ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 22 МАТЕМАТИКИ Выпуск 5
2015

В. О. Мironкин, **А. Б. Чухно** (Москва, ТВП). **Задача о t-коллизиях для случайного отображения конечного множества в себя.**

Задачи, связанные со случайными отображениями, составляют одно из динамично развивающихся направлений современной теории вероятностей. Об этом свидетельствует большое количество научных публикаций, посвященных рассматриваемой проблематике [1–3, 5–8]. Актуальность подобных задач продиктована широким их применением в современных практических приложениях. В частности, ряд задач, касающихся свойств случайных подстановок, использует подобные результаты [4].

В настоящей работе исследуются вероятностные характеристики для кратных коллизий двух случайных отображений.

Рассмотрим множество $S = \{0, 1, \ldots, N-1\}$, $N > 1$, и множество $\mathfrak{J}$ всех отображений $f : S \to S$. Зададим на $\mathfrak{J}$ равномерную меру и рассмотрим два произвольных отображения $f, g \in \mathfrak{J}$. Будем использовать табличное представление соответствующих отображений:

$$f = \begin{pmatrix} 0 & 1 & \ldots & N-2 & N-1 \\ f(0) & f(1) & \ldots & f(N-2) & f(N-1) \end{pmatrix},$$

$$g = \begin{pmatrix} 0 & 1 & \ldots & N-2 & N-1 \\ g(0) & g(1) & \ldots & g(N-2) & g(N-1) \end{pmatrix}.$$

О п р е д е л е н и е. Два отображения $f, g \in \mathfrak{J}$ образуют t-коллизию, $t \in \overline{2, N}$, если t является максимальным числом, для которого существует хотя бы одна пара значений x и y, таких, что

$$\begin{aligned} &f(x) = g(y), \\ &f(x + 1(\bmod N)) = g(y + 1(\bmod N)), \\ &\ldots \\ &f(x + t - 1(\bmod N)) = g(y + t - 1(\bmod N)). \end{aligned}$$

В общей постановке задачи оценки вероятности наличия t-коллизии для двух отображений вычисление точных выражений при комбинаторном подходе представляется аналитически сложным, поэтому в работе получены оценки искомой вероятности.

Обозначим через $P_t^{(f,g)}$ вероятность t-коллизии для отображений t и g. Для указанной вероятности верно следующее

Предложение 1. *Для произвольных отображений $f, g \in \mathfrak{J}$ справедливо*:

$$\frac{(N-1)^{N-t}}{N^N} < P_t^{(f,g)} < \frac{1}{N^{t-2}}, \quad t \in \{2, 3, \ldots, N-1\},$$

$$P_N^{(f,g)} < \frac{1}{N^N}.$$

З а м е ч а н и е. При $t = 2$ правая оценка вероятности появления t-коллизии является тривиальной.

Обозначим через $X_{f,g}(t)$ случайную величину, равную числу пар элементов множества S, образующих t-коллизию для отображений f и g. Для этой случайной величины получено следующее

Предложение 2. *Для произвольных отображений* $f, g \in \mathfrak{J}$ *справедливы оценки*:

$$\begin{aligned}
&\mathbf{E}\, X_{f,g}(t) \leqslant \frac{(N-1)^2}{N^t}, \qquad 1 < t < \left[\frac{N}{2}\right],\\
&\mathbf{E}\, X_{f,g}(t) = \frac{(N-1)^2}{N^t}, \qquad \left[\frac{N}{2}\right] < t < N-1,\\
&\mathbf{E}\, X_{f,g}(N-1) = \frac{N-1}{N^t}, \quad \mathbf{E}\, X_{f,g}(N) = \frac{1}{N^N}.
\end{aligned}$$

СПИСОК ЛИТЕРАТУРЫ

1. *Колчин В. Ф.* Случайные отображения. М.: Наука, 1984, 208 с.
2. *Колчин В. Ф.* Случайные графы (2-е изд.). М.: Физматлит, 2004, 256 с.
3. *Колчин В. Ф.*, *Севастьянов Б. А.*, *Чистяков В. П.* Случайные размещения. М.: Наука, 1976, 224 с.
4. *Миронкин В. О.* Вероятность t-коллизий для двух случайных подстановок. — Обозрение прикл. и промышл. матем., 2014, т. 21, в. 4, с. 70–73.
5. *Сачков В. Н.* Курс комбинаторного анализа. М.–Ижевск: НИЦ «Регулярная и хаотическая динамика», 2013, 336 с.
6. *Сачков В. Н.* Вероятностные методы в комбинаторном анализе. М.: Наука, 1978, 287 с.
7. *Сачков В. Н.* Введение в комбинаторные методы дискретной математики. М.: Наука, 1982, 384 с.
8. *Flajolet P.*, *Odlyzko A. M.* Random Mapping Statistics. — In: Advances in Cryptology–EUROCRYPT'89. Proceedings of Workshop on the Theory and Application of Cryptographic Techniques. (Houthalen, Belgium, April 10-13, 1989.) / Ed. by J.-J. Quisquater, J. Vandewalle. Heidelberg etc.: Springer, 1990, p. 329–354. (Ser. Lect. Notes Comput. Sci. V. 434.)