ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 22 МАТЕМАТИКИ Выпуск 1
2015

В. О. Мironкин (Москва, ТВП). **Вероятностные характеристики слоев в графе степени случайного отображения.**

В последние годы активно развивается направление теории вероятностей, связанное с изучением случайных отображений. Модель случайных отображений достаточно хорошо изучена, и в данном направлении имеется разработанная теория и методика решения возникающих в этой области проблем. Среди наиболее интересных работ, посвященных рассматриваемой тематике, следует упомянуть работы В. Н. Сачкова [9], В. Ф. Колчина [2–4], В. Е. Степанова [10, 11], В. Г. Проскурина [8], А. М. Зубкова [1] и В. Г. Михайлова [6, 7], а также зарубежных авторов — например, P. Flajolet, A. Odlyzko, B. Harris [12–15]. Однако современные тенденции требуют рассмотрения более сложных математических моделей, в частности, степеней случайных равновероятных отображений.

В настоящей работе продолжены исследования свойств и характеристик степеней случайных равновероятных отображений, начатые ранее в [5].

Рассматривается конечное множество $S = \{1, 2, \ldots, N\}$, $N > 1$, и множество $\mathfrak{J}$ всех отображений $f : S \to S$, на котором задается равномерная мера. Объектом исследования является k-я степень случайного отображения f:

$$f^k : S \to S, \quad k \in \mathbf{N}.$$

В работе используется представление случайных отображений в виде случайных графов, хорошо известное, например, по книгам [2–4, 9].

О п р е д е л е н и е. Назовем t-м слоем, $t \geqslant 0$, в графе отображения f^k, $k \in \mathbf{N}$, множество вершин $H_t^{(k)}$, для которых длина подхода к циклу $\alpha_N^{(k)}(x_0) = t$:

$$H_t^{(k)} = \bigl\{x \in S : \alpha_N^{(k)}(x_0) = t\bigr\}.$$

З а м е ч а н и е. Множество вершин $H_0^{(k)}$ графа отображения f^k совпадает с множеством циклических вершин графа отображения f, которое было подробно изучено (см., например, [9]).

О п р е д е л е н и е. Подходом вершины $x_0 \in S$ в графе отображения f^k, $k \in \mathbf{N}$, назовем последовательность ребер, пройденных из вершины x_0 до первого попадания в циклическую вершину.

Для любых $i_0, i_1 \in \mathbf{R}$, $i_0 > i_1$ будем полагать $\prod_{j=i_0}^{i_1}(\ldots) \equiv 1$, $\sum_{j=i_0}^{i_1}(\ldots) \equiv 0$.

Теорема 1. *Пусть $f \in \mathfrak{J}$ и $k \in \mathbf{N}$. Тогда для произвольной вершины $x_0 \in S$ при $t \geqslant 1$ справедливо равенство*

$$\mathbf{P}\bigl\{x_0 \in H_t^{(k)}\bigr\} = \frac{1}{N}\sum_{p=0}^{k-1}\sum_{l=1}^{N-tk+p}\prod_{j=1}^{tk-p+l-1}\Bigl(1 - \frac{j}{N}\Bigr).$$

Через $\mu_t^{(k)}$, $t \geqslant 1$, обозначим случайную величину, равную числу вершин, лежащих в слое $H_t^{(k)}$.

Следствие. *Пусть* $f \in \mathfrak{J}$ *и* $k \in \mathbf{N}$. *Тогда при* $t \geqslant 1$ *справедливо равенство*

$$\mathbf{E}\mu_t^{(k)} = \sum_{p=0}^{k-1} \sum_{l=1}^{N-tk+p} \prod_{j=1}^{tk-p+l-1} \Big(1 - \frac{j}{N}\Big).$$

Теорема 2. *Пусть* $f \in \mathfrak{J}$ *и* $k \in \mathbf{N}$. *Тогда при* $t \geqslant 1$ *справедливо равенство*

$$\mathbf{D}\mu_t^{(k)} = \sum_{p=0}^{k-1} \Bigg(\sum_{l=1}^{N-2(tk-p)} l \prod_{j=1}^{2(tk-p)+l-1} \Big(1 - \frac{j}{N}\Big) + \sum_{i=0}^{tk-p-1} \sum_{l=1}^{N-tk+p-i} \prod_{j=1}^{tk-p+l+i-1} \Big(1 - \frac{j}{N}\Big) \Bigg)$$
$$+ \sum_{p=0}^{k-1} \Bigg(\sum_{l=1}^{N-2(tk-p)-1} \sum_{m=1}^{N-2(tk-p)-l} \prod_{j=1}^{2(tk-p)+l+m-1} \Big(1 - \frac{j}{N}\Big) - \Bigg(\sum_{l=1}^{N-tk+p} \prod_{j=1}^{tk-p+l-1} \Big(1 - \frac{j}{N}\Big) \Bigg)^2 \Bigg).$$

О п р е д е л е н и е. Назовем $H_t^{(k)}(l)$, $t \geqslant 0$, множество вершин слоя $H_t^{(k)}$, лежащих на подходах к циклу длины l в графе отображения f^k, $k \in \mathbf{N}$.

Согласно сделанному выше замечанию будем рассматривать множества $H_t^{(k)}(l)$, $t \geqslant 1$.

Теорема 3. *Пусть* $f \in \mathfrak{J}$ *и* $k \in \mathbf{N}$. *Тогда для произвольной вершины* $x_0 \in S$ *при* $t \geqslant 1$ *справедливо равенство*

$$\mathbf{P}\big\{x_0 \in H_t^{(k)}(l)\big\} = \frac{1}{N} \sum_{p=0}^{k-1} \sum_{\substack{m=1,\\ m \mid kl\\ m \nmid kq\\ 1 \leqslant q < l}}^{\min(kl, N-tk+p)} \prod_{j=1}^{tk-p+m-1} \Big(1 - \frac{j}{N}\Big).$$

Через $\mu_t^{(k)}(l)$ $t \geqslant 1$, обозначим случайную величину, равную числу вершин, лежащих в слое $H_t^{(k)}$.

Следствие. *Пусть* $f \in \mathfrak{J}$ *и* $k \in \mathbf{N}$. *Тогда при* $t \geqslant 1$ *справедливо равенство*

$$\mathbf{E}\mu_t^{(k)}(l) = \sum_{p=0}^{k-1} \sum_{l=1}^{N-tk+p} \prod_{j=1}^{tk-p+l-1} \Big(1 - \frac{j}{N}\Big).$$

СПИСОК ЛИТЕРАТУРЫ

1. *Зубков А. М.* Вычисление распределения характеристик чисел компонент и циклических точек случайного отображения. — Матем. вопросы криптографии, 2010, т. 1, № 2, с. 5–18.
2. *Колчин В. Ф.* Случайные отображения. М.: Наука, 1984.
3. *Колчин В. Ф.* Случайные графы (2-е изд.). М.: Физматлит, 2004.
4. *Колчин В. Ф.*, *Севастьянов Б. А.*, *Чистяков В. П.* Случайные размещения. М.: Наука, 1976.
5. *Миронкин В. О.* Исследование свойств и характеристик степени случайного отображения. — Обозрение прикл. и промышл. матем., 2014, т. 21, в. 1, с. 70–73.
6. *Михайлов В. Г.* Исследование комбинаторно-вероятностной модели автоматов из регистров с неравномерным движением. — В кн.: Труды по дискретной математике. Т. 6. М.: Физматлит, 2002, с. 139–149.

7. *Михайлов В. Г.* Исследование числа циклических точек автомата из регистров с неравномерным движением. — В кн.: Труды по дискретной математике. Т. 5. М.: Физматлит, 2002, с. 167–172.
8. *Проскурин Г. В.* О распределении числа вершин в слоях случайного отображения. — Теория вероятн. и ее примен., 1973, т. 18, в. 4, с. 846–852.
9. *Сачков В. Н.* Вероятностные методы в комбинаторном анализе. М.: Наука, 1978.
10. *Степанов В. Е.* О распределении числа вершин в слоях случайного дерева. — Теория вероятн. и ее примен., 1969, т. 14, в. 1, с. 64–77.
11. *Степанов В. Е.* Предельные распределения некоторых характеристик случайных отображений. — Теория вероятн. и ее примен., 1969, т. 14, в. 4, с. 639–653.
12. *Flajolet P.*, *Odlyzko A.* Random Mapping Statistics. — In: Advances in Cryptology–EUROCRYPT89. Workshop on the Theory and Application of Cryptographic Techniques. (Houthalen, Belgium, April 1013, 1989)./ Ed. by J.-J. Quisquater, J. Vandewalle. Heidelberg etc.: Springer, 1989, p. 329–354. (Ser. Lect. Notes Comput. Sci. B. 434.)
13. *Flajolet P.*, *Sedgewick R.* Analytic Combinatorics. — Web Edition: http://algo.inria.fr/flajolet/Publications/books.html, 2007.
14. *Harris B.* A survey of the early history of the theory of random mapping. — В кн.: Вероятностные методы дискретной математики. Труды третьей Петрозаводской конференции./ Под ред. В. Я. Козлова, В. Ф. Колчина, Ю. Л. Павлова и Ю. В. Прохорова. М./Utrecht: ТВП/VSP, 1993, p. 1–22.
15. *Harris B.* Probability distributions related to random mapping. — Ann. Math. Statist., 1960, v. 31, № 4, p. 1045–1062.