

## ЦЕПИ МАРКОВА ИТЕРАЦИОННЫХ СИСТЕМ ПРЕОБРАЗОВАНИЙ

В. Н. САЧКОВ

В статье рассматриваются свойства матрицы переходных вероятностей  $\Pi_n$  цепи Маркова итерационной системы преобразований для случаев, когда соответствующая матрица  $n\Pi_n$  частот конфигураций подстановки  $s \in S_n$  определяется группами  $(\mathbf{GF}(2^m), \oplus)$  и  $(N_n, +)$ . Для группы  $(N_n, +)$  получен критерий эргодичности цепи Маркова для четного  $n$  и достаточные условия эргодичности для нечетного  $n$ . Для случайной равновероятной подстановки  $s \in S_n$  найдены оценки среднего и вероятностные границы для максимального элемента матрицы  $\Pi_n$ , которые в случае  $(\mathbf{GF}(2^m), \oplus)$  улучшают известные оценки из статей [2] и [3]. Приведены выраженные через перманенты вероятностные распределения и формулы для моментов дефицита случайной равновероятной подстановки; установлена связь этого распределения с распределением числа положительных диагональных элементов соответствующей матрицы.

### § 1. ВВЕДЕНИЕ

Пусть  $(A, \otimes)$  — конечная аддитивная абелева группа с  $n$ -элементным множеством, операцией  $\otimes$  и нейтральным элементом  $e$ . В дальнейшем будем рассматривать два типа абелевых групп:

$(\mathbf{GF}(2^m), \oplus)$  — аддитивная группа поля  $\mathbf{GF}(2^m)$ ;

$(N_n, +)$  — аддитивная группа кольца вычетов по модулю  $n$ ,  $N_n = \{0, 1, \dots, n-1\}$ .

Обозначим через  $S_n$  совокупность всех подстановок степени  $n$ , действующих на множестве  $A$ . Для рассматриваемых типов групп и подстановки  $s \in S_n$  положим

$$h_{ij} = |\{\nu: s(\nu \otimes i) = s(\nu) \otimes j, \nu \in A\}| \quad (1.1)$$

для всех  $i, j \in A \setminus \{e\}$ ,  $\otimes \in \{\oplus, +\}$ .

Рассмотрим простую однородную цепь Маркова, состояниями которой являются элементы множества  $A \setminus \{e\}$ , с матрицей переходных вероятностей

$$\Pi_n = (P_{ij}), \quad i, j \in A \setminus \{e\}, \quad (1.2)$$

где  $P_{ij} = h_{ij}/n$ .

Для группы  $(\mathbf{GF}(2^m), \oplus)$ ,  $n = 2^m$ , цепи Маркова данного вида рассматривались в ряде работ в качестве вероятностных моделей шифрования с применением итерационных систем преобразований в связи с оценкой эффективности применения к этим моделям известного метода дифференциального криптоанализа [1–3].

Эффективность этого метода зависит от структуры и матрицы  $\Pi_n$  и величины ее максимального элемента. В связи с этим в работе [2] показано, что при случайном равновероятном выборе подстановки  $s \in S_n$ ,  $n = 2^m$ , среднее значение максимального элемента матрицы при достаточно больших  $m$  удовлетворяет неравенству

$$\mathbf{E} P^*(m) \leq \frac{m}{2^{m-1}}. \quad (1.3)$$

В статье [3] при тех же условиях получено, что при  $m \rightarrow \infty$

$$\mathbf{P} \left( \frac{m \ln 2}{2^{m-1} \ln m} \leq \max_{1 \leq i, j \leq 2^{m-1}} P_{ij} \leq \frac{m}{2^{m-1}} \right) \rightarrow 1. \quad (1.4)$$

В § 1 настоящей работы при  $m \rightarrow \infty$  получена оценка

$$\mathbf{E} P^*(m) \leq \frac{m \ln 2}{2^{m-2} \ln m} \left( 1 + \frac{1}{\ln \ln m} \right) + O \left( \frac{1}{2} \exp \left\{ -\frac{m 2 \ln 2}{\ln \ln m} \left( 1 + O \left( \frac{(\ln \ln m)^2}{\ln m} \right) \right) \right\} \right), \quad (1.5)$$

которая улучшает оценку (1.3) примерно в  $1/2 \ln m$  раз. Кроме того, установлено, что при  $m \rightarrow \infty$

$$\mathbf{P} \left( \frac{1}{2} \leq \frac{2^{m-2} \ln m}{m \ln 2} \max_{1 \leq i, j \leq 2^{m-1}} P_{ij} \leq 1 + \frac{1}{\ln \ln m} \right) \rightarrow 1. \quad (1.6)$$

В соотношении (1.6) отношение главного члена верхней оценки к главному члену нижней оценки равно примерно 2, в то время как в соотношении (1.4) такое отношение равно  $\frac{\ln m}{\ln 2}$ .

В этом же параграфе для группы  $(N_n, +)$  при  $n \rightarrow \infty$  получена оценка для среднего значения максимального элемента  $P_n^*$  матрицы  $\Pi_n$  вида

$$\mathbf{E} P_n^* \leq \frac{2 \ln n}{n \ln \ln n} \left( 1 + \frac{1}{\ln \ln \ln n} \right) + O \left( \frac{1}{n} \exp \left\{ -\frac{2 \ln n}{\ln \ln \ln n} \left( 1 + O \left( \frac{(\ln \ln \ln n)^2}{\ln \ln n} \right) \right) \right\} \right), \quad (1.7)$$

а также показано, что

$$\mathbf{P} \left( P_n^* \leq \frac{2 \ln n}{n \ln \ln n} \left( 1 + \frac{1}{\ln \ln \ln n} \right) \right) \rightarrow 1. \quad (1.8)$$

В § 3 для группы  $(N_n, +)$  предложен критерий неразложимости матрицы  $\Pi_n$ , который при четном  $n$  является также и критерием примитивности этой матрицы. Для нечетного  $n$  приводятся достаточные условия примитивности неразложимой матрицы. Даны достаточные условия неразложимости матрицы  $\Pi_n$ , проверка которых имеет полиномиальную сложность.

В § 4 для случайной равновероятной подстановки  $s \in S_n$  в группе  $(N_n, +)$  рассматривается задача о вероятностном распределении случайной величины  $\zeta$ , равной числу положительных элементов матрицы  $\Pi_n$ . Найдено выражение для среднего значения

$$\mathbf{E}(\zeta) = (n-1)^2 \left( 1 - \sum_{0 \leq k \leq n/2} \frac{(-1)^k}{k!} \frac{\binom{n}{k} e}{\binom{n}{2k}} \right)$$

и асимптотика при  $n \rightarrow \infty$

$$\mathbf{E} \zeta = (1 - e^{-1})(n-1)^2(1 + o(1)).$$

Установлена связь распределения числа положительных элементов на главной диагонали матрицы  $\Pi_n$  с распределением дефицита  $\xi_n$  случайной подстановки  $s \in S_n$ . Указывается точное распределение  $\xi_n$ , выраженное через перманенты циклических  $(0,1)$ -матриц, а также приводятся точные и асимптотические формулы для биномиальных моментов, среднего и дисперсии. Указываются также некоторые результаты из статьи автора [4], касающиеся распределения числа положительных элементов в строке матрицы  $\Pi_n$ .

## § 2. ВЕРОЯТНОСТНЫЕ СВОЙСТВА МАТРИЦЫ $\Pi_n$

Вероятностные свойства матрицы  $\Pi_n$  для случайной подстановки  $s \in S$  будем рассматривать отдельно для групп  $(N_n, +)$  и  $\mathbf{GF}(2^m, \oplus)$ ,  $n = 2^m$ .

а) *Группа  $(N_n, +)$ .* На множестве подстановок  $S_n$  зададим равномерное вероятностное распределение.

Для случайной подстановки  $s \in S_n$  рассмотрим такую случайную величину  $\xi_{n\nu}(i, j)$ ,  $1 \leq i, j \leq n-1$ , что

$$\xi_{n\nu}(i, j) = \begin{cases} 1, & \text{если существует такое } \nu, 1 \leq \nu \leq n-1, \\ & \text{что } s(\nu+j) = s(\nu) + j, \\ 0, & \text{если такого } \nu \text{ не существует.} \end{cases} \quad (2.1)$$

Случайную величину  $\eta_n(i, j)$  определим равенством

$$\eta_n(i, j) = \sum_{0 \leq \nu \leq n-1} \xi_{n\nu}(i, j), \quad i, j = 1, 2, \dots, n-1. \quad (2.2)$$

Используя известную формулу (см. [5]) для биномиальных моментов  $B_{kn}$  случайной величины  $\eta_n(i, j)$

$$B_{kn} = \sum_{0 \leq \nu_1 < \dots < \nu_k \leq n-1} \mathbf{P} \{ \xi_{n\nu_1}(i, j) = 1, \dots, \xi_{n\nu_k}(i, j) = 1 \}, \quad k = 0, 1, \dots, n-1,$$

и равенство

$$\mathbf{P} \{ \xi_{n\nu_1}(i, j) = 1, \dots, \xi_{n\nu_k}(i, j) = 1 \} = \frac{k!(n-2k)!}{n!},$$

находим, что

$$B_{kn} = \begin{cases} \frac{1}{k!} \frac{(n)_k^2}{(n)_{2k}}, & 0 \leq k \leq n/2, \\ 0, & k > n/2. \end{cases} \quad (2.3)$$

Распределение  $\eta_n(i, j)$  не зависит от  $(i, j)$ , поэтому, полагая  $\eta_n = \eta_n(i, j)$ , из известной формулы (см. [5])

$$\mathbf{P}(\eta_n = r) = \sum_{r \leq k \leq n/2} (-1)^{k-r} \binom{k}{r} B_{kn}, \quad 0 \leq r \leq n/2, \quad (2.4)$$

находим, что при  $n \rightarrow \infty$  для любого фиксированного  $r = 0, 1, \dots$

$$\mathbf{P}(\eta_n = r) \rightarrow \frac{1}{r!} e^{-1} \quad (2.5)$$

в силу соотношения

$$B_{kn} \rightarrow \frac{1}{k!}, \quad (2.6)$$

справедливого при  $n \rightarrow \infty$  для фиксированного  $k = 0, 1, \dots$

Кроме того, из неравенств Бонферрони следует, что (см. [5])

$$\mathbf{P}(\eta_n \geq r) \leq B_{rn}, \quad r = 0, 1, \dots \quad (2.7)$$

Рассмотрим случайную величину

$$\eta_n^* = \max_{1 \leq i, j \leq n-1} \eta_n(i, j). \quad (2.8)$$

Из равенств

$$\mathbf{P}(\eta_n^* = r) = \mathbf{P}\left(\bigcup_{1 \leq i, j \leq n-1} \left(\{\eta_n(i, j) = r\} \cap \bigcap_{1 \leq \mu, \nu \leq n-1, (\mu, \nu) \neq (i, j)} \{\eta_n(\mu, \nu) \leq r\}\right)\right),$$

$$r = 0, 1, \dots, \quad (2.9)$$

находим, что

$$\mathbf{P}(\eta_n^* = r) \leq (n-1)^2 \mathbf{P}(\eta_n = r), \quad r = 0, 1, \dots \quad (2.10)$$

Из соотношений (2.9), (2.6) и (2.2) вытекает, что

$$\mathbf{P}\{\eta_n^* = r\} \leq \frac{(n-1)^2}{r!} \frac{(n)_r^2}{(n)_{2r}}, \quad 0 \leq r \leq n/2; \quad (2.11)$$

$$\mathbf{P}\{\eta_n^* = r\} = 0, \quad r > n/2.$$

Отсюда следует, что при  $n \rightarrow \infty$  для всех

$$r \geq \frac{2 \ln n}{\ln \ln n} \left(1 + \frac{1}{\ln \ln \ln n}\right) \quad (2.12)$$

справедлива оценка

$$\mathbf{P}\{\eta_n^* = r\} \leq \exp \left\{ -\frac{2 \ln n}{\ln \ln \ln n} \left(1 + O\left(\frac{(\ln \ln \ln n)^2}{\ln \ln n}\right)\right) \right\}. \quad (2.13)$$

Полагая

$$h = \frac{2 \ln n}{\ln \ln n} \left(1 + \frac{1}{\ln \ln \ln n}\right), \quad (2.14)$$

для среднего значения  $\eta_n^*$  получаем оценку

$$E_n = \mathbf{E} \eta_n^* \leq h + R_n(h), \quad (2.15)$$

где

$$R_n(h) = \sum_{h \leq r \leq n/2} r \mathbf{P}\{\eta_n^* = r\}. \quad (2.16)$$

Из соотношений (2.13)–(2.16) находим, что при  $n \rightarrow \infty$

$$E_n \leq \frac{2 \ln n}{\ln \ln n} \left( 1 + \frac{1}{\ln \ln \ln n} \right) + O \left( \exp \left\{ -\frac{2 \ln n}{\ln \ln \ln n} \left( 1 + O \left( \frac{(\ln \ln \ln n)^2}{\ln \ln n} \right) \right) \right\} \right). \quad (2.17)$$

Для любых событий  $A_1, A_2, \dots, A_k$  имеет место неравенство

$$\mathbf{P}(A_1 \cap \dots \cap A_k) \geq 1 - \sum_{i=1}^k (1 - P(A_i)). \quad (2.18)$$

С использованием неравенства (2.18) находим, что

$$\mathbf{P} \left( \bigcap_{1 \leq i, j \leq n-1} \{\eta_n(i, j) \leq r\} \right) \geq 1 - \sum_{1 \leq i, j \leq n-1} \mathbf{P}\{\eta_n(i, j) \geq r\}. \quad (2.19)$$

Из неравенств (2.19) и (2.7) и формулы (1.2) получаем, что

$$\mathbf{P} \left( \bigcap_{1 \leq i, j \leq n-1} \{\eta_n(i, j) \leq r\} \right) \geq 1 - \frac{(n-1)^2 (n_r)^2}{r! (n)_{2r}}, \quad r = 0, 1, \dots \quad (2.20)$$

Из неравенства (2.20) следует оценка

$$\mathbf{P}(\eta_n^* \leq r) \geq 1 - \frac{(n-1)^2 (n_r)^2}{r! (n)_{2r}}. \quad (2.21)$$

Следовательно, для всех  $r$ , удовлетворяющих условию (2.12),

$$\mathbf{P}(\eta_n^* \leq r) \geq 1 - \varepsilon_1, \quad (2.22)$$

где  $\varepsilon_1 \geq 0$  и при  $n \rightarrow \infty$

$$\varepsilon_1 = O \left( \exp \left\{ -\frac{2 \ln n}{\ln \ln \ln n} \left( 1 + O \left( \frac{(\ln \ln \ln n)^2}{\ln \ln n} \right) \right) \right\} \right).$$

Из условия (2.12) и неравенства (2.22) вытекает, что при  $n \rightarrow \infty$

$$\mathbf{P} \left( \eta_n^* \leq \frac{2 \ln n}{\ln \ln n} \left( 1 + \frac{1}{\ln \ln \ln n} \right) \right) \geq 1 - \varepsilon_2, \quad (2.23)$$

где  $\varepsilon_2 \geq 0$  и при  $n \rightarrow \infty$

$$\varepsilon_2 = O \left( \exp \left\{ -\frac{2 \ln n}{\ln \ln n} \left( 1 + O \left( \frac{(\ln \ln \ln n)^2}{\ln \ln n} \right) \right) \right\} \right).$$

При случайном равновероятном выборе подстановки  $s \in S_n$  элемент  $P_{ij} = P_{ij}(s)$  матрицы  $\Pi_n$ ,  $1 \leq i, j \leq n-1$ , является случайной величиной, причем в соответствии с равенством (2.2) имеет место соотношение

$$P_{ij} = P_{ij}(s) = \frac{1}{n} \eta_n(i, j), \quad 1 \leq i, j \leq n-1. \quad (2.24)$$

Из соотношений (2.8), (2.17) и (2.22) при  $n \rightarrow \infty$  для среднего значения случайной величины

$$P_n^* = \max_{1 \leq i, j \leq n-1} P_{ij} \quad (2.25)$$

получаем оценку

$$\begin{aligned} \mathbf{E} P_n^* &\leq \frac{2 \ln n}{n \ln \ln n} \left( 1 + \frac{1}{\ln \ln \ln n} \right) + \\ &+ O \left( \frac{1}{n} \exp \left\{ -\frac{2 \ln n}{\ln \ln \ln n} \left( 1 + O \left( \frac{(\ln \ln \ln n)^2}{\ln \ln n} \right) \right) \right\} \right). \end{aligned} \quad (2.26)$$

Кроме того,

$$\mathbf{P} \left( P_n^* \leq \frac{2 \ln n}{n \ln \ln n} \left( 1 + \frac{1}{\ln \ln \ln n} \right) \right) \geq 1 - \varepsilon_3, \quad (2.27)$$

где  $\varepsilon_3 \geq 0$  и при  $n \rightarrow \infty$

$$\varepsilon_3 = O \left( \frac{1}{n} \exp \left\{ -\frac{2 \ln n}{\ln \ln \ln n} \left( 1 + O \left( \frac{(\ln \ln \ln n)^2}{\ln \ln n} \right) \right) \right\} \right).$$

Таким образом, при случайном равновероятном выборе подстановки  $s \in S_n$  максимальный элемент  $P_n^*$  матрицы  $\Pi_n$  при  $n \rightarrow \infty$  удовлетворяет условиям

$$\mathbf{P} \left( P_n^* \leq \frac{2 \ln n}{n \ln \ln n} \left( 1 + \frac{1}{\ln \ln \ln n} \right) \right) \rightarrow 1. \quad (2.28)$$

б) Группа  $(\mathbf{GF}(2^m), \oplus)$ . В этом случае так же, как и в соотношении (2.1), определяются случайные величины  $\xi_\nu^{(m)}(i, j)$  и рассматривается случайная величина

$$\eta^{(m)}(i, j) = \sum_{0 \leq \nu \leq 2^m - 1} \xi_\nu^{(m)}(i, j). \quad (2.29)$$

Из свойства операции  $\oplus$  следует, что случайная величина  $\eta^{(m)}(i, j)$  принимает только четные значения.

Поэтому рассматривается случайная величина  $(1/2)\eta^{(m)}(i, j)$ , для которой биномиальные моменты выражаются формулой

$$B_k^{(m)} = \frac{2^k (2^{m-1})^2}{k! (2^m)_{2k}}, \quad k = 0, 1, \dots, 2^{m-1}. \quad (2.30)$$

Вывод формулы (2.30) аналогичен выводу формулы (2.3).

Таким образом, аналогично формуле (2.4)

$$\mathbf{P}(\eta^{(m)}(i, j) = 2r) = \sum_{r \leq k \leq 2^{m-1}} (-1)^{k-r} \binom{k}{r} B_k^{(m)}, \quad r = 0, 1, \dots, 2^{m-1}, \quad (2.31)$$

и при  $m \rightarrow \infty$  в силу соотношения

$$B_k^{(m)} \rightarrow \frac{1}{2^k} \frac{1}{k!}, \quad (2.32)$$

справедливого для любого фиксированного  $k = 0, 1, \dots$ , находим, что для любого фиксированного  $r$

$$\mathbf{P}(\eta^{(m)} = 2r) \rightarrow \frac{1}{2^r r!} e^{-1/2}, \quad r = 0, 1, \dots, \quad (2.33)$$

где

$$\eta^{(m)} = \eta^{(m)}(i, j), \quad 1 \leq i, j \leq 2^m - 1.$$

Кроме того, в соответствии с соотношением (2.7)

$$\mathbf{P}(\eta^{(m)} \geq 2r) \leq B_r^{(m)}, \quad r = 0, 1, \dots \quad (2.34)$$

Так же, как и в соотношении (2.10), для случайной величины

$$\eta^*(m) = \max_{1 \leq i, j \leq 2^{m-1}} \eta^{(m)}(i, j) \quad (2.35)$$

справедлива оценка

$$\mathbf{P}(\eta^*(m) = 2r) \leq (2^m - 1)^2 \mathbf{P}(\eta^{(m)} = 2r), \quad r = 0, 1, \dots \quad (2.36)$$

Из соотношений (2.36), (2.34) и (2.30) находим, что

$$\mathbf{P}(\eta^*(m) = 2r) \leq \frac{(2^m - 1)^2 2^r (2^{m-1})_r^2}{r! (2^m)_{2r}}, \quad 0 \leq r \leq 2^{m-1}, \quad (2.37)$$

$$\mathbf{P}(\eta^*(m) = 2r) = 0, \quad r > 2^{m-1}.$$

Отсюда следует, что при  $m \rightarrow \infty$  и

$$r \geq \frac{m2 \ln 2}{\ln m} \left( 1 + \frac{1}{\ln \ln m} \right), \quad (2.38)$$

справедливо соотношение

$$\mathbf{P}(\eta^*(m) = 2r) \leq \exp \left\{ -\frac{m2 \ln 2}{\ln \ln m} \left( 1 + O \left( \frac{(\ln \ln m)^2}{\ln m} \right) \right) \right\}. \quad (2.39)$$

Поэтому для среднего значения  $E^{(m)} = \mathbf{E} \eta^*(m)$  при  $m \rightarrow \infty$  получаем оценку

$$E^{(m)} \leq \frac{m4 \ln 2}{\ln m} \left( 1 + \frac{1}{\ln \ln m} \right) + O \left( \exp \left\{ -\frac{m2 \ln 2}{\ln \ln m} \left( 1 + O \left( \frac{(\ln \ln m)^2}{\ln m} \right) \right) \right\} \right). \quad (2.40)$$

Вывод неравенства (2.40) аналогичен выводу неравенства (2.17).

Так же, как соотношение (2.21), выводится неравенство

$$\mathbf{P}(\eta^*(m) \leq 2r) \geq 1 - \frac{(2^m - 1)^2 2^r (2^{m-1})_r^2}{r! (2^m)_{2r}}, \quad r = 0, 1, \dots \quad (2.41)$$

Из неравенства (2.41) для всех  $r$ , удовлетворяющих условию (1.37), получаем оценку

$$\mathbf{P}(\eta^*(m) \leq 2r) \geq 1 - \varepsilon_4, \quad (2.42)$$

где  $\varepsilon_4 \geq 0$  и при  $m \rightarrow \infty$

$$\varepsilon_4 = O \left( \exp \left\{ -\frac{m2 \ln 2}{\ln \ln m} \left( 1 + O \left( \frac{(\ln \ln m)^2}{\ln m} \right) \right) \right\} \right).$$

Отсюда следует, что

$$\mathbf{P} \left( \eta^*(m) \leq \frac{m4 \ln 2}{\ln m} \left( 1 + \frac{1}{\ln \ln m} \right) \right) \geq 1 - \varepsilon_5, \quad (2.43)$$

где  $\varepsilon_5 \geq 0$  и при  $m \rightarrow \infty$

$$\varepsilon_5 = O \left( \exp \left\{ -\frac{m2 \ln 2}{\ln \ln m} \left( 1 + O \left( \frac{(\ln \ln m)^2}{\ln m} \right) \right) \right\} \right).$$

Для случая группы  $(\mathbf{GF}(2^m), \oplus)$  при случайном равновероятном выборе подстановки  $s \in S_{2^m}$  элемент матрицы  $\Pi_n$  имеет следующее выражение:

$$P_{ij} = P_{ij}(s) = \frac{1}{2^m} \eta^{(m)}(i, j),$$

и, следовательно, для среднего значения максимального элемента

$$P^*(m) = \max_{1 \leq i, j \leq 2^m - 1} P_{ij}$$

при  $m \rightarrow \infty$  в соответствии с (2.40) справедлива оценка

$$\begin{aligned} \mathbf{E} P^*(m) &\leq \frac{m \ln 2}{2^{m-2} \ln m} \left( 1 + \frac{1}{\ln \ln m} \right) + \\ &+ O \left( \frac{1}{2^m} \exp \left\{ -\frac{m 2 \ln 2}{\ln \ln m} \left( 1 + O \left( \frac{(\ln \ln m)^2}{\ln m} \right) \right) \right\} \right), \end{aligned} \quad (2.44)$$

которая примерно в  $(1/2) \ln m$  раз снижает известную оценку (1.3) из [2].

Далее, из соотношения (2.42) следует, что

$$\mathbf{P} \left( P^*(m) \leq \frac{m \ln 2}{2^{m-2} \ln m} \left( 1 + \frac{1}{\ln \ln m} \right) \right) \geq 1 - \varepsilon_6, \quad (2.45)$$

где  $\varepsilon_6 \geq 0$  и при  $m \rightarrow \infty$

$$\varepsilon_6 = O \left( \exp \left\{ -\frac{m 2 \ln 2}{\ln \ln m} \left( 1 + O \left( \frac{(\ln \ln m)^2}{\ln m} \right) \right) \right\} \right).$$

Соотношение (2.44) позволяет улучшить вероятностную оценку максимального элемента матрицы  $\Pi_n$  вида (1.4), полученную в [3].

Из (1.4) и (2.44) при  $m \rightarrow \infty$  получаем соотношение

$$\mathbf{P} \left( \frac{1}{2} \leq \frac{2^{m-2} \ln m}{m \ln 2} \max_{1 \leq i, j \leq 2^m - 1} P_{ij} \leq 1 + \frac{1}{\ln \ln m} \right) \rightarrow 1. \quad (2.46)$$

В соотношении (2.46) отношение главного члена верхней границы оценки к нижней равно примерно 2, в то время как в соотношении (1.4) такое отношение равно  $(\ln m) / \ln 2$ .

### §3. УСЛОВИЯ НЕРАЗЛОЖИМОСТИ, ПРИМИТИВНОСТИ И ВПОЛНЕ НЕРАЗЛОЖИМОСТИ МАТРИЦЫ $\Pi_n$

Напомним, что неотрицательная квадратная матрица  $A = (a_{ij})$ ,  $i, j = 1, 2, \dots, n$ , называется разложимой, если существует такая подстановочная матрица  $\Pi$  порядка  $n$ , что

$$\text{ПАП}^T = \begin{pmatrix} B & O \\ C & D \end{pmatrix},$$

где  $O$  — нулевая матрица,  $B$  и  $D$  — квадратные матрицы и  $T$  — знак транспонирования.

Если  $C$  — нулевая матрица, то матрица называется вполне разложимой.

Матрица  $A$  называется неразложимой, если она не является разложимой.

Условие неразложимости матрицы удобно сформулировать в виде леммы, доказательство которой следует прямо из определения неразложимости.

**ЛЕММА 1.** Для неразложимости неотрицательной матрицы  $A = (a_{ij})$ ,  $i, j = 1, 2, \dots, n$ , необходимо и достаточно, чтобы для любого  $k$ ,  $1 \leq k \leq n - 1$ , и любого  $k$ -сочетания  $1 \leq i_1 < \dots < i_k \leq n$  существовали такие  $\mu$  и  $\nu$ ,  $1 \leq \nu \leq k$ ,  $1 \leq \nu \leq n - k$ , что  $a_{i_\mu j_\nu} > 0$ , где  $\{j_1, j_2, \dots, j_{n-k}\} = \{1, 2, \dots, n\} \setminus \{i_1, i_2, \dots, i_k\}$ .

Разложимая дважды стохастическая матрица является вполне разложимой. Поэтому при проверке выполнения критерия, сформулированного в лемме 1, для случая дважды стохастических матриц можно ограничиться значениями  $k$ , удовлетворяющими условию  $1 \leq k \leq n/2$ .

Неотрицательная матрица  $A$  называется примитивной, если существует такое натуральное значение  $\gamma$ , что  $A^\gamma > 0$ , т. е.  $A^\gamma$  — матрица, все элементы которой положительны. Минимальное значение  $\gamma$ , удовлетворяющее условию  $A^\gamma > 0$ , называется экспонентом матрицы  $A$ .

Неотрицательной матрице  $A = (a_{ij})$ ,  $i, j = 1, 2, \dots, n$ , поставим в соответствие ориентированный граф  $\Gamma(A)$ , вершины которого помечены элементами  $1, 2, \dots, n$ , и вершины  $i$  и  $j$  соединены дугой  $(i, j)$ , если  $a_{ij} > 0$ .

**ЛЕММА 2.** Матрица  $A$  неразложима тогда и только тогда, когда граф  $\Gamma(A)$  сильно связан. Матрица примитивна тогда и только тогда, когда длины контуров сильно связного графа  $\Gamma(A)$  имеют наибольший общий делитель, равный единице.

**СЛЕДСТВИЕ 1.** Неразложимая матрица  $A = (a_{ij})$ ,  $i, j = 1, 2, \dots, n$ , примитивна, если существует такое  $i$ , что  $a_{ii} > 0$ ,  $1 \leq i \leq n$ . Условие взаимной простоты длин циклов графа  $\Gamma(A)$  эквивалентно ацикличности матрицы  $A$ .

Прежде, чем установить условия неразложимости и примитивности матрицы  $P_n$ , рассмотрим некоторые вспомогательные понятия.

Пусть  $S_n$  — множество подстановок, действующих на группе  $(N_n, +)$ . Будем говорить, что подстановка  $s \in S_n$  для элемента  $\delta \in N_n$  образует  $(i, j)$ -конфигурацию, если

$$s(\delta + i) = s(\delta) + j, \quad i, j \in N_n \setminus \{0\}.$$

Подстановка  $s \in S_n$  образует  $(i, j)$ -конфигурацию для элемента  $\delta \in N_n$  тогда и только тогда, когда подстановка  $s^{-1}t^{-i}st^j$  содержит единичный цикл с элементом  $s(\delta) = s(\delta + i) - j$ , где  $t$  — полноцикловая подстановка ви-

да  $t = (0, n-1, n-2, \dots, 1)$ . Иными словами, это означает, что подстановка  $s^{-1}t^{-i}s$  непротиворечива с подстановкой  $t^{-j}$  на  $s(\delta)$ -м месте.

Разностной характеристикой подстановки  $s \in S_n$  называется вектор  $\Delta(s) = (\Delta_0, \Delta_1, \dots, \Delta_{n-1})$ , где  $\Delta_i$  — наименьший неотрицательный вычет, определяемый условием

$$\Delta_i \equiv (s(i) - i) \pmod{n}, \quad i = 0, 1, \dots, n-1.$$

Теперь сформулируем критерий неразложимости дважды стохастической матрицы  $\Pi_n = (P_{ij})$ ,  $i, j = 1, 2, \dots, n-1$ , определенной равенствами (1.1) и (1.2) для случая группы  $(N_n, +)$ .

**ТЕОРЕМА 1.** Для неразложимости матрицы  $\Pi_n$  необходимо и достаточно, чтобы для любого  $k$ ,  $1 \leq k \leq n/2$ , и любого  $k$ -сочетания  $1 \leq i_1 < \dots < i_k \leq n-1$  существовали такие  $\mu$  и  $\nu$ ,  $1 \leq \mu \leq k$ ,  $1 \leq \nu \leq n-k-1$ , что разностная характеристика  $\Delta(s^{-1}t^{-i_\mu}s)$  содержала элемент  $j_\nu$ , где  $\{j_1, j_2, \dots, j_{n-k-1}\} = \{1, 2, \dots, n-1\} \setminus \{i_1, i_2, \dots, i_k\}$ .

Действительно, в соответствии с леммой 1 для неразложимости матрицы  $\Pi_n$  должны существовать указанные в теореме  $\mu$  и  $\nu$  такие, что  $P_{i_\mu j_\nu} > 0$ . Это эквивалентно условию, что подматрица  $\Pi_n(i_1, \dots, i_k; j_1, \dots, j_{n-k-1})$  матрицы  $\Pi_n$ , расположенная на пересечении строк и столбцов с номерами  $i_1, \dots, i_k$  и  $j_1, \dots, j_{n-k-1}$ , соответственно, является ненулевой. Данное условие выполнено тогда и только тогда, когда существует  $(i_\mu, j_\nu)$ -конфигурация для  $1 \leq \mu \leq k$ ,  $1 \leq \nu \leq n-k-1$ . Такая  $(i_\mu, j_\nu)$ -конфигурация существует в том и только том случае, когда подстановка  $s^{-1}t^{-i_\mu}s$  непротиворечива с подстановкой  $t^{-j_\nu}$ , т. е. подстановка  $s^{-1}t^{-i_\mu}st^{j_\nu}$  имеет единичный цикл. Это условие выполнено тогда и только тогда, когда разностная характеристика  $\Delta(s^{-1}t^{-i_\mu}s)$  содержит элемент  $j_\nu$ ,  $1 \leq \mu \leq k$ ,  $1 \leq \nu \leq n-k-1$ .

Сложность проверки условий теоремы 1 носит экспоненциальный характер и имеет порядок  $O(n2^n)$ . Поэтому представляют интерес достаточные условия неразложимости матрицы  $\Pi_n$ , сложность проверки которых имеет полиномиальный характер. Приведем некоторые из таких условий, вытекающих из теоремы 1.

Будем говорить, что векторы  $(x_1, \dots, x_n)$  и  $(y_1, \dots, y_n)$  совпадают при зеркальном отображении, если  $(y_1, y_2, \dots, y_n) = (x_n, x_{n-1}, \dots, x_1)$ . Вектор  $(x_1, \dots, x_n)$  зеркально симметричен, если  $(x_n, x_{n-1}, \dots, x_1) = (x_1, x_2, \dots, x_n)$ .

Из свойств подстановок  $s^{-1}t^{-1}s, s^{-1}t^{-2}s, \dots, s^{-1}t^{-(n-1)}s$  следует, что разностные характеристики  $\Delta(s^{-1}t^{-1}s), \Delta(s^{-1}t^{-2}s), \dots, \Delta(s^{-1}t^{-(n-1)}s)$  содержат только положительные вычеты по модулю  $n$ , причем первичные спецификации  $\Delta(s^{-1}t^{-i}s)$  и  $\Delta(s^{-1}t^{-(n-i)})$  совпадают для  $1 \leq i \leq n-1$ . Из свойств разностей  $\Delta(s^{-1}t^{-i}s)$ ,  $1 \leq i \leq n-1$ , следует, что строки матрицы  $\Pi_n$  с номерами  $i$  и  $n-i$ ,  $1 \leq i \leq n-1$ , совпадают при зеркальном отображении, причем при четном  $n$  единственная средняя строка обладает свойством зеркальной

симметрии. Например, при  $n = 6$  для подстановки  $s = (15420)(3)$  имеем

$$\begin{aligned}\Delta(s^{-1}t^{-1}s) &= (135342), & \Delta(s^{-1}t^{-2}s) &= (411)(255), \\ \Delta(s^{-1}t^{-3}s) &= (33)(24)(42), & \Delta(s^{-1}t^{-4}s) &= (552)(114), \\ \Delta(s^{-1}t^{-5}s) &= (234135).\end{aligned}$$

Матрица  $\Pi_6$  имеет вид

$$\Pi_6 = \begin{pmatrix} 1/6 & 1/6 & 1/3 & 1/6 & 1/6 \\ 1/3 & 1/6 & 0 & 1/6 & 1/3 \\ 0 & 1/3 & 1/3 & 1/3 & 0 \\ 1/3 & 1/6 & 0 & 1/6 & 1/3 \\ 1/6 & 1/6 & 1/3 & 1/6 & 1/6 \end{pmatrix}.$$

Пусть  $k_i$  — число отсутствующих положительных вычетов в характеристике  $\Delta(s^{-1}t^{-i}s)$ ,  $1 \leq i \leq n-1$ . Из определения матрицы  $\Pi_n$  следует, что  $k_i$  равно числу нулевых элементов в  $i$ -ой строке матрицы  $\Pi_n$ . При четном  $n$  общее число нулей в матрице  $\Pi_n$  в силу совпадения строк при зеркальном отображении равно  $2(k_1 + \dots + k_{n/2-1}) + k_{n/2}$ , причем в силу зеркальной симметрии средней строки  $k_{n/2}$  — четное число. При нечетном  $n$  число нулевых элементов  $\Pi_n$  равно  $2(k_1 + \dots + k_{(n-1)/2})$ . Очевидно, что для разложимости дважды стохастической матрицы  $\Pi_n$  необходимо наличие в ней не менее, чем  $2(n-2)$  нулей. Отсюда вытекает следующее утверждение.

**СЛЕДСТВИЕ 2.** Для неразложимости матрицы достаточно, чтобы были выполнены неравенства:

а) при четном  $n$

$$k_1 + \dots + k_{n/2-1} + \frac{1}{2}k_{n/2} \leq n-2;$$

б) при нечетном  $n$

$$k_1 + \dots + k_{(n-1)/2} < n-2.$$

В приведенном выше примере

$$k_1 = 0, \quad k_2 = 1, \quad k_3 = 2,$$

и, следовательно, соответствующая матрица  $\Pi_6$  неразложима. Поскольку все диагональные элементы  $\Pi_6$  положительны, она также и примитивна.

Отметим, что сложность проверки условий следствия 2 имеет порядок  $O(n^2)$ .

Сформулируем теперь условие примитивности неразложимой матрицы.

**ТЕОРЕМА 2.** *Неразложимая матрица  $\Pi_n$ , соответствующая подстановке  $s \in S_n$ , является примитивной, если существует такое  $i$ ,  $0 \leq i \leq n - 1$ , что подстановка  $s$  имеет  $(i, i)$ -конфигурацию.*

Действительно, для неразложимой дважды стохастической матрицы  $\Pi_n$  наличие  $(i, i)$ -конфигураций для подстановки  $s \in S_n$  означает, что матрица  $\Pi_n$  является и ациклической. Следовательно, матрица  $\Pi_n$  примитивна.

Отметим, что если  $n$  — четное число, то условия теоремы 2 всегда выполнены.

Действительно, если  $(i, i)$ -конфигурация не существует ни при каком  $i$ ,  $0 \leq i \leq n - 1$ , то это означает, что в разностной характеристике  $\Delta = (\Delta_0, \Delta_1, \dots, \Delta_{n-1})$  все  $\Delta_0, \Delta_1, \dots, \Delta_{n-1}$  различны, т. е.

$$\Delta_0 + \Delta_1 + \dots + \Delta_{n-1} = 1/2n(n - 1).$$

В силу условия  $\Delta_0 + \Delta_1 + \dots + \Delta_{n-1} = 0 \pmod{n}$  это равенство невозможно при четном  $n$ .

Таким образом, для четных  $n$  из теорем 1 и 2 вытекает следующий критерий примитивности матрицы  $\Pi_n$ .

**ТЕОРЕМА 3.** *При четном  $n$  для примитивности матрицы  $\Pi_n$  необходимо и достаточно, чтобы для любого  $k$ ,  $1 \leq k \leq n/2$ , и любого  $k$ -сочетания  $1 \leq i_1 < \dots < i_k \leq n - 1$  существовали такие  $\mu$  и  $\nu$ ,  $1 \leq \mu \leq k$ ,  $1 \leq \nu \leq n - k - 1$ , что разностная характеристика  $\Delta(s^{-1}t^{-i_\mu}s)$  содержала элемент  $j_\nu$ , где  $\{j_1, j_2, \dots, j_{n-k-1}\} = \{1, 2, \dots, n - 1\} \setminus \{i_1, i_2, \dots, i_k\}$ .*

Сформулируем теперь условие вполне неразложимости матрицы  $\Pi_n$ .

Напомним, что неотрицательная матрица  $A = (a_{ij})$ ,  $i, j = 1, 2, \dots, n$ , называется частично разложимой, если она имеет такую нулевую подматрицу размеров  $s \times (n - s)$ , где  $s$  — натуральное число, что  $1 \leq s \leq n - 1$ . Матрица  $A$ , не являющаяся частично разложимой, называется вполне неразложимой. Очевидно, что всякая разложимая матрица является частично разложимой и всякая вполне неразложимая матрица является неразложимой (см. [5]).

Условия вполне неразложимости матрицы удобно сформулировать в виде леммы.

**ЛЕММА 3.** *Для вполне неразложимости неотрицательной матрицы  $A = (a_{ij})$ ,  $i, j = 1, 2, \dots, n$ , необходимо и достаточно, чтобы для любых  $k$  и  $l$ ,  $1 \leq k, l \leq n - 1$ , таких, что  $k + l = n$ , и любого  $k$ -сочетания  $1 \leq j_1 < \dots < j_k \leq n$  существовали такие  $\mu$  и  $\nu$ ,  $1 \leq \mu \leq k$ ,  $1 \leq \nu \leq l$ , что  $a_{i_\mu j_\nu} > 0$ .*

Доказательство леммы следует непосредственно из определения вполне неразложимости матрицы  $A$ .

Отметим, что если матрица дважды стохастическая, то для проверки вполне неразложимости достаточно рассматривать  $k \leq n/2$ .

Следующая теорема дает критерий вполне неразложимости матрицы  $\Pi_n$ .

**ТЕОРЕМА 4.** *Для вполне неразложимости дважды стохастической матрицы  $\Pi_n$ , соответствующей подстановке  $s \in S_n$ , необходимо и достаточно,*

чтобы для каждого  $k$ ,  $1 \leq k \leq n/2$ , и любых  $k$ -сочетаний  $1 \leq i_1 < \dots < i_k \leq n-1$  и любых  $(n-k-1)$ -сочетаний  $1 \leq j_1 < \dots < j_{n-k-1} \leq n-1$  существовали такие  $\mu$  и  $\nu$ ,  $1 \leq \mu \leq k$ ,  $1 \leq \nu \leq n-k-1$ , что разностная характеристика  $\Delta(s^{-1}t^{-i_\mu}s)$  содержала элемент  $j_\nu \in \{j_1, j_2, \dots, j_{n-k-1}\}$ .

Доказательство теоремы 4 с использованием леммы 3 проводится аналогично доказательству теоремы 1.

**СЛЕДСТВИЕ 3.** При выполнении условий теоремы 4 матрица  $\Pi_n$  является примитивной.

Следствие 3 вытекает из известного факта, состоящего в том, что вполне неразложимая матрица является примитивной (см. [5]).

Простая однородная цепь Маркова, имеющая примитивную матрицу переходных вероятностей, является эргодической. Поэтому приведенные выше теоремы 1, 2 и 3 в совокупности определяют условия эргодичности рассматриваемой цепи Маркова с матрицей переходных вероятностей  $\Pi_n$ .

#### § 4. ЧИСЛО ПОЛОЖИТЕЛЬНЫХ ЭЛЕМЕНТОВ МАТРИЦЫ $\Pi_n$ И ДЕФИЦИТ ПОДСТАНОВКИ

Обозначим через  $w_n$  число положительных элементов матрицы  $\Pi_n$ . Ясно, что  $w_n$  совпадает с числом положительных элементов матрицы

$$H_n = (h_{ij}), \quad i, j = 1, 2, \dots, n-1, \quad (4.1)$$

элементы которой определяются равенством (1.1). Будем рассматривать случай группы  $(N_n, +)$ . При случайном равновероятном выборе подстановки  $s \in S_n$  будем рассматривать отвечающую матрице  $H_n$  случайную матрицу

$$W_n = (\eta_n(ij)), \quad i, j = 1, 2, \dots, n-1, \quad (4.2)$$

где случайные величины  $\eta_n(i, j)$  определяются равенствами (2.1) и (2.2). Величине  $w_n$  соответствует случайная величина  $\zeta_n$ , равная числу положительных элементов в случайной матрице  $W_n$ .

Из формул (2.3) и (2.4) следует, что

$$P(\eta_n(i, j) > 0) = 1 - \sum_{1 \leq k \leq n/2} \frac{(-1)^k}{k!} \frac{\binom{n}{k}^2}{\binom{n}{2k}}, \quad 1 \leq i, j \leq n-1, \quad (4.3)$$

и при  $n \rightarrow \infty$

$$P(\eta_n(i, j) > 0) \rightarrow 1 - e^{-1}. \quad (4.4)$$

Поэтому среднее значение  $\zeta_n$  выражается формулой

$$E \zeta_n = (n-1)^2 \left( 1 - \sum_{0 \leq k \leq n/2} \frac{(-1)^k}{k!} \frac{\binom{n}{k}^2}{\binom{n}{2k}} \right), \quad (4.5)$$

из которой при  $n \rightarrow \infty$  следует, что

$$\frac{E \zeta_n}{(n-1)^2} \rightarrow 1 - e^{-1}. \quad (4.6)$$

В решении трудной задачи отыскания вероятностного распределения случайной величины  $\zeta_n$  в настоящее время каких-либо результатов нет.

В данном параграфе укажем два результата, которые дают некоторую информацию о распределении нулевых и положительных элементов матрицы  $\Pi_n$  для случайной равновероятной подстановки  $s$ .

Пусть подстановка  $s \in S_n$  имеет разностную характеристику

$$\Delta(s) = (\Delta_0, \Delta_1, \dots, \Delta_{n-1}).$$

Число  $d(s)$  отсутствующих в  $\Delta(s)$  элементов полной системы наименьших неотрицательных вычетов по модулю  $n$  называется *дефицитом* подстановки  $s$ . Число отсутствующих в  $\Delta(s)$  положительных вычетов из той же системы называется *положительным дефицитом* подстановки  $s$ . Определенная в § 3 величина  $k_i$  представляет собой положительный дефицит подстановки  $s^{-1}t^{-1}s$ ,  $1 \leq i \leq n-1$ , в терминах которого может быть переформулировано следствие 1.

Из определения диагональных элементов матрицы  $H = (h_{ij})$ ,  $i, j = 1, 2, \dots, n-1$ , следует, что

$$h_{ii} = |\{\nu: \Delta_{\nu+i} = \Delta_\nu, 0 \leq \nu \leq n-1\}|, \quad i = 1, 2, \dots, n-1. \quad (4.7)$$

Из этих равенств находим, что

$$h_{11} = h_{22} = \dots = h_{n-1, n-1} = 0;$$

тогда и только тогда, когда  $d(s) = 0$ . При четном  $n$  дефицит  $d(s)$  для любой подстановки  $s \in S_n$  положителен. Отсюда следует, что при четном  $n$  главная диагональ матрицы содержит по крайней мере один положительный элемент.

Для случайной равновероятной подстановки  $s \in S_n$  обозначим через  $\xi_n$  значение дефицита в случайно выбранной подстановке  $s$ .

В 50–60-х годах прошлого столетия ряд математиков занимался задачей отыскания простого выражения для вероятностного распределения  $\xi_n$  — дефицита случайной подстановки. В связи с некоторыми задачами в криптографии эта сложная задача получила название «проблемы параллельных перепаяек». Сложность этой задачи подтвердилась после установления ее связи с трудной классической проблемой вычисления перманентов.

В 1956 г. В. Н. Сачковым было получено выражение распределения  $\xi_n$  через перманенты циклических  $(0,1)$ -матриц. Соответствующая формула имеет вид

$$P(\xi_n = r) = \frac{1}{n!} \sum_{k=r}^n (-1)^{k-r} \binom{k}{r} \sum_{0 \leq j_1 < \dots < j_k \leq n-1} \text{per}(J_n - C^{j_1} - \dots - C^{j_k}), \quad (4.8)$$

$$r = 0, 1, \dots, n-1,$$

где  $J_n$  — матрица  $n \times n$ , все элементы которой равны 1,  $C$  — подстановочная матрица, соответствующая подстановке  $t^{-1} = (0, 1, \dots, n-1)$  и  $\text{per} A$  — перманент матрицы  $A$ .

Формула (4.8) выводится с использованием метода включения-исключения и может быть использована для определения распределения дефицита  $d_n$  случайной подстановки  $s \in S_n$ . Для достаточно больших  $n$  требуется применение компьютерной техники. Порядок сложности точного вычисления перманента, например, с использованием формулы Райзера оценивается величиной  $O(n^{2^{2n}})$ . Поэтому сложность вычисления по формуле (4.8) имеет порядок  $O(n^{2^{2^{2n}}})$ .

Биномиальные моменты  $B_{kn}$  случайной величины  $d_n$  равны

$$B_{kn} = \frac{1}{n!} \sum_{0 \leq j_1 < \dots < j_k \leq n-1} \text{per}(J_n - C^{j_1} - \dots - C^{j_k}), \quad (4.9)$$

$$k = 0, 1, \dots, n-1,$$

и при  $n \rightarrow \infty$  имеет место асимптотика

$$B_{kn} = \frac{\binom{n}{k}}{k!} e^{-k} (1 + o(1)), \quad k = 0, 1, \dots \quad (4.10)$$

Среднее и дисперсия  $\xi_n$  выражаются с помощью формул

$$E \xi_n = n \frac{h_n}{n!}, \quad (4.11)$$

$$D \xi_n = \frac{2}{n!} \sum_{\delta=1}^{n-1} \sum_{t=1}^{d-1} \delta \binom{d-1}{t} U_{(d-2t)n/d} + n \frac{h_n}{n!} - \left( n \frac{h_n}{n!} \right)^2, \quad (4.12)$$

где

$$h_n = n! \sum_{k=0}^n \frac{(-1)^k}{k!}, \quad U_n = \sum_{k=0}^n (-1)^k \frac{2n}{2n-k} \binom{2n-k}{k} (n-k)!$$

Заметим, что числа  $h_n$  определяют число подстановок  $s \in S_n$ , противоречивых с единичной подстановкой  $e \in S_n$ ,  $u_n$  — число подстановок  $s \in S_n$ , противоречивых с подстановками  $e$  и  $t^{-1} = (0, 1, \dots, n-1)$ . Эти числа фигурируют в классических комбинаторных задачах, известных как задача о встречах и задача о гостях, соответственно.

Из формул (4.11) и (4.12) при  $n \rightarrow \infty$  следуют асимптотики

$$E \xi_n = \frac{n}{e} + O\left(\frac{1}{n!}\right), \quad (4.13)$$

$$D \xi_n = \frac{e-2}{e^2}n + \frac{n}{2e^2(n-2)} + O\left(\frac{1}{n}\right). \quad (4.14)$$

Необходимо отметить, что формула (4.11) впервые была получена Д. К. Фаддеевым другим методом, не использующим перманенты.

Другой подход к изучению свойств матрицы  $W_n$ , касающийся распределения заданного числа положительных элементов в строке этой матрицы, изложен в статье В. Н. Сачкова [4] и связан с понятием  $(\alpha; j_1, \dots, j_m)$ -конфигурации.

Для  $1 \leq j_1 < \dots < j_m \leq n-1$ ,  $1 \leq \alpha \leq n-1$  подстановка  $s \in S$  образует  $(\alpha; j_1, \dots, j_m)$ -конфигурацию для данного  $i$ ,  $1 \leq i \leq n$ , если существует такое  $\nu$ ,  $1 \leq \nu \leq m$ , что в группе  $(N_n, +)$  имеет место равенство  $s(i+\alpha) = s(i) + j_\nu$ . В работе [4] доказана следующая теорема.

**ТЕОРЕМА 5.** Пусть  $\eta_m(\alpha; j_1, \dots, j_m)$  — число  $(\alpha; j_1, \dots, j_m)$ -конфигураций в случайной равновероятной подстановке  $s \in S_n$  и пусть

$$l = \frac{n}{(n, \alpha)}, \quad d_\nu = \frac{n}{(n, j_\nu)}, \quad 1 \leq \nu \leq m,$$

$$\gamma = |\{i: d_i = 2, 1 \leq i \leq m\}|,$$

где  $(n, z)$  — наибольший общий делитель  $n$  и  $z$ . При  $n \rightarrow \infty$  имеют место два случая:

а) если  $l > 2$ , то случайная величина  $\eta_m(\alpha; j_1, \dots, j_m)$  в пределе имеет распределение Пуассона с параметром  $\lambda = m$ ;

б) если  $l = 2$ , то предельным является распределение, представляющее собой композицию распределений Пуассона с параметрами  $\lambda_1 = \gamma/2$  и  $\lambda_2 = m - \gamma$ .

## СПИСОК ЛИТЕРАТУРЫ

1. Lai X., Massay J., Murphy S. Marcov ciphers and differential analysis. — Eurocrypt'91, 1991, p. 17–38.
2. O'Connor L. On the distribution of characteristics in bijective mappings. — Eurocrypt'95, 1995, p. 13–23.

3. *Hawkes P., O'Connor L.* XOR and non-XOR differential probabilities. — Eurocrypt'99, 1999, p. 272–285.
4. *Sachkov V. N.* Probability distributions of the number of configurations and discordances of random permutations from regular cyclic classes. — In: Probabilistic methods in Discrete Mathematics. — Utrecht: VSP, 2002, p. 23–40.
5. *Сачков В. Н.* Введение в комбинаторные методы дискретной математики. — М.: Наука, 1982.