Math-Net.Ru

Общероссийский математический портал

М. В. Федюкин, О полугруппе преобразований конечно-
го множества, порожденной случайными образующими,
Дискрет. матем., 2001, том 13, выпуск 2, 99–110

DOI: <https://doi.org/10.4213/dm280>

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: 35.173.219.12

26 апреля 2023 г., 17:21:03

УДК 519.2

О полугруппе преобразований конечного множества, порожденной случайными образующими

© 2001 г. М. В. Федюкин

Исследуется полугруппа, порожденная случайными отображениями и случайными биективными отображениями конечного множества Ω_n мощности n в себя. Изучается вопрос включения в эту полугруппу всех отображений Ω_n в себя с фиксированной мощностью k образа множества Ω_n . При $n \rightarrow \infty$ определены множества значений k , при которых данное включение выполнено с вероятностью стремящейся к 0 или к 1, а также определены две промежуточные области значений k , для представителей которых получены оценки вероятностей включения.

Пусть $\Omega_n = \{1, 2, \dots, n\}$. Обозначим через $\tilde{\mathfrak{S}}_n$ полугруппу всех отображений множества Ω_n в себя. Подмножество отображений из полугруппы $\tilde{\mathfrak{S}}_n$, состоящее из отображений A множества Ω_n в себя, таких, что

$$|A(\Omega_n)| = k,$$

обозначим через $\tilde{\mathfrak{S}}_{n,k}$. Таким образом, симметрическая группа $\mathfrak{S}_n$ есть $\tilde{\mathfrak{S}}_{n,n}$. Знакопеременную группу на множестве Ω_n обозначим через $\mathfrak{A}_n$.

Пусть

$$\mathfrak{H}_{k,l} = \langle A_1, A_2, \dots, A_k, B_1, B_2, \dots, B_l \rangle, \quad (1)$$

где $A_i, i = 1, \dots, k$, выбираются случайно и равновероятно из $\tilde{\mathfrak{S}}_n$, а $B_i, i = 1, \dots, l$, выбираются случайно и равновероятно из $\mathfrak{S}_n$. Если в (1) отсутствуют A_i , то соответствующую полугруппу, являющуюся в этом случае группой, обозначим через $\mathfrak{H}_{0,l}$. В [6] было показано, что при $n \rightarrow \infty$ с вероятностью, стремящейся к единице, выполнено либо равенство $\mathfrak{H}_{0,2} = \mathfrak{A}_n$, либо равенство $\mathfrak{H}_{0,2} = \mathfrak{S}_n$, и получена оценка скорости сходимости.

В [5] было показано, что для $l \geq 2$ при $n \rightarrow \infty$ с вероятностью, стремящейся к единице, выполнено либо равенство $\mathfrak{H}_{0,l} = \mathfrak{A}_n$, либо равенство $\mathfrak{H}_{0,l} = \mathfrak{S}_n$, и получена оценка скорости сходимости, улучшающая в случае $l = 2$ оценку работы [6].

Целью данной работы является оценка вероятности того, что при заданном k множество $\tilde{\mathfrak{S}}_{n,k}$ содержится в полугруппе $\mathfrak{H}_{m,l}$ при $l \geq 2$ или не содержится в ней.

Предложение 1. Пусть $p(n)$ — многочлен от n , l — натуральное число. Тогда при $n \rightarrow \infty$

$$P\{\mathfrak{H}_{p(n),l} = \bar{\mathfrak{S}}_n\} \rightarrow 0.$$

Доказательство. Для $A, B \in \bar{\mathfrak{S}}_n$ таких, что $|A(\Omega_n)|, |\Omega_n| < n$, имеет место неравенство

$$|AB(\Omega_n)| \leq \min(|A(\Omega_n)|, |\Omega_n|)$$

поэтому для выполнения равенства $\mathfrak{H}_{p(n),l} = \bar{\mathfrak{S}}_n$ необходимо, чтобы $A_i \in \bar{\mathfrak{S}}_{n,n-1}$ при некотором $i = 1, \dots, p(n)$. Вероятность случайного равновероятного выбора $A_i \in \bar{\mathfrak{S}}_{n,n-1}$ в условиях предложения 1 равна

$$\frac{\binom{n}{2}[n]_{n-1}}{n^n} = \frac{n(n-1)n!}{2n^n} \leq \frac{\sqrt{2\pi nn(n-1)}}{2e^{n-1/(12n)}}.$$

Поэтому

$$P\{\mathfrak{H}_{p(n),l} = \bar{\mathfrak{S}}_n\} \leq \frac{p(n)\sqrt{2\pi nn(n-1)}}{2e^{n-1/(12n)}},$$

и, значит, $P\{\mathfrak{H}_{p(n),l} = \bar{\mathfrak{S}}_n\} \rightarrow 0$ при $n \rightarrow \infty$.

Обозначим через r отображение множества натуральных чисел в себя такое, что при любом n выполнено неравенство $r(n) \leq n$.

Теорема 1. Пусть $n \rightarrow \infty$, $k = k(n)$ и

$$\frac{n}{er(n)!} \rightarrow \lambda, \quad m \geq 1, \quad l \geq 2,$$

тогда

$$P\{\mathfrak{H}_{m,l} \supseteq \bar{\mathfrak{S}}_{n,k}\} \rightarrow 1$$

при $1 \leq k \leq \lfloor n/r(n) \rfloor$;

$$P\{\mathfrak{H}_{m,l} \supseteq \bar{\mathfrak{S}}_{n,k}\} \geq 1 - (1 - e^{-\lambda})^m$$

при $\lfloor n/r(n) \rfloor + 1 \leq k \leq \lfloor n/(r(n) - 1) \rfloor$;

$$P\{\mathfrak{H}_{m,l} \not\supseteq \bar{\mathfrak{S}}_{n,k}\} \geq 1 - e^{-m\lambda}$$

при $\lfloor n/(r(n) - 1) \rfloor \leq k \leq \lfloor n/(r(n) - 2) \rfloor - 1$;

$$P\{\mathfrak{H}_{m,l} \not\supseteq \bar{\mathfrak{S}}_{n,k}\} \rightarrow 1$$

при $\lfloor n/(r(n) - 2) \rfloor \leq k \leq n - 1$.

Для доказательства теоремы 1 потребуются дополнительно следующие понятия и определения.

Напомним, что первичной спецификацией (см. [4]) отображения $A: \Omega_n \rightarrow \Omega_n$ называется вектор $(a_1, \dots, a_n)$, где a_i — число прообразов элемента i , $i = 1, \dots, n$. Таким образом, $a_1 + \dots + a_n = n$. Если упорядочить эти величины по возрастанию, то полученный ряд $a_{(1)}, \dots, a_{(n)}$ называется вариационным рядом отображения. Вторичной спецификацией отображения A называется вектор $(b_1, \dots, b_n)$, где b_i — число элементов первичной спецификации, равных i , $i = 1, \dots, n$. Таким образом,

$$\sum_{i=1}^n ib_i = n.$$

Для отображения A через $\bar{A}$ будем обозначать множество всех отображений из $\bar{\mathfrak{S}}_n$, имеющих такую же вторичную спецификацию, что и A . Пусть также

$$\begin{aligned} A_k &= \{A^{-1}(i) \mid a_i = k\}, \\ \Pi(A) &= \{A^{-1}(i) \mid i \in \Omega_n, A^{-1}(i) \neq 0\}, \\ \Pi_k(A) &= \{A^{-1}(i) \mid a_i > k\}, \\ M_k(A) &= \{A^{-1}(i) \mid a_i \leq k\}, \\ p_k(A) &= |\Pi_k(A)|, \\ m_k(A) &= |M_k(A)|, \\ \mu_k(A) &= \sum_{i=1}^k ib_i, \\ \pi_k(A) &= \sum_{i=k+1}^n ib_i. \end{aligned}$$

Предложение 2. Пусть $A \in \bar{\mathfrak{S}}_{n,k}$, $k = 1, \dots, n-2$. Тогда

$$\bar{A} \subseteq \langle A, \mathfrak{A}_n \rangle.$$

Доказательство. Рассмотрим множество $\mathfrak{A}_n A \mathfrak{A}_n$. Пусть $B \in \bar{A}$. Тогда найдется элемент $i_0 \in \Omega_n$ такой, что $|A^{-1}(i_0)| \geq 2$. Так как $B \in \bar{A}$, можно установить биекцию

$$\kappa: \Pi(A) \rightarrow \Pi(B)$$

такую, что для $\{B^{-1}(j) = \kappa(\{A^{-1}(i)\})$ имеет место равенство

$$|B^{-1}(j)| = |A^{-1}(i)|$$

при любом $\{A^{-1}(i)\} \in \Pi(A)$. В силу равномощности $B^{-1}(j)$ и $A^{-1}(i)$ можно построить биекцию

$$\alpha_i: A^{-1}(i) \rightarrow B^{-1}(j).$$

Пусть

$$\begin{aligned} a_1, a_2 &\in A^{-1}(i_0), \quad \{B^{-1}(j_0)\} = \kappa(\{A^{-1}(i_0)\}), \\ b_1, b_2 &\in \kappa(\{A^{-1}(i_0)\}), \quad \alpha_1(a_1) = b_1, \quad \alpha_1(a_2) = b_2. \end{aligned}$$

Построим подстановки C_1 и C'_1 на Ω_n следующим образом. Положим

$$\begin{aligned} C_1(a) &= \alpha_1^{-1}(a), \text{ если } a \in B^{-1}(j), \\ C'_1(a) &= \alpha_i^{-1}(a), \text{ если } a \in B^{-1}(j), j \neq j_0, \\ C'_1(a) &= \alpha_0^{-1}(a), \text{ если } a \in B^{-1}(j_0), a \neq b_1, b_2, \\ C'_1(b_1) &= \alpha_1^{-1}(b_2), \\ C'_1(b_2) &= \alpha_1^{-1}(b_1). \end{aligned}$$

Ясно, что либо C_1 , либо C'_1 содержится в $\mathfrak{A}_n$. Без ограничения общности будем считать, что $C_1 \in \mathfrak{A}_n$.

Пусть теперь $a_1, a_2 \in \Omega_n \setminus A(\Omega_n)$, $a_1 \neq a_2$. Построим подстановки C_2 и C'_2 , положив

$$\begin{aligned} C_2(a) &= C'_2(a) = b, & \text{если } \kappa(\{A^{-1}(a)\}) &= B^{-1}(b), \\ C_2(a) &= b, & \text{если } a &\in \Omega_n \setminus A(\Omega_n), \\ C'_2(a) &= b, & \text{если } a &\in \Omega_n \setminus A(\Omega_n) \setminus \{a_1, a_2\}, \\ C'_2(a_1) &= C_2(a_2), \\ C'_2(a_2) &= C_2(a_1). \end{aligned}$$

Очевидно, что одна из двух подстановок (будем считать, что C_2) содержится в $\mathfrak{A}_n$. Тогда по построению C_1 и C_2 имеет место равенство $C_1 A C_2 = B$. Предложение доказано.

Сначала рассмотрим полугруппу $\mathfrak{H}_{1,l}$.

Лемма 1. Пусть A — отображение Ω_n в себя с вторичной спецификацией

$$(b_0, b_1, \dots, b_n), \quad b_r \neq 0, \quad b_i = 0, \quad i = r+1, \dots, n,$$

$$s = \lfloor n/(r-1) \rfloor, \quad B_1, B_2 \in \mathfrak{S}_n.$$

Тогда при $k = s, \dots, n-1$ имеют место соотношения

$$\tilde{\mathfrak{S}}_{n,k} \not\subseteq \langle A, B_1, B_2 \rangle.$$

Доказательство. Пусть $C \in \langle A, B_1, B_2 \rangle$ и C имеет представление в виде слова следующего вида

$$C = B'_1 A B'_2 A \dots A B'_t,$$

где B'_i , $i = 1, \dots, t$, $t \geq 2$, содержатся в группе, порожденной подстановками B_1 и B_2 . Так как максимальный элемент первичной спецификации произведения двух отображений не меньше максимума элементов первичных спецификаций сомножителей, максимальный элемент первичной спецификации C не меньше r .

Рассмотрим отображение D множества Ω_n в себя следующего вида:

$$D((r-1)t+l) = t+1, \quad t = 0, 1, \dots, s-1, \quad l = 1, \dots, r-1.$$

Очевидно, что $D \in \tilde{\mathfrak{S}}_{n,s}$. Максимальный элемент первичной спецификации D равен $r-1$, поэтому

$$D \notin \langle A, B_1, B_2 \rangle.$$

Значит,

$$\tilde{\mathfrak{S}}_{n,s} \not\subseteq \langle A, B_1, B_2 \rangle,$$

а поэтому и

$$\tilde{\mathfrak{S}}_{n,k} \not\subseteq \langle A, B_1, B_2 \rangle, \quad k = s, \dots, n-1.$$

Лемма доказана.

Лемма 2. Пусть $A_1, A_2 \in \tilde{\mathfrak{S}}_n \setminus \mathfrak{S}_n \setminus \tilde{\mathfrak{S}}_{n,n-1}$ и при любом $k = 0, 1, \dots, n-1$

$$\pi_k(A_2) \geq \pi_k(A_1) + k p_k(A_2). \quad (2)$$

Тогда

$$A_2 \in \langle A_1, \mathfrak{A}_n \rangle.$$

Доказательство. Построим последовательно функции

$$\psi_{n-1}: \Pi_{n-1}(A_1) \rightarrow \Pi_{n-1}(A_2), \psi_{n-2}: \Pi_{n-2}(A_1) \rightarrow \Pi_{n-2}(A_2), \dots, \psi_0: \Pi_0(A_1) \rightarrow \Pi_0(A_2)$$

такие, что при любом $\{\Delta\} \in \Pi(A_2)$ имеет место неравенство

$$\sum_{\Gamma: \psi_k(\{\Gamma\})=\{\Delta\}} |\Gamma| \leq |\Delta|.$$

Пусть $k = n - 1$, тогда либо

$$\pi_{n-1}(A_2) \geq \pi_{n-1}(A_1) + n - 1,$$

то есть

$$\pi_{n-1}(A_2) = n, \quad \pi_{n-1}(A_1) = 0,$$

и поэтому $\Pi_{n-1}(A_1) = \emptyset$, и отображение ψ_{n-1} тривиально, либо $\pi_{n-1}(A_2) = 0$, то есть

$$\pi_{n-1}(A_2) = 0, \quad \pi_{n-1}(A_1) = 0.$$

Тогда

$$\Pi_{n-1}(A_1) = \Pi_{n-1}(A_2) = \emptyset$$

и ψ_{n-1} — снова тривиальное отображение.

Пусть $k < n - 1$. Построим отображение ψ_k . Если $\Pi_k(A_1) = \emptyset$, то ψ_k тривиально. Пусть $\Pi_k(A_1) \neq \emptyset$. Положим

$$\psi_k(\{\Lambda\}) = \psi_{k+1}(\{\Lambda\}), \quad \{\Lambda\} \in \Pi_{k+1}(A_1).$$

Определим теперь ψ_k на $\Pi_k(A_1) \setminus \Pi_{k+1}(A_1)$. Для этого установим на этом множестве произвольное отношение линейного порядка $<_1$, а также определим линейное отношение порядка $<_2$ на $\Pi(A_2)$, приняв для $\{\Lambda\}, \{M\} \in \Pi(A_2)$, что $\{\Lambda\} <_2 \{M\}$, если $|\Lambda| < |M|$, а в случае $|\Lambda| = |M|$ установим отношение произвольным образом. Значения ψ_k на элементах $\Pi_k(A_1) \setminus \Pi_{k+1}(A_1)$ будем определять последовательно в соответствии с введенным отношением линейного порядка $<_1$, начиная с максимального элемента. Значение $\psi_k(\{\Lambda\})$ для очередного элемента $\{\Lambda\} \in \Pi_k(A_1) \setminus \Pi_{k+1}(A_1)$, определим следующим образом.

В множестве $\Pi_k(A_2)$ выбирается наибольший относительно введенного отношения порядка $<_2$ элемент $\{\Delta\}$, удовлетворяющий условию

$$|\Delta| - \sum_{\Gamma: \psi_k(\{\Gamma\})=\{\Delta\}} |\Gamma| \geq k + 1,$$

где $\psi(\{\Gamma\})$ — множество уже определенных значений функции ψ_k . Тогда положим $\psi_k(\{\Lambda\}) = \{\Delta\}$. Допустим, что такого Δ не существует. Тогда, во-первых,

$$\pi_k(A_1) > \sum_{\{\Gamma\} \in \mathfrak{B}} |\Gamma|, \quad (3)$$

где $\mathfrak{B}$ — множество элементов $\Pi(A_1)$, на которых функция ψ_k уже определена, и, во-вторых, при любом $\{\Delta\} \in \Pi_k(A_2)$ имеет место неравенство

$$|\Delta| - \sum_{\Gamma: \psi_k(\{\Gamma\})=\{\Delta\}} |\Gamma| \leq k. \quad (4)$$

Суммируя неравенства (4) по всем $\{\Delta\} \in \Pi_k(A_2)$, получаем, что

$$\sum_{\{\Delta\} \in \Pi_k(A_2)} |\Delta| \leq k|\Pi_k(A_2)| + \sum_{\{\Delta\} \in \Pi_k(A_2)} \sum_{\Gamma: \psi_k(\{\Gamma\})=\{\Delta\}} |\Gamma|,$$

или, записав последние выражения иначе,

$$\pi_k(A_2) \leq kp_k(A_2) + \sum_{\{\Gamma\} \in \mathfrak{B}} |\Gamma|.$$

С учетом неравенства (3) получаем, что

$$\pi_k(A_2) < kp_k(A_2) + \pi_k(A_1),$$

что противоречит неравенству (2). Поэтому необходимый элемент $\{\Delta\}$ множества $\Pi_k(A_2)$ всегда найдется и отображение ψ_k , таким образом, построено. Пусть

$$\begin{aligned} C_1, C_2 &\in \tilde{\mathfrak{S}}_{n,n} \setminus \mathfrak{S}_n \setminus \tilde{\mathfrak{S}}_{n,n-1}, \\ \Pi(C_1) &= \mathfrak{C} \cup \{\Delta\} \cup \{\Gamma\}, \\ \Pi(C_2) &= \mathfrak{C} \cup \{\Delta \cup \Gamma\}, \end{aligned}$$

тогда $C_2 \in \langle C_1, \mathfrak{A}_n \rangle$. Действительно, подобрав соответствующее $A_1 \in \mathfrak{A}_n$, можно построить отображение $A_1 C_1$ такое, что при любом $i \in C_1(\Omega_n)$ имеет место равенство

$$(A_1 C_1)^{-1}(i) = \{a_1 \dots a_m\},$$

где $a_1 = C_1(b)$ при некотором $b \in \Omega_n$, а

$$a_1, \dots, a_m \in \Omega_n \setminus C_1(\Omega_n).$$

Пусть $|\Delta| \geq 2$,

$$\begin{aligned} \Delta &= \{a_1^\Delta, \dots, a_t^\Delta\}, \\ \Gamma &= \{a_1^\Gamma, \dots, a_s^\Gamma\}. \end{aligned}$$

Положим подстановку A_2 равной транспозиции (a_2^Δ, a_1^Γ) , A_3 равной транспозиции (b_1, b_2) , где $b_1, b_2 \in \Omega_n \setminus C_1(\Omega_n)$. Очевидно, что $A_1 A_2 A_3 \in \mathfrak{A}_n$ и вторичная спецификация отображения $C_1 A_1 A_2 A_3 C_1$ такая же, как у C_2 . Поэтому, подобрав подстановки $A_4, A_5 \in \mathfrak{A}_n$, по предложению 2 получим, что

$$C_2 = A_4 C_1 A_1 A_2 A_3 C_1 A_5.$$

Пусть $|\Delta| = |\Gamma| = 1$. В силу условий леммы существует элемент $i \in \Omega_n$ такой, что

$$C_1^{-1}(i) = \{a_1, \dots, a_t\}, \quad t \geq 2.$$

Обозначив $\Delta = \{a_\Delta\}$, $\Gamma = \{a_\Gamma\}$, и взяв в качестве A_2 произведение двух транспозиций (a_1, a_Δ) , (a_2, a_Γ) , получим, что $A_1 A_2 \in \mathfrak{A}_n$, так как все $a_1, a_\Delta, a_2, a_\Gamma$ различны. Вторичная спецификация $C_1 A_1 A_2 C_1$ такая же, как и у C_2 . Поэтому, подобрав соответствующие подстановки A_4 и A_5 из $\mathfrak{A}_n$, в силу предложения 2, получим равенство

$$C_2 = A_4 C_1 A_1 A_2 C_1 A_5.$$

По индукции легко получаем, что для $C_1, C_2 \in \tilde{\mathfrak{S}}_{n,n} \setminus \mathfrak{S}_n \setminus \tilde{\mathfrak{S}}_{n,n-1}$ таких, что

$$\begin{aligned}\Pi(C_1) &= \bigcup_{i \in I} \bigcup_{j_i \in J_i} \{\Delta_{i,j_i}\}, \\ \Pi(C_2) &= \bigcup_{i \in I} \left\{ \bigcup_{j_i \in J_i} \Delta_{i,j_i} \right\},\end{aligned}$$

имеет место включение

$$C_2 \in \langle C_1, \mathfrak{A}_n \rangle.$$

Рассмотрим построенное выше отображение ψ_0 . По условию при любом $\{\Delta\} \in \Pi(A_2)$ имеет место неравенство

$$\sum_{B: \psi_0(\{B\})=\{C\}} |B| \leq |C|. \quad (5)$$

Суммируя по всем $\{C\} \in \Pi(A_2)$, получаем, что

$$n = \sum_{\{C\} \in \Pi(A_2)} \sum_{B: \psi_0(\{B\})=\{C\}} |B| \leq \sum_{\{C\} \in \Pi(A_2)} |C| = n.$$

Поэтому среди неравенств (5) нет ни одного строгого неравенства и при любом $\{C\} \in \Pi(A_2)$ имеют места равенства

$$\sum_{B: \psi_0(\{B\})=\{C\}} |B| = |C|.$$

Значит, элементы $\Pi(A_2)$ представляют собой множества, являющиеся объединениями множеств, входящих в качестве элементов в $\Pi(A_1)$. Поэтому

$$A_2 \in \langle A_1, \mathfrak{A}_n \rangle.$$

Лемма доказана.

В дальнейшем будем использовать сокращенные обозначения

$$\ln_2 n = \ln \ln n, \quad \ln_3 n = \ln \ln \ln n, \quad \ln_4 n = \ln \ln \ln \ln n.$$

Элемент C множества $\tilde{\mathfrak{S}}_n$ называется c -типовым ($c = c(n)$, $|c(n)|$ ограничены некоторой постоянной), если его вторичная спецификация удовлетворяет следующим условиям:

при $k = 1, \dots, \lfloor \ln n / (\ln_2 n \ln_3 n) \rfloor$ выполнены неравенства

$$b_k \geq \frac{n}{ek!} - \frac{n}{ek! \ln n},$$

при $k > c \ln n / \ln_2 n$ выполнены равенства $b_k = 0$.

Замечание 1. В [3] показано, что существует $c = c(n) \rightarrow 1$ при $n \rightarrow \infty$ такая, что при случайном и равновероятном выборе C из $\tilde{\mathfrak{S}}_n$ вероятность того, что $b_k = 0$ при $k > c \ln n / \ln_2 n$, стремится к 1 при $n \rightarrow \infty$.

Лемма 3. Пусть $r(n) = \lfloor c \ln n / \ln_2 n \rfloor$ и C_1 является c -типовым отображением. Тогда при достаточно большом n_0 при всех $n \geq n_0$ и $m \leq \lfloor n/r(n) \rfloor$ имеют место включения

$$\tilde{\mathfrak{S}}_{n,m} \subseteq \langle C_1, \mathfrak{A}_n \rangle.$$

Доказательство. Покажем, что из включения $\tilde{\mathfrak{S}}_{n,m} \subseteq \langle C_1, \mathfrak{A}_n \rangle$, следует, что $\tilde{\mathfrak{S}}_{n,m-1} \subseteq \langle C_1, \mathfrak{A}_n \rangle$. Действительно, пусть C — произвольное преобразование Ω_n такое, что $|C(\Omega_n)| = m$. Найдется подстановка $A_1 \in \mathfrak{A}_n$ такая, что для любого элемента $a \in (A_1 C)(\Omega_n)$ имеет место равенство $(A_1 C)(a) = a$. Пусть существует элемент $a \in (A_1 C)^{-1}(\Omega_n)$ такой, что $|(A_1 C)^{-1}(a)| \geq 3$. Положим

$$(A_1 C)^{-1}(a) = \{a, a_2, \dots, a_t\}, \quad t \geq 3.$$

Пусть $B(c) = (A_1 C)(c)$ при $c \neq a_t$ и $B(a_t) = a_t$. Ясно, что $B \in \tilde{\mathfrak{S}}_{n,m}$. Пусть $A_2 = (a, a_2, a_t)$, тогда

$$\begin{aligned} (A_2 B)(c) &= B(c), & c \in \Omega_n \setminus \{a_2, a_t\}, \\ (A_2 B)(a_2) &= a_t, & (A_2 B)(a_t) = B(a_2) = a. \end{aligned}$$

Поэтому

$$\begin{aligned} BA_2 B(c) &= B(c), & c \in \Omega_n \setminus \{a_2, a_t\}, \\ BA_2 B(a_2) &= a, & BA_2 B(a_t) = a, \end{aligned}$$

то есть $BA_2 B = C$.

Если для любого $a \in (AC)(\Omega_n)$ имеет место неравенство $|(AC)^{-1}(\Omega_n)| \leq 2$, то найдутся элементы a, b такие, что

$$|(AC)^{-1}(a)| = |(AC)^{-1}(b)| = 2.$$

Пусть

$$(AC)(a) = (AC)(a_2) = a, \quad (AC)(b) = (AC)(b_2) = b.$$

Положим

$$B(c) = C(c), \quad c \in \Omega_n \setminus \{a_2\}, \quad B(a_2) = a + 2.$$

Пусть $(a, b)(a_2, b_2)$. Рассмотрим преобразование $BA_2 BA_2$. Ясно, что

$$\begin{aligned} (BA_2 BA_2)(c) &= C(c), & c \in \Omega_n \setminus \{a, b, a_2, b_2\}, \\ (BA_2 BA_2)(a) &= (A_2 BA_2)(a) = (BA_2)(b) = A_2(b) = a, \\ (BA_2 BA_2)(a_2) &= (A_2 BA_2)(a_2) = (BA_2)(a) = A_2(a) = b, \\ (BA_2 BA_2)(b_2) &= (A_2 BA_2)(b) = (BA_2)(a) = A_2(a) = b. \end{aligned}$$

Таким образом, $C = BA_2 BA_2$.

Поэтому достаточно доказать включение только для $m = \lfloor n/r(n) \rfloor$.

Пусть $k \leq \lfloor \ln n / (\ln_2 n \ln_3 n) \rfloor$. Оценим сверху значения $\pi_k(C_1)$. Так как при $k = 1, \dots, \lfloor \ln n / (\ln_2 n \ln_3 n) \rfloor$

$$\frac{1}{e} \leq \frac{1}{e} \sum_{t=0}^{k-1} \leq 1,$$

справедливы оценки

$$\begin{aligned}\pi_k(C_1) &= n - \sum_{t=1}^k t|(C_1)_t| \leq n - \frac{n}{e} \left(1 - \frac{1}{\ln n}\right) \sum_{t=0}^{k-1} \frac{1}{t!}, \\ \pi_k(C_1) &\leq n \left(1 - \frac{1}{e}\right) + \frac{n}{\ln n}.\end{aligned}\quad (6)$$

Пусть теперь $k \geq \lfloor \ln n / (\ln_2 n \ln_3 n) \rfloor + 1 = k_0$. При достаточно большом n выполнено неравенство

$$\frac{1}{5} \ln n \geq \max\{\ln n \ln_3 n / \ln_2 n, \ln n \ln_4 n / \ln_2 n, \ln n / \ln_2 n, \ln_2 n \ln_3 n\}.$$

Поэтому

$$\frac{\ln n}{\ln_2 n \ln_3 n} \left(\ln \left(\frac{\ln n}{\ln_2 n \ln_3 n} \right) - 1 \right) \geq \ln_2 n.$$

Отсюда следует, что

$$\ln k_0! \geq \sqrt{2\pi} k_0^{k_0} e^{-k_0} \geq \ln_2 n,$$

значит,

$$\frac{n}{k_0!} \leq \frac{n}{\ln n}, \quad \pi_k(C_1) \leq \frac{2n}{\ln n}.\quad (7)$$

Пусть $C_2 \in \bar{\mathfrak{S}}_{n,m}$, тогда

$$\begin{aligned}p_k(C_2) + m_k(C_2) &= \lfloor n/r(n) \rfloor, \\ \pi_k(C_2) + \mu_k(C_2) &= n, \\ \mu_k(C_2) &\leq k m_k(C_2), \\ \pi_k(C_2) &\geq n - k m_k(C_2).\end{aligned}$$

Поэтому

$$\begin{aligned}m_k(C_2) &= \lfloor n/r(n) \rfloor - p_k(C_2), \\ \pi_k(C_2) &\geq n - k \lfloor n/r(n) \rfloor + k p_k(C_2) \\ &\geq n - k \lfloor n/r(n) \rfloor + k,\end{aligned}$$

так как $p_k(C_2) \geq 1$ при $k \leq r(n) - 1$.

При $k = 1, \dots, \lfloor \ln n / (\ln_2 n \ln_3 n) \rfloor$ получаем, что

$$\begin{aligned}\pi_k(C_2) &\geq n - k \lfloor n/r(n) \rfloor + k \\ &\geq n - \frac{kn \ln_2 n}{c \ln n} - dk + k \geq n - \frac{kn \ln_2 n}{c \ln n},\end{aligned}\quad (8)$$

где $d \in [0, 1]$. Так как при $k \leq \ln n / (\ln_2 n \ln_3 n)$ имеет место неравенство

$$\frac{kn \ln_2 n}{c \ln n} \leq \frac{n}{c \ln_3 n},$$

выражение (6) не меньше

$$n - \frac{n}{c \ln_3 n}.\quad (9)$$

Пусть теперь $[\ln n / (\ln_2 n \ln_3 n)] + 1 \leq k \leq r(n) - 1$. Тогда имеют место неравенства

$$\begin{aligned} \pi_k(C_2) &\geq n - (r(n) - 1)n/r(n) + k \\ &= n - (r(n) - 1)n/r(n) + d + k \geq n/r(n), \end{aligned} \quad (10)$$

так как $d \geq 0$.

Проверим выполнение условий леммы 2. При $k = 1, \dots, [\ln n / (\ln_2 n \ln_3 n)]$ из (9) и (6) получаем цепочку неравенств

$$\pi_k(C_2) \geq n - \frac{n}{c \ln_3 n} \geq \frac{n}{\ln n} + \frac{2n}{e} \geq \pi_k(C_1)$$

при достаточно больших n .

При $k = [\ln n / (\ln_2 n \ln_3 4n)] + 1, \dots, r(n) - 1$ из (10) и (7) получаем цепочку неравенств

$$\pi_k(C_2) \geq \frac{n}{r(n)} = \frac{n \ln_2 n}{c \ln n} \geq \frac{2n}{\ln n} \geq \pi_k(C_1)$$

при достаточно больших n .

При $k \geq r(n)$ получаем неравенство

$$\pi_k(C_2) \geq 0 = \pi_k(C_1).$$

Поэтому существует такое n_0 , что при всех $n \geq n_0$ выполнены условия леммы 2, и, значит, имеет место включение

$$C_2 \in \langle C_1, \mathfrak{A}_n \rangle.$$

Лемма доказана.

Лемма 4. Пусть функция $c = c(n)$ такая, как в замечании 1. Тогда при $n \rightarrow \infty$ вероятность $P_{\text{тип}}^{(n)}(C)$ случайного равновероятного выбора из множества всех отображений Ω_n в себя c -типового отображения стремится к единице.

Доказательство. Очевидно, что

$$P_{\text{тип}}^{(n)}(C) \geq 1 - \sum_{k=1}^{[\ln n / (\ln_2 n \ln_3 n)]} \mathbf{P} \left\{ |C_k| \leq \frac{n}{ek!} - \frac{n}{ek! \ln n} \right\} - P_{\max},$$

где $P_{\max}$ — вероятность того, что максимальный член вариационного ряда отображения C больше $c \ln n / \ln_2 n$. Из [1] следует, что $P_{\max} \rightarrow 0$ при $n \rightarrow \infty$.

Оценим

$$\mathbf{P} \left\{ |C_k| \leq \frac{n}{ek!} - \frac{n}{ek! \ln n} \right\}.$$

Как известно (см. [2]), дисперсия случайной величины, равной числу элементов Ω_n , имеющих по k прообразов в случайном равновероятном отображении Ω_n в себя, имеет при $n \rightarrow \infty$ дисперсию, ограниченную величиной

$$\frac{n}{ek!} \left(1 - \frac{1}{ek!} - \frac{(1-k)^2}{ek!} \right) \leq \frac{n}{ek!}.$$

В силу неравенства Чебышева

$$\mathbf{P}\left\{\left|C_k - \frac{n}{ek!}\right| \geq \frac{n}{ek! \ln n}\right\} \leq \frac{n}{ek!} \left(\frac{n}{ek! \ln n}\right)^{-2} = \frac{1}{n} (\ln n)^2 ek!. \quad (11)$$

Пусть $k \leq \ln n / (\ln_2 n \ln_3 n)$. Покажем, что

$$\frac{1}{n} (\ln n)^2 ek! \leq \frac{1}{\sqrt{n}}.$$

При достаточно больших n справедлива цепочка неравенств

$$\begin{aligned} \ln((\ln n)^2 ek!) &\leq \ln((\ln n)^2 e \sqrt{2\pi} \exp\left\{(k + 1/2) \ln k - k + \frac{1}{12n}\right\}) \\ &\leq 3 \ln_2 n + \frac{\ln n}{\ln_3 n} + \frac{1}{2} \ln_2 n + \frac{\ln_2 n \ln_3 n}{12 \ln n} + 1 + \frac{1}{2} \ln(2\pi). \end{aligned} \quad (12)$$

При достаточно больших n имеет место неравенство

$$\frac{1}{8} \ln n \geq \max\left\{3 \ln_2 n, \frac{\ln n}{\ln_3 n}, \frac{1}{2} \ln_2 n, \frac{\ln_2 n \ln_3 n}{12 \ln n}\right\},$$

поэтому

$$\ln((\ln n)^2 ek!) \leq \frac{1}{2} \ln n$$

и, значит,

$$\frac{(\ln n)^2 ek!}{n} \leq \frac{1}{\sqrt{n}}.$$

Из полученной оценки, так как $\ln n \leq n^\alpha$ при любом $\alpha > 0$ и достаточно больших n , следует, что

$$P_{\text{typ}}^{(n)}(C) \geq 1 - [\ln n / (\ln_2 n \ln_3 n)] n^{-1/2} - P_{\text{max}} \geq 1 - n^{-1/4} - P_{\text{max}},$$

где $P_{\text{max}} \rightarrow 0$ при $n \rightarrow \infty$. Поэтому $P_{\text{typ}}^{(n)}(C) \rightarrow 1$. Лемма доказана.

Предложение 3. Пусть $n \rightarrow \infty$ и $n/(er(n)!) \rightarrow \lambda$, тогда при $1 \leq k \leq \lfloor n/r(n) \rfloor$

$$\mathbf{P}\{\mathfrak{H}_{1,2} \supseteq \tilde{\mathfrak{S}}_{n,k}\} \rightarrow 1; \quad (13)$$

при $\lfloor n/r(n) \rfloor < k \leq \lfloor n/(r(n) - 1) \rfloor$

$$\mathbf{P}\{\mathfrak{H}_{1,2} \supseteq \tilde{\mathfrak{S}}_{n,k}\} \geq e^{-\lambda}; \quad (14)$$

при $\lfloor n/(r(n) - 1) \rfloor < k \leq \lfloor n/(r(n) - 2) \rfloor - 1$

$$\mathbf{P}\{\mathfrak{H}_{1,2} \not\supseteq \tilde{\mathfrak{S}}_{n,k}\} \geq 1 - e^{-\lambda}. \quad (15)$$

при $\lfloor n/(r(n) - 2) \rfloor, \dots, n - 1$

$$\mathbf{P}\{\mathfrak{H}_{1,2} \supseteq \tilde{\mathfrak{S}}_{n,k}\} \rightarrow 1; \quad (16)$$

Доказательство. По следствию 2 из параграфа 5 главы 1 книги [3] вероятность того, что случайное равновероятное отображение A_1 имеет максимальный элемент вариационного ряда, равный $r(n) - 1$, стремится к $e^{-\lambda}$. Нетрудно видеть, что $r(n) - 1$ стремится к $c \ln n / \ln 2 n$ при $n \rightarrow \infty$, поэтому по лемме 4 вероятность того, что A_1 — c -типовое отображение, стремится к единице при $n \rightarrow \infty$. По лемме 3, если A_1 есть c -типовое отображение, то при достаточно большом n

$$\tilde{\mathfrak{S}}_{n,m} \subseteq \langle A_1, \mathfrak{A}_n \rangle,$$

где $m \leq \lfloor n/(r(n) - 1) \rfloor$. Этим доказано предельное соотношение (14).

Случайное отображение A_1 с вероятностью, стремящейся к $1 - e^{-\lambda}$ при $n \rightarrow \infty$, имеет максимальный элемент вариационного ряда, равный $r(n)$. По лемме 3 в этом случае при достаточно больших n имеет место включение

$$\tilde{\mathfrak{S}}_{n,m} \subseteq \langle A_1, \mathfrak{A}_n \rangle,$$

где $m \leq \lfloor n/r(n) \rfloor$. Этим доказано (13). По лемме 3 для A_1 рассматриваемого вида с вероятностью, в пределе не меньшей $1 - e^{-\lambda}$, при $k = \lfloor n/(r(n) - 1) \rfloor, \dots, n - 1$ справедливо соотношение $\tilde{\mathfrak{S}}_{n,k} \not\subseteq \mathfrak{H}_{1,2}$.

С вероятностью, стремящейся к $e^{-\lambda}$, отображение A_1 имеет максимальный элемент вариационного ряда, равный $r(n) - 1$, в этом случае имеет место соотношение $\mathfrak{H}_{1,2} \supseteq \tilde{\mathfrak{S}}_{n,k}$ при $k = \lfloor n/(r(n) - 2) \rfloor, \dots, n - 1$. Значит существует предел (15) и справедливо предельное неравенство (16). Предложение доказано.

Теперь утверждение теоремы 1 следует непосредственно из предложения 3.

Автор выражает благодарность В. Н. Сачкову за обсуждение рассматриваемых в статье вопросов и ряд замечаний, способствовавших совершенствованию доказательств утверждений, содержащихся в статье.

Список литературы

1. Викторова И. И., Севастьянов Б. А., О предельном поведении максимума в полиномиальной схеме. *Матем. заметки* (1967) 1, №3, 331–338.
2. Колчин В. Ф., Севастьянов Б. А., Чистяков В. П., *Случайные размещения*. Наука, Москва, 1976.
3. Колчин В. Ф., *Случайные отображения*. Наука, Москва, 1984.
4. Сачков В. Н., *Комбинаторные методы дискретной математики*. Наука, Москва, 1977.
5. Сачков В. Н., Группы подстановок и полугруппы преобразований с заданным числом образующих. *Труды по дискретной математике*. (2000) 3, 215–234.
6. Dixon J. D., The probability of generating the symmetric group. *Math. Z.* (1969) 110, №3, 199–205.

Статья поступила 19.12.1997.

Переработанный вариант поступил 12.07.1998.