

## ОПЕРАТОР РЕДУЦИРОВАНИЯ. I

В. Н. САЧКОВ

В работе определяется новое понятие оператора редуцирования, отображающего множество постановок степени  $n$  в множество подстановок степени  $n-k$ ,  $1 \leq k \leq n-1$ . Получена формула для вероятности сохранения четности при редуцировании случайной подстановки. Найдены точные и при  $n \rightarrow \infty$  предельные выражения для условных распределений числа единичных циклов и общего числа циклов случайной подстановки при условиях, что число единичных циклов и, соответственно, общее число циклов в соответствующей редуцированной подстановке заданы.

### ВВЕДЕНИЕ

В работе дается определение оператора редуцирования и рассматриваются его свойства. Оператор редуцирования  $R(M)$  определяется как отображение

$$R(M): S_n \rightarrow S_{n-k},$$

где  $M$  — фиксированное  $k$ -подмножество  $n$ -множества  $X$ ,  $S_n$  и  $S_{n-k}$  — совокупности всех подстановок, действующих на множествах  $X$  и  $X \setminus M$  соответственно. Действие  $R(M)$  на подстановку  $s \in S_n$ , имеющее вид  $R(M)(s) = s' \in S_{n-k}$ , состоит в разложении подстановки  $s$  в произведение независимых циклов, удалении из них всех элементов множества  $M$  и построении  $s'$  как произведения прореженных таким образом циклов.

В § 1 устанавливаются некоторые свойства оператора редуцирования. Показано, что совокупность операторов редуцирования, определенных на булеане  $2^X$ , образует коммутативную полугруппу идемпотентов. Для оператора редуцирования  $R(M)$  определяется совокупность обратных операторов, которые применяются для решения систем уравнений, содержащих операторы редуцирования. В частности, даются необходимые и достаточные условия совместности системы уравнений и оценивается число решений.

В § 2 для случайной равновероятной подстановки  $s \in S_n$  находится условное распределение  $P\{\xi_n = \mu \mid \bar{\xi}_{n-k} = \nu\}$ ,  $\mu = \nu, \nu + 1, \dots, n$ , где  $\xi_n$  и  $\bar{\xi}_{n-k}$  — числа циклов в подстановках  $s$  и  $s' = R(M)(s)$ , а  $M$  — фиксированное  $k$ -подмножество  $n$ -множества  $X$ . С использованием производящей функции условного распределения выводится формула для вероятности  $P(n, k)$  сохранения четности случайной подстановки  $s \in S_n$  при редуцировании. В

теореме 1 описаны пределы рассматриваемых условных распределений при  $n \rightarrow \infty$ . При  $\frac{n}{n-k} \rightarrow \infty$  предельное распределение является нормальным, а при  $\frac{n}{n-k} \rightarrow \alpha \geq 1$  — пуассоновским. Найдены точные и асимптотические формулы для среднего и дисперсии условного распределения.

В § 3 получена точная формула для условного распределения  $P\{\eta^{(1)} = \mu \mid \bar{\eta}^{(1)} = \nu\}$ , где  $\eta^{(1)}$  — число единичных циклов в случайной подстановке  $s \in S_n$ , а  $\bar{\eta}^{(1)}$  — число единичных циклов в подстановке  $R(M)(s) = s' \in S_{n-k}$ . В теореме 2 дано описание пределов этих условных распределений при  $\frac{n}{k} \rightarrow \gamma, n \rightarrow \infty$ . Предельное распределение может быть либо пуассоновским, либо вырожденным, либо совпадать с распределением суммы двух независимых случайных величин, имеющих, соответственно, распределение Пуассона с параметром  $\lambda = \gamma$  и биномиальное распределение с числом испытаний  $\nu$  и вероятностью успеха  $p = 1 - \gamma$ .

Оператор редуцирования относится к типу сжимающих отображений, представляющих значительный интерес для криптографии. В частности, оператор редуцирования является математической моделью некоторых шифров колонной замены, осуществляющих шифрование в двух алфавитах.

В дальнейшем автор предполагает провести исследование более общих операторов редуцирования, определенных на множествах произвольных отображений конечного множества.

### § 1. ОПРЕДЕЛЕНИЕ И ОСНОВНЫЕ СВОЙСТВА ОПЕРАТОРА РЕДУЦИРОВАНИЯ

Пусть  $X$  — множество, содержащее  $n$  элементов, и  $M$  — фиксированное  $k$ -подмножество  $X, 1 \leq k \leq n$ . Обозначим через  $S_n$  и  $S_{n-k}$  множества всех подстановок, действующих на  $X$  и  $X \setminus M$ , соответственно.

Отображение

$$R(M): S_n \rightarrow S_{n-k} \tag{1.1}$$

для каждой подстановки  $s \in S_n$  определим равенством

$$R(M)(s) = s', \quad s' \in S_{n-k}, \tag{1.2}$$

которое означает, что в записи подстановки  $s$  в виде произведения независимых циклов удаляются все элементы, принадлежащие множеству  $M$ , а оставшиеся в циклах элементы рассматриваются как разложимые подстановки  $s' \in S_{n-k}$  в произведение независимых циклов. Отметим, что при удалении элементов множества  $M$  некоторые циклы подстановки  $s \in S_n$  могут оказаться пустыми.

Отображение  $R(M)$  вида (1.1) будем называть *оператором редуцирования*. Оператор редуцирования можно доопределить для всех  $M \subset X$ . Если  $M = \emptyset$ , то полагаем  $R(\emptyset)(s) = s$ ; при  $M = X$  считаем, что  $R(X)(s) = \theta$ , где  $\theta$  — пустой элемент множества  $S_0$ .

Область определения оператора  $R(M)$  можно распространить также на все подстановки степени, меньшей  $n$ . Рассмотрим  $m$ -подмножество  $\tilde{X}$  множества  $X$  и обозначим через  $S_m$  совокупность всех подстановок, действующих на множестве  $\tilde{X}$ . Для любой подстановки  $\tilde{s} \in S_m$  действие оператора  $R(M)$

определим равенством

$$R(M)(\tilde{s}) = R(M \cap \tilde{X})(\tilde{s}) = \tilde{s}', \quad (1.3)$$

где подстановка  $\tilde{s}'$  действует на множестве  $\tilde{X} \setminus (M \cap \tilde{X})$ .

Пусть  $2^X$  — булеан, т. е. совокупность всех подмножеств множества  $X$ . Для любых  $M_1, M_2 \in 2^X$  определим операцию умножения  $R(M_1)$  и  $R(M_2)$  равенствами

$$\begin{aligned} R(M_1)R(M_2)(s) &= T(M_1)(R(M_2 \setminus M_1)(s)) \\ &= R(M_1 \setminus M_2)(R(M_2)(s)) = R(M_1 \cup M_2)(s), \end{aligned} \quad (1.4)$$

где  $s \in S_n$ .

Из определения следует, что умножение операторов коммутативно:

$$R(M_1)R(M_2)(s) = R(M_2)R(M_1)(s), \quad (1.5)$$

и обладает свойством идемпотентности:

$$R^2(M)(s) = R(M)(s), \quad (1.6)$$

где  $s \in S_n$ . Таким образом, совокупность операторов редуцирования  $\{R(M) : M \in 2^X\}$  образует коммутативную полугруппу идемпотентов. Эта полугруппа изоморфна полугруппе, в которой элементами являются все подмножества множества  $X$ , а операцией — объединение множеств.

Полный прообраз отображения  $R(M)$ ,  $M \subset X$ , вида (1.1) будем называть *обратным оператором*  $R^*(M)$  по отношению к оператору редуцирования  $R(M)$ . Таким образом,

$$R^*(M)(s') = \{s : R(M)(s) = s', s \in S_n\}, \quad s' \in S_{n-k}. \quad (1.7)$$

Будем рассматривать сужение обратного оператора  $R^*(M)$  на фиксированную подстановку  $s' \in S_{n-k}$ . В этом случае действие оператора  $R^*(M)$  определяет расстановку элементов множества  $M$  в циклах подстановки  $s'$  и образование самостоятельных циклов так, чтобы в результате была получена подстановка  $s \in S_n$ , редуцируемая в  $s' \in S_{n-k}$ . Число таких расстановок элементов множества  $M$  и образования циклов равно  $(n)_k$  и, следовательно, многозначный оператор  $R^*(M)$  при фиксированной подстановке  $s' \in S_{n-k}$  имеет  $(n)_k$  значений, которые можно перенумеровать и использовать запись

$$R^*(M)(s') = \{R_\nu^*(M)(s'), \nu = 1, 2, \dots, (n)_k\},$$

где значение каждого оператора  $R_\nu^*(M)(s')$ ,  $1 \leq \nu \leq (n)_k$ , соответствует фиксированной расстановке элементов множества  $M$ , и выполнены равенства

$$R(M)(R_\nu^*(M)(s')) = s', \quad \nu = 1, 2, \dots, (n)_k. \quad (1.8)$$

Использование обратных операторов можно продемонстрировать при изучении уравнений, содержащих операторы редуцирования. Рассмотрим систему уравнений

$$\begin{aligned} R(M_1)(Z) &= D_1, \\ R(M_2)(Z) &= D_2, \end{aligned} \quad (1.9)$$

где  $D_1$  и  $D_2$  — известные подстановки, действующие на множествах  $X \setminus M_1$  и  $X \setminus M_2$ , соответственно, а  $Z$  — неизвестная подстановка, действующая на множестве  $X$ .

Выясним условия, при которых система (1.9) совместна. Для этого рассмотрим систему уравнений вида

$$\begin{aligned} R(M_1 \setminus (M_1 \cap M_2))(Y) &= D_1, \\ R(M_2 \setminus (M_1 \cap M_2))(Y) &= D_2, \end{aligned} \quad (1.10)$$

где  $Y$  — неизвестная подстановка, действующая на множестве  $X \setminus (M_1 \cap M_2)$ . Если система (1.9) имеет решение  $Z$ , то

$$Y = R(M_1 \cap M_2)(Z) \quad (1.11)$$

— решение системы (1.10). Обратное, если система (1.10) совместна и  $Y_0$  — некоторое ее решение, то для любого решения  $Z = Z_0$  уравнения (1.11) с  $Y = Y_0$  имеем

$$\begin{aligned} R(M_1 \setminus (M_1 \cap M_2))(R(M_1 \cap M_2)(Z_0)) &= D_1, \\ R(M_2 \setminus (M_1 \cap M_2))(R(M_1 \cap M_2)(Z_0)) &= D_2, \end{aligned} \quad (1.12)$$

Из равенства (1.4) следует, что (1.12) есть другая запись системы (1.9) при  $Z = Z_0$ . Таким образом, из совместности системы (1.10) следует совместность системы (1.9).

Установим два свойства системы (1.9).

**Свойство 1.** *Необходимое и достаточное условие совместности системы (1.9) состоит в том, что*

$$R(M_2 \setminus (M_1 \cap M_2))(D_1) = R(M_1 \setminus (M_1 \cap M_2))(D_2). \quad (1.13)$$

Так как совместность системы (1.9) эквивалентна совместности системы (1.10), то необходимость условия (1.13) очевидна.

Для доказательства достаточности рассмотрим подстановку

$$s' = R(M_2 \setminus (M_1 \cap M_2))(D_1) = R(M_1 \setminus (M_1 \cap M_2))(D_2),$$

действующую на множестве  $X \setminus (M_1 \cup M_2)$ , и выберем однозначно определяемые обратные операторы

$$\begin{aligned} R_\gamma^*(M_1 \setminus (M_1 \cap M_2))(s') &\in R^*(M_1 \setminus (M_1 \cap M_2))(s'), \\ R_\delta^*(M_2 \setminus (M_1 \cap M_2))(s') &\in R^*(M_2 \setminus (M_1 \cap M_2))(s') \end{aligned} \quad (1.14)$$

такие, что

$$\begin{aligned} R_\delta^*(M_2 \setminus (M_1 \cap M_2))(R(M_2 \setminus (M_1 \cap M_2))(D_1)) &= D_1, \\ R_\gamma^*(M_1 \setminus (M_1 \cap M_2))(R(M_1 \setminus (M_1 \cap M_2))(D_2)) &= D_2, \end{aligned} \quad (1.15)$$

где подстановки  $D_1$  и  $D_2$  действуют на множествах  $X \setminus M_1$  и  $X \setminus M_2$ , соответственно.

Определим действие оператора  $R_\gamma^*(M_1 \setminus (M_1 \cap M_2))$  на подстановку  $D_1$  и оператора  $R_\delta^*(M_2 \setminus (M_1 \cap M_2))$  на подстановку  $D_2$  следующим образом. Оператор  $R_\gamma^*(M_1 \setminus (M_1 \cap M_2))$  расставляет элементы множества  $M_1 \setminus (M_1 \cap M_2)$  в циклах подстановки  $D_1$  и образует самостоятельные циклы так, что после удаления элементов множества  $M_2 \setminus (M_1 \cap M_2)$  получается подстановка, совпадающая с  $D_2$ . Аналогично, оператор  $R_\delta^*(M_2 \setminus (M_1 \cap M_2))$  расставляет элементы множества  $M_2 \setminus (M_1 \cap M_2)$  в циклах подстановки  $D_2$  и образует самостоятельные циклы так, что после удаления элементов множества  $M_1 \setminus (M_1 \cap M_2)$  получается подстановка, совпадающая с  $D_1$ . Так как  $(M_1 \setminus (M_1 \cap M_2)) \cap (M_2 \setminus (M_1 \cap M_2)) = \emptyset$ , то взаимное расположение элементов множеств  $M_1 \setminus (M_1 \cap M_2)$  и  $M_2 \setminus (M_1 \cap M_2)$  можно выбрать таким образом, чтобы было выполнено равенство

$$Y_0 = R_\gamma^*(M_1 \setminus (M_1 \cap M_2))(D_1) = R_\delta^*(M_2 \setminus (M_1 \cap M_2))(D_2), \quad (1.16)$$

где  $Y_0$  — подстановка степени  $|X \setminus (M_1 \cap M_2)|$ .

По этой же причине порядок действия обратных операторов  $R_\gamma^*(M_1 \setminus (M_1 \cap M_2))$  и  $R_\delta^*(M_2 \setminus (M_1 \cap M_2))$  не существен. Из равенств (1.8), (1.13), (1.15) и (1.16) следует, что  $Y_0$  является решением системы (1.10) и, стало быть, система (1.9) совместна.

**СВОЙСТВО 2.** Если  $\alpha = |M_1 \cap M_2|$ ,  $\beta = |M_1 \cup M_2|$ , то  $d(\alpha, \beta)$  — число решений совместной системы (1.9) — удовлетворяет неравенствам

$$(n)_\alpha \leq d(\alpha, \beta) \leq (n)_\beta. \quad (1.17)$$

Так как системы (1.9) и (1.10) совместны одновременно и в силу равенства (1.11) каждому решению  $Y_0$  системы (1.10) соответствуют  $(n)_\alpha$  решений системы (1.9), то  $d(\alpha, \beta) \geq (n)_\alpha$ . Число решений совместной системы (1.9) не превосходит числа решений уравнения

$$\begin{aligned} R(M_1 \cup M_2)(Z) &= R(M_2 \setminus (M_1 \cap M_2))(D_1) \\ &= R(M_1 \setminus (M_1 \cap M_2))(D_2), \end{aligned}$$

равного  $(n)_\beta$ , т. е.  $d(\alpha, \beta) \leq (n)_\beta$ .

## § 2. РАСПРЕДЕЛЕНИЕ ЧИСЛА ЦИКЛОВ В РЕДУЦИРУЕМОЙ ПОДСТАНОВКЕ

На множестве  $S_n$  подстановок, действующих на  $n$ -множестве  $X$ , зададим равномерное вероятностное распределение и обозначим через  $\xi_n$  случайную величину, равную числу циклов в случайной подстановке  $s \in S_n$ . Для фиксированного  $k$ -множества  $M \subseteq X$  рассмотрим оператор редуцирования  $R(M)$  и положим  $R(M)(s) = s'$ ,  $s' \in S_{n-k}$ . Для случайной подстановки  $s \in S_n$  и любой фиксированной подстановки  $s'_0 \in S_{n-k}$  имеем:

$$\mathbf{P} \{s' = s'_0\} = \frac{1}{(n-k)!}, \quad (2.1)$$

т. е. при заданных условиях оператор редуцирования индуцирует на множестве  $S_{n-k}$  равномерное распределение.

Обозначим через  $\bar{\xi}_{n-k}$  число циклов в случайной подстановке  $s' \in S_{n-k}$ . Рассмотрим условное распределение

$$\mathbf{P}\{\xi_n = \mu \mid \bar{\xi}_{n-k} = \nu\} = \frac{\mathbf{P}\{\xi_n = \mu, \bar{\xi}_{n-k} = \nu\}}{\mathbf{P}\{\bar{\xi}_{n-k} = \nu\}}, \quad \mu = \nu, \nu + 1, \dots, n. \quad (2.2)$$

Докажем, что

$$\mathbf{P}\{\xi_n = \mu \mid \bar{\xi}_{n-k} = \nu\} = \frac{1}{\binom{n}{k}} \sum_{j=0}^{k-\mu+\nu} \binom{n-k+j-1}{j} \mathbf{P}\{\xi_{k-j} = \mu - \nu\}, \quad (2.3)$$

$\mu = \nu, \nu + 1, \dots, n$ .

Обозначим через  $C_{n\mu}$  число подстановок степени  $n$ , имеющих  $\mu$  циклов, а через  $C_{n\mu}(k, \nu)$  — число таких подстановок  $s \in S_n$ , действующих на множестве  $X$  и имеющих  $\mu$  циклов, что подстановка  $R(M)(s) = s' \in S_{n-k}$ , где  $M \subseteq X$ ,  $|M| = k$ , имеет  $\nu$  циклов. Имеет место соотношение

$$C_{n\mu}(k, \nu) = C_{n-k, \nu} \sum_{j=0}^{k-\mu+\nu} \binom{k}{j} C_{k-j, \mu-\nu}(n-k+j-1)_j. \quad (2.4)$$

Действительно, при построении полного прообраза отображения  $R(M)$  с областью определения  $s'$  рассмотрим совокупность таких обратных операторов  $R_t^*$ ,  $1 \leq t \leq (n)_k$ , при действии которых  $j$  элементов множества  $M$  включаются в циклы подстановки  $R(M)(s) = s' \in S_{n-k}$ , а  $k-j$  элементов образуют новые циклы подстановки  $s \in S_n$ . Число обратных операторов  $R_t^*$ ,  $1 \leq t \leq (n)_k$ , такого вида равно

$$\binom{k}{j} (n-k+j-1)_j C_{k-j, \mu-\nu}.$$

Суммируя по  $j$ , получаем  $C_{n\mu}(k, \nu)$  — число всех подстановок  $s \in S_n$ , обладающих указанными свойствами.

Так как

$$\mathbf{P}\{\xi_n = \mu, \bar{\xi}_{n-k} = \nu\} = \frac{C_{n\mu}(k, \nu)}{n!} \quad (2.5)$$

и имеет место равенство (2.1), то из соотношения (2.4) после очевидных преобразований следует равенство (2.3). Используя выражение для распределения числа циклов в случайной подстановке степени  $n$  (см. [1])

$$\mathbf{P}\{\xi_n = \mu\} = \frac{|s(n, \mu)|}{n!}, \quad \mu = 1, 2, \dots, n, \quad (2.6)$$

где  $s(n, \mu)$  — числа Стирлинга первого рода, из равенства (2.3) получаем формулу для условного распределения вида (2.2)

$$\mathbf{P}\{\xi_n = \mu \mid \bar{\xi}_{n-k} = \nu\} = \frac{1}{\binom{n}{k}} \sum_{j=0}^{k-\mu+\nu} \binom{n-k+j-1}{j} \frac{|s(k-j, \mu-\nu)|}{(k-j)!}, \quad (2.7)$$

$\mu = \nu, \nu + 1, \dots, n$ .

Известно [1], что случайная величина  $\xi_n$  имеет производящую функцию

$$P_n(x) = \sum_{\mu=0}^n \mathbf{P}\{\xi_n = \mu\} x^\mu = \binom{n+x-1}{n}. \quad (2.8)$$

С учетом формулы (2.8) из соотношения (2.3) получаем производящую функцию условного распределения

$$\begin{aligned} P_{nk}(x; \nu) &= \sum_{\mu=\nu}^n \mathbf{P}\{\xi_n = \mu \mid \bar{\xi}_{n-k} = \nu\} x^\mu \\ &= \frac{x^\nu}{\binom{n}{k}} \sum_{j=0}^k \binom{n-k+j-1}{j} \binom{k-j+x-1}{k-j}. \end{aligned} \quad (2.9)$$

Из тождества

$$\binom{n+x-1}{k} = \sum_{j=0}^k \binom{n-k+j-1}{j} \binom{k-j+x-1}{k-j}$$

и равенств (2.9) вытекает, что производящая функция  $P_{nk}(x; \nu)$  имеет вид

$$P_{nk}(x; \nu) = x^\nu \frac{\binom{n+x-1}{k}}{\binom{n}{k}} = x^\nu \frac{\Gamma(n+x) \Gamma(n-k+1)}{\Gamma(n+1) \Gamma(n-k+x)}, \quad (2.10)$$

где  $\Gamma$  — гамма-функция.

Функция (2.10) позволяет получить выражение для вероятности  $P(n, k)$  того, что случайная равновероятная подстановка  $s \in S_n$  сохраняет четность при применении к ней оператора редуцирования  $R(M)$ , где  $M$  — фиксированное  $k$ -множество. Покажем, что

$$P(n, k) = \begin{cases} \frac{1}{2} \left( 1 + \frac{(n-k)(n-k-1)}{n(n-1)} \right), & k \text{ — четное,} \\ \frac{1}{2} \left( 1 - \frac{(n-k)(n-k-1)}{n(n-1)} \right), & k \text{ — нечетное.} \end{cases} \quad (2.11)$$

Полагая в формуле (2.10)  $x = 1$  и  $x = -1$ , находим, что

$$P^{(1)}(n, k) = \sum_{j=0}^k \mathbf{P}\{\xi_n = \nu + 2j \mid \bar{\xi}_{n-k} = \nu\} = \frac{1}{2} \left( 1 + \frac{(n-k)(n-k-1)}{n(n-1)} \right), \quad (2.12)$$

$$P^{(2)}(n, k) = \sum_{j=0}^k \mathbf{P}\{\xi_n = \nu + 2j + 1 \mid \bar{\xi}_{n-k} = \nu\} = \frac{1}{2} \left( 1 - \frac{(n-k)(n-k-1)}{n(n-1)} \right). \quad (2.13)$$

Если число циклов подстановки  $s \in S_n$  равно  $\mu$ , причем число циклов подстановки  $R(M)(s) = s' \in S_{n-k}$  равно  $\nu$ , то декременты подстановок  $s$  и  $s'$  равны  $\delta = n - \mu$ ,  $\delta' = n - k - \nu$ , соответственно. При четном  $k$  четность декрементов  $\delta$  и  $\delta'$  совпадает тогда и только тогда, когда  $\mu = \nu + 2j$ ,  $j = 0, 1, \dots$ . Для случайной подстановки  $s \in S_n$  вероятность такого события равна  $P^{(1)}(n, k)$  и

определяется формулой (2.12). При нечетном  $k$  совпадение четности декрементов  $\delta$  и  $\delta'$  имеет место тогда и только тогда, когда  $\mu = \nu + 2j + 1$ ,  $j = 0, 1, \dots$ . Для случайной подстановки  $s \in S_n$  вероятность этого события равна  $P^{(2)}(n, k)$  и определяется формулой (2.13). Из формул (2.12) и (2.13) следуют формулы (2.11).

Рассмотрим теперь предельное поведение условного распределения (2.2) при  $n \rightarrow \infty$ .

ТЕОРЕМА 1. При  $n \rightarrow \infty$  справедливы следующие утверждения:

а) если  $\frac{n}{n-k} \rightarrow \infty$ , то для функции распределения

$$F_{nk}(x) = \mathbf{P} \left\{ \frac{\xi_n - \nu - \ln \frac{n}{n-k}}{\sqrt{\ln \frac{n}{n-k}}} \leq x \mid \bar{\xi}_{n-k} = \nu \right\} \quad (2.14)$$

имеет место предельное соотношение

$$F_{nk}(x) \rightarrow \frac{1}{\sqrt{2\pi}} \int_{-\infty}^x e^{-u^2/2} du; \quad (2.15)$$

б) если  $\frac{n}{n-k} \rightarrow \alpha \in [1, \infty)$ , то

$$P_{n,k}(r) = \mathbf{P} \{ \xi_n - \nu = r \mid \bar{\xi}_{n-k} = \nu \} \rightarrow \frac{\lambda^r}{r!} e^{-\lambda}, \quad r = 0, 1, \dots, \quad (2.16)$$

где  $\lambda = \ln \alpha$ .

Для доказательства теоремы используем асимптотическое представление

$$\frac{\Gamma(n+x)}{\Gamma(n+1)} = n^{x-1}(1+o(1)), \quad (2.17)$$

в котором остаточный член стремится к нулю при  $n \rightarrow \infty$  равномерно для всех  $x \in (1-\delta, 1+\delta)$ ,  $0 < \delta < 1$ . Это представление доказывается с помощью формулы Стирлинга для  $\Gamma$ -функции.

Если  $\frac{n}{n-k} \rightarrow \infty$  и  $n-k \rightarrow \infty$ , то из формул (2.10) и (2.17) находим, что

$$P_{nk}(x; \nu) = x^\nu \left( \frac{n}{n-k} \right)^{x-1} (1+o(1)), \quad (2.18)$$

где остаточный член стремится к нулю равномерно для всех  $x \in (1-\delta, 1+\delta)$ ,  $0 < \delta < 1$ . Для производящей функции моментов  $M_{nk}(t; \nu)$  условного распределения, определяемого функцией распределения  $F_{nk}(x)$ , имеет место формула (см. [1])

$$M_{nk}(t; \nu) = \exp \left\{ -\frac{m+\nu}{\sigma} t \right\} P_{nk}(e^{t/\sigma}; \nu), \quad (2.19)$$

где  $m = \sigma^2 = \ln \frac{n}{n-k}$ .

В силу соотношений (2.18) и (2.19) при  $n \rightarrow \infty$  для любого  $t$

$$M_{nk}(t; \nu) = \exp \left\{ -\frac{mt}{\sigma} + (e^{t/\sigma} - 1) \ln \frac{n}{n-k} \right\} (1+o(1)). \quad (2.20)$$

Если  $\frac{n}{n-k} \rightarrow \infty$  и  $n-k$  ограничено, то асимптотическая формула для  $M_{nk}(t; \nu)$  имеет вид

$$M_{nk}(t; \nu) = \exp \left\{ -\frac{mt}{\sigma} + (e^{t/\sigma} - 1) \ln n \right\} (1+o(1)). \quad (2.21)$$

Из формул (2.20) и (2.21) следует, что

$$M_{nk}(t; \nu) \rightarrow e^{t^2/2} \quad \text{при} \quad \frac{n}{n-k} \rightarrow \infty. \quad (2.22)$$

Согласно теореме Куртисса [3] из соотношения (2.22) следует справедливость п. а) теоремы 1.

В п. б) теоремы из условия  $\frac{n}{n-k} \rightarrow \alpha \in [1, \infty)$  следует, что  $n-k \rightarrow \infty$ , и, значит, для  $P_{nk}(x; \nu)$  имеет место асимптотическое представление (2.18). Производящая функция моментов  $\widetilde{M}_{nk}(t; \nu)$  условного распределения  $P_{nk}(r)$ ,  $r = 0, 1, \dots$ , определенного в соотношении (2.16), следующим образом выражается через производящую функцию  $P_{nk}(x; \nu)$  (см. [1]):

$$\widetilde{M}_{nk}(t; \nu) = e^{-\nu t} P_{nk}(e^t; \nu). \quad (2.23)$$

Из формул (2.18) и (2.23) при  $n \rightarrow \infty$  для любого  $t$  имеем:

$$\widetilde{M}_{nk}(t; \nu) = \exp \left\{ (e^t - 1) \ln \frac{n}{n-k} \right\} (1 + o(1)). \quad (2.24)$$

Поэтому при  $\frac{n}{n-k} \rightarrow \alpha$  для любого  $t$

$$\widetilde{M}_{nk}(t; \nu) \rightarrow \exp \{ (e^t - 1) \ln \alpha \}. \quad (2.25)$$

В соответствии с теоремой Куртисса из соотношения (2.25) следует справедливость п. б) теоремы.

Выведем формулы для среднего  $E_{nk}(\nu)$  и дисперсии  $D_{nk}(\nu)$  условного распределения  $\xi_n$  при условии  $\xi_{n-k} = \nu$ .

Вычисляя первую и вторую производные производящей функции  $P_{nk}(x; \nu)$  в точке  $x = 1$ , находим, что

$$\begin{aligned} E_{nk}(\nu) &= \nu + H_n - H_{n-k}, \\ D_{nk}(\nu) &= H_n - H_{n-k} - \gamma_n + \gamma_{n-k}, \end{aligned}$$

где

$$H_n = \sum_{j=1}^n \frac{1}{j}, \quad \gamma_n = \sum_{j=1}^n \frac{1}{j^2}.$$

Используя при  $n \rightarrow \infty$  асимптотические формулы

$$\sum_{j=1}^n \frac{1}{j} = \ln n + C + o(1), \quad \sum_{j=1}^n \frac{1}{j^2} = \frac{\pi^2}{6} + o(1),$$

где  $C = 0,5772\dots$  есть постоянная Эйлера, при  $n-k \rightarrow \infty$  получаем, что

$$\begin{aligned} E_{nk}(\nu) &= \nu + \ln \frac{n}{n-k} + o(1), \\ D_{nk}(\nu) &= \ln \frac{n}{n-k} + o(1). \end{aligned}$$

Если  $n-k = d < \infty$ , то при  $n \rightarrow \infty$  имеем:

$$\begin{aligned} E_{nk}(\nu) &= \nu + \ln n + C - \gamma_d + o(1), \\ D_{nk}(\nu) &= \ln n + C + H_d + \gamma_d + o(1). \end{aligned}$$

### § 3. РАСПРЕДЕЛЕНИЕ ЧИСЛА ЕДИНИЧНЫХ ЦИКЛОВ

Зафиксировав  $k$ -подмножество  $M$  в  $n$ -множестве  $X$ , будем рассматривать распределение числа единичных циклов в случайной равновероятной подстановке  $s \in S_n$  при условии, что число единичных циклов в подстановке  $R(M)(s) \in S_{n-k}$  задано.

Обозначим через  $H_{n\mu}(k; \nu)$  число таких подстановок  $s \in S_n$ , имеющих  $\mu$  единичных циклов, что подстановка  $R(M)(s) \in S_{n-k}$  имеет  $\nu$  единичных циклов.

Заметим, что

$$H_{n\mu}(k; \nu) = 0 \quad \text{при} \quad |\mu - \nu| > k, \quad (3.1)$$

поэтому в дальнейшем предполагаем, что  $|\mu - \nu| \leq k$ . Кроме того, если  $t$  единичных циклов подстановки  $R(M)(s) \in S_{n-k}$  одновременно являются единичными циклами подстановки  $s \in S_n$ , то

$$\frac{\mu + \nu - k}{2} \leq t \leq \min(\mu, \nu). \quad (3.2)$$

Для любой фиксированной подстановки  $R(M)(s) \in S_{n-k}$  с  $\nu$  единичными циклами найдем число таких подстановок  $s \in S_n$  с  $\mu$  единичными циклами, которые могут быть получены применением к ней обратного оператора  $R^*(M)$ .

Число подстановок степени  $n - k$  с  $\nu$  единичными циклами равно (см. [2])

$$\binom{n-k}{\nu} h_{n-k-\nu} = \frac{(n-k)!}{\nu!} \sum_{j=0}^{n-k-\nu} \frac{(-1)^j}{j!}, \quad (3.3)$$

где  $h_d$  — число подстановок степени  $d$  без единичных циклов.

Пусть  $R(M)(s)$  и  $s$  имеют  $t$  общих единичных циклов. Тогда в результате действия оператора  $R^*(M)$  остальные  $\nu - t$  единичных циклов подстановки  $R(M)(s)$  переходят в некоторые неединичные циклы подстановки  $s \in S_n$  за счет размещения в этих циклах каких-то  $i$  элементов,  $\nu - t \leq i \leq k$ , из множества  $M$ . Часть подстановки  $s \in S_n$ , соответствующая этим циклам, строится следующим образом. Образует  $i!((\nu - t)! l_1 \dots l_{\nu-t})^{-1}$  способами подстановку степени  $i$  с  $\nu - t$  циклами длин  $l_1, \dots, l_{\nu-t}$ , а затем  $(\nu - t)!$  способами распределим элементы  $\nu - t$  единичных циклов подстановки  $R(M)(s)$  по циклам построенной подстановки, по одному в каждом цикле, и далее  $l_1 l_2 \dots l_{\nu-t}$  способами расположим эти элементы внутри циклов подстановки. Известно [2], что если  $C_{nk}(A)$  — число подстановок степени  $n$ , имеющих  $k$  циклов, длины которых являются элементами заданной последовательности  $A$ , то

$$C_{nk}(A) = \frac{n!}{k!} \sum_{\substack{x_1 + \dots + x_k = n \\ x_i \in A, 1 \leq i \leq k}} \frac{1}{x_1 x_2 \dots x_k}. \quad (3.4)$$

В соответствии с формулой (3.4) общее число вариантов указанного выше построения части подстановки  $s \in S_n$  равно

$$\frac{i!}{(\nu - t)!} \sum_{\substack{l_1 + \dots + l_{\nu-t} = i \\ l_i \geq 1}} \frac{1}{l_1 \dots l_{\nu-t}} l_1 \dots l_{\nu-t} (\nu - t)! = \binom{i-1}{\nu-t-1} i!. \quad (3.5)$$

Далее, при применении оператора  $R^*(M)$  в неединичные циклы подстановки  $R(M)(s)$ , содержащие  $n - k - \nu$  элементов, вставляются  $j - i$  элементов из  $M$ ,  $i \leq j \leq k$ , числом способов, равным

$$(n - k - \nu)(n - k - \nu + 1) \cdots (n - k - \nu - j - i - 1) = \binom{n - k - \nu + j - i - 1}{j - i} (j - i)!. \quad (3.6)$$

Наконец, количество способов построения части подстановки  $s$ , которая полностью уничтожается при редуцировании и которая имеет  $\mu - t$  единичных циклов, в соответствии с формулой (3.3) равно

$$\binom{k - j}{\mu - t} h_{k - j - \mu + t} = \frac{(k - j)!}{(\mu - t)!} \sum_{l=0}^{k - j - \mu + t} \frac{(-1)^l}{l!}. \quad (3.7)$$

Теперь из равенств (3.5), (3.6), (3.7) выводим формулу

$$\begin{aligned} H_{n\mu}(k; \nu) &= \binom{n - k}{\nu} h_{n - k - \nu} \\ &\times \sum_{t=\max(0, \frac{\mu + \nu - k}{2})}^{\min(\mu, \nu)} \binom{\nu}{t} \sum_{j=\nu-t}^k \sum_{i=\nu-t}^j \binom{k}{j} \binom{j}{i} \binom{i-1}{\nu-t-1} \binom{n - k - \nu + j - i - 1}{j - i} \\ &\times \binom{k - j}{\mu - t} h_{k - j - \mu + t} i! (j - i)!. \end{aligned} \quad (3.8)$$

Используя равенства

$$\begin{aligned} &\sum_{i=\nu-t}^j \binom{n - k - \nu + j - i - 1}{j - i} \binom{i-1}{\nu-t-1} \\ &= \sum_{i=0}^{j-\nu+t} \binom{n - k - \nu + (j - \nu + t - i) - 1}{j - \nu + t - i} \binom{\nu - t + i - 1}{i} \\ &= \binom{n - k + j - \nu - 1}{j - \nu + t} \end{aligned} \quad (3.9)$$

и проводя необходимые упрощения, из формулы (3.8) получаем, что

$$\begin{aligned} H_{n\mu}(k, \nu) &= U_{n-k-\nu} k! (n - k)! \sum_{t=\max(0, \frac{\mu + \nu - k}{2})}^{\min(\mu, \nu)} \frac{1}{t! (\nu - t)! (\mu - t)!} \\ &\times \sum_{j=\nu-t}^k \binom{n - k + j - \nu - 1}{j - \nu + t} U_{k - j - \mu + t}, \end{aligned} \quad (3.10)$$

где

$$U_d = \sum_{l=0}^d \frac{(-1)^l}{l!}. \quad (3.11)$$

Заметим, что

$$\begin{aligned} & \sum_{j=\nu-t}^k \binom{n-k+j-\nu-1}{j-\nu+t} U_{k-j-\mu+t} \\ &= \sum_{r=0}^{k-\mu-\nu+2t} \frac{(-1)^r}{r!} \sum_{j=0}^{k-\mu-\nu+2t-r} \binom{n-k-t+j-1}{j}. \end{aligned} \quad (3.12)$$

Кроме того,

$$\sum_{j=0}^{k-\mu-\nu+2t-r} \binom{n-k-t+j-1}{j} = \binom{n-\mu-\nu+t-r}{k-\mu-\nu+2t-r}. \quad (3.13)$$

Используя равенства (3.12) и (3.13), формулу (3.11) представим в следующем виде:

$$\begin{aligned} H_{n\mu}(k; \nu) &= U_{n-k-\nu} k! (n-k)! \sum_{t=\max(0, \frac{\mu+\nu-k}{2})}^{\min(\mu, \nu)} \frac{1}{t! (\mu-t)! (\nu-t)!} \\ &\times \sum_{r=0}^{k-\mu-\nu+2t} \frac{(-1)^r}{r!} \binom{n-\mu-\nu+t-r}{k-\mu-\nu+2t-r}. \end{aligned} \quad (3.14)$$

Из формулы (3.14) следует, в частности, что

$$H_{n0}(k; \nu) = U_{n-k-\nu} k! (n-k)! \frac{1}{\nu!} \sum_{r=0}^{k-\nu} \frac{(-1)^r}{r!} \binom{n-\nu-r}{k-\nu-r}, \quad (3.15)$$

$$H_{n\mu}(k; 0) = U_{n-k} k! (n-k)! \frac{1}{\mu!} \sum_{r=0}^{k-\mu} \frac{(-1)^r}{r!} \binom{n-\mu-r}{k-\mu-r}. \quad (3.16)$$

Перейдем теперь к формулировке и доказательству результатов вероятностного характера. На множестве подстановок  $S_n$  зададим равномерное вероятностное распределение и обозначим через  $\eta^{(1)}$  число единичных циклов в случайной подстановке  $s \in S_n$ , а через  $\bar{\eta}^{(1)}$  — число единичных циклов в случайной подстановке  $R(M)(s) \in S_{n-k}$ , где  $M$  — фиксированное  $k$ -множество. Рассмотрим условное распределение

$$\mathbf{P}\{\eta^{(1)} = \mu \mid \bar{\eta}^{(1)} = \nu\} = \frac{\mathbf{P}\{\eta^{(1)} = \mu, \bar{\eta}^{(1)} = \nu\}}{\mathbf{P}\{\bar{\eta}^{(1)} = \nu\}}. \quad (3.17)$$

Так как

$$\mathbf{P}\{\eta^{(1)} = \mu, \bar{\eta}^{(1)} = \nu\} = \frac{H_{\nu\mu}(k; \nu)}{n!}, \quad \mu = 0, 1, \dots, n, \quad (3.18)$$

$$\mathbf{P}\{\bar{\eta}^{(1)} = \nu\} = \frac{U_{n-k-\nu}}{\nu!}, \quad \nu = 0, 1, \dots, n-k,$$

то согласно (3.17)

$$\mathbf{P}\{\eta^{(1)} = \mu \mid \bar{\eta}^{(1)} = \nu\} = \frac{\nu! H_{n\mu}(k; \nu)}{n! U_{n-k-\nu}}. \quad (3.19)$$

Из формул (3.16) и (3.19) получаем выражение для условного распределения:

$$\mathbf{P}\{\eta^{(1)} = \mu \mid \bar{\eta}^{(1)} = \nu\} = \frac{1}{\binom{n}{k}} \sum_{t=\max(0, \frac{\mu+\nu-k}{2})}^{\min(\mu, \nu)} \frac{(\nu)_t}{t! (\mu-t)!} \times \sum_{r=0}^{k-\mu-\nu+2t} \frac{(-1)^r}{r!} \binom{n-\mu-\nu+t-r}{k-\mu-\nu+2t-r}, \quad \mu = 0, 1, \dots, n. \quad (3.20)$$

В частности, для  $\nu = 0$  распределение принимает вид

$$\mathbf{P}\{\eta^{(1)} = \mu \mid \bar{\eta}^{(1)} = 0\} = \frac{1}{\binom{n}{k}} \frac{1}{\mu!} \sum_{r=0}^{k-\mu} \frac{(-1)^r}{r!} \binom{n-\mu-r}{k-\mu-r}, \quad \mu = 0, 1, \dots, k. \quad (3.21)$$

Асимптотическое поведение условного распределения (3.20) при  $n \rightarrow \infty$  описывает следующая теорема.

**ТЕОРЕМА 2.** Пусть  $n \rightarrow \infty$  и  $k/n \rightarrow \gamma$ . Тогда

а) при  $\gamma = 0$

$$\mathbf{P}\{\eta^{(1)} = \mu \mid \bar{\eta}^{(1)} = \nu\} \rightarrow \begin{cases} 1, & \mu = \nu, \\ 0, & \mu \neq \nu; \end{cases} \quad (3.22)$$

б) при  $\gamma = 1$

$$\mathbf{P}\{\eta^{(1)} = \mu \mid \bar{\eta}^{(1)} = \nu\} \rightarrow \frac{1}{\mu!} e^{-1}, \quad \mu = 0, 1, \dots; \quad (3.23)$$

в) при  $0 < \gamma < 1$

$$\mathbf{P}\{\eta^{(1)} = \mu \mid \bar{\eta}^{(1)} = \nu\} \rightarrow e^{-\gamma} \sum_{t=0}^{\min(\mu, \nu)} \binom{\nu}{t} (1-\gamma)^t \frac{\gamma^{\mu+\nu-2t}}{(\mu-t)!}, \quad \mu = 0, 1, \dots. \quad (3.24)$$

Для доказательства теоремы при  $0 \leq \gamma < 1$  используем формулу (3.20). Внутреннюю сумму в правой части этой формулы, поделенную на  $\binom{n}{k}$ , разобьем на две суммы с пределами суммирования, определяемыми неравенствами

$$0 \leq r \leq [k^{1/2-\varepsilon}], \quad [k^{1/2-\varepsilon}] + 1 \leq r \leq k - \mu - \nu + 2t, \quad 0 < \varepsilon < 1/2.$$

Используя при  $0 < \gamma < 1$  оценку

$$\binom{n-\mu-\nu+t-r}{k-\mu-\nu+2t-r} = \binom{n}{k} \gamma^{\mu+\nu-2t+r} (1-\gamma)^t (1+o(1)) \quad \text{при } n \rightarrow \infty,$$

равномерную для всех  $0 \leq r \leq [k^{1/2-\varepsilon}]$ , для первой суммы получаем асимптотическое представление

$$e^{-\gamma} \gamma^{\mu+\nu-2t} (1-\gamma)^t (1+o(1)). \quad (3.25)$$

Вторая сумма имеет порядок

$$O\left(\sqrt{k} \left(\frac{\gamma e}{k^{1/2-\varepsilon}}\right)^{k^{1/2-\varepsilon}}\right) \quad (3.26)$$

и, следовательно, стремится к нулю при  $n \rightarrow \infty$ . Теперь соотношение (3.24) следует из оценок (3.25) и (3.26) и формулы (3.20).

Если  $\gamma = 1$ , то при  $n \rightarrow \infty$

$$\frac{1}{\binom{n}{k}} \binom{n - \mu - \nu + t - r}{k - \mu - \nu + 2t - r} = \begin{cases} 1 + o(1), & t = 0, \\ o(1), & t > 0, \end{cases}$$

и поэтому из формулы (3.20) следует соотношение (3.23).

**СЛЕДСТВИЕ.** Если  $n \rightarrow \infty$  и  $k/n \rightarrow \gamma$ ,  $0 \leq \gamma \leq 1$ , то

$$P\{\eta^{(1)} = \mu \mid \bar{\eta}^{(1)} = 0\} \rightarrow \frac{\gamma^\mu}{\mu!} e^{-\gamma}, \quad \mu = 0, 1, \dots \quad (3.27)$$

Непосредственным вычислением устанавливается, что предельное распределение условного распределения числа единичных циклов имеет производящую функцию

$$f(x; \nu) = e^{\gamma(x-1)} (\gamma + (1-\gamma)x)^\nu. \quad (3.28)$$

Из вида производящей функции (3.28) следует, что предельное распределение совпадает с предельным распределением суммы двух независимых случайных величин, одна из которых имеет распределение Пуассона с параметром  $\lambda = \gamma$ , а другая — биномиальное распределение с числом испытаний  $\nu$  и вероятностью успеха  $p = 1 - \gamma$ . Среднее и дисперсия предельного распределения имеют вид

$$\begin{aligned} E(\gamma, \nu) &= \gamma + \nu(1 - \gamma), \\ D(\gamma, \nu) &= \gamma + \nu\gamma(1 - \gamma). \end{aligned} \quad (3.29)$$

При  $\gamma = 1$  условное распределение совпадает с распределением Пуассона с параметром  $\lambda = 1$ , т.е. с предельным распределением числа единичных циклов в случайной подстановке, когда ее степень стремится к бесконечности.

## СПИСОК ЛИТЕРАТУРЫ

1. Сачков В. Н. Вероятностные методы в комбинаторном анализе. М.: Наука, 1978, 287 с.
2. Сачков В. Н. Введение в комбинаторные методы дискретной математики. М.: Наука, 1982, 384 с.
3. Curtiss I. H. A note on the theory of moment generating functions. — Ann. Math. Statist., 1942, v. 13, № 3, p. 430–433.