega_k a_k)^{-1} \Omega(z_0)^{-l(z)}. \quad (25)$$

Так как $l(v) = 0$, из (25) и (16) следует, что

$$g_k a_k h (g_k a_k)^{-1} x^{-l(z)} \in H_1. \quad (26)$$

Согласно (16) $h \in H_1 x^{l(z)}$, таким образом, $x^{l(z)} \in H_1$, и из соотношения (26) следует, что

$$g_k a_k h (g_k a_k)^{-1} \in H_1, \quad h \in H_1, \quad k \in \{1, \dots, s\},$$

тем самым (24) доказано.

Докажем, что при $L = H_1$ выполнено (4). Зафиксируем $k \in \{1, \dots, s\}$ и рассмотрим единичное слово $v = (a_k, z_0, a_k^{-1}, z_0^{-1}) \in C_0$. Аналогично (25) можно получить равенство

$$\Omega(v) = \Omega_k a_k \Omega(z_0) (\Omega_k a_k)^{-1} \Omega(z_0)^{-1}. \quad (27)$$

Так как $l(v) = 0$, из (27) и (16) следует, что для любых $k \in \{1, \dots, s\}$

$$g_k a_k x (g_k a_k)^{-1} \in H_1 x. \quad (28)$$

Из соотношений (24) и (28) следует, что (4) выполнено при $L = H_1$.

Итак, включение $H \subset H_1$ доказано.

Докажем, что $H_1 \subset H$. Согласно приведенному выше (см. (15)) определению H_1 , достаточно показать, что соотношение (15) выполнено при $L = H$. Пусть

$$F_0 = \{(v, z_i^\varepsilon, v^{-1}) \mid v \in C, i = 1, 2, \dots, p, \varepsilon = \pm 1\}, \quad F_0 \subset C_0.$$

Элементам C соответствуют элементы свободной группы $F(a_1, a_2, \dots, a_s)$, порожденной свободными образующими $a_1, a_2, \dots, a_s$ (рассматриваемыми как символы, а не как элементы группы G). Слово z принадлежит C_0 тогда и только тогда, когда z принадлежит нормальному замыканию множества $\{z_1, z_2, \dots, z_p\}$ в группе $F(a_1, a_2, \dots, a_s)$ (см. теорему 4.4 в [3]). Следовательно, для каждого $z \in C_0$ существуют элементы $w_1, w_2, \dots, w_t \in F_0$ такие, что слова z и $w = (w_1, w_2, \dots, w_t)$ представляют один и тот же элемент в свободной группе $F(a_1, a_2, \dots, a_s)$, то есть слово z может быть получено из слова w конечным числом вписываний и вычеркиваний подслов вида $(a_k^\varepsilon, a_k^{-\varepsilon})$, $k \in \{1, \dots, s\}$, $\varepsilon \in \{1, -1\}$. В этом случае, как нетрудно видеть,

$$l(z) = l(w) = l(w_1) + l(w_2) + \dots + l(w_t). \quad (29)$$

Докажем, что также справедливо равенство

$$H\Omega(z) = H\Omega(w). \quad (30)$$

Для доказательства равенства (30) достаточно рассмотреть случай, когда, например, слово z получено из слова w одним вычеркиванием подслоа вида $(a_k^\varepsilon, a_k^{-\varepsilon})$, где $k \in \{1, 2, \dots, s\}$, $\varepsilon \in \{1, -1\}$, и применить затем индукцию по числу вписываний–вычеркиваний.

Заметим, что соотношения (3), (4), (5) выполняются при $L = H$. Кроме того, из (4) следует, что

$$g_k a_k H = H g_k a_k, \quad k \in \{1, 2, \dots, s\}. \quad (31)$$

Из соотношений (3), (4) (при $L = H$) и (31) можно получить соотношения

$$\begin{aligned} \Omega(v)a(v) &\subset Hg(v), & Hg(v) &= g(v)H, \\ Hx &= xH, & Hxg(v) &= g(v)Hx, \quad v \in C. \end{aligned} \quad (32)$$

Пусть $z = (u, v)$, $w = (u, a_k, a_k^{-1}, v)$ для некоторых $u, v \in C$ и $k \in \{1, \dots, s\}$. Используя (18), (23), (32) и (3) (при $L = H$), получим цепочку равенств

$$\begin{aligned} H\Omega(w) &= H\Omega(u)a(u)\Omega(a_k, a_k^{-1})\Omega(v)a(u)^{-1} = \Omega(u)a(u)H\Omega_k\Omega_k^{-1}\Omega(v)a(u)^{-1} \\ &= H\Omega(u)a(u)\Omega(v)a(u)^{-1} = H\Omega(z), \end{aligned}$$

и (30) в данном случае доказано.

Пусть $z = (u, v)$, $w = (u, a_k^{-1}, a_k, v)$ для некоторых $u, v \in C$ и $k \in \{1, \dots, s\}$. Заметим, что из (18), (31) и (3) (при $L = H$) следует, что

$$\Omega(a_k^{-1}, a_k) = a_k^{-1}\Omega_k^{-1}\Omega_k a_k \subset (g_k a_k)^{-1} H g_k a_k = H. \quad (33)$$

Из соотношений (18), (32), (33) следует цепочка равенств

$$\begin{aligned} H\Omega(w) &= H\Omega(u)a(u)\Omega(a_k^{-1}, a_k)\Omega(v)a(u)^{-1} = \Omega(u)a(u)H\Omega(a_k^{-1}, a_k)\Omega(v)a(u)^{-1} \\ &= H\Omega(u)a(u)\Omega(v)a(u)^{-1} = H\Omega(z). \end{aligned}$$

Таким образом, соотношение (30) полностью доказано.

Из соотношений (30) и (32) следует равенство

$$H\Omega(z) = H\Omega(w_1)H\Omega(w_2) \dots \Omega(w_t). \quad (34)$$

Но тогда из (29) и (34) следует, что для доказательства (15) при $L = H$ и произвольном единичном слове z достаточно показать справедливость (15) для любого $z \in F_0$.

Пусть $v \in C$, $i \in \{1, 2, \dots, p\}$, $\varepsilon \in \{1, -1\}$. Используя соотношения (18), (19), (32) и (5) (при $L = H$), получим цепочку соотношений

$$\begin{aligned} \Omega(v, z_i^\varepsilon, v^{-1}) &= \Omega(v)a(v)\Omega(z_i)^\varepsilon(\Omega(v)a(v))^{-1} \\ &\subset Hg(v)(Hx)^{l(z_i)\varepsilon}g(v)^{-1}H = H(x)^{l(z_i)\varepsilon}, \end{aligned}$$

что и требовалось доказать.

Итак, включение $H_1 \subset H$, а с ним равенство (17) доказаны.

Так как $H = H_1$ и $x = x_1$, число r_1 , определенное в разделе 3 статьи [2], совпадает с числом r . Кроме того, в качестве элементов $\sigma_{1,j}$, $j \in \{1, \dots, n\}$, определенных там же, могут быть выбраны элементы $g(b_j)b_j^{-1}$, $j \in \{1, \dots, n\}$. Согласно теореме из раздела 3 в [2], последовательность распределений случайных величин $\mu_a^{(s_N)}$ имеет предел при $N \rightarrow \infty$ тогда и только тогда, когда существует такое $l \in \{0, 1, \dots, r-1\}$, что $m_N \equiv l \pmod{r}$ при всех достаточно больших N , и при выполнении этого условия данный предел есть равновероятное распределение на множестве $Hx^l g(a)a^{-1}$. Так как $\omega_a^{(s_N)} = \mu_a^{(s_N)} a$ для всех $N \geq 1$, отсюда следует утверждение доказываемой теоремы.

Из доказательства теоремы вытекает справедливость следующего утверждения.

Следствие 1. Пусть $a \in \mathfrak{A}a_1^v$, где $v \in \{0, 1, \dots, d-1\}$ и $l \in \{0, 1, \dots, r-1\}$, $m \geq 1$, $s = v + d(l + rm)$ таковы, что $a \in \Omega(x^{(s)})$. Тогда

$$\Omega(\omega_a^{(s)}) \subset Hx^l g(a), \quad (35)$$

причем при всех достаточно больших $m \geq 1$ имеет место равенство

$$\Omega(\omega_a^{(s)}) = Hx^l g(a).$$

Следствие 2. Значение случайной величины $\omega^{(N)}$ однозначно определяется значением случайной величины $x^{(N)}$ для любого $N \geq 1$ тогда и только тогда, когда одновременно выполняются условия

$$\Omega_k = \{g_k\}, \quad k \in \{1, \dots, s\}, \quad (36)$$

$$g_k a_k x = x g_k a_k, \quad k \in \{1, \dots, s\}, \quad (37)$$

$$g(z_i) = x^{l(z_i)}, \quad i \in \{1, \dots, p\}. \quad (38)$$

Если соотношения (36), (37), (38) выполнены, то для любого $s \geq 1$, $s = v + d(l + rm)$, где $v \in \{0, 1, \dots, d-1\}$, $l \in \{0, 1, \dots, r-1\}$, $m \geq 1$ произвольны, верно равенство

$$\omega^{(s)} = x^l g(x^{(s)}). \quad (39)$$

Доказательство. Равенство $|\Omega(\omega_a^{(s)})| = 1$ для любого $s \geq 1$ и $a \in \Omega(x^{(s)})$, согласно следствию 1, равносильно условию $H = \{e_G\}$. Последнее выполняется тогда и только тогда, когда соотношения (3), (4), (5) выполнены при $L = \{e_G\}$, то есть когда имеют место (36), (37), (38). В этом случае (39) следует из (35).

Заметим, что подгруппа H , а также подгруппа группы G , порожденная смежным классом xH , являются нормальными делителями подгруппы группы G , порожденной множеством $\Omega(\xi_1 \zeta_1)$ (см. соотношение (4) при $L = H$). Используя это свойство, нетрудно доказать следующее утверждение.

Следствие 3. Соотношение $\Omega(\omega_a^{(N)}) = G$ выполняется для любого $a \in \mathfrak{A}$ и всех достаточно больших N тогда и только тогда, когда множество $\Omega(\xi_1 \zeta_1)$ является системой образующих элементов группы G и группа G не содержит собственного нормального делителя L , удовлетворяющего соотношениям (3), (4), (5). При выполнении этого условия для всех $a \in \mathfrak{A}$ последовательность распределений случайных величин $\omega_a^{(N)}$, $N \geq 1$, имеет своим пределом при $N \rightarrow \infty$ равновероятное распределение на G .

Список литературы

1. Глухов М. М., О числовых параметрах, связанных с заданием конечных групп системами образующих элементов. *Труды по дискретной математике* (1997) **1**, 43–66.
2. Горчинский Ю. Н., Круглов И. А., Капитонов В. М., Вопросы теории распределений на конечных группах. *Труды по дискретной математике* (1997) **1**, 85–112.
3. Ольшевский А. Ю., *Геометрия определяющих соотношений в группах*. Наука, Москва, 1995.

Статья поступила 27.06.2006.