Math-Net.Ru

Общероссийский математический портал

В. Г. Михайлов, Число разложений случайной подстановки в композицию двух инволюций с заданным циклом в одном из сомножителей, *Матем. вопр. криптогр.*, 2017, том 8, выпуск 1, 80–94

DOI: <https://doi.org/10.4213/mvk216>

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: 3.85.183.62

26 апреля 2023 г., 12:58:08

**Число разложений случайной подстановки
в композицию двух инволюций
с заданным циклом в одном из сомножителей
В. Г. Михайлов**

Математический институт им. В. А. Стеклова Российской академии наук, Москва

Получено 30.V.2016

Аннотация. Исследуется число разложений случайной равновероятной подстановки порядка n в композицию двух инволюций при фиксации цикла в одном из сомножителей. Доказаны теоремы об асимптотической нормальности логарифма числа таких разложений при $n \rightarrow \infty$.

Ключевые слова: случайные подстановки, разложение подстановки, произведение инволюций, асимптотическая логарифмическая нормальность

The number of decomposition of random permutation into the product of two involutions with given cycle in one of multipliers

V. G. Mikhailov

Steklov Mathematical Institute of the Russian Academy of Sciences, Moscow

Abstract. We investigate the number of decompositions of random permutation of the n -th order into the product of two involutions with given cycle in one of multipliers. Theorems on the asymptotical logarithmic normality of this number as $n \rightarrow \infty$ are proved.

Key words: random permutations, decomposition of permutation, product of involutions, asymptotic logarithmic normality

Citation: *Mathematical Aspects of Cryptography*, 2017, v. 8, № 1, pp. 81–94 (Russian)

© Академия криптографии Российской Федерации, 2017 г.

1. Введение

Напомним, что инволюцией называется подстановка, все циклы которой имеют длину один или два. Для числа a_n инволюций в симметрической группе S_n выполнено соотношение (см. [1, с. 583], впервые доказано в [2])

$$a_n = \frac{1}{\sqrt[4]{8\pi e n}} \sqrt{n!} e^{\sqrt{n}} (1 + o(1)), \quad n \rightarrow \infty. \quad (1)$$

Таким образом, число пар инволюций асимптотически заметно больше общего числа подстановок $n!$ в S_n :

$$\frac{a_n^2}{n!} = \frac{e^{2\sqrt{n}}}{\sqrt{8\pi e n}} (1 + o(1)), \quad n \rightarrow \infty.$$

Поэтому можно ожидать, что любая подстановка из S_n представляется в виде композиции двух инволюций. Это действительно так; формула для числа таких представлений получена в [3].

Теорема 1. Пусть π — подстановка из S_n с c_k циклами длины k , $k = 1, 2, \dots, n$. Тогда число разложений подстановки π в композицию $\pi = \tau \circ \sigma$ инволюций σ и τ равно

$$F_n(\pi) = \prod_{k=1}^n f(c_k, k), \quad \text{где} \quad f(r, k) = \sum_{j=0}^{\lfloor r/2 \rfloor} \frac{r!}{(r-2j)! j! 2^j} k^{r-j}. \quad (2)$$

Очевидно, что максимальное значение величины $F_n(\pi)$ достигается на тождественной подстановке и равно числу всех инволюций. Минимальное значение $F_n(\pi)$ при $n \geq 2$ достигается на подстановках с двумя циклами (один — длины 1, а другой — длины $n-1$) и равно $n-1$ (см. [3, 4]).

Распределение числа разложений случайной равновероятной подстановки степени n (обозначим ее $\tilde{\pi}$) исследовалось в [3, 5]. В [3] было высказано предположение об асимптотической нормальности величины $F_n(\tilde{\pi})$ при $n \rightarrow \infty$. Доказательство этого предположения было получено совсем недавно в [5].

Теорема 2. Пусть $\tilde{\pi}$ — равновероятная случайная подстановка степени n . Если $n \rightarrow \infty$, то при всех $-\infty < x < \infty$

$$\mathbf{P} \left\{ \frac{\ln F_n(\tilde{\pi}) - \frac{1}{2} \ln^2 n}{\sqrt{\frac{1}{3} \ln^3 n}} < x \right\} \rightarrow \frac{1}{\sqrt{2\pi}} \int_{-\infty}^x e^{-u^2/2} du.$$

Ниже для удобства ссылок приведено другое доказательство теоремы 2, полученное независимо от [5], но использующее те же соображения.

В работе исследуются свойства разложений $\pi = \tau \circ \sigma$ случайной равновероятной подстановки степени n в том случае, когда фиксирован один цикл в сомножителе σ . Эти свойства существенно зависят от того, какова длина фиксированного цикла — один или два. В обоих случаях изучено предельное поведение распределения числа однозначно определившихся переходов в каждом из сомножителей и доказаны теоремы об асимптотической нормальности логарифма числа таких разложений при $n \rightarrow \infty$.

2. Формулировки

Введем обозначение I_n для множества инволюций степени n и обозначение $I_n(i, j)$ (при $1 \leq i \leq j \leq n$) для множества инволюций из I_n , имеющих цикл (i, j) . Тогда $I_n(i, i)$ будет соответствовать множеству инволюций из I_n , имеющих неподвижную точку i . Пусть $F_n^{(i,j)}(\pi)$ — число разложений подстановки π в композицию $\tau \circ \sigma = \pi$, где $\sigma \in I_n(i, j)$, $\tau \in I_n$.

Теорема 3. Пусть $\tilde{\pi}$ — равновероятная случайная подстановка степени n и $1 \leq i \leq n$. Если $n \rightarrow \infty$, то при всех $-\infty < x < \infty$

$$\mathbf{P} \left\{ \frac{\ln F_n^{(i,i)}(\tilde{\pi}) - \frac{1}{2} \ln^2 n}{\sqrt{\frac{1}{3} \ln^3 n}} < x \right\} \rightarrow \frac{1}{\sqrt{2\pi}} \int_{-\infty}^x e^{-u^2/2} du. \quad (3)$$

Теорема 4. Пусть $\tilde{\pi}$ — равновероятная случайная подстановка степени n и $1 \leq i < j \leq n$. Тогда

$$\mathbf{P} \{ F_n^{(i,j)}(\tilde{\pi}) > 0 \} = \frac{n+1}{2(n-1)}, \quad (4)$$

а если $n \rightarrow \infty$, то при всех $-\infty < x < \infty$

$$\mathbf{P} \left\{ \frac{\ln F_n^{(i,j)}(\tilde{\pi}) - \frac{1}{2} \ln^2 n}{\sqrt{\frac{1}{3} \ln^3 n}} < x \mid F_n^{(i,j)}(\tilde{\pi}) > 0 \right\} \rightarrow \frac{1}{\sqrt{2\pi}} \int_{-\infty}^x e^{-u^2/2} du. \quad (5)$$

При наличии разложения $\pi = \tau \circ \sigma$ и условии $\sigma \in I_n(i, j)$ некоторые циклы инволюций $\sigma \in I_n(i, j)$ и τ определяются однозначно. Как именно это происходит, будет описано в разделе 4 при доказательстве лемм 2 и 3.

Обозначим $\zeta^{(i,j)}(\pi)$ число циклов инволюции σ , однозначно определяющихся условиями $\pi = \tau \circ \sigma$, $\sigma \in I_n(i, j)$, $\tau \in I_n$. Столько же циклов определяется в инволюции τ . Если разложения $\pi = \tau \circ \sigma$ не существует, то полагаем $\zeta^{(i,j)}(\pi) = 0$.

Теорема 5. Пусть подстановка $\tilde{\pi}$ в правой части уравнения $\tau \circ \sigma = \tilde{\pi}$ является равновероятной случайной подстановкой степени n . Тогда:

а) если $1 \leq i \leq n$, то

$$\mathbf{P}\{\zeta^{(i,i)}(\tilde{\pi}) = k\} = \frac{1}{n}, \quad k = 1, \dots, n, \quad (6)$$

и при всех $0 \leq x \leq 1$

$$\mathbf{P}\{\zeta^{(i,i)}(\tilde{\pi}) < nx\} \rightarrow x, \quad n \rightarrow \infty, \quad (7)$$

б) если $1 \leq i < j \leq n$, то при всех $0 \leq x \leq 1$

$$\mathbf{P}\left\{\zeta^{(i,j)}(\tilde{\pi}) < nx \mid \zeta^{(i,j)}(\tilde{\pi}) > 0\right\} \rightarrow x^2, \quad n \rightarrow \infty. \quad (8)$$

Расположение материала в работе следующее. В разделе 3 приведен наш вариант доказательства теоремы 2. В разделе 4 изложено доказательство теоремы 5. В заключительном разделе 5 из теорем 2 и 5 выводятся теоремы 3 и 4.

3. Доказательство теоремы 2

Пусть $c_k(\pi)$ — число циклов длины k у подстановки π , а

$$B_n(\pi) = \sum_{k=1}^n c_k(\pi) \ln k.$$

Вычислим $\mathbf{E} B_n(\tilde{\pi})$ и $\mathbf{D} B_n(\tilde{\pi})$ для случайной равновероятной подстановки $\tilde{\pi}$ степени n .

Известно (см., например, [6, с. 186]), что

$$\mathbf{E}(c_k(\tilde{\pi}))_r = \frac{1}{k^r}, \quad k = 1, 2, \dots, [n/r]. \quad (9)$$

Если же $k > [n/r]$, то $\mathbf{E}(c_k(\tilde{\pi}))_r = 0$. Здесь и далее используется обозначение $(m)_r = m(m-1) \cdots (m-r+1)$.

Нетрудно показать также, что

$$\mathbf{E} c_k(\tilde{\pi}) c_l(\tilde{\pi}) = \frac{1}{kl}, \quad k, l \geq 0, \quad k \neq l, \quad k+l \leq n. \quad (10)$$

Если же $k+l > n$, то $\mathbf{E} c_k(\tilde{\pi}) c_l(\tilde{\pi}) = 0$.

Из (9) следует, что

$$\mathbf{E} c_k^2(\tilde{\pi}) = \frac{1}{k} + \frac{1}{k^2}, \quad \text{если } 1 \leq k \leq \frac{n}{2}, \quad (11)$$

$$\mathbf{E} c_k^2(\tilde{\pi}) = \frac{1}{k}, \quad \text{если } \frac{n}{2} < k \leq n. \quad (12)$$

Из (9)–(12) следуют равенства

$$\mathbf{E} B_n(\tilde{\pi}) = \sum_{k=1}^n \mathbf{E} c_k(\tilde{\pi}) \ln k = \sum_{k=1}^n \frac{\ln k}{k} = \frac{1}{2} \ln^2 n + O(1), \quad (13)$$

$$\begin{aligned} \mathbf{D} B_n(\tilde{\pi}) &= \mathbf{E} B_n^2(\tilde{\pi}) - (\mathbf{E} B_n(\tilde{\pi}))^2 = \\ &= \sum_{k=1}^n \mathbf{E} c_k^2(\tilde{\pi}) \ln^2 k + \sum_{k \neq l} \mathbf{E} c_k(\tilde{\pi}) c_l(\tilde{\pi}) \ln k \ln l - \\ &\quad - \sum_{k, l=1}^n \mathbf{E} c_k(\tilde{\pi}) \mathbf{E} c_l(\tilde{\pi}) \ln k \ln l = \\ &= \sum_{k=1}^n \frac{\ln^2 k}{k} + \sum_{k=1}^{[n/2]} \frac{\ln^2 k}{k^2} + \sum_{k \neq l, 1 < k+l \leq n} \frac{\ln k \ln l}{kl} - \sum_{k, l=1}^n \frac{\ln k \ln l}{kl} = \\ &= \sum_{k=1}^n \frac{\ln^2 k}{k} - \sum_{k=[n/2]+1}^n \frac{\ln^2 k}{k^2} - \sum_{k \neq l, n < k+l \leq 2n} \frac{\ln k \ln l}{kl}. \end{aligned}$$

Ясно, что вторая сумма в последнем выражении при $n \rightarrow \infty$ стремится к нулю. Кроме того, при $n \rightarrow \infty$

$$\begin{aligned} \sum_{k \neq l, n < k+l \leq 2n} \frac{\ln k \ln l}{kl} &= \sum_{k \neq l, n < k+l \leq 2n} \frac{(\ln(k/n) + \ln n)(\ln(l/n) + \ln n)}{(k/n)(l/n)} \frac{1}{n^2} = \\ &= O \left(\int_{1 < x+y \leq 2} (\ln x + \ln n) (\ln y + \ln n) \frac{dx}{x} \frac{dy}{y} \right) = \\ &= O \left(\int_{1 < e^u + e^v \leq 2} (u + \ln n) (v + \ln n) du dv \right) = O(\ln^2 n). \end{aligned}$$

Поэтому

$$\mathbf{D} B_n(\tilde{\pi}) = \sum_{k=1}^n \frac{\ln^2 k}{k} + O(\ln^2 n) = \frac{1}{3} \ln^3 n + O(\ln^2 n). \quad (14)$$

Теперь докажем совпадение предельных распределений случайных величин

$$\frac{\ln F_n(\tilde{\pi}) - \frac{1}{2} \ln^2 n}{\sqrt{\frac{1}{3} \ln^3 n}} \quad \text{и} \quad \tilde{B}_n(\tilde{\pi}) = \frac{B_n(\tilde{\pi}) - \frac{1}{2} \ln^2 n}{\sqrt{\frac{1}{3} \ln^3 n}}. \quad (15)$$

Согласно (2)

$$\ln f(r, k) = r \ln k + \ln \left(\sum_{j=0}^{[r/2]} \frac{r!}{(r-2j)! j! (2k)^j} \right).$$

Заметим, что

$$1 \leq \sum_{j=0}^{[r/2]} \frac{r!}{(r-2j)! j! (2k)^j} < \sum_{j=0}^{\infty} \frac{1}{j!} \left(\frac{r(r-1)}{2k} \right)^j = \exp \left\{ \frac{r(r-1)}{2k} \right\}.$$

Поэтому

$$0 \leq \ln \left(\sum_{j=0}^{[r/2]} \frac{r!}{(r-2j)! j! (2k)^j} \right) \leq \frac{r(r-1)}{2k},$$

т. е.

$$\ln f(r, k) = r \ln k + \theta_k \frac{r(r-1)}{2k}, \quad \text{где} \quad 0 < \theta_k < 1. \quad (16)$$

Подставив (16) в (2), получим $\ln F_n(\tilde{\pi}) = \sum_{k=1}^n \ln f(c_k(\tilde{\pi}), k) = B_n(\tilde{\pi}) + \theta R_n(\tilde{\pi})$. Здесь $0 < \theta < 1$, а

$$R_n(\tilde{\pi}) = \sum_{k=1}^n \frac{c_k(\tilde{\pi}) (c_k(\tilde{\pi}) - 1)}{2k}. \quad (17)$$

Согласно (10) и (17)

$$\mathbf{E} R_n(\tilde{\pi}) = \sum_{k=1}^n \frac{1}{2k^3} < \sum_{k=1}^{\infty} \frac{1}{2k^3} < 1.$$

Отсюда следует, что $R_n(\tilde{\pi})$ — ограниченная по вероятности неотрицательная случайная величина, а так как $\mathbf{D} B_n(\tilde{\pi}) \rightarrow \infty$, то

$$\frac{\theta R_n(\tilde{\pi})}{\sqrt{\mathbf{D} B_n(\tilde{\pi})}} = \frac{\ln F_n(\tilde{\pi}) - B_n(\tilde{\pi})}{\sqrt{\mathbf{D} B_n(\tilde{\pi})}}$$

стремится по вероятности к нулю. Из этого свойства, а также из формул (13) и (14) следует, что предельные распределения случайных величин в (15) совпадают.

Осталось воспользоваться результатом работы [7] (см. также [8–12]), согласно которому функция распределения случайной величины $\tilde{B}_n(\tilde{\pi})$ при $n \rightarrow \infty$ сходится к функции стандартного нормального распределения.

Теорема 2 доказана. $\square$

4. Доказательство теоремы 5

Напомним, что обозначение $I_n(i, j)$ используется для множества инволюций из I_n , имеющих цикл (i, j) , а обозначение $I_n(i, i)$ — для инволюций из I_n , имеющих неподвижную точку i . В основе наших рассуждений лежит следующее свойство.

Лемма 1. Пусть $1 \leq i < j \leq n$, σ и τ — инволюции, $\sigma \in I_n(i, j)$ и $\tau \in I_n$. Тогда точки i и j принадлежат одному циклу подстановки $\pi = \tau \circ \sigma$ или двум ее разным циклам одинаковой длины.

Докажем эту лемму, используя схему рассуждений из [3]. Инволюция σ может быть изображена графом с множеством вершин $\mathcal{N} = \{1, \dots, N\}$ и множеством ребер $\bigcup_{a \in \mathcal{N}} \{(a, \sigma(a))\}$ ($(a, \sigma(a))$ и $(\sigma(a), a)$ — это одно и то же ребро). Каждой вершине этого графа инцидентно только одно ребро.

Любая пара инволюций (σ, τ) однозначно описывается графом на $\mathcal{N}$ с ребрами двух цветов, со своими цветами для ребер из σ и τ (σ -ребра и τ -ребра). Этот граф обозначается $\sigma \cup \tau$ и называется *суперпозицией*. Каждой паре инволюций σ и τ отвечает свой граф $\sigma \cup \tau$, который определяет $\tau \circ \sigma$ однозначно.

Каждой вершине графа $\sigma \cup \tau$ инцидентны по одному ребру каждого цвета. Связная компонента графа $\sigma \cup \tau$ является либо *путем*, либо *циклом*.

Путь представляет собой цепочку ребер, в которой смежные ребра имеют разные цвета. Концевые вершины пути помимо ребра, ведущего к смежной вершине, имеют около себя петлю, цвет которой отличается от цвета смежного ребра. Пути графа $\sigma \cup \tau$, содержащему k вершин, в подстановке $\pi = \tau \circ \sigma$ отвечает цикл длины k .

Цикл в $\sigma \cup \tau$ представляет собой цикл, смежные ребра которого имеют разные цвета. Цикл в $\sigma \cup \tau$ обязательно имеет четное число вершин. Циклу в $\sigma \cup \tau$ с $2k$ вершинами отвечают два цикла длины k в подстановке $\pi = \tau \circ \sigma$.

Из этого описания следует, что вершины одной компоненты графа $\sigma \cup \tau$ не могут оказаться в циклах разных длин подстановки $\pi = \tau \circ \sigma$.

Лемма 1 доказана. $\square$

Лемма 2. Условия $\tau \circ \sigma = \pi$, $\sigma \in I_n(i, i)$, $\tau \in I_n$ однозначно определяют переходы инволюций σ и τ на всех точках цикла подстановки π , которому принадлежит точка i .

Доказательство леммы 2. Пусть $i, \pi(i), \pi^2(i), \dots, \pi^{k-1}(i)$ — цикл подстановки π , которому принадлежит точка i . Разложим этот цикл в композицию заданных на множестве $\{i, \pi(i), \pi^2(i), \dots, \pi^{k-1}(i)\}$ инволюций $\sigma' \in I_k(i, i)$ и $\tau' \in I_k$.

Точка i является неподвижной точкой инволюции σ' , ей соответствует концевая вершина i с σ' -петлей на некотором пути длины k в графе $\sigma' \cup \tau'$. Остальные вершины этого пути, если проходить их через одну, отвечают точкам $\pi(i), \pi^2(i), \dots, \pi^{k-1}(i)$. Этим они определяются однозначно.

В графе $\sigma' \cup \tau'$ вершины, связанные σ' -ребрами, образуют циклы инволюции σ' , а вершины, связанные τ' -ребрами, образуют циклы инволюции τ' . Поэтому обе инволюции $\sigma' \in I_k(i, i)$ и $\tau' \in I_k$ определены полностью.

Лемма 2 доказана. $\square$

Лемма 3. Если $\sigma \in I_n(i, j)$, $\tau \in I_n$ и точки i и j принадлежат циклам разной длины подстановки π , то подстановка π не может быть разложена в произведение $\pi = \tau \circ \sigma$.

Если $\sigma \in I_n(i, j)$ и точки i и j принадлежат одному циклу или двум циклам одинаковой длины подстановки π , то переходы инволюций σ и τ определяются однозначно на всех точках тех циклов подстановки π , которым принадлежат точки i и j .

Доказательство леммы 3. Случай, когда точки i и j принадлежат циклам разной длины подстановки π , невозможен. Это следует из леммы 1.

Пусть $j \neq i$ и точки i и j принадлежат одному k -циклу подстановки π . Случай $k = 2$ тривиален. Поэтому далее считаем, что $k \geq 3$.

Одна из точек $j = \sigma(i)$, i (скажем, i) не является концевой вершиной графа $\sigma \cup \tau$. Выйдя из i , пройдем (каждый раз сначала по σ -ребру, а потом по τ -ребру) последовательно вершины, отвечающие $i, \pi(i), \pi^2(i), \dots, \pi^{k-1}(i)$. Среди них есть вершина, отвечающая $j = \pi^\alpha(i)$ при некотором $\alpha \in \{1, \dots, k-1\}$. Значит, в графе $\sigma \cup \tau$ есть σ -ребро $(i, j = \pi^\alpha(i))$ и τ -ребро $(j = \pi^\alpha(i), \pi(i))$.

Сделав два шага из вершины $\pi^\alpha(i)$, сначала по τ -ребру, а потом по σ -ребру, придем к вершине $\pi^{\alpha-1}(i)$. Поэтому в графе присутствуют σ -ребро $(\pi(i), \pi^{\alpha-1}(i))$ и τ -ребро $(\pi^{\alpha-1}(i), \pi^2(i))$.

Далее аналогичным образом последовательно определяются все остальные σ -ребра $(\pi(i), \pi^{\alpha-l}(i))$ и τ -ребра $(\pi^{\alpha-l}(i), \pi^{1+l}(i))$, $l \geq 2$.

Случай, когда точки i и j принадлежат разным k -циклам подстановки π , рассматривается аналогично (см. [3]).

Лемма 3 доказана. $\square$

Лемма 4. Пусть подстановка $\tilde{\pi}$ в правой части уравнения $\tau \circ \sigma = \tilde{\pi}$ является равновероятной случайной подстановкой степени n .

Тогда при всех $1 \leq i < j \leq n$

$$\mathbf{P}\{F_n^{(i,j)}(\tilde{\pi}) > 0\} = \frac{n+1}{2(n-1)}.$$

Доказательство леммы 4. Предположим, что подстановка $\tilde{\pi}$ выбрана равновероятно из множества подстановок с заданной цикловой структурой $(c_1, c_2, \dots, c_n)$. Вычислим вероятность события, состоящего в том, что элементы пары (i, j) отвечают требованиям леммы 3. Здесь для удобства рассуждений можно заменить задачу на эквивалентную и считать, что подстановка $\tilde{\pi}$ задана: $\tilde{\pi} = \pi$, а пара (i, j) , $i < j$, выбирается с равными вероятностями из соответствующего множества.

1) Для каждого цикла длины k подстановки π имеется C_k^2 вариантов выбора пары (i, j) из множества элементов цикла. При любом выборе этот цикл может быть разложен в произведение инволюций $\sigma' \in I_k(i, j)$, $\tau' \in I_k$.

2) Для каждой из $C_{c_k}^2$ пар циклов длины k имеется k вариантов выбора точки i из множества точек первого цикла и k вариантов выбора j из множества точек второго цикла (всего k^2 вариантов).

Вместе это дает

$$\sum_{k=1}^n \left(c_k \frac{k(k-1)}{2} + \frac{c_k(c_k-1)}{2} k^2 \right)$$

вариантов выбора пары (i, j) , приводящих к разложению затронутых ею циклов подстановки $\tilde{\pi}$ в произведение инволюций σ' и τ' (на множестве точек затронутых циклов), при котором инволюция σ' имеет цикл (i, j) . Разделив указанное число на общее число C_n^2 способов выбора пары (i, j) , получим для вероятности $P(c_1, c_2, \dots, c_n)$ наличия этого разложения формулу

$$P(c_1, c_2, \dots, c_n) = \frac{1}{n(n-1)} \sum_{k=1}^n (c_k k(k-1) + c_k(c_k-1)k^2). \quad (18)$$

Используя формулу полной вероятности, формулы (18) и (9), получаем следующее:

$$\begin{aligned}
 \mathbf{P} \{F_n^{(i,j)}(\tilde{\pi}) > 0\} &= \\
 &= \sum_{\substack{c_1, c_2, \dots, c_n \geq 0 \\ c_1 + 2c_2 + \dots + nc_n = n}} P(c_1, c_2, \dots, c_n) \mathbf{P} \{c_1(\tilde{\pi}) = c_1, \dots, c_n(\tilde{\pi}) = c_n\} = \\
 &= \frac{1}{n(n-1)} \sum_{k=1}^n \sum_{c_k} (c_k k(k-1) + c_k (c_k - 1) k^2) \mathbf{P} \{c_k(\tilde{\pi}) = c_k\} = \\
 &= \frac{1}{n(n-1)} \sum_{k=1}^n (k(k-1) \mathbf{E} c_k(\tilde{\pi}) + k^2 \mathbf{E} c_k(\tilde{\pi}) (c_k(\tilde{\pi}) - 1)) = \\
 &= \frac{1}{n(n-1)} \sum_{k=1}^n ((k-1) + 1) = \frac{n+1}{2(n-1)}. \tag{19}
 \end{aligned}$$

Лемма 4 доказана. $\square$

Доказательство теоремы 5. а) Пусть $j = i$. В этом случае согласно лемме 2 величина $\zeta^{(i,i)}(\tilde{\pi})$ выражает длину цикла случайной подстановки, в который входит фиксированная точка i . Легко проверить, что

$$\mathbf{P} \{\zeta^{(i,i)}(\tilde{\pi}) = k\} = \frac{1}{n}, \quad k = 1, \dots, n.$$

Поэтому справедлива формула (6), а распределение случайной величины $\zeta(\tilde{\pi})$ при $n \rightarrow \infty$ слабо сходится к равномерному распределению на $[0, 1]$.

б) Пусть $j \neq i$ и пусть $\tilde{\pi}$ — фиксированная подстановка, а пара (i, j) выбирается из множества всех C_n^2 пар с равными вероятностями. В этом случае, рассуждая так же, как при выводе формулы (18), получаем

$$\mathbf{P} \{\zeta^{(i,j)}(\pi) = k\} = \frac{1}{n(n-1)} \sum_{k=1}^n k(k-1) c_k, \tag{20}$$

если число k нечетно, и

$$\mathbf{P} \{\zeta^{(i,j)}(\pi) = k\} = \frac{1}{n(n-1)} \left(\sum_{k=1}^n k(k-1) c_k + \sum_{k=1}^n \left(\frac{k}{2}\right)^2 c_{k/2} (c_{k/2} - 1) \right), \tag{21}$$

если число k четно.

Из формул (20) и (21) аналогично (19) получаем:

$$\begin{aligned}
 \mathbf{E} \zeta^r(\tilde{\pi}) &= \\
 &= \frac{1}{n(n-1)} \sum_{k=1}^n k^{r+1}(k-1) \mathbf{E} c_k(\tilde{\pi}) + \\
 &\quad + \frac{1}{n(n-1)} \sum_{l=1}^{[n/2]} (2l)^r l^2 \mathbf{E} c_l(\tilde{\pi}) (c_l(\tilde{\pi}) - 1) = \\
 &= \frac{1}{n(n-1)} \sum_{k=1}^n k^r (k-1) + \frac{1}{n(n-1)} \sum_{l=1}^{[n/2]} (2l)^r = \\
 &= \frac{1}{n(n-1)} \sum_{k=1}^n k^{r+1} - \frac{1}{n(n-1)} \sum_{k=1}^n k^r \mathbf{I}\{k \text{ нечетное}\}. \quad (22)
 \end{aligned}$$

В нашем случае

$$\mathbf{E} ((\zeta(\tilde{\pi}))^r | \zeta(\tilde{\pi}) > 0) = \frac{\mathbf{E} \zeta^r(\tilde{\pi})}{\mathbf{P}\{\zeta(\tilde{\pi}) > 0\}}.$$

Поэтому из (22) и леммы 4 получаем равенство

$$\begin{aligned}
 \mathbf{E} ((\zeta^{(i,j)}(\tilde{\pi}))^r | \zeta(\tilde{\pi}) > 0) &= \\
 &= \frac{2}{n(n+1)} \left(\sum_{k=1}^n k^{r+1} - \sum_{k=1}^n k^r \mathbf{I}\{k \text{ нечетное}\} \right) = \\
 &= n^r \frac{2}{n(1+1/n)} \left(\sum_{k=1}^n \left(\frac{k}{n}\right)^{r+1} \frac{1}{n} - \frac{1}{n} \left(\sum_{k=1}^n \left(\frac{k}{n}\right)^r \frac{\mathbf{I}\{k \text{ нечетное}\}}{n} \right) \right).
 \end{aligned}$$

Из него следует, что все моменты случайной величины $\zeta(\tilde{\pi})/n$ сходятся при $n \rightarrow \infty$ к моментам распределения с плотностью $2x$ на $[0, 1]$:

$$\mathbf{E} \left(\left(\frac{\zeta(\tilde{\pi})}{n} \right)^r | \zeta(\tilde{\pi}) > 0 \right) \rightarrow \frac{2}{r+2} = \int_0^1 x^r 2x dx, \quad r = 1, 2, \dots$$

Это распределение определяется своими моментами однозначно. Значит, сходимость (8) имеет место.

Теорема 5 доказана. $\square$

5. Доказательства теорем 3 и 4

Доказательство теоремы 3. Лемма 2 позволяет записать формулу

$$\ln F_n^{(i,i)} = \sum_{k=1}^n \mathbf{I} \{ \zeta^{(i,i)}(\tilde{\pi}) = k \} \ln F_{n-k}(\tilde{\pi}_{n-k}), \quad (23)$$

где k — длина цикла, которому принадлежит точка i , $\tilde{\pi}_{n-k}$ — равновероятная случайная подстановка степени $n-k$, а $F_{n-k}(\tilde{\pi}_{n-k})$ — число всех разложений подстановки $\tilde{\pi}_{n-k}$ в композицию инволюций.

Пусть $n' = n - [n/\ln n]$, а $n \rightarrow \infty$. Согласно теореме 2 при $1 \leq k \leq n'$ для всех $-\infty < x < \infty$

$$\mathbf{P} \left\{ \frac{\ln F_{n-k}(\tilde{\pi}_{n-k}) - \frac{1}{2} \ln^2(n-k)}{\sqrt{\frac{1}{3} \ln^3(n-k)}} < x \right\} \rightarrow \frac{1}{\sqrt{2\pi}} \int_{-\infty}^x e^{-u^2/2} du, \quad (24)$$

причем эта сходимость равномерна по $1 \leq k \leq n'$. Легко проверить, что

$$\ln(n-k) = \ln n + O(\ln |\ln n|),$$

$$\ln^2(n-k) = \ln^2 n + O(\ln n \ln |\ln n|),$$

$$\ln^3(n-k) = \ln^3 n \left(1 + O\left(\frac{\ln |\ln n|}{\ln n}\right) \right),$$

опять же равномерно по $1 \leq k \leq n'$. Поэтому из (24) следует, что

$$\mathbf{P} \left\{ \frac{\ln F_{n-k}(\tilde{\pi}_{n-k}) - \frac{1}{2} \ln^2 n}{\sqrt{\frac{1}{3} \ln^3 n}} < x \right\} \rightarrow \frac{1}{\sqrt{2\pi}} \int_{-\infty}^x e^{-u^2/2} du \quad (25)$$

равномерно по k из диапазона $1 \leq k \leq n'$ для всех $-\infty < x < \infty$.

Из (23) и (6) следует, что

$$\mathbf{P} \left\{ \frac{\ln F_n^{(i,i)} - \frac{1}{2} \ln^2 n}{\sqrt{\frac{1}{3} \ln^3 n}} < x \right\} = \frac{1}{n} \sum_{k=1}^n \mathbf{P} \left\{ \frac{\ln F_{n-k}(\tilde{\pi}_{n-k}) - \frac{1}{2} \ln^2 n}{\sqrt{\frac{1}{3} \ln^3 n}} < x \right\}, \quad (26)$$

причем

$$\frac{1}{n} \sum_{k=n'+1}^n \mathbf{P} \left\{ \frac{\ln F_{n-k}(\tilde{\pi}_{n-k}) - \frac{1}{2} \ln^2 n}{\sqrt{\frac{1}{3} \ln^3 n}} < x \right\} \leq \frac{1}{|\ln n|}. \quad (27)$$

При $n \rightarrow \infty$ из (25)–(27) вытекает соотношение (3).

Теорема 3 доказана. $\square$

Доказательство теоремы 4. Равенство (4) доказано в лемме 4. Докажем соотношение (5).

Наряду с (23) выполнена формула

$$\ln F_n^{(i,j)} = \sum_{k=1}^n \mathbf{I} \{ \zeta^{(i,j)}(\tilde{\pi}) = k \} \ln F_{n-k}(\tilde{\pi}_{n-k}). \quad (28)$$

Из (28) получаем, что

$$\begin{aligned} \mathbf{P} \left\{ \frac{\ln F_n^{(i,j)} - \frac{1}{2} \ln^2 n}{\sqrt{\frac{1}{3} \ln^3 n}} < x \mid F_n^{(i,j)}(\tilde{\pi}) > 0 \right\} = \\ = \sum_{k=1}^n \mathbf{P} \{ \zeta^{(i,j)}(\tilde{\pi}) = k \mid \zeta^{(i,j)}(\tilde{\pi}) > 0 \} \mathbf{P} \left\{ \frac{\ln F_{n-k}(\tilde{\pi}_{n-k}) - \frac{1}{2} \ln^2 n}{\sqrt{\frac{1}{3} \ln^3 n}} < x \right\}. \end{aligned} \quad (29)$$

Кроме того,

$$\begin{aligned} \sum_{k=n'+1}^n \mathbf{P} \{ \zeta^{(i,j)}(\tilde{\pi}) = k \mid \zeta^{(i,j)}(\tilde{\pi}) > 0 \} \mathbf{P} \left\{ \frac{\ln F_{n-k}(\tilde{\pi}_{n-k}) - \frac{1}{2} \ln^2 n}{\sqrt{\frac{1}{3} \ln^3 n}} < x \right\} \leq \\ \leq \mathbf{P} \{ \zeta^{(i,j)}(\tilde{\pi}) > n' \mid \zeta^{(i,j)}(\tilde{\pi}) > 0 \} \rightarrow 0 \end{aligned} \quad (30)$$

(здесь мы воспользовались соотношением (8)).

Из (25), (29) и (30) вытекает соотношение (5).

Теорема 4 доказана. $\square$

Автор признателен А. М. Зубкову и В. О. МIRONКИНУ за полезные замечания.

Список литературы

- [1] Flajolet P., Sedgewick W., *Analytic Combinatorics*, Cambridge: Cambridge Univ. Press, 200, 824 pp.
- [2] Chovla S., Herstein I. N., Moore W. K., "On recursions connected with symmetric groups. I", *Canad. J. Math.*, **3** (1951), 328–334.

- [3] Lugo M., “The cycle structure of compositions of random involutions”, arXiv:0911.3604v1 [math.CO] 18 Nov 2009.
- [4] Lugo M., *Profiles of large combinatorial structures*, PhD Thesis, Univ. Pennsylvania, 2010.
- [5] Burnette Ch., Schmutz E., “Representing random permutations as the product of two involutions”, arXiv: 1507.05701v1 [math.CO] 21 Jul 2015.
- [6] Сачков В. Н., *Вероятностные методы в комбинаторном анализе*, М.: Наука, 1978, 288 с.
- [7] Erdős P., Turán P., “On some problems of a statistical group-theory. III”, *Acta. Math. Acad. Sci. Hungar.*, **18** (1967), 309–320.
- [8] Колчин В. Ф., *Случайные отображения*, М.: Наука, 1984, 208 с.
- [9] Arratia R., Barbour A. D., Tavaré S., “Limit theorems for combinatorial structures”, *Ann. Probab.*, **28**:4 (2000), 1620–1644.
- [10] Arratia R., Tavaré S., “Limit theorems for combinatorial structures via discrete process approximations”, *Rand. Struct. & Algor.*, **3**:3 (1992), 321–345.
- [11] DeLaurentis J. M., Pittel B. G., “Random permutations and Brownian motion”, *Pacific J. Math.*, **119**:2 (1985), 287–301.
- [12] Manstavicius E., “The Berry – Esseen bound in the theory of random permutations”, *Ramanujan J.*, **2**:1-2 (1998), 185–199.