

Литература

1. MacWilliams F.J., Sloane N.J.A. *The Theory of Error-Correcting Codes*. 2nd Edition. North-holland Publishing Company, 1978.
2. Odlyzko A.M. *Asymptotic Enumeration Methods*. In: Handbook of Combinatorics. R.L. Graham, M. Groetschel and L. Lovasz eds.. Vol. 2. Elsevier. 1995. P. 1063–1229.
3. Szabados T. *A Simple Wide Range Approximation of Symmetric Binomial Distributions*. 2016. arXiv: 1612.01112 [math.PR].

ОБ АСИМПТОТИЧЕСКОЙ МОЩНОСТИ НЕКОТОРЫХ ТЕСТОВ ЧИСТОЙ СЛУЧАЙНОСТИ ДВОИЧНОЙ ПОСЛЕДОВАТЕЛЬНОСТИ

Волошко В.А., Трубей А.И.

Белгосуниверситет, НИИ прикладных проблем математики и информатики
Независимости 4, 220030 Минск, Беларусь
valeravoloshko@yandex.ru, trubeia@mail.ru

Пусть наблюдается двоичная случайная последовательность $x_1, x_2, \dots, x_n \in \{0, 1\}$ длины $n \in \mathbb{N}$. Нулевая гипотеза H_0 состоит в предположении чистой случайности наблюдаемой последовательности, то есть в равномерном распределении ее вероятностей:

$$P\{(x_1, \dots, x_n) = q\} = 2^{-n}, \quad \forall q \in \{0, 1\}^n.$$

Альтернатива H_1 предполагает, что наблюдаемая последовательность есть стационарная цепь Маркова некоторого произвольного фиксированного порядка $s \in \mathbb{N}$, для которой переходные вероятности имеют вид

$$P\{x_t = 0 | (x_{t-1}, \dots, x_{t-s}) = q\} = 1/2 + \delta(q), \quad q \in \{0, 1\}^s.$$

Будем говорить, что альтернатива H_1 континуально сближается с нулевой гипотезой H_0 , если при $n \rightarrow \infty$ имеет место следующая асимптотика:

$$\sum_{q \in \{0,1\}^s} \delta^2(q) = \mathcal{O}(n^{-1}).$$

Тесты многомерной дискретной равномерности основаны на статистиках хи-квадрат для L -грам, $L \in \mathbb{N}$, встреченных в наблюдаемой последовательности $\{x_i\}_{i=1}^n$. Базовая статистика хи-квадрат имеет следующий общий вид:

$$S_L^\tau = k^{-1} 2^L \sum_{q \in \{0,1\}^L} (f_q - k \cdot 2^{-L})^2,$$

где τ – тип теста ($\tau = \pi$ ($\tau = \nu$) для теста по пересекающимся (по непересекающимся) L -граммам), $k \in \mathbb{N}$ – общее число встреченных L -грамм, $f_q : \{0, 1\}^L \rightarrow \mathbb{Z}$ – число встреченных L -грамм, равных $q \in \{0, 1\}^L$. Для теста МДРН(L) многомерной дискретной равномерности по непересекающимся L -граммам требуется, чтобы n делилось на L , а встреченные L -граммы – это $k = n/L$ непересекающихся L -блоков, на которые разбивается наблюдаемая последовательность. Для теста МДРП(L) многомерной дискретной равномерности по пересекающимся L -граммам $k = n$, а встреченные L -граммы – это все n подслов $q = (x_{i+1}, \dots, x_{i+L})$, $i = 1, \dots, n$, длины L в “закольцованной” наблюдаемой последовательности $x_1, \dots, x_n, x_1, \dots, x_n, x_1, \dots$. Статистика теста МДРН(L) имеет вид $S = S_L^\nu$. Статистика теста МДРП(L) имеет вид $S = S_L^\pi - S_{L-1}^\pi$. Каждый из тестов принимает гипотезу H_0 при $S \leq S_\alpha$, и принимает альтернативу H_1 в противном случае. Здесь $S_\alpha \in \mathbb{R}$ – порог теста, отвечающий вероятности ошибки первого рода $\alpha \in (0, 1)$. В докладе для асимптотики континуального сближения Марковской альтернативы H_1 с нулевой гипотезой H_0 найдены пределы вероятностей ошибки второго рода β для тестов МДРН(L) и МДРП(L): они в явном виде выражены через функцию $\delta(q)$ отклонения переходных вероятностей Марковской альтернативы.

Литература

1. Трубей А.И., Палуха В.Ю., Пирштук И.К., Мальцев М.В., Ращенья Н.А. *Методика тестирования случайных последовательностей на основе статистического расстояния и закона повторного логарифма* // Проблемы защиты информации. Сборник научных статей. 2020. № 16. С. 64–94.
2. Волошко В.А., Вечерко Е.В. *Новые верхние границы для функции нецентрального хи-квадрат распределения* // Журнал Белорусского государственного университета. Математика. Информатика. 2020. № 1. С. 70–74.

О ПРИМЕНЕНИИ ТЕСТА МОНОБИТ ДЛЯ СТАТИСТИЧЕСКОГО ТЕСТИРОВАНИЯ КОРОТКИХ СЛУЧАЙНЫХ И ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

А.Н. Гайдук

Белгосуниверситет, НИИ прикладных проблем математики и информатики
Независимости 4, 220030 Минск, Беларусь gaidukan@bsu.by

В работе [1] предлагается два подхода к оценке результатов тестирования случайных и псевдослучайных последовательностей: определение доли последовательностей с p -значением, превышающим определенную границу, и распределение p -значений на отрезке $[0,1]$. Для проверки распределения p -значений на отрезке $[0,1]$ используется тест хи-квадрат, который разбивает отрезок $[0,1]$ на 10 одинаковых частей с вероятностью попадания p -значения в любой подинтервал равной 0.1.

При тестировании коротких последовательностей возникают две основные проблемы. Первая заключается в том, что согласно [2] аппроксимирующие распределения не могут быть применены, и должны быть заменены на точные значения распределений, которые трудно найти. Вторая проблема заключается в том, что вероятность попадания p -значения в подинтервал не одинакова для всех подинтервалов. Это следует из того факта, что рассматриваются дискретные случайные величины, а не их аппроксимации непрерывными случайными величинами. Для решения этих проблем в работе [2] предложен альтернативный подход, который предполагает использовать исходное распределение p -значений. Затем, для каждого теста вычисляется вероятность попадания p -значения в каждый подинтервал. Обозначим $p_i = P(\frac{i}{10} \leq p\text{-value} \leq \frac{i+1}{10})$ для $i = 0, \dots, 9$.

В работе [2] рассмотрены значения длин последовательности $n = 128, 160, 256$. В таблице 1 представлены теоретическое распределение p -значений в зависимости от длины последовательности $n = 192, 512, 1024$ для теста монобит.

Литература

1. Rukhin, A., A statistical test suite for random and pseudorandom number generators for cryptographic applications. NIST Special Publication 800-22 Revision 1a (2010) / A. Rukhin // <http://csrc.nist.gov/groups/ST/toolkit/rng/documents/SP800-22rev1a.pdf>.
2. Sulak, F. *Evaluation of Randomness Test Results for Short Sequences* // Sequences and Their Applications – SETA 2010. – 2010. – Springer. – 309–319 P.