

сходятся к функции распределения и моментам стандартного нормального распределения.

Доказательства теорем 1 и 2 основаны на модификации метода Янсона [12], предложенной в работе В. Г. Михайлова [13].

ЛИТЕРАТУРА

1. *Guibas L. J. and Odlyzko A. M.* Long repetitive patterns in random sequences // *Z. Wahrscheinlichkeitstheorie verw. Geb.* 1980. No. 1. P. 241–262.
2. *Зубков А. М., Михайлов В. Г.* Предельные распределения случайных величин, связанных с длинными повторениями в последовательности независимых испытаний // *Теория вероятн. и ее примен.* 1974. Т. 19. № 1. С. 173–181.
3. *Михайлов В. Г.* Оценка точности сложной пуассоновской аппроксимации для распределения числа совпадающих цепочек // *Теория вероятн. и ее примен.* 2001. Т. 46. № 4. С. 713–723.
4. *Kruglov V. and Zubkov A.* Number of pairs of template matchings in q -ary tree with randomly marked vertices // *LNCS.* 2017. V. 10684. P. 336–346.
5. *Hoffmann C. M. and O'Donnell M. J.* Pattern matching in trees // *J. ACM.* 1982. V. 29. No. 1. P. 68–95.
6. *Steyaert J.-M. and Flajolet P.* Patterns and pattern-matching in trees: an analysis // *Inf. & Control.* 1983. V. 58. No. 1. P. 19–58.
7. *Singh G., Smolka S. A., and Ramakrishnan I. V.* Distributed algorithms for tree pattern matching // *LNCS.* 1988. V. 312. P. 92–107.
8. *Tahraoui M. A., Pinel-Sauvagnat K., Laitang C., et al.* A survey on tree matching and XML retrieval // *Computer Science Rev.* 2013. No. 8. P. 1–23.
9. *Зубков А. М., Круглов В. И.* Повторения цепочек на бинарном дереве со случайными метками вершин // *Дискретная математика.* 2015. Т. 27. № 4. С. 38–48.
10. *Kruglov V. I.* On coincidences of tuples in a q -ary tree with random labels of vertices // *Discr. Math. Appl.* 2018. V. 28. No. 5. P. 293–307.
11. *Михайлов В. Г., Круглов В. И.* Об асимптотической нормальности в задаче о повторениях цепочек в помеченном полном дереве // *Матем. вопр. криптогр.* 2021. Т. 12. № 4. С. 59–64.
12. *Janson S.* Normal convergence by higher semiinvariants with applications to sums of dependent random variables and random graphs // *Ann. Probab.* 1988. V. 16. No. 1. P. 306–312.
13. *Михайлов В. Г.* Об одной теореме Янсона // *Теория вероятн. и ее примен.* 1991. Т. 36. № 1. С. 168–170.

УДК 519.214

DOI 10.17223/2226308X/15/3

О ТОЧНОСТИ НОРМАЛЬНОЙ АППРОКСИМАЦИИ ДЛЯ РАСПРЕДЕЛЕНИЯ ЧИСЛА КРАТНЫХ ПОВТОРЕНИЙ ЗНАКОВ В СТАЦИОНАРНОЙ СЛУЧАЙНОЙ ПОСЛЕДОВАТЕЛЬНОСТИ

В. Г. Михайлов, Н. М. Меженная

Изучается задача об асимптотической нормальности числа r -кратных повторений знаков в отрезке длины n стационарной в узком смысле случайной последовательности со значениями в конечном множестве, удовлетворяющей условию равномерно сильного перемешивания. Показано, что если существует такое число $\alpha > 0$, что коэффициент равномерно сильного перемешивания $\varphi(t)$ убывает

как $t^{-6-\alpha}$, то расстояние в равномерной метрике между функцией распределения стандартизованного числа повторений и функцией распределения стандартного нормального закона с увеличением длины отрезка последовательности n убывает со скоростью $O(n^{-\delta})$ для любого $\delta \in (0, \alpha(32 + 4\alpha)^{-1})$.

Ключевые слова: кратные повторения, зависимые случайные величины, равномерно сильное перемешивание, нормальная аппроксимация, оценка скорости сходимости.

С развитием вычислительной техники всё большую роль играет метод статистического моделирования изучаемых природных явлений и теоретических построений. Этот метод предполагает генерацию последовательностей случайных или псевдослучайных чисел, что делает необходимой проверку соответствия их свойств требованиям модели. Особенно важно это для криптографических применений. Для такой проверки в криптографической литературе разработаны наборы статистических тестов [1, 2]. Обоснование этих тестов использует свойства последовательностей независимых случайных величин.

Теоретические исследования дискретных случайных последовательностей вышли за пределы этих чисто утилитарных потребностей. В частности, сформировалось отдельное научное направление, изучающее предельное поведение распределения числа повторений, в том числе кратных, в независимых и конечно зависимых последовательностях случайных величин. Наиболее успешными оказались исследования условий сходимости распределений чисел повторений к распределению Пуассона [3, 4]. В качестве примера построения достаточных условий асимптотической нормальности числа повторений следует привести работу А. М. Шойтова [5].

В последние годы активно велись исследования повторяемости знаков в дискретных цепях Маркова. Например, в работах [6–8] исследована возможность аппроксимации распределения чисел повторений цепочек в цепи Маркова распределением Пуассона. Аналогичная задача о доказательстве центральной предельной теоремы для таких случайных величин решена в [9]. В частности, в [9, теорема 3] установлена оценка скорости сходимости к нормальному закону для числа кратных совпадений знаков в конечной стационарной цепи Маркова. В настоящей работе показано, что вместо цепей Маркова можно рассматривать более широкий класс — стационарные случайные последовательности, удовлетворяющие условию равномерно сильного перемешивания.

Пусть $X_1, \dots, X_n$ — отрезок стационарной (в узком смысле) случайной последовательности со значениями из множества $\{1, \dots, N\}$, стационарным распределением $P[X_1 = k] = p_k$, $k = 1, \dots, N$, $p_1 + \dots + p_N = 1$, удовлетворяющей условию равномерно сильного перемешивания.

Напомним, что процесс $\{X_t\}_{t=-\infty}^{\infty}$ называется стационарным (в узком смысле), если распределения случайных векторов вида $(X_{t_1+h}, \dots, X_{t_s+h})$ при всех натуральных s не зависят от h . Стационарная последовательность $\{X_t\}_{t=-\infty}^{\infty}$ обладает свойством *равномерно сильного перемешивания*, если

$$\varphi(t) = \sup_{A \in \mathcal{F}_{-\infty}^0, B \in \mathcal{F}_t^{\infty}} |P[B|A] - P[B]| \downarrow 0, \quad t \rightarrow \infty,$$

где $\mathcal{F}_a^b$ — σ -алгебра событий, порождённая величинами $X_a, \dots, X_b$. Величину $\varphi(t)$ называют коэффициентом равномерно сильного перемешивания.

Рассмотрим случайную величину

$$\xi_r = \sum_{1 \leq j_1 < \dots < j_r \leq n} I\{X_{j_1} = \dots = X_{j_r}\} \quad (1)$$

— число r -кратных повторений знаков в отрезке $X_1, \dots, X_n$.

Для исследования распределения случайной величины (1) определим случайные величины

$$\zeta_k = \sum_{t=1}^n I\{X_t = k\}, \quad k = 1, \dots, N,$$

— числа одинаковых знаков в $X_1, \dots, X_n$, и пусть $\eta_k = \zeta_k - np_k$. Обозначим

$$U_n = \frac{1}{(r-1)!} \sum_{k=1}^N p_k^{r-1} \eta_k,$$

$$\xi_r^* = \frac{\xi_r}{n^{r-1} \sqrt{\mathbf{D}U_n}} - \frac{1}{n^{r-1} r! \sqrt{\mathbf{D}U_n}} \sum_{k=1}^N \left(\prod_{j=0}^{r-1} (np_k - j) \right).$$

Теорема 1. Пусть $X_1, \dots, X_n$ — отрезок стационарной (в узком смысле) случайной последовательности со значениями из множества $\{1, \dots, N\}$, стационарным распределением $P[X_1 = k] = p_k > 0$, $k = 1, \dots, N$, $p_1 + \dots + p_N = 1$ (причём среди вероятностей $p_1, \dots, p_N$ есть различные), удовлетворяющей условию равномерно сильного перемешивания с коэффициентом φ , таким, что при некотором $\alpha > 0$ выполнено условие

$$\varphi(t) \leq t^{-(6+\alpha)}.$$

Тогда для любого $0 < \delta < \frac{\alpha}{4(8+\alpha)}$

$$\sup_{-\infty < x < \infty} |P[\xi_r^* \leq x] - \Phi(x)| = O(n^{-\delta}), \quad n \rightarrow \infty.$$

ЛИТЕРАТУРА

1. Иванов М. А., Чугунков И. В. Теория, применение и оценка качества генераторов псевдослучайных последовательностей. М.: КУДИЦ-ОБРАЗ, 2003. 240 с.
2. Rukhin A., Soto J., Nechvatal J., et al. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. NIST, Apr. 2010. <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-22r1a.pdf>.
3. Михайлов В. Г. Предельная теорема пуассоновского типа для числа пар почти полностью совпавших цепочек // Теория вероятностей и ее применения. 2008. Т. 53. Вып. 1. С. 59–71.
4. Михайлов В. Г., Шойтов А. М. О числах множеств эквивалентных цепочек в последовательности независимых случайных величин // Математические вопросы криптографии. 2013. Т. 4. Вып. 1. С. 77–86.
5. Шойтов А. М. Нормальное приближение в задаче об эквивалентных цепочках // Труды по дискретной математике. 2007. Т. 10. С. 326–349.
6. Михайлов В. Г. Оценки точности пуассоновской аппроксимации для распределения числа серии повторений длинных цепочек в цепи Маркова // Дискретная математика. 2015. Т. 27. Вып. 4. С. 67–78.
7. Михайлов В. Г., Шойтов А. М. О длинных повторениях цепочек в цепи Маркова // Дискретная математика. 2014. Т. 26. Вып. 3. С. 79–89.
8. Михайлов В. Г., Шойтов А. М. Многократные повторения длинных цепочек в цепи Маркова // Математические вопросы криптографии. 2015. Т. 6. Вып. 3. С. 117–134.
9. Михайлов В. Г., Меженная Н. М., Волгин А. В. Об условиях асимптотической нормальности числа повторений в стационарной случайной последовательности // Дискретная математика. 2021. Т. 33. Вып. 3. С. 64–78.