**ОБОЗРЕНИЕ**
**ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ**
**Том 21 МАТЕМАТИКИ Выпуск 1**
**2014**

**В. О. Мironкин** (Москва, ТВП). **Исследование свойств и характеристик степени случайного отображения.**

О том, что задача исследования свойств случайных отображений не теряет своей актуальности, свидетельствует большое количество научных публикаций, посвященных рассматриваемой проблематике. Так, например, в работе [4] с использованием вероятностных методов было получено асимптотическое значение числа образов для степени случайного отображения.

В работе, представленной данным сообщением, рассматривается класс отображений, построенных на основе случайного отображения, а именно, *степень* случайного отображения. Посредством комбинаторных методов получены точные значения некоторых характеристик для указанного класса отображений. В работе используется представление случайных отображений в виде случайных графов, хорошо известное по книгам [1–3].

**1. Длина отрезка апериодичности.** Рассмотрим множество $S = \{1, 2, \ldots, N\}$, $N > 1$ и множество $\mathfrak{J}$ всех отображений $f\colon S \to S$. Зададим на $\mathfrak{J}$ равномерную меру и рассмотрим $k$-ю степень случайного отображения $f$, т. е. $f^k\colon S \to S$, $k \in \mathbf{N}$.

Для произвольной вершины $x_0 \in S$ графа отображения $f^k$ обозначим $\tau_N^{(k)}(x_0)$ отрезок апериодичности отображения $f^k$ для вершины $x_0 \in S$, т. е. число ребер графа отображения $f^k$, пройденных из вершины $x_0$ до первого попадания в уже встречавшуюся вершину:

$$\tau_N^{(k)}(x_0) = \min_{t \in \mathbf{N}} \bigl\{ t \,|\, f^{tk}(x_0) \in \bigl\{ x_0, f^k(x_0), \ldots, f^{(t-1)k}(x_0) \bigr\} \bigr\}.$$

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

$$\mathbf{P}\bigl\{\tau_N^{(k)}(x_0) > t\bigr\} = \frac{1 + o(1)}{k} \sum_{d=1}^{k} \biggl\{ \frac{1}{t} \bigl( (a+b) e^{-(t/(a+b))^2} - a e^{-(t/a)^2} \bigr) - \sqrt{2} \biggl( \Phi\biggl( \frac{t\sqrt{2}}{a} \biggr) - \Phi\biggl( \frac{t\sqrt{2}}{a+b} \biggr) \biggr) \biggr\},$$

*где $a = 1/k$, $b = 1/(\text{Н. О. Д.}(d,k)) - 1/k$.*

**Следствие 1.** *В условиях теоремы 1 имеет место точное выражение*

$$\mathbf{P}\bigl\{\tau_N^{(k)}(x_0) > t\bigr\} = \sum_{d=1}^{k} \sum_{a,b} \frac{1}{N} \prod_{j=1}^{a+b-1} \biggl( 1 - \frac{j}{N} \biggr),$$

*где внутреннее суммирование производится по таким $a$, $b$, что*

$$\biggl[ \frac{a+k-1}{k} \biggr] + \frac{b}{(d,k)} > 1, \quad b \equiv d(k).$$

Здесь и далее для любых $i_0, i_1 \in \mathbf{N}$, $i_0 > i_1$ положим $\prod_{j=i_0}^{i_1}(\cdots) \equiv 1$.

**Теорема 2.** *Пусть $f \in \mathfrak{J}$. Тогда для любого $k \in \mathbf{N}$, $z \in \mathbf{Z}$ и произвольной вершины $x_0 \in S$ справедливы равенства*

$$\mathbf{P}\{\tau_N^{(k)}(x_0) = z\} = \frac{1}{N}\sum_{l\in Q(zk,z,N)}\prod_{i=1}^{l-1}\Big(1-\frac{i}{N}\Big) + \frac{1}{N}\sum_{s=1}^{z-1}\sum_{t=(s-1)k+1}^{\min\{N-1,sk\}}\sum_{l\in Q((z-s)k,z-s,N-t)}\prod_{i=1}^{t+l-1}\Big(1-\frac{i}{N}\Big), \quad 1 \leqslant z \leqslant N,$$

$$\mathbf{P}\{\tau_N^{(k)}(x_0) = z\} = 0, \quad z < 1 \text{ или } z > N,$$

*где* $Q(q_1,q_2,q_3) = \{l :\ l \nmid pk, l|q_1, 1 \leqslant p < q_2, l \leqslant q_3\}$.

**Следствие 2.** *Пусть $f \in \mathfrak{J}$. Тогда для любого $k \in \mathbf{N}$ и произвольной вершины $x_0 \in S$ справедливо равенство*

$$\mathbf{M}\,\tau_N^{(k)}(x_0) = \frac{1}{N}\sum_{z=1}^{N} z\Big(\sum_{l\in Q(zk,z,N)}\prod_{i=1}^{l-1}\Big(1-\frac{i}{N}\Big) + \sum_{s=1}^{z-1}\sum_{t=(s-1)k+1}^{\min\{N-1,sk\}}\sum_{l\in Q((z-s)k,z-s,N-t)}\prod_{i=1}^{t+l-1}\Big(1-\frac{i}{N}\Big)\Big), \quad z = 1,2,\ldots,N.$$

**Теорема 3.** *Пусть $f \in \mathfrak{J}$. Тогда для любого $k \in \mathbf{N}$, $z \in \mathbf{Z}$ и произвольной вершины $x_0 \in S$ справедливы равенства*

$$\mathbf{P}\{\tau_N^{(k)}(x_0) > 0\} = 1, \quad \mathbf{P}\{\tau_N^{(k)}(x_0) = z\} = 0, \quad z \geqslant N,$$

$$\mathbf{P}\{\tau_N^{(k)}(x_0) > z\} = \frac{1}{N}\sum_{t=(z-1)k+1}^{N-1}\sum_{l=1}^{N-t}\prod_{i=1}^{l+t-1}\Big(1-\frac{i}{N}\Big) + \frac{1}{N}\sum_{s=1}^{z-1}\sum_{t=(s-1)k+1}^{\min\{N-1,sk\}}\sum_{l\in\overline{Q}(z-s,N-t)}\prod_{i=1}^{l-1}\Big(1-\frac{i}{N}\Big) + \frac{1}{N}\sum_{l\in\overline{Q}(z,N)}\prod_{i=1}^{l-1}\Big(1-\frac{i}{N}\Big), \quad 1 \leqslant z \leqslant N-1,$$

*где* $\overline{Q}(q_1,q_2) = \{l\ ;\ l \nmid pk, 1 \leqslant p < q_1, l \leqslant q_2\}$.

**Следствие 3.** *При условии теоремы* 3 *справедливо равенство*

$$\mathbf{M}\,\tau_N^{(k)}(x_0) = 1 + \frac{1}{N}\sum_{z=1}^{N-1}\Big(\sum_{t=(z-1)k+1}^{N-1}\sum_{l=1}^{N-t}\prod_{i=1}^{l+t-1}\Big(1-\frac{i}{N}\Big) + \sum_{s=1}^{z-1}\sum_{t=(s-1)k+1}^{\min\{N-1,sk\}}\sum_{l\in\overline{Q}(z-s,N-t)}\prod_{i=1}^{l-1}\Big(1-\frac{i}{N}\Big) + \sum_{l\in\overline{Q}(z,N)}\prod_{i=1}^{l-1}\Big(1-\frac{i}{N}\Big)\Big).$$

.

**2. Среднее число прообразов произвольной глубины.** Будем говорить, что произвольная точка $x_0 \in S$ *имеет прообраз* $y \in S$ *на глубине* $l \in \mathbf{N}$ *при отображении* $f$, если выполняется $f^l(y) = x_0$ и $f^k(y) \neq x_0$ для всех $k \in \mathbf{N}$, $k < l$.

Обозначим $\xi_r^{(k)}(x_0)$ случайную величину, равную числу прообразов точки $x_0(s)$ на глубине, не превосходящей $r$, при отображении $f^k$.

**Теорема 4.** *Пусть $f \in \mathfrak{J}$. Тогда для любого $k \in \mathbf{N}$ и произвольной вершины $x_0 \in S$ справедливо равенство $\mathbf{M}\,\xi_r^{(k)}(x_0) = \sum_{m=1}^{r} \prod_{l=1}^{mk}(1 - l/N)$.*

**Следствие 4.1.** *Пусть $f \in \mathfrak{J}$. Тогда для любого $k \in \mathbf{N}$ и произвольной вершины $x_0 \in S$ при $N \to \infty$ справедливо асимптотическое выражение $\mathbf{M}\,\xi_r^{(k)}(x_0) \sim \sum_{m=1}^{r} e^{-(mk)^2/(2N)}$.*

**Следствие 4.2.** *Среднее число прообразов для произвольной точки $x_0 \in S$ при отображении $f^k$, $f \in \mathfrak{J}$, асимптотически оценивается выражением $\mathbf{M}\,\xi_1^{(k)}(x_0) \sim e^{-k^2/(2N)}$ при $N \to \infty$.*

**3. Среднее число вершин, лежащих на заданном расстоянии от циклов.** Обозначим $\mu_r^{(k)}$ случайную величину, равную числу точек графа отображения $f^k$, $f \in \mathfrak{J}$, лежащих на расстоянии $r$ от циклов.

**Теорема 5.** *Пусть $f \in \mathfrak{J}$. Тогда для любого $k \in \mathbf{N}$ справедливы равенства*

$$\mathbf{M}\,\mu_0^{(k)} = \sum_{i=1}^{N} \prod_{j=1}^{i-1} \left(1 - \frac{j}{N}\right), \quad \mathbf{M}\,\mu_r^{(k)} = \sum_{i=1}^{N-r-k+1} \prod_{j=1}^{r+k+i-2} \left(1 - \frac{j}{N}\right), \quad r = 1, 2, \ldots, N-1.$$

**Следствие 5.1.** *Пусть $f \in \mathfrak{J}$. Тогда для любого $k \in \mathbf{N}$ при $N \to \infty$ справедливо асимптотическое выражение*

$$\mathbf{M}\,\mu_0^{(k)} \sim \sum_{i=1}^{N} e^{-(i-1)^2/(2N)} \text{ и } \mathbf{M}\,\mu_0^{(k)} < 1 + \frac{1}{k}\sqrt{\pi N/2},$$

$$\mathbf{M}\,\mu_r^{(k)} \sim \sum_{i=1}^{N-r-k+1} e^{-(r+k+i-2)^2/(2N)}, \quad r = 1, 2, \ldots, N-1.$$

**Следствие 5.2.** *Среднее число вершин графа случайного отображения $f \in \mathfrak{J}$, лежащих на заданном расстоянии $r = 0, 1, \ldots, N-1$ от циклов асимптотически оценивается величиной*

$$\mathbf{M}\,\mu_0^{(1)} \sim \sum_{i=1}^{N} e^{-(i-1)^2/(2N)} \quad \text{и} \quad \mathbf{M}\,\mu_0^{(1)} < 1 + \sqrt{\pi N/2},$$

$$\mathbf{M}\,\mu_r^{(1)} \sim \sum_{i=1}^{N-r} e^{-(r+i-1)^2/(2N)}, \quad r = 1, 2, \ldots, N-1.$$

**4. Среднее значение мощности множества образов.** Произвольная точка $x \in S$ называется *циклической точкой* отображения $f$, если она лежит на некотором цикле графа $G$ отображения $f$.

Введем следующие обозначения: $h(x) = \min_{l=0,1,2,\ldots}\{l\colon f^l(x)$ — циклическая точка $f\}$ для $x \in S$; $H_t = \{x \in S\colon h(x) = t\}$ — множество точек, лежащих на расстоянии $t$ до соответствующих им циклов отображения $f$, $t \geqslant 0$; $A_0 = S$, $A_1 = f(A_0)$, $A_2 = f(A_1)$, ...

Пусть на $\mathfrak{J}$ задана равномерная мера, тогда мощность множества $A_k$ — множества образов отображения $f^k$ — является случайной величиной, распределение которой индуцируется случайным отображением $f^k$. Вычислим $\mathbf{M}\,|A_k|$ — среднюю мощность множества образов отображения $f^k$.

Заметим, что множество $A_k$ можно представить в виде $A_k = H_0 \cup (\cup_{t=1}^{N-k} H_{t.k})$, где $H_{t.k} = \{x \in H_t\colon x$ имеет прообраз на глубине $k\}$.

**Теорема 6.** *Пусть $f \in \mathfrak{J}$. Тогда для любого $k \in \mathbf{N}$ справедливо равенство*

$$\mathbf{M}\,|A_k| = 1 + \sum_{t=2}^{N} \prod_{l=1}^{t-1} \left(1 - \frac{l}{N}\right) + \sum_{t=1}^{N-k} \sum_{m=1}^{N-k-t} \prod_{l=1}^{k+l+m-1} \left(1 - \frac{l}{N}\right).$$

З а м е ч а н и е. Если $k > N-1$ превышает длину максимального подхода в графе отображения $f$, то образ $f^k$ состоит только из циклических точек. И тогда результат теоремы 6 имеет вид

$$\mathbf{M}\,|A_k| = 1 + \sum_{t=2}^{N} \prod_{l=1}^{t-1} \left(1 - \frac{l}{N}\right), \quad \mathbf{M}\,|A_k| < 1 + \frac{1}{k}\sqrt{\frac{\pi N}{2}} \quad \text{при} \quad N \to \infty.$$

## СПИСОК ЛИТЕРАТУРЫ

1. *Колчин В. Ф.* Случайные отображения. М.: Наука, 1984.
2. *Михайлов В. Г.* Труды по дискретной математике. М.: Физматлит, 2002.
3. *Степанов В. Е.* О распределении числа вершин в слоях случайного дерева. — Теория вероятн. и ее примен., 1969, т. XIV, № 1, с. 64–77.
4. *Flajolet Ph.*, *Odlyzko A.* Random Mapping Statistics. — In: EUROCRYPT'89. Berlin etc.: Springer, 1989, p. 329–354. (Ser. Lect. Notes Comput. Sci. V. 434).