Журнал Белорусского государственного университета. Математика. Информатика. 2026;1:16–21
Journal of the Belarusian State University. Mathematics and Informatics. 2026;1:16–21

УДК 519.22 + 519.248

АСИМПТОТИЧЕСКАЯ НЕОТРИЦАТЕЛЬНАЯ КОРРЕЛИРОВАННОСТЬ РЯДА СТАТИСТИК, ИСПОЛЬЗУЕМЫХ ПРИ ПРОВЕРКЕ КАЧЕСТВА ГЕНЕРАТОРОВ СЛУЧАЙНЫХ ЧИСЕЛ

М. П. САВЕЛОВ[1)]

[1)]*Математический институт им. В. А. Стеклова РАН, ул. Губкина, 8, 119333, г. Москва, Россия*

Аннотация. Рассматривается задача о проверке гипотезы, которая заключается в том, что тестируемая последовательность является последовательностью независимых случайных величин, имеющих известное полиномиальное распределение. Для решения этой задачи используются четыре типа статистик, представляющих собой обобщения статистик критериев пакетов NIST STS, TestU01 и др. Доказываются асимптотическая неотрицательная коррелированность многих из данных статистик, в том числе 10 статистик пакета NIST STS, и асимптотическая некоррелированность отдельных из них, в частности некоторых из 10 статистик пакета NIST STS.

Ключевые слова: NIST STS; асимптотически неотрицательно коррелированные статистики; асимптотически некоррелированные статистики; совместное распределение статистик; предельные распределения; пакет TestU01; генераторы случайных чисел.

Благодарность. Автор выражает признательность доктору физико-математических наук А. М. Зубкову за постоянную помощь в подготовке работы.

ASYMPTOTIC NON-NEGATIVE CORRELATION OF SOME STATISTICS USED IN TESTING THE QUALITY OF RANDOM NUMBER GENERATORS

M. P. SAVELOV[a]

[a]*Steklov Mathematical Institute of Russian Academy of Sciences, 8 Gubkina Street, Moscow 119333, Russia*

Abstract. The problem of testing the hypothesis, stating that the tested sequence consists of independent random variables with a given polynomial distribution, is considered. To solve this problem four types of statistics that are generalisations of statistics of tests of the NIST STS, TestU01 and other packages are used. It is proved that many of these statistics, including 10 statistics of the NIST STS, are asymptotically non-negatively correlated, and some of them, in particular some of the 10 statistics of the NIST STS, are asymptotically uncorrelated.

Keywords: NIST STS; asymptotically non-negatively correlated statistics; asymptotically uncorrelated statistics; joint distribution of statistics; limit distributions; TestU01 package; random number generators.

Acknowledgements. The author expresses his gratitude to doctor of science (physics and mathematics) A. M. Zubkov for constant assistance in preparing work.

Образец цитирования:
Савелов МП. Асимптотическая неотрицательная коррелированность ряда статистик, используемых при проверке качества генераторов случайных чисел. *Журнал Белорусского государственного университета. Математика. Информатика.* 2026;1:16–21 (на англ.).
EDN: AJDZWV

For citation:
Savelov MP. Asymptotic non-negative correlation of some statistics used in testing the quality of random number generators. *Journal of the Belarusian State University. Mathematics and Informatics.* 2026;1:16–21.
EDN: AJDZWV

Автор:
Максим Павлович Савелов – кандидат физико-математических наук; старший научный сотрудник отдела дискретной математики.

Author:
Maxim P. Savelov, PhD (physics and mathematics); senior researcher at the department of discrete mathematics.
savelovmp@gmail.com
https://orcid.org/0000-0001-7751-6281

Introduction

One of the most famous tools used to test random and pseudorandom number generators is the National Institute of Standards and Technology statistical test suite (here and further – NIST STS) [1]. In recent years many papers have been published on this topic (e. g., articles [2–12]).

In this study we consider four types of statistics defined in works [6; 7]. They are generalisations of statistics of some tests of the NIST STS and other packages. We analyse the question about asymptotic uncorrelation and asymptotic non-negative correlation of these statistics.

Main results

We need some definitions from papers [6; 7]. Let us formulate them.

Let $\varepsilon_1, \varepsilon_2, \dots, \varepsilon_n$ be random variables, taking values in the set $\{0, 1, \dots, R-1\}$. Consider the hypothesis H_0 that the tested sequence consists of independent random variables with a known polynomial distribution. Let N_{lb} and L_{sb} be natural numbers (they are the parameters, by which the statistics T_{lb} and T_{sb} will be constructed). We analyse the case when N_{lb} and L_{sb} are fixed and n tends to infinity. Put

$$L_{lb} = \left[\frac{n}{N_{lb}}\right],\ N_{sb} = \left[\frac{n}{L_{sb}}\right].$$

If the last $n - N_{lb} L_{lb}$ elements are discarded from the sequence $\varepsilon_1, \varepsilon_2, \dots, \varepsilon_n$, then the remaining elements may be divided into N_{lb} «long» non-intersecting blocks of length L_{lb}: the first block consists of random variables $\varepsilon_1, \varepsilon_2, \dots, \varepsilon_{L_{lb}}$, the second block consists of random variables $\varepsilon_{L_{lb}+1}, \varepsilon_{L_{lb}+2}, \dots, \varepsilon_{2L_{lb}}$, etc. Similarly, we can discard the last $n - L_{sb} N_{sb}$ elements and split the remaining ones into N_{sb} «short» blocks of length L_{sb}.

Next we need to fix natural numbers $m_{\text{sum}}, m_{lb}, K_{sb}$ and also three functions $f_{\text{sum}} : \{0, 1, \dots, R-1\}^{m_{\text{sum}}} \to \mathbb{R}$, $f_{lb} : \{0, 1, \dots, R-1\}^{m_{lb}} \to \mathbb{R}$ and $f_{sb} : \{0, 1, \dots, R-1\}^{L_{sb}} \to \mathbb{R}$. Let us partition the set of values of the function f_{sb} into $K_{sb}+1$ non-empty disjoint subsets: $f_{sb}\left(\{0, 1, \dots, R-1\}^{L_{sb}}\right) = \coprod_{i=0}^{K_{sb}} \alpha_{sb}(i)$. We will be interested in the case, when the numbers $R, p_0, \dots, p_{R-1}, m_{\text{sum}}, m_{lb}, N_{lb}, L_{sb}, K_{sb}$, the functions $f_{\text{sum}}, f_{lb}, f_{sb}$ and the sets $\alpha_{sb}(0), \dots, \alpha_{sb}(K_{sb})$ are fixed, do not depend on n and n tends to infinity.

Put

$$E_{\text{sum}} = \mathbf{E} f_{\text{sum}}\left(\varepsilon_1, \varepsilon_2, \dots, \varepsilon_{m_{\text{sum}}}\right),$$

$$\sigma_{\text{sum}}^2 = \mathbf{D} f_{\text{sum}}\left(\varepsilon_1, \varepsilon_2, \dots, \varepsilon_{m_{\text{sum}}}\right) + 2\sum_{i=2}^{m_{\text{sum}}} \operatorname{cov}\left(f_{\text{sum}}\left(\varepsilon_i, \varepsilon_{i+1}, \dots, \varepsilon_{i+m_{\text{sum}}-1}\right),\ f_{\text{sum}}\left(\varepsilon_1, \varepsilon_2, \dots, \varepsilon_{m_{\text{sum}}}\right)\right),$$

where it's supposed that $\sigma_{\text{sum}} \geq 0$.

Definition 1. If $\sigma_{\text{sum}} > 0$, then a statistic of the form

$$T_{\text{sum}} = \frac{\sum_{i=1}^{n-m_{\text{sum}}+1} \left(f_{\text{sum}}\left(\varepsilon_i, \varepsilon_{i+1}, \dots, \varepsilon_{i+m_{\text{sum}}-1}\right) - E_{\text{sum}}\right)}{\sigma_{\text{sum}}\sqrt{n - m_{\text{sum}} + 1}} \tag{1}$$

is called a summing statistic.

Note that in paper [5], under the assumption that the tested sequence is binary, statistics similar to summing statistics are considered.

Put

$$W_k = \sum_{j=L_{lb}(k-1)+1}^{L_{lb}k - m_{lb}+1} f_{lb}\left(\varepsilon_j, \varepsilon_{j+1}, \dots, \varepsilon_{j+m_{lb}-1}\right),\ 1 \leq k \leq N_{lb},$$

$$E_{lb} = \mathbf{E} f_{lb}\left(\varepsilon_1, \varepsilon_2, \dots, \varepsilon_{m_{lb}}\right),$$

$$\sigma_{lb}^2 = \mathbf{D} f_{lb}\left(\varepsilon_1, \varepsilon_2, \dots, \varepsilon_{m_{lb}}\right) + 2\sum_{i=2}^{m_{lb}} \operatorname{cov}\left(f_{lb}\left(\varepsilon_i, \varepsilon_{i+1}, \dots, \varepsilon_{i+m_{lb}-1}\right), f_{lb}\left(\varepsilon_1, \varepsilon_2, \dots, \varepsilon_{m_{lb}}\right)\right),$$

where it is supposed that $\sigma_{lb} \geq 0$. Note that $\mathbf{E} W_k = \left(L_{lb} - m_{lb} + 1\right) E_{lb},\ 1 \leq k \leq N_{lb}$.

Definition 2. If $\sigma_{lb} > 0$, then a statistic of the form

$$T_{lb} = \frac{\sum_{k=1}^{N_{lb}} \left(W_k - (L_{lb} - m_{lb} + 1) E_{lb}\right)^2}{L_{lb}\sigma_{lb}^2}$$

is called a long-block statistic with N_{lb} blocks.

For $0 \le j \le K_{sb}$ put

$$w(j) = \sum_{i=1}^{N_{sb}} I_{f_{sb}\left(\varepsilon_{L_{sb}(i-1)+1}, \varepsilon_{L_{sb}(i-1)+2}, \ldots, \varepsilon_{L_{sb}i}\right) \in \alpha_{sb}(j)},$$

$$E_{sb}(j) = \mathbf{P}\left(f_{sb}\left(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{L_{sb}}\right) \in \alpha_{sb}(j)\right).$$

Note that $\mathbf{E}w(j) = N_{sb}E_{sb}(j)$, $0 \le j \le K_{sb}$.

Definition 3. If $E_{sb}(j) > 0$ for all $0 \le j \le K_{sb}$, then a statistic of the form

$$T_{sb} = \sum_{j=0}^{K_{sb}} \frac{\left(w(j) - N_{sb}E_{sb}(j)\right)^2}{N_{sb}E_{sb}(j)}$$

is called a short-block statistic with blocks of length L_{sb}.

Next for each $1 \le q \le Q_{\text{quad}}$ fix a natural number $m_{\text{sum}}^{[q]}$ and a function $f_{\text{sum}}^{[q]} : \{0, 1, \ldots, R-1\}^{m_{\text{sum}}^{[q]}} \to \mathbb{R}$ and put

$$T_{\text{sum}}^{[q]} = \frac{\sum_{i=1}^{n - m_{\text{sum}}^{[q]} + 1} \left(f_{\text{sum}}^{[q]}\left(\varepsilon_i, \varepsilon_{i+1}, \ldots, \varepsilon_{i + m_{\text{sum}}^{[q]} - 1}\right) - E_{\text{sum}}^{[q]}\right)}{\sigma_{\text{sum}}^{[q]}\sqrt{n - m_{\text{sum}}^{[q]} + 1}}, \tag{2}$$

where the quantities $E_{\text{sum}}^{[q]}$ and $\sigma_{\text{sum}}^{[q]}$ are defined in the same way as the quantities E_{sum} and σ_{sum} in summing statistic (1). The statistics $T_{\text{sum}}^{[1]}, \ldots, T_{\text{sum}}^{[Q_{\text{quad}}]}$ are summing statistics.

Definition 4. Consider a positive integer τ_{quad} and real numbers $d_{\text{quad}}(i, q)$, $1 \le i \le \tau_{\text{quad}}$, $1 \le q \le Q_{\text{quad}}$. A statistic of the form

$$T_{\text{quad}} = \sum_{i=1}^{\tau_{\text{quad}}} \left(\sum_{q=1}^{Q_{\text{quad}}} d_{\text{quad}}(i, q) T_{\text{sum}}^{[q]}\right)^2$$

is called a quadratic statistic constructed from the statistics $T_{\text{sum}}^{[1]}, \ldots, T_{\text{sum}}^{[Q_{\text{quad}}]}$.

Remark. The relationship between the summing, long-block, short-block and quadratic statistics and the statistics from NIST STS [1], TestU01 and other packages was discussed in papers [6; 7]. In particular, the following was proved with respect to the NIST STS in article [6]. Let $R = 2$, $p_0 = p_1 = \frac{1}{2}$ and the hypothesis H_0 be true. The statistics T_{fr}, T_{templ} of tests «Frequency test within a block» and «Non-overlapping template matching test» are long-block statistics, the statistics T_{longrun}, T_{matrix}, T_{lincompl} of tests «Test for the longest run of ones in a block», «Binary matrix rank test», «Linear complexity test» are short-block statistics (taking into account the caveat from example 7 [6]), the statistic T_{mon} of test «Monobit test» is a summing one, the statistic T_{runs} of test «Runs test» coincides up to $o_P(1)$ with the summing statistic, statistics T_{serial1}, T_{serial2} of the test «Serial test» and the statistic T_{entr} of test «Approximate entropy test» coincide up to $o_P(1)$ with some quadratic statistics.

We will call the numbers $m_{\text{sum}}, m_{lb}, N_{lb}, L_{sb}, K_{sb}$, the functions $f_{\text{sum}}, f_{lb}, f_{sb}$ and the sets $\alpha_{sb}(0), \ldots, \alpha_{sb}(K_{sb})$ the parameters of the statistics $T_{\text{sum}}, T_{lb}, T_{sb}$. The numbers Q_{quad}, τ_{quad} and $d_{\text{quad}}(i, q)$, $1 \le i \le \tau_{\text{quad}}$, $1 \le q \le Q_{\text{quad}}$, as well as the parameters of the statistics $T_{\text{sum}}^{[1]}, \ldots, T_{\text{sum}}^{[Q_{\text{quad}}]}$, are called the parameters of the statistic T_{quad}. Further we will assume that they do not depend on n and are fixed.

Let us consider Q triples of statistics $\left(T_{\text{sum}}^{[q]}, T_{lb}^{[q]}, T_{sb}^{[q]}\right)$, $1 \le q \le Q$, where $T_{\text{sum}}^{[q]}$, $T_{lb}^{[q]}$ and $T_{sb}^{[q]}$ are the summing, long-block and short-block statistics, respectively. We will use the following notation. As in equality (2), all parameters related to $T_{\text{sum}}^{[q]}$ will be marked with the subscript «sum» and the superscript $[q]$. Similarly, $N_{lb}^{[q]}$ is the number of long blocks used to construct the statistic $T_{lb}^{[q]}$, $L_{sb}^{[q]}$ is the length of short blocks used in constructing the statistic $T_{sb}^{[q]}$, etc. The triple of statistics $\left(T_{\text{sum}}^{[q]}, T_{lb}^{[q]}, T_{sb}^{[q]}\right)$ is constructed from functions $f_{\text{sum}}^{[q]}, f_{lb}^{[q]}, f_{sb}^{[q]}$.

Consider J quadratic statistics $T_{\text{quad}}^{[1]}, \ldots, T_{\text{quad}}^{[J]}$ constructed from $T_{\text{sum}}^{[1]}, \ldots, T_{\text{sum}}^{[Q]}$:

$$T_{\text{quad}}^{[j]} = \sum_{i=1}^{\tau_{\text{quad}}^{[j]}} \left(\sum_{q=1}^{Q} d_{\text{quad}}^{[j]}(i, q) T_{\text{sum}}^{[q]} \right)^2.$$

Definition 5. Let $\vec{T}$ and $\vec{T}^*$ be multivariate statistics constructed from the sample $\varepsilon_1, \ldots, \varepsilon_n$. Following the paper [9], we say that they are asymptotically uncorrelated if there exist random vectors $\vec{\zeta}$ and $\vec{\zeta}^*$ such that $\left(\vec{T}, \vec{T}^*\right) \xrightarrow{d} \left(\vec{\zeta}, \vec{\zeta}^*\right)$ as $n \to \infty$ and $\operatorname{cov}\left(\vec{\zeta}, \vec{\zeta}^*\right) = 0$. We say that univariate statistics T and T^* are asymptotically non-negatively correlated if there exist random variables ζ and ζ^* such that $\left(T, T^*\right) \xrightarrow{d} \left(\zeta, \zeta^*\right)$ as $n \to \infty$ and the inequality $\operatorname{cov}\left(\zeta, \zeta^*\right) \geq 0$ is satisfied.

Theorem. *Let the hypothesis H_0 be true. If the parameters of the statistics $T_{\text{sum}}^{[1]}, T_{lb}^{[1]}, T_{sb}^{[1]}, \ldots, T_{\text{sum}}^{[Q]}, T_{lb}^{[Q]}, T_{sb}^{[Q]}$, $T_{\text{quad}}^{[1]}, \ldots, T_{\text{quad}}^{[J]}$ are fixed, then the vectors $\left(T_{\text{sum}}^{[1]}, \ldots, T_{\text{sum}}^{[Q]}\right)$ and $\left(T_{lb}^{[1]}, T_{sb}^{[1]}, \ldots, T_{lb}^{[Q]}, T_{sb}^{[Q]}, T_{\text{quad}}^{[1]}, \ldots, T_{\text{quad}}^{[J]}\right)$ are asymptotically uncorrelated, and the components of the second of these vectors are pairwise asymptotically non-negatively correlated.*

Note that using theorem 1 [7] one can find the covariance matrix of the vector to which the vector $\left(T_{\text{sum}}^{[1]}, T_{lb}^{[1]}, T_{sb}^{[1]}, \ldots, T_{\text{sum}}^{[Q]}, T_{lb}^{[Q]}, T_{sb}^{[Q]}, T_{\text{quad}}^{[1]}, \ldots, T_{\text{quad}}^{[J]}\right)$ converges in distribution, not only in the case of H_0 but also in the case of alternatives H_1 «close» to H_0 (see examples of such alternatives in article [6]).

Further explicit formulas for the statistics $T_{\text{mon}}, T_{\text{runs}}, T_{\text{fr}}, T_{\text{longrun}}, T_{\text{matrix}}, T_{\text{templ}}, T_{\text{lincompl}}, T_{\text{serial1}}, T_{\text{serial2}}, T_{\text{entr}}$ of the NIST STS, as well as the definition of the parameters of these statistics, are presented in papers [6; 7]. In particular, N_{fr} is the number of blocks in the long-block statistic T_{fr}, L_{matrix} is the length of blocks of short-block statistic of the test «Matrix test», m_{templ} is the length of the template from which the long-block statistic T_{templ} is constructed, etc.

Corollary. *Let $R = 2$, $p_0 = p_1 = \dfrac{1}{2}$ and the hypothesis H_0 be true. If the parameters of the statistics $T_{\text{mon}}, T_{\text{runs}}, T_{\text{fr}}, T_{\text{longrun}}, T_{\text{matrix}}, T_{\text{templ}}, T_{\text{lincompl}}, T_{\text{serial1}}, T_{\text{serial2}}, T_{\text{entr}}$ are fixed, then the components of the vector $\left(T_{\text{mon}}, T_{\text{runs}}, T_{\text{fr}}, T_{\text{longrun}}, T_{\text{matrix}}, T_{\text{templ}}, T_{\text{lincompl}}, T_{\text{serial1}}, T_{\text{serial2}}, T_{\text{entr}}\right)$ are pairwise asymptotically non-negatively correlated, the statistics T_{mon} and T_{runs} and the vector $\left(T_{\text{fr}}, T_{\text{longrun}}, T_{\text{matrix}}, T_{\text{templ}}, T_{\text{lincompl}}, T_{\text{serial1}}, T_{\text{serial2}}, T_{\text{entr}}\right)$ are pairwise asymptotically uncorrelated.*

The assertion of corollary intersects with the results of works [9–12] and with the results of some other papers of M. P. Savelov and complements them.

Lemma 1. *Suppose that conditions of corollary hold and the parameter m_{serial} of the statistic T_{serial2} satisfies the inequality $m_{\text{serial}} \geq 2$. Then statistics T_{fr} and T_{serial2} are asymptotically uncorrelated.*

Let us prove the results formulated above. We will need the following statement, which is proven in article [9, formula (15)].

Lemma 2. *Let (ξ, η) be a two-dimensional random vector with a normal distribution and zero mean. Then*

$$\operatorname{cov}\left(\xi, \eta^2\right) = 0,\ \operatorname{cov}\left(\xi^2, \eta^2\right) = 2\operatorname{cov}(\xi, \eta),\ \operatorname{cov}\left(\xi^2, \xi\right) = 0.$$

P r o o f o f t h e t h e o r e m. Put

$$N = \prod_{q=1}^{Q} N_{lb}^{[q]},\ h = \prod_{q=1}^{Q} L_{sb}^{[q]},\ s = h + \max_{1 \leq q \leq Q} \max\left(m_{\text{sum}}^{[q]}, m_{lb}^{[q]}\right) - 1.$$

As noted in article [7], the hypothesis H_0 satisfies the conditions $\mathbf{I}(N, s, h)$ and $\mathbf{II}\left(N, s, h, \vec{0}\right)$ defined in work [7]. Let the vectors $\zeta_1^{[q]}, \ldots, \zeta_{N_{lb}^{[q]}}^{[q]}$, $1 \leq q \leq Q$, be the same as in paper [7] (we do not give the explicit form of these vectors due to its cumbersomeness). Applying theorem 1 of article [7], we obtain that the vector

$$\left(T_{\mathrm{sum}}^{[1]},\, T_{lb}^{[1]},\, T_{sb}^{[1]},\, \ldots,\, T_{\mathrm{sum}}^{[Q]},\, T_{lb}^{[Q]},\, T_{sb}^{[Q]},\, T_{\mathrm{quad}}^{[1]},\, \ldots,\, T_{\mathrm{quad}}^{[J]}\right)$$

converges in distribution to the vector

$$\left(\sum_{k=1}^{N_{lb}^{[1]}} \zeta_k^{[1]}\left(K_{sb}^{[1]}+2\right),\, N_{lb}^{[1]}\sum_{k=1}^{N_{lb}^{[1]}}\left(\zeta_k^{[1]}\left(K_{sb}^{[1]}+1\right)\right)^2,\, L_{sb}^{[1]}\sum_{j=0}^{K_{sb}^{[1]}}\left(\sum_{k=1}^{N_{lb}^{[1]}}\zeta_k^{[1]}(j)\right)^2,\ldots,\right.$$

$$\left.\sum_{k=1}^{N_{lb}^{[Q]}} \zeta_k^{[Q]}\left(K_{sb}^{[Q]}+2\right),\, N_{lb}^{[Q]}\sum_{k=1}^{N_{lb}^{[Q]}}\left(\zeta_k^{[Q]}\left(K_{sb}^{[Q]}+1\right)\right)^2,\, L_{sb}^{[Q]}\sum_{j=0}^{K_{sb}^{[Q]}}\left(\sum_{k=1}^{N_{lb}^{[Q]}}\zeta_k^{[Q]}(j)\right)^2,\, \theta^{[1]},\ldots,\theta^{[J]}\right)$$

as $n \to \infty$, where

$$\theta^{[j]} = \sum_{i=1}^{\tau_{\mathrm{quad}}^{[j]}}\left(\sum_{q=1}^{Q} d_{\mathrm{quad}}^{[j]}(i, q)\sum_{k=1}^{N_{lb}^{[q]}}\zeta_k^{[q]}\left(K_{sb}^{[q]}+2\right)\right)^2,\ 1 \le j \le J,$$

and, in addition, the vectors $\zeta_1^{[q]}, \ldots, \zeta_{N_{lb}^{[q]}}^{[q]}$, $1 \le q \le Q$, are linear functions of the centered Gaussian random vector ξ defined in paper [7]. From here, by virtue of lemma 2, the statement of theorem follows.

Proof of the corollary. By remark, there exist statistics $T_{\mathrm{sum}}^{[1]}$, $T_{\mathrm{sum}}^{[2]}$, $T_{lb}^{[1]}$, $T_{lb}^{[2]}$, $T_{sb}^{[1]}$, $T_{sb}^{[2]}$, $T_{sb}^{[3]}$, $T_{\mathrm{quad}}^{[1]}$, $T_{\mathrm{quad}}^{[2]}$, $T_{\mathrm{quad}}^{[3]}$ such that

$$T_{\mathrm{mon}} = T_{\mathrm{sum}}^{[1]},\, T_{\mathrm{runs}} = T_{\mathrm{sum}}^{[2]} + o_P(1),\, T_{\mathrm{fr}} = T_{lb}^{[1]},\, T_{\mathrm{templ}} = T_{lb}^{[2]},$$

$$T_{\mathrm{longrun}} = T_{sb}^{[1]},\, T_{\mathrm{matrix}} = T_{sb}^{[2]},\, T_{\mathrm{lincompl}} = T_{sb}^{[3]},\, T_{\mathrm{serial1}} = T_{\mathrm{quad}}^{[1]} + o_P(1),$$

$$T_{\mathrm{serial2}} = T_{\mathrm{quad}}^{[2]} + o_P(1),\, T_{\mathrm{entr}} = T_{\mathrm{quad}}^{[3]} + o_P(1).$$

Put $Q = 3$, $J = 3$, $T_{\mathrm{sum}}^{[3]} = T_{\mathrm{sum}}^{[1]}$, $T_{lb}^{[3]} = T_{lb}^{[1]}$. Applying theorem, we obtain that the vectors $\left(T_{\mathrm{mon}},\, T_{\mathrm{runs}}\right)$ and $\left(T_{\mathrm{fr}},\, T_{\mathrm{longrun}},\, T_{\mathrm{matrix}},\, T_{\mathrm{templ}},\, T_{\mathrm{lincompl}},\, T_{\mathrm{serial1}},\, T_{\mathrm{serial2}},\, T_{\mathrm{entr}}\right)$ are asymptotically uncorrelated, and the components of the second of these vectors are pairwise asymptotically non-negatively correlated. It remains to show that T_{mon} and T_{runs} are asymptotically uncorrelated.

Consider the statistic T_{templ}^* constructed from $N_{\mathrm{templ}}^* = N_{\mathrm{fr}}$ long blocks and some template of length $m_{\mathrm{templ}}^* \ge 2$. Applying assertion 1 of article [9] to the vector $\left(T_{\mathrm{mon}},\, T_{\mathrm{fr}},\, T_{\mathrm{templ}}^*,\, T_{\mathrm{runs}}\right)$, we obtain that this vector converges (as $n \to \infty$) in distribution to a vector, first and last components of which are uncorrelated. Note that in [9] it is additionally assumed that n is divisible by N_{fr} [9, p. 55] but an analysis of the proof shows that this condition can be discarded. Thus, the statistics T_{mon} and T_{runs} are asymptotically uncorrelated.

Corollary is proved.

Proof of lemma 1. Reasoning in the same way as above in the proof of theorem and applying lemma 3 of work [7], we obtain that the statistics T_{fr} and T_{serial2} are asymptotically independent and, as a consequence, asymptotically uncorrelated (see a similar result in lemma 2 [12]).

Lemma 1 is proved.

Conclusions

We considered four types of statistics that are generalisations of statistics of tests of the NIST STS, TestU01 and other packages. We proved that many of these statistics are asymptotically non-negatively correlated and some of them are asymptotically uncorrelated. We obtained asymptotic non-negative correlation of 10 statistics of the NIST STS and asymptotic uncorrelation of some of these 10 statistics.

References

1. Rukhin AL, Soto J, Nechvatal JR, Smid ME, Barker EB, Leigh SD, et al. *A statistical test suite for random number generators and pseudorandom number generators for cryptographic applications.* Gaithersburg: National Institute of Standards and Technology; 2010. 131 p.

2. Voloshko VA, Kharin YuS, Trubey AI. On power comparison for some tests on pure randomness under Markov high-order dependencies. In: Kharin YuS, editor. *Computer data analysis and modeling: stochastics and data science. Proceedings of the 13th International conference; 2022 September 6–10; Minsk, Belarus.* Minsk: Belarusian State University; 2022. p. 211–217.

3. Zubkov AM, Serov AA. Experimental study of NIST statistical test suite ability to detect long repetitions in binary sequences. *Matematicheskie voprosy kriptografii.* 2023;14(2):137–145. DOI: 10.4213/mvk443.

4. Kharin YuS, Zubkov AM. On statistical testing of composite hypotheses on *s*-dimensional uniform probability distribution of binary sequences. *Diskretnaya matematika.* 2024;36(1):116–135. Russian. DOI: 10.4213/dm1806.

5. Voloshko VA. On the asymptotic properties of the family of χ^2-tests of pure randomness of a binary sequence. In: Kharin YuS. *Theoretical and applied cryptography. Proceedings of the 2nd International scientific conference; 2023 October 19–20; Minsk, Belarus.* Minsk: Belarusian State University; 2023. p. 15–43. Russian.

6. Savelov MP. The limit joint distributions of statistics of tests of the NIST package and their generalisations. *Diskretnaya matematika.* 2024;36(2):71–116. Russian. DOI: 10.4213/dm1824.

7. Savelov MP. Asymptotic independence of statistics of tests of the NIST package and their generalisations. *Diskretnaya matematika.* 2025;37(1):76–111. Russian. DOI: 10.4213/dm1862.

8. Savelov MP. Analogue of the Berry – Esseen inequality for the joint cumulative distribution function of several statistics. *Diskretnaya matematika.* 2025;37(2):66–108. Russian. DOI: 10.4213/dm1875.

9. Savelov MP. The limit joint distributions of statistics of four tests of the NIST package. *Discrete Mathematics and Applications.* 2023;33(1):55–64. DOI: 10.1515/dma-2023-0006.

10. Savelov MP. Limit joint distribution of the statistics of «Monobit test», «Frequency test within a block» and «Test for the longest run of ones in a block». *Discrete Mathematics and Applications.* 2024;34(5):291–301. DOI: 10.1515/dma-2024-0026.

11. Savelov MP. Limit joint distribution of the statistics of «Monobit test», «Frequency test within a block» and «Binary matrix rank test». *Discrete Mathematics and Applications.* 2025;35(4):249–259. DOI: 10.1515/dma-2025-0019.

12. Savelov MP. Limit joint distribution of «Monobit test», «Frequency test within a block», and «Serial test» statistics. *Diskretnaya matematika.* 2023;35(1):88–106. Russian. DOI: 10.4213/dm1744.

Received 24.12.2025 / revised 19.01.2026 / accepted 29.01.2026.