UDC 519.212.2+519.214+519.216.221

Limit theorem for the image size of a subset under compositions of random mappings

A. M. Zubkov[*], **A. A. Serov**[†]

[*] *Department of Discrete Mathematics, Steklov Mathematical Institute of the Russian Academy of Sciences, Gubkina str. 8, Moscow, 119991, Russia*

[†] *Department of Discrete Mathematics, Steklov Mathematical Institute of the Russian Academy of Sciences, Gubkina str. 8, Moscow, 119991, Russia*

Abstract. Let $\mathcal{X}_\mathcal{N}$ be a set consisting of N elements and $F_1, F_2, \ldots$ be a sequence of random independent equiprobable mappings $\mathcal{X}_\mathcal{N} \to \mathcal{X}_\mathcal{N}$. For a subset $S_0 \subset \mathcal{X}_\mathcal{N}$, $|S_0| = n$, we consider a sequence of its images $S_t = F_t(\ldots F_2(F_1(S_0))\ldots)$, $t = 1, 2 \ldots$ The conditions on n, t, $N \to \infty$ under which the distribution of image sizes $|S_t|$ is asymptotically normal are presented.

Keywords: random equiprobable mappings, compositions of random mappings, image sizes.

1. Introduction

Let $F\colon \mathcal{X}_N \to \mathcal{X}_N$ be a mapping of a finite set $\mathcal{X}_N = \{1, 2, \ldots, N\}$ to itself, $N \in \mathbb{N}$. Denote by Σ_N the set of all N^N mappings $\mathcal{X}_N$ to itself and specify on the set Σ_N uniform distribution. Consider the probability space with a set of elementary events $\Omega = \Sigma_N$, $|\Omega| = N^N$. *The random equiprobable mapping* $F : \mathcal{X}_N \to \mathcal{X}_N$ is a random variable having an equiprobable distribution on the set Σ_N.

Let $S_0 \subseteq \mathcal{X}_N$ be an initial subset, $|S_0| = n$, and $F_i : \mathcal{X}_N \to \mathcal{X}_N$, $i = 1, 2, \ldots, t$, be the mappings, then

$$F_t\left(\ldots F_2\left(F_1\left(S_0\right)\right)\ldots\right)$$

be the images of the subset S_0 under composition of t mappings. Everywhere later, it is assumed that $F_1, \ldots, F_t$ are random independent equiprobable mappings, and we consider images S_0 under the sequential action on it the mappings $F_1, \ldots, F_t$:

$$S_1 = F_1(S_0),\ S_2 = F_2(F_1(S_0)), \ldots, S_t = F_t(F_{t-1}(\ldots(F_1(S_0))\ldots)). \quad (1)$$

It is obviously that the sequences $\{S_k\}_{k=0}^t$ and $\{|S_k|\}_{k=0}^t$ are Markov chains with nonincreasing trajectories.

Many articles are devoted to the estimates of the sizes of the images $\{S_k\}_{k=0}^t$ (see, for example, [3], [4], [5], [6], [7], [8]), particularly, in [7] and [8] the explicit two-sided estimates of the probability that an arbitrary element $X \in \mathcal{X}_N$ belongs to S_k, $k \geq 1$, are obtained. The publications devoted to

the research of the distributions of image sizes $\{S_k\}_{k=0}^{t}$ are not known for the authors.

Further, we study the relations between n, t and N, under which the limiting distribution of image sizes S_t tends to standard normal distribution.

The obtained conditions may be useful under considering the simplified mathematical model of the construction process of one «rainbow» table, proposed in [4], such model corresponds to the variant of the "time-memory tradeoff" method, for the first time described in 1980 by M. Hellman [2].

2. Main section

Assertion 1 *If the images of the initial subset $S_0 \subset \mathcal{X}_N$, $|S_0| = n$, are calculated according to the formulas* (1)*, then the following identities are true:*

$$\mathbf{P}\left\{|S_t| = n \,\middle|\, |S_0| = n\right\} = \left(\prod_{q=1}^{n-1}\left(1 - \frac{q}{N}\right)\right)^t,$$

$$\mathbf{P}\left\{|S_t| = n-1 \,\middle|\, |S_0| = n\right\} = \frac{n}{2}\left(1 - \left(1 - \frac{n-1}{N}\right)^t\right)\left(\prod_{q=1}^{n-2}\left(1 - \frac{q}{N}\right)\right)^t.$$

Assertion 2 *If $n = CN^{1/3}$, then*

$$1 - \frac{C^2}{2N^{1/3}} \leq \mathbf{P}\left\{|S_i| = n \,\middle|\, |S_{i-1}| = n\right\} \leq e^{-\frac{n(n-1)}{2N}} < \\ < 1 - \frac{C^2}{2N^{1/3}} + \frac{C}{2N^{1/3}} \cdot \frac{C^3+4}{4N^{1/3}},$$

$$\frac{C^2}{2N^{1/3}}\left(1 - \frac{C^2 + 2/C}{2N^{1/3}}\right) \leq \mathbf{P}\left\{|S_i| = n-1 \,\middle|\, |S_{i-1}| = n\right\} \leq \\ \leq \frac{C^2}{2N^{1/3}}\left(1 - \frac{C^2}{2N^{1/3}} + \frac{C(C^3+16)}{8N^{2/3}} - \frac{C^3}{2N}\right),$$

$$\mathbf{P}\left\{|S_i| < n-1 \,\middle|\, |S_{i-1}| = n\right\} \leq \frac{C\left(C^3+2\right)}{4N^{2/3}}.$$

Let

$$p_0(n) = \mathbf{P}\left\{|S_1| = n \,\middle|\, |S_0| = n\right\}, \quad p_1(n) = \mathbf{P}\left\{|S_1| = n-1 \,\middle|\, |S_0| = n\right\},$$
$$p_2(n) = \mathbf{P}\left\{|S_1| < n-1 \,\middle|\, |S_0| = n\right\}.$$

Assertion 3 *If $n = CN^{1/3}$, then*

$$1 - p_0(2) < 1 - p_0(3) < \ldots < 1 - p_0(n) \leqslant \frac{C^2}{2N^{1/3}}\,,$$
$$\frac{C\left(C^3+2\right)}{4N^{2/3}} \geq p_2(n) > p_2(n-1) > \ldots > p_2(3) > p_2(2).$$

Theorem 1 *If n, m, t, $N \to \infty$ in such a way that n has the order $N^{1/4}$ and $m = o(n)$, then for any fixed $x \in \mathbb{R}$ and*

$$t = 2N\left(\frac{1}{m} - \frac{1}{n}\right) + (1+o(1))x\,\frac{2N}{\sqrt{3}}\sqrt{\left(\frac{1}{m^3} - \frac{1}{n^3}\right)},$$

the following relation is true:

$$\mathbf{P}\left\{|S_t| \leq \frac{2n\,N}{n\,t+2N}\right\} \to \Phi(x)\,,$$

where $\Phi(x)$ is the standard normal distribution function.

Acknowledgments

This work was supported by the Russian Science Foundation under grant no. 14-50-00005.

References

1. *Borovkov A. A.* Probability Theory. — New York: Gordon & Breach, 1998. — 474 pp.
2. *Hellman M.E.* A cryptanalytic time–memory trade-off // IEEE Trans. Inf. Theory, 1980. — P. 401–406.
3. *Flajolet P., Odlyzko A. M.* Random mapping statistics // Eurocrypt'89. Lect. Notes Comput. Sci. — 1990. — Vol. 434. — P. 329–354.
4. *Oechslin P.* Making a faster cryptanalytic time-memory trade-off // Lect. Notes Comput. Sci. — Vol. 2729. — 2003. — P. 617–630.
5. *Hong J., Moon S.* A comparison of cryptanalytic tradeoff algorithms // J. Cryptology. — Vol. 26. —- 2013. — P. 559–637.
6. *Pilshchikov D. V.* Estimation of the characteristics of time-memory-data tradeoff methods via generating functions of the number of particles and the total number of particles in the Galton-Watson process // Matematicheskie Voprosy Kriptografii. — Vol. 5:2. — 2014. — P. 103–108.

7. *Zubkov A. M., Serov A. A.* Images of subset of finite set under iterations of random mappings // Discrete Math. Appl. — Vol. 25:3. — 2015. — P. 179–185.
8. *Serov A. A.* Images of a finite set under iterations of two random dependent mappings // Discrete Math. Appl. — 2016. — 26:3. — P. 175–181.