ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 22 МАТЕМАТИКИ Выпуск 5
2015

А. М. Зубков, А. А. Серов (Москва, МИАН). **Двусторонние неравенства для средних чисел элементов в объединениях образов конечного множества при итерациях случайных равновероятных отображений.**

Пусть $\mathcal{N} = \{1, \dots, N\}$ — конечное множество, в множестве $\mathcal{N}$ выбирается начальное подмножество S_0, $|S_0| = n$, и вычисляются его образы

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

где $F_1, F_2, \dots, F_t$ — независимые случайные отображения множества $\mathcal{N}$ в себя, имеющие равновероятное распределение на множестве Σ_N всех таких отображений, $|\Sigma_N| = N^N$. Пусть $\Psi_t = \{S_1 \cup S_2 \cup \dots \cup S_t\}$.

3pt

Теорема. *Для любого элемента $x \in \mathcal{N}$, не зависящего от итерируемых отображений $F_1, F_2, \dots$, при любых $1 \leqslant k, t, n \leqslant N$ справедливы неравенства*

$$\frac{n}{N}\left(1 - \frac{(n-1)k}{2N}\right) \leqslant \mathbf{P}\{x \in S_k \,\big|\, |S_0| = n\} \leqslant \frac{n}{N}\left(1 - \frac{(n-1)k}{2N} + \frac{n^2k^2}{3N^2}\right),$$

$$\frac{nt}{N}\left(1 - \frac{3n(t+1)}{4N}\right) < \mathbf{P}\left\{x \in \Psi_t \,\big|\, |S_0| = n\right\} < \frac{nt}{N}\left(1 - \frac{(n-1)t}{4N} + \frac{n^2(t+1)^2}{9N^2}\right).$$

Справедливы также следующие оценки:

$$n\left(1 - \frac{(n-1)k}{2N}\right) < \mathbf{M}\{|S_k| \,\big|\, |S_0| = n\} < n\left(1 - \frac{(n-1)k}{2N} + \frac{n^2k^2}{3N^2}\right),$$

$$nt\left(1 - \frac{3n(t+1)}{4N}\right) < \mathbf{M}\left\{|\Psi_t| \,\big|\, |S_0| = n\right\} < nt\left(1 - \frac{(n-1)t}{4N} + \frac{n^2(t+1)^2}{9N^2}\right),$$

$$1 + \frac{1 - \exp\left\{-\frac{(n-1)k}{N-n+1}\right\}}{1 - \exp\left\{-\frac{k}{N-n+1}\right\}} \exp\left\{-\frac{k}{N-n+1}\right\} \leqslant \mathbf{M}\{|S_k| \,\big|\, |S_0| = n\},$$

$$N\left(1 - e^{-\frac{nt}{N}}\right)\left(1 - \frac{n(t+1)}{4N}\right) < \mathbf{M}\left\{|\Psi_t| \,\big|\, |S_0| = n\right\}$$
$$< N\left(1 - \exp\left\{-\frac{nt}{N-n}\left(1 - \frac{(n-1)t}{4N} + \frac{n^2(t+1)^2}{9N^2}\right)\right\}\right),$$

$$\mathbf{D}\{|S_k| \,\big|\, |S_0| = n\} < \frac{kn^3}{N}\left(1 + \frac{(n+2)k}{4nN}\right).$$

Верхние и нижние оценки теоремы асимптотически эквивалентны при $N, n, t \to \infty$, если $nt = o(N)$, и дают содержательную информацию в случаях, когда $nt = O(N)$.

Работа поддержана РФФИ, грант № 14-01-00318.

СПИСОК ЛИТЕРАТУРЫ

1. *Harris B.* Probability distributions related to random mappings. — Ann. Math. Statist., 1960, v. 31, № 2, p. 1045–1062.
2. *Hellman M. E.* A cryptanalytic time-memory trade-off. — IEEE Trans. Inform. Theory, 1980, v. IT-26, is. 4, p. 401–406.
3. *Колчин В. Ф.*, *Севастьянов Б. А.*, *Чистяков В. П.* Случайные размещения. М.: Наука, 1976, 224 с.
4. *Колчин В. Ф.* Случайные отображения. М.: Наука, 1984, 208 с.
5. *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.)
6. *Oechslin Ph.* Making a faster cryptanalytic time-memory trade-off. — In: Advances in Cryptology–CRYPTO 2003. Proceedings of the 23rd Annual International Cryptology Conference. (Santa Barbara, California, August 17–21, 2003.) / Ed. by D. Boneh. Heidelberg etc.: Springer, 2003, p. 617–630. (Ser. Lect. Notes Comput. Sci. V. 2729.)