

ЛИТЕРАТУРА

1. *Novoselov S. A. and Boltnev Y. F.* Characteristic polynomials of the curve $y^2 = x^{2g+1} + ax^{g+1} + bx$ over finite fields // Прикладная дискретная математика. Приложение. 2019. № 12. С. 44–46.
2. *Cohen H. and Frey G.* Handbook of Elliptic and Hyperelliptic Curve Cryptography. Chapman and Hall/CRC, 2006.
3. *Blake I. F., Seroussi G., and Smart N. P.* Elliptic Curves in Cryptography. Cambridge University Press, 1999.
4. *Menezes A.* Elliptic curve public key cryptosystem. Kluwer Academic Publ., 1993.
5. *Tafazolian S.* A family of maximal hyperelliptic curves // J. Pure Appl. Algebra. 2012. V. 216. No. 7. P. 1528–1532.
6. *Novoselov S. A.* Hyperelliptic curves, Cartier — Manin matrices and Legendre polynomials // Прикладная дискретная математика. 2017. № 37. С. 20–31.
7. *Von zur Gathen J. and Gerhard J.* Modern Computer Algebra. Cambridge University Press, 2013.
8. *Kodama T., Top J., and Washio T.* Maximal hyperelliptic curves of genus three // Finite Fields Their Appl. 2009. V. 15. No. 3. P. 392–403.

УДК 519.214

DOI 10.17223/2226308X/14/2

ЦЕНТРАЛЬНАЯ ПРЕДЕЛЬНАЯ ТЕОРЕМА ДЛЯ U -СТАТИСТИК ОТ ЦЕПОЧЕК МЕТОК ВЕРШИН НА ПОЛНОМ ГРАФЕ

Н. М. Меженная, В. Г. Михайлов

В полном графе с вершинами $1, 2, \dots, n$ вершины $2, 3, \dots, n$ снабжены независимыми случайными метками, принимающими значения из конечного множества $\mathcal{A}_N$. Рассматривается совокупность всех цепей по s смежных рёбер, каждая из которых выходит из вершины 1 и не проходит через одну и ту же вершину дважды. Каждой цепи соответствует s -цепочка из случайных меток пройденных вершин. Рассматривается U -статистика $U_k(s)$ с ядром, зависящим от k таких s -цепочек. Число $k \geq 2$ считается фиксированным, а $s \geq 1$ может меняться. Установлено, что достаточным условием асимптотической нормальности $U_k(s)$ (при обычной стандартизации) является условие вида $\mathbf{D}U_k(s) \geq Cn^{2(k-1)+\varkappa}$, где $C, \varkappa > 0$.

Ключевые слова: U -статистика, центральная предельная теорема, полный граф, цепочка, случайные метки.

Исследование свойств выборочных характеристик и статистических критериев привело к необходимости изучения распределений функционалов от последовательностей случайных величин $X_1, \dots, X_n$ вида

$$U_n = U_n(X_1, \dots, X_n) = \sum_{1 \leq j_1 < \dots < j_r \leq n} f(X_{j_1}, \dots, X_{j_r}), \quad (1)$$

называемых U -статистиками [1]. Число r называется *порядком* U -статистики. Функционалы вида (1) широко используются для проверки свойств случайных последовательностей, качества датчиков псевдослучайных чисел, наличия или отсутствия зависимости между членами последовательности, наличия образцов или повторений специального вида и в задачах, связанных с защитой информации.

Основные результаты об асимптотическом поведении распределений U -статистик с непрерывными ядрами можно найти в [2]. Результаты для U -статистик от дискрет-

ных последовательностей, например для числа пар одинаковых знаков, пар одинаковых цепочек и пар эквивалентных цепочек, получены в [3] и [4] соответственно.

В работе [5] установлено, что для последовательности случайных величин, удовлетворяющей условию абсолютной регулярности [6] с коэффициентом $\beta(t) \leq t^{-h(t)}$, где $h(t) > 0$ и $h(t) \rightarrow \infty$ ($t \rightarrow \infty$) (например, для цепи Маркова), достаточным условием асимптотической нормальности является условие на дисперсию $\mathbf{D}U_n \geq Cn^{2(r-1)+\varkappa}$, где $\varkappa > 0$. Разумеется, это относится и к последовательности независимых случайных величин. Как известно [3], в последовательности независимых одинаково распределённых случайных величин на конечном алфавите при их неравновероятном распределении число k -кратных повторений s -цепочек имеет дисперсию порядка n^{2k-1} и сходится (при подходящей стандартизации) по распределению к нормальному распределению при $n \rightarrow \infty$.

В настоящей работе приведён аналогичный результат для U -статистики от цепочек меток вершин на полном графе.

Введём несколько определений. Пусть K_n — полный граф с n вершинами из множества $V = \{1, \dots, n\}$ и C_n^2 рёбрами; $\alpha_2, \dots, \alpha_n$ — независимые в совокупности случайные величины, принимающие значения из множества $\mathcal{A}_N = \{0, 1, \dots, N-1\}$, причём

$$P[\alpha_j = k] = p_k \in (0; 1), \quad k \in \mathcal{A}_N, \quad \sum_{k=0}^{N-1} p_k = 1.$$

Далее будем считать, что α_j — метка вершины с номером j , $j \in V \setminus \{1\}$.

Обозначим через $\{w(s)\}$ цепь (связный путь без повторения рёбер) из $s \geq 1$ рёбер в графе K_n , начинающийся из вершины с номером 1, не имеющей метки, и не проходящий через одну и ту же вершину дважды. Обозначим через $\alpha(\{w(s)\})$ соответствующую цепи $\{w(s)\}$ последовательность из s меток вершин, через которые проходит цепь (с учётом их порядка). Число таких путей равно числу способов выбрать оставшиеся s вершин из $n-1$ вершин графа (кроме вершины с номером 1) с учётом порядка, поэтому в K_n всего $T = A_{n-1}^s = \frac{(n-1)!}{(n-s-1)!}$ цепей длины s с требуемыми свойствами.

Занумеруем их и будем писать $\{w_u(s)\}$, $u = 1, \dots, T$.

Пусть f — ограниченная по абсолютной величине константой F функция от $k \geq 2$ s -мерных векторных аргументов, симметричная относительно их перестановки. Рассмотрим U -статистику вида

$$U_k(s) = \sum_{1 \leq u_1 < \dots < u_k \leq T} f(\alpha(\{w_{u_1}(s)\}), \dots, \alpha(\{w_{u_k}(s)\})). \quad (2)$$

Здесь аргументами функции f выступают последовательности из s меток вершин, образованных цепями рассматриваемого вида в K_n .

Обозначим $\mathcal{N}(0; 1)$ стандартный нормальный закон распределения; $\rightarrow_d$ — сходимость по распределению.

Теорема 1. Пусть число $k \geq 2$ фиксировано, $s \geq 1$. Если $\mathbf{D}U_k(s) \geq Cn^{2(ks-1)+\varkappa}$, где $C, \varkappa > 0$, то

$$\frac{U_k(s) - \mathbf{E}U_k(s)}{\sqrt{\mathbf{D}U_k(s)}} \rightarrow_d \mathcal{N}(0; 1), \quad n \rightarrow \infty.$$

Теорема 1 сводит доказательство асимптотической нормальности для таких U -статистик, как число повторений цепочек в последовательности дискретных случайных

величин, к проверке скорости роста их дисперсий. В ряде случаев это упрощает обоснование их использования в практических задачах (примеры см. в [7]).

Для доказательства теоремы 1 использовался топологический вариант метода моментов, предложенный в [8].

ЛИТЕРАТУРА

1. *Hoeffding W.* A class of statistics with asymptotically normal distribution // Ann. Math. Statist. 1948. Vol. 19. No. 3. P. 293–325.
2. *Королук В. С., Боровских Ю. В.* Теория U -статистик. Киев: Наук. думка, 1989.
3. *Михайлов В. Г.* Центральная предельная теорема для числа неполных данных повторений // Теория вероятн. и ее примен. 1975. Т. 20. Вып. 4. С. 880–884.
4. *Шойтов А. М.* Нормальное приближение в задаче об эквивалентных цепочках // Тр. по дискр. матем. 2007. Т. 10. С. 326–349.
5. *Mikhailov V. G. and Mezhenaya N. M.* Normal approximation for U - and V -statistics of a stationary absolutely regular sequence // Sib. Elektron. Mat. Izv. 2020. V. 17. P. 672–682.
6. *Doukhan P.* Mixing: Properties and Examples. Lecture Notes in Statistics 85. N.Y.: Springer Verlag, 1994.
7. *Rukhin A., Soto J., Nechvatal J., et al.* A statistical test suite for random and pseudorandom number generators for cryptographic applications. NIST Special Publication 800-22r1a. Natl. Inst. Stand. Technol. Spec. Publ., 2010.
8. *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. 293–325.

УДК 519.1

DOI 10.17223/2226308X/14/3

О НАИБОЛЬШЕМ ПОРЯДКЕ ПОДСТАНОВОК ЗАДАННОЙ СТЕПЕНИ

В. М. Фомичёв

Необходимым требованием к системе шифрования является достаточно большой порядок группы, которая ассоциируется с шифром (то есть порождается подстановками шифра). В связи с этим представляет интерес величина $\mu(n)$, оценивающая порядки циклических групп подстановок степени n , в том числе циклических групп, порождённых шифрующими подстановками. Известно, что порядок подстановки равен наименьшему общему кратному длин её циклов. Однако мало изучена функция $\mu(n)$, принимающая значения, равные наибольшему порядку подстановки степени n . Показана монотонность функции $\mu(n)$, получена двухсторонняя оценка её значений: $\prod_{\omega(n)} \leq \mu(n) \leq \lceil \sqrt{2(n-1)} \rceil!$, где $\prod_{\omega(n)}$ — произведение всех первых (в порядке возрастания) простых чисел, сумма которых не больше n . Получена асимптотическая оценка нижней границы при больших n :

$$\mu(n) > 224k!(1,665)^k (\ln k)^{(k-15)/2}$$

при любом $n \geq 1000$ и $k = \lfloor \sqrt{2n/\ln n} \rfloor$.

Ключевые слова: порядок подстановки, цикловая структура подстановки, простое число.

Каждая подстановка есть произведение независимых циклов. Если длины циклов подстановки g равны $l_1, \dots, l_m$, то её порядок равен

$$\text{ord } g = \text{НОК}(l_1, \dots, l_m).$$