

ЛОКАЛЬНАЯ ИНФОРМАЦИОННАЯ ГЕОМЕТРИЯ ДЛЯ СТАТИСТИЧЕСКОГО АНАЛИЗА ДВОИЧНЫХ ЦЕПЕЙ МАРКОВА ВЫСОКОГО ПОРЯДКА

В. А. ВОЛОШКО^{1), 2)}

¹⁾Белорусский государственный университет, пр. Независимости, 4, 220030, г. Минск, Беларусь

²⁾Научно-исследовательский институт прикладных проблем математики и информатики БГУ,
пр. Независимости, 4, 220030, г. Минск, Беларусь

Аннотация. На 14-й Международной научной конференции «Компьютерный анализ данных и моделирование: стохастика и анализ данных» автором были представлены некоторые новые результаты относительно асимптотических свойств статистик от чисто случайной (равномерно распределенной) двоичной последовательности растущей длины. Эти результаты получены с применением методов информационной геометрии к многообразиям марковских распределений вероятностей на множестве бесконечных двоичных последовательностей. В данной статье более детально описываются информационно-геометрическая теория и техника доказательств. На нескольких примерах показывается, как нахождение вероятностно-статистических свойств сводится к геометрическим и комбинаторным вычислениям.

Ключевые слова: информационная геометрия; касательное пространство; асимптотическое распределение; двоичная последовательность; марковское многообразие.

LOCAL INFORMATION GEOMETRY FOR STATISTICAL ANALYSIS OF HIGH-ORDER BINARY MARKOV CHAINS

V. A. VOLOSHKO^{a, b}

^aBelarusian State University, 4 Niezaliezhnasci Avenue, Minsk 220030, Belarus

^bResearch Institute for Applied Problems of Mathematics and Informatics,
Belarusian State University, 4 Niezaliezhnasci Avenue, Minsk 220030, Belarus

Abstract. At the 14th International conference «Computer data analysis and modelling: stochastics and data analysis» the author presented some new results on asymptotic properties of statistics derived from purely random (uniformly distributed) binary sequence of increasing length. These results are obtained by methods of information geometry applied to manifolds of Markov probability distributions on the set of infinite binary sequences. In this paper the underlying information-geometric theory and the technics of proofs are describe in more detail. By few examples, it is shown how finding probabilistic and statistical properties comes down to geometric and combinatorial computations.

Keywords: information geometry; tangent space; asymptotic distribution; binary sequence; Markov manifold.

Образец цитирования:

Волошко ВА. Локальная информационная геометрия для статистического анализа двоичных цепей Маркова высокого порядка. *Журнал Белорусского государственного университета. Математика. Информатика.* 2026;1:61–74 (на англ.). EDN: OGPXRN

For citation:

Voloshko VA. Local information geometry for statistical analysis of high-order binary Markov chains. *Journal of the Belarusian State University. Mathematics and Informatics.* 2026;1:61–74. EDN: OGPXRN

Автор:

Валерий Анатольевич Волошко – кандидат физико-математических наук; доцент кафедры математического моделирования и анализа данных факультета прикладной математики и информатики¹⁾, заведующий сектором компьютерного анализа данных²⁾.

Author:

Valeriy A. Voloshko, PhD (physics and mathematics); associate professor at the department of mathematical modelling and data analysis, faculty of applied mathematics and computer science^a, and head of the sector of computer data analysis^b.
valoshka@bsu.by
<https://orcid.org/0000-0002-9693-0688>



Markov manifolds and tangent spaces

Let $x_1, \dots, x_n \in Y := \{0, 1\}$ be purely random (uniformly distributed) binary sequence of length $n \in \mathbb{N} : P\{x_1^n = q\} \equiv 2^{-n}$, $q \in Y^n$, $x_1^n := (x_i)_{i=1}^n$. For convenience, we consider index i of x_i as discrete time and use corresponding «temporal» terminology. The new results on asymptotic properties of statistics derived from x_1^n as $n \rightarrow +\infty$ presented in article [1] are obtained by methods of information geometry [2] applied to manifolds of Markov probability distributions (Markov manifolds for brevity) on the set $Y^{\mathbb{Z}} := \{x = (x_i)_{i \in \mathbb{Z}} : x_i \in Y\}$ of two-sided infinite binary sequences.

Introduce some notations: $a | b$ means « a divides b »; $\ell\{\cdot\}$ is the probability distribution of a random variable; $\text{cov}\{\cdot, \cdot\}$, $\text{cor}\{\cdot, \cdot\}$ are the covariance and the correlation coefficient for a pair of random variables, respectively; « $\lim_{\text{cov}}$ » and « $\lim_{\text{cor}}$ » briefly denote their limits as $n \rightarrow +\infty$; $\mathbb{Z}_m = \{0, \dots, m-1\}$ is the ring of integers modulo $m \in \mathbb{N}$ standardly associated with a non-negative integer interval; $a \stackrel{m}{=} b$ and $a \stackrel{m}{+} b$ are equality and summation modulo m , respectively; $\text{span}\{\cdot\}$ is a linear span of subset of linear space; $\text{lcd}(\cdot, \cdot)$, $\text{gcd}(\cdot, \cdot)$ are lowest common dominator and greatest common divisor, respectively; $[a : b] = \{a, a+1, \dots, b\}$, $a, b \in \mathbb{Z}$, $a \leq b$.

We consider two nested Markov manifolds.

The first Markov manifold $\mathbb{M}$ consists of distributions of stationary Markov chains of all orders $s \in \mathbb{N}_0 = \{0, 1, \dots\}$ determined by stationarity condition and Markov equation:

$$P\{x_i = 0 | x_{i-j} = q_j, j \in \mathbb{N}\} = \frac{1 + \omega(q)}{2}, q = (q_j)_{j \in \mathbb{N}} \in Y^{\mathbb{N}}, i \in \mathbb{Z}, \quad (1)$$

where the function $\omega : Y^{\mathbb{N}} \rightarrow \mathbb{R}$ depends only on finite number of components $\{q_j\}$ and $\|\omega\|_{\infty} = \max_{q \in Y^{\mathbb{N}}} |\omega(q)| < 1$.

We call order of ω and denote by $\text{ord}(\omega)$ the minimal value $s \in \mathbb{N}_0$ such that $\omega(q)$ does not depend on $\{q_j : j > s\}$. Manifold $\mathbb{M}$ is in a bijection with the set of functions ω , so we identify them as

$$\mathbb{M} = \{\omega : \text{ord}(\omega) < +\infty, \|\omega\|_{\infty} < 1\}.$$

The uniform distribution $u \in \mathbb{M}$ corresponds to zero function $\omega(q) \equiv 0$, $q \in Y^{\mathbb{N}}$. If we take off the norm limitation $\|\omega\|_{\infty} < 1$, we get the model of tangent space [2] (linearised neighbourhood) of uniform distribution u within the Markov manifold $\mathbb{M}$:

$$\mathbb{T} = \{\omega : \text{ord}(\omega) < +\infty\}.$$

The fundamental object of information geometry defined on this tangent space is the Fisher – Riemann dot product [2]. It has the following form in our notation:

$$\langle \omega, \omega' \rangle = 2^{-s} \sum_{q \in Y^s} \omega(q \| 0^{\infty}) \omega'(q \| 0^{\infty}), \omega, \omega' \in \mathbb{T}, s = \max\{\text{ord}(\omega), \text{ord}(\omega')\},$$

where $\|$ is concatenation; $0^{\infty} \in Y^{\mathbb{N}}$ is one-sided zero binary sequence. We call elements $\omega \in \mathbb{T}$ tangent vectors that is the standard name for elements of tangent spaces.

Under local information geometry (locality refers to neighbourhood of u) we understand here the structure of tangent space $\mathbb{T}$ with Fisher – Riemann dot product on it, the objects defined on this structure and the meaningful quantities that can be computed based on it.

An orthonormal base of characters [3] $\chi = \{\chi^{(Q)}\}_{Q \in Y^+}$ is defined on $\mathbb{T}$:

$$\chi^{(Q)} \in \mathbb{T}, \chi^{(Q)}(q) := e\left(\bigoplus_{j \in \mathbb{N}} Q_j q_j\right), Q \in Y^+, q \in Y^{\mathbb{N}}, \quad (2)$$

where $Y^+ \subset Y^{\mathbb{N}}$ is the subset of one-sided binary sequences of the finite Hamming weight $\|Q\| := \sum_{j \in \mathbb{N}} Q_j < +\infty$

(with finite number of ones); $e(z) := (-1)^z$ is a discrete exponent. Infinite XOR in formula (2) is correct because it contains only a finite number of ones due to $Q \in Y^+$. Note that Y^+ is a countable subset of a continuous set $Y^{\mathbb{N}}$. Many important tangent subspaces $T \subset \mathbb{T}$ are linear spans of subsets of the characters base (2): we call χ -canonic such subspaces T . The notion of order is naturally transferred from $\mathbb{T}$ to Y^+ by formula (2):

$$\text{ord}(Q) := \text{ord}(\chi^{(Q)}), Q \in Y^+, Y^+[s] := \{Q \in Y^+ : \text{ord}(Q) = s\}, s \in \mathbb{N}_0. \quad (3)$$

Zero sequence has zero order: $\text{ord}(0^\infty) = 0$. For non-zero sequences $Q \in Y^+$, $\|Q\| > 0$, the order is the position of the rightmost unit: $Q_{\text{ord}(Q)} = 1$, $Q_i \equiv 0$, $i > \text{ord}(Q)$.

Submanifolds $M(s) \subset M$ and subspaces $T(s) \subset T$ are defined as follows:

$$M(s) := \{\omega \in M : \text{ord}(\omega) \leq s\}, \quad T(s) := \{\omega \in T : \text{ord}(\omega) \leq s\}, \quad s \in \mathbb{N}_0.$$

Obviously $M(s) \subset M(s')$, $T(s) \subset T(s')$ for any $0 \leq s < s'$. Space $T(s)$ is the tangent space of u within the manifold $M(s)$. Denote by $\partial T(s)$, $s > 0$, an orthogonal complement of $T(s-1)$ within $T(s)$ with regard to the Fisher – Riemann dot product. For $s = 0$ set $\partial T(0) = T(0)$. Spaces $T(s)$, $\partial T(s)$ are χ -canonic and have the following dimensions:

$$\dim(T(s)) = 2^s = \sum_{s'=0}^s \gamma[s'], \quad \dim(\partial T(s)) = \gamma[s] := 2^{\max\{0, s-1\}}, \quad s \in \mathbb{N}_0. \quad (4)$$

Base of characters for $\partial T(s)$ is $\{\chi^{(Q)} : Q \in Y^+[s]\}$, $\gamma[s] = |Y^+[s]|$ (see formulas (3) and (4)).

Let us call random sequence $x \in Y^{\mathbb{Z}}$: Δ -stationary if its probability distribution is invariant under shift by $\Delta \in \mathbb{N}$, i. e. $\ell(x_i)_i = \ell(x_{i+\Delta})_i$; semi-stationary if it is Δ -stationary for some $\Delta \in \mathbb{N}$. «Usual» stationarity is 1-stationarity in these terms.

The second Markov manifold that we consider is $M^\pi = \bigcup_{\Delta \in \mathbb{N}} M^\pi\{\Delta\}$, where the submanifold $M^\pi\{\Delta\} \subset M^\pi$ consists of distributions of Δ -periodic Δ -stationary Markov chains determined by Δ -stationarity condition and Δ -periodic generalisation of Markov equation (1):

$$P\{x_i = 0 | x_{i-j} = q_j, j \in \mathbb{N}\} = \frac{1 + \omega_i(q)}{2}, \quad q \in Y^{\mathbb{N}}, \quad i \in \mathbb{Z}, \quad (5)$$

$\omega_i : \mathbb{Z} \rightarrow M$ is Δ -periodic with regard to $i \in \mathbb{Z}$ M -valued sequence: $\omega_i \equiv \omega_{i+\Delta}$. We identify the set of such sequences with $M^\pi\{\Delta\}$, and with M^π for all $\Delta \in \mathbb{N}$. Denote by T^π the tangent space of u within M^π . Obviously $M \subset M^\pi$ and $T \subset T^\pi$. The model of T^π is the set of periodic T -valued sequences $\omega_i : \mathbb{Z} \rightarrow T$, where the subspace $T^\pi\{\Delta\} \subset T^\pi$ of Δ -periodic ones forms the tangent space of u within $M^\pi\{\Delta\}$ (we use braces $M^\pi\{\cdot\}$, $T^\pi\{\cdot\}$ to avoid confusion with the notations $M(\cdot)$, $T(\cdot)$). Spaces $\{T^\pi\{\Delta\}\}$ are nested by periods divisibility: $T^\pi\{\Delta\} \subset T^\pi\{\Delta'\}$ for any $\Delta | \Delta'$ (similarly for manifolds $\{M^\pi\{\Delta\}\}$). In particular, $T^\pi\{1\} \subset T^\pi\{\Delta\}$ for any $\Delta \in \mathbb{N}$, where $T^\pi\{1\}$ is the subspace of constant sequences $\omega_i \equiv \text{const}_i$. This subspace implements the embedding $T \rightarrow T^\pi$, i. e. $T^\pi\{1\}$ is T embedded into T^π . Denote by $\text{per}(\omega)$ the minimal period $\min\{\Delta \in \mathbb{N} : \omega \in T^\pi\{\Delta\}\}$ of $\omega \in T^\pi$. Fisher – Riemann dot product on T^π has the form

$$\langle \omega, \omega' \rangle = \Delta^{-1} \sum_{i=1}^{\Delta} \langle \omega_i, \omega'_i \rangle, \quad \omega, \omega' \in T^\pi, \quad \Delta = \text{lcd}(\text{per}(\omega), \text{per}(\omega')),$$

where $\langle \omega_i, \omega'_i \rangle$ is the Fisher – Riemann dot product on T .

The space T^π is representable as a tensor product

$$T^\pi = T \otimes \Pi, \quad (6)$$

where $\Pi = \bigcup_{\Delta \in \mathbb{N}} \Pi\{\Delta\}$ is a space of two-sided periodic real-valued sequences $a_i : \mathbb{Z} \rightarrow \mathbb{R}$, $\Pi\{\Delta\}$ is its subspace of Δ -periodic sequences $a_i \equiv a_{i+\Delta}$. By tensor product $U \otimes V$ of two spaces, we mean the linear span of tensor product $\{u_i\} \otimes \{v_j\} = \{u_i \otimes v_j\}$ (pairwise) of their bases $\{u_i\} \subset U$, $\{v_j\} \subset V$. Tensor product $\tilde{\omega} = \omega \otimes a \in T^\pi$ of two single elements $\omega \in T$ and $a \in \Pi$ is

$$\tilde{\omega} = (\tilde{\omega}_i)_{i \in \mathbb{Z}}, \quad \tilde{\omega}_i = a_i \omega. \quad (7)$$

In these terms $T^\pi\{\Delta\} = T \otimes \Pi\{\Delta\}$, $\Delta \in \mathbb{N}$. On the space Π a dot product similar to representation (6) is defined as

$$\langle a, a' \rangle = \Delta^{-1} \sum_{i=1}^{\Delta} \langle a_i, a'_i \rangle, \quad a, a' \in \Pi, \quad \Delta = \text{lcd}(\text{per}(a), \text{per}(a')), \quad (8)$$

and under tensor product (7) dot products on $\mathbb{T}$ and on Π are multiplied:

$$\langle \tilde{\omega}, \tilde{\omega}' \rangle = \langle \omega, \omega' \rangle \langle a, a' \rangle, \quad \omega, \omega' \in \mathbb{T}, \quad a, a' \in \Pi, \quad \tilde{\omega} = \omega \otimes a, \quad \tilde{\omega}' = \omega' \otimes a'. \quad (9)$$

Denote canonic orthonormal base $\psi^{(\Delta)} = \left\{ \psi^{(t, \Delta)} \right\}_{t \in \mathbb{Z}_\Delta}$ of $\Pi \{ \Delta \}$:

$$\psi^{(t, \Delta)} \in \Pi \{ \Delta \}, \quad \psi_i^{(t, \Delta)} = \sqrt{\Delta} \cdot 1 \left\{ i \equiv t \right\}, \quad \Delta \in \mathbb{N}, \quad t \in \mathbb{Z}_\Delta. \quad (10)$$

Note that the combined set $\psi = \bigcup_{\Delta \in \mathbb{N}} \psi^{(\Delta)}$ is not orthonormal, and, moreover, it is linearly dependent. Tensor product of the bases $\psi^{(\Delta)} \otimes \chi$ forms orthonormal base of $\mathbb{T}^\pi \{ \Delta \}$, $\Delta \in \mathbb{N}$. In these tensor terms the embedding $\mathbb{T} \rightarrow \mathbb{T}^\pi$ is made by tensor product with the constant sequence $\psi^{(0,1)} \in \Pi$, $\psi_i^{(0,1)} \equiv 1$, $i \in \mathbb{Z}$: $\mathbb{T} \mapsto \mathbb{T} \otimes \psi^{(0,1)} = \mathbb{T}^\pi \{ 1 \} \subset \mathbb{T}^\pi$. Further for brevity we omit $\otimes \psi^{(0,1)}$ for subspaces $\mathbb{T} \subset \mathbb{T}$ and write $\mathbb{T} \subset \mathbb{T}^\pi$ instead of $\mathbb{T} \otimes \psi^{(0,1)} \subset \mathbb{T}^\pi$.

Similarly to the characters base (2) on $\mathbb{T}$, many important tangent subspaces $\mathbb{T} \subset \mathbb{T}^\pi$ are linear spans of subsets of $\psi^{(\Delta)} \otimes \chi$ for some $\Delta \in \mathbb{N}$. Therefore, combination of the characters base (2) and the tensor product representation (6) provides powerful tool for working in the tangent space $\mathbb{T}^\pi$. Below we illustrate it briefly.

Family of chi-square statistics «coded» by tangent subspaces

There is a family of chi-square statistics $S_{\mathbb{T}} = S_{\mathbb{T}} \left[x_1^n \right]$ bijectively «coded» by finite-dimensional tangent subspaces $\mathbb{T} \subset \mathbb{T}^\pi$. More precisely, for each $\mathbb{T}$ there is a class of asymptotically equivalent statistics as $n \rightarrow +\infty$. These equivalent statistics behave asymptotically identically for uniformly distributed binary sequence $\{ x_1^n \}$ and in some neighbourhood of this assumption called contigual asymptotics [4; 5], when $\ell \{ x \} \rightarrow u$ along the Markov manifold $\ell \{ x \} \in \mathbb{M}^\pi$ with a «speed» $O \left(n^{-\frac{1}{2}} \right)$ as $n \rightarrow +\infty$. Up to this equivalence, we can talk about statistics $S_{\mathbb{T}}$ without specifying which one is it from the equivalence class.

The family of statistics $S_{\mathbb{T}}$ can be derived from another family of $\mathbb{T}^\pi$ -valued normalised sufficient statistics (NSS) related to sufficient statistics of exponential families of Markov chains [6]:

$$W_{\mathbb{T}} = W_{\mathbb{T}} \left[x_1^n \right] \in \mathbb{T}, \quad S_{\mathbb{T}} = \| W_{\mathbb{T}} \|^2, \quad (11)$$

where norm is the Fisher – Riemann one. Similarly to $S_{\mathbb{T}}$, NSS $W_{\mathbb{T}}$ represents a class of asymptotically equivalent statistics as $n \rightarrow +\infty$. Under null hypothesis $W_{\mathbb{T}}$ has asymptotically standard normal distribution on $\mathbb{T} \subset \mathbb{T}^\pi$ with regard to the Fisher – Riemann dot product. Under contigual alternative H_1 (i. e. satisfying contigual asymptotics) limit normal distribution of $W_{\mathbb{T}}$ becomes non-centred but preserves identity covariance matrix. NSS (11) (i. e. their equivalence classes) are «projectively agreed»:

$$W_{T_2} = \text{proj} \left(W_{T_1} \mid T_2 \right), \quad T_2 \subset T_1, \quad (12)$$

where $\text{proj}(\omega \mid \mathbb{T})$ is an orthogonal projection of $\omega \in \mathbb{T}^\pi$ onto finite-dimensional tangent subspace $\mathbb{T} \subset \mathbb{T}^\pi$ with regard to the Fisher – Riemann dot product.

Let us call T-test a chi-square statistical test of null hypothesis $H_0 : \ell \{ x \} = u$ associated with statistics $S_{\mathbb{T}}$. Under null hypothesis $S_{\mathbb{T}}$ is asymptotically chi-square distributed with $d = \dim(\mathbb{T})$ degrees of freedom: $\ell \{ S_{\mathbb{T}} \mid H_0 \} \rightarrow \chi_d^2$. Under contigual alternative $\ell \{ S_{\mathbb{T}} \mid H_1 \} \rightarrow \chi_{d, \lambda}^2$, where $\chi_{d, \lambda}^2$ is non-central chi-square distribution with non-centrality parameter $\lambda = \lim \left\| \mathbb{E} \{ W_{\mathbb{T}} \} \right\|^2 \geq 0$, depending on space $\mathbb{T}$ and on deviation of alternative from null hypothesis (distance from $\ell \{ x \}$ to u in information metric). Asymptotic power of T-test at the significance level $\alpha \in (0, 1)$ equals $1 - F_{d, \lambda} \left(F_{d, 0}^{-1} (1 - \alpha) \right)$, where $F_{d, \lambda}(\cdot)$ and $F_{d, \lambda}^{-1}(\cdot)$ are cumulative distribution function and quantile function for $\chi_{d, \lambda}^2$, respectively. Table presents some tangent subspaces $\mathbb{T} \subset \mathbb{T}^\pi$ and their T-tests with equivalent analogues.

Let us fix some step $\Delta \in \mathbb{N}$, gram length $L \in \mathbb{N}$ and consider frequencies statistics

$$f^{(L, \Delta)}(q) = \sum_{i=0}^{N^{(L, \Delta)}-1} 1 \{ x_{i\Delta+j} = q_j, j \in [1:L] \}, \quad q \in \Upsilon^L, \quad N^{(L, \Delta)} = \left\lfloor \frac{n-L}{\Delta} \right\rfloor. \quad (13)$$

Denote standard chi-square statistics based on frequencies (13):

$$m^{(L, \Delta)} = \sum_{q \in Y^L} \frac{\left(f^{(L, \Delta)}(q) - 2^{-L} N^{(L, \Delta)} \right)^2}{2^{-L} N^{(L, \Delta)}}. \quad (14)$$

For $\Delta \geq L$ the L -grams in sum (13) do not overlap, whence $m^{(L, \Delta)}$ has asymptotic chi-square distribution under null hypothesis and belongs to the family $\{S_T\}_{T \subset T^\pi}$. For $\Delta < L$ this asymptotic distribution is generalised chi-square one and $m^{(L, \Delta)}$ does not belong to the family $\{S_T\}$. The following two types of chi-square statistics [1] based on formula (14) both belong to the family $\{S_T\}$:

$$M_1^{(s, \Delta)} = m^{((s+1)\Delta, \Delta)} - m^{(s\Delta, \Delta)}, \quad D_1^{(s, \Delta)} = 2^{s\Delta} (2^\Delta - 1), \quad s \geq 0, \quad (15)$$

$$M_2^{(s, \Delta)} = M_1^{(s, \Delta)} - M_1^{(s-1, \Delta)}, \quad D_2^{(s, \Delta)} = 2^{(s-1)\Delta} (2^\Delta - 1)^2, \quad s \geq 1, \quad (16)$$

where $m^{(0, \Delta)} \equiv 0$. Chi-square statistics $M_i^{(s, \Delta)}$ have $D_i^{(s, \Delta)}$ degrees of freedom. Statistics of the second type $M_2^{(s, \Delta)}$ are asymptotically mutually independent for different $s \geq 1$ under any fixed $\Delta \in \mathbb{N}$. T-test based on $M_1^{(0, \Delta)}$ is the standard test of uniform distribution of non-overlapping Δ -blocks $(x_{i\Delta+1}, x_{i\Delta+2}, \dots, x_{(i+1)\Delta})$ (FIPS Poker test [7] for $\Delta = 4$). Tests based on $M_1^{(s, 1)}$ and $M_2^{(s, 1)}$ are the NIST Serial tests [8] of types I and II, respectively (with parameter $m = s + 1$). Test based on $M_1^{(0, 1)}$ is the Monobit test. Test based on $M_2^{(1, 1)}$ is asymptotically equivalent to the Runs test.

A remarkable feature of the family of chi-square statistics $\{S_T\}_{T \subset T^\pi}$ following from properties (11) and (12) is that their asymptotic probabilistic properties are «consistent» with geometric properties of corresponding tangent subspaces $T \subset T^\pi$. Due to this feature, obtaining asymptotic probabilistic properties of $\{S_T\}$ comes down to calculation of geometric quantities based on Fisher – Riemann dot product or combinatorial quantities, e. g., for large orthonormal bases considered as combinatorial objects.

Introduce two operations on the subspaces $T_1, T_2 \subset T^\pi$: $T_1 \boxplus T_2$ for direct sum of orthogonal subspaces $T_1 \perp T_2$; $T_1 \boxminus T_2 := T_1 \cap T_2^\perp$ for orthogonal complement of nested subspace $T_2 \subset T_1$ within a larger one T_1 . The use of these operations implies that the spaces are obviously satisfy the properties of orthogonality (for $\boxplus$) or nesting (for $\boxminus$). For instance, $\partial T(s) = T(s) \boxminus T(s-1)$, $s \geq 1$, and $T = \lim_{s \rightarrow +\infty} T(s)$ breaks into a sum

$$T = \boxplus_{s \in \mathbb{N}_0} \partial T(s). \quad (17)$$

Tangent subspaces $T \subset T^\pi$ and their T-tests

Tangent subspace $T \subset T^\pi$	Degrees of freedom $\dim(T)$	Equivalent T-tests from NIST [8] and FIPS [7]
$T(0)$	1	NIST Monobit test, NIST Serial test (type I, $m = 1$)
$\partial T(1)$	1	NIST Runs test, NIST Serial test (type II, $m = 2$)
$T(s), s \geq 0$	2^s	NIST Serial test (type I, $m = s + 1$), NIST Approximate entropy test ($m = s + 1$)
$\partial T(s), s \geq 1$	2^{s-1}	NIST Serial test (type II, $m = s + 1$)
$\sum_{t \in \mathbb{Z}_4} T(t) \otimes \psi^{(t, 4)}$	15	FIPS Poker test

Theorem 1. The following properties hold for subspaces $T_1, T_2 \subset T^\pi$:

- under contiguous alternative S_{T_1} and S_{T_2} are asymptotically independent iff $T_1 \perp T_2$;
- $S_{T_1 \boxplus T_2} = S_{T_1} + S_{T_2}$, $S_{T_1 \boxminus T_2} = S_{T_1} - S_{T_2}$ (additivity).

Proof. Follows directly from properties of normal distribution, properties (11) and (12), and asymptotic normality of NSS $\{\mathbb{W}_T\}_{T \subset \mathbb{T}^\pi}$ with identity covariance matrices.

Proof is complete.

Let $\xi^{(i)} = \left(\xi_j^{(i)} \right)_{j=1}^{d_i} \in \mathbb{R}^{d_i}$, $i \in \{1, 2\}$, be two dependent standard Gaussian vectors with cross-covariations $\text{cov} \left\{ \xi_j^{(1)}, \xi_k^{(2)} \right\} = 1 \{j = k \leq d_3\} \theta_j$, $\theta_1, \dots, \theta_{d_3} \neq 0$, $d_3 \leq \min \{d_1, d_2\}$. Squared Euclidean norms of these Gaussian vectors are chi-square distributed: $\sigma_i = \left\| \xi^{(i)} \right\|^2 \sim \chi_{d_i}^2$. Joint probability distribution of $\sigma = (\sigma_1, \sigma_2) \in \mathbb{R}_+^2$ depends on (d_1, d_2) and on the multiset $\Lambda = \{\lambda_i\}_{i=1}^{d_3}$, $\lambda_i = \theta_i^2$. By multiset we mean possible multiplicity of its elements, e. g., multiset $\{1, 1, 2\}$ consists of 1 (twice) and 2 (once). Denote this bivariate chi-square distribution $\chi_{d_1, d_2}^{2 \times 2}(\Lambda) := \ell \{ \sigma \}$. The case of independence of σ_1 and σ_2 is $\Lambda = \emptyset$. The case of semi-independence with correlation coefficient $\text{cor} \{ \sigma_1, \sigma_2 \} = \frac{d_3}{d_1}$ is $d_1 = d_2$ and $\Lambda = \{1, \dots, 1\}$ consisting of d_3 ones. In general case

$$\text{cov} \{ \sigma_1, \sigma_2 \} = \sum_{j=1}^{d_3} \text{cov} \left\{ \left(\xi_j^{(1)} \right)^2, \left(\xi_j^{(2)} \right)^2 \right\} = 2 \sum_{\lambda \in \Lambda} \lambda. \quad (18)$$

Let $\text{proj}(T_1 | T_2)$, $T_1, T_2 \subset \mathbb{T}^\pi$, be linear operator $T_1 \rightarrow T_2$ of orthogonal projection of space T_1 onto T_2 ; $\Lambda(T_1, T_2)$ be a multiset of non-zero squared singular numbers of projection operator $\text{proj}(T_1 | T_2)$ (it is commutative $\Lambda(T_1, T_2) = \Lambda(T_2, T_1)$ as $\text{proj}(T_1 | T_2)$ and $\text{proj}(T_2 | T_1)$ are adjoint operators and have the same singular numbers). We further call $\Lambda(T_1, T_2)$ Jordan multiset of a pair of tangent subspaces because Jordan principal angles [9] are closely related to it.

Corollary 1. Let $T_1, T_2 \subset \mathbb{T}^\pi$ be arbitrary tangent subspaces of finite dimensions $d_i = \dim(T_i)$. Under null hypothesis the pair (S_{T_1}, S_{T_2}) is asymptotically $\chi_{d_1, d_2}^{2 \times 2}(\Lambda(T_1, T_2))$ -distributed, and its asymptotic covariance admits the following equivalent expressions:

$$\lim \text{cov} \{ S_{T_1}, S_{T_2} \} = 2 \sum_{\lambda \in \Lambda(T_1, T_2)} \lambda = 2 \sum_{j, k} \left\langle \omega^{(j)}, \tilde{\omega}^{(k)} \right\rangle^2 = 2 \left\| \text{proj}(T_1 | T_2) \right\|_{\text{Fr}}^2, \quad (19)$$

where $\{\omega^{(j)}\} \subset T_1$, $\{\tilde{\omega}^{(k)}\} \subset T_2$ are arbitrary orthonormal bases; $\|\cdot\|_{\text{Fr}}$ is a Frobenius norm of linear operator.

Proof. Projection operator $\text{proj}(T_1 | T_2)$ is represented by a matrix of entries $\left\langle \omega^{(j)}, \tilde{\omega}^{(k)} \right\rangle$ in a pair of bases $\{\omega^{(j)}\}$, $\{\tilde{\omega}^{(k)}\}$. Sum of these squared entries and sum of squared singular numbers are two representations of squared Frobenius norm for $\text{proj}(T_1 | T_2)$, whence we get the second and the third equalities of expression (19). Now let us choose the left and the right singular vectors of $\text{proj}(T_1 | T_2)$ for the bases $\{\omega^{(j)}\}$, $\{\tilde{\omega}^{(k)}\}$, and set asymptotically standard normal vectors:

$$\xi^{(1)} = \left(\xi_j^{(1)} \right), \quad \xi^{(2)} = \left(\xi_k^{(2)} \right), \quad \xi_j^{(1)} = \left\langle \mathbb{W}_T, \omega^{(j)} \right\rangle, \quad \xi_k^{(2)} = \left\langle \mathbb{W}_T, \tilde{\omega}^{(k)} \right\rangle, \quad T = T_1 + T_2.$$

Their asymptotic cross-covariations by construction are

$$\lim \text{cov} \left\{ \xi_j^{(1)}, \xi_k^{(2)} \right\} = \left\langle \omega^{(j)}, \tilde{\omega}^{(k)} \right\rangle = 1 \{j = k \leq d_3\} \sqrt{\lambda_j}, \quad \Lambda(T_1, T_2) = \{\lambda_j\}_{j=1}^{d_3}.$$

By properties (11) and (12), we have $\left\| \xi^{(r)} \right\|^2 = S_{T_r}$, $r \in \{1, 2\}$, whence follows the needed asymptotic distribution of the pair (S_{T_1}, S_{T_2}) according to definition of $\chi^{2 \times 2}$ -distribution. The first equality of expression (19) follows from formula (18).

Proof is complete.

Let us call subspaces $T_1, T_2 \subset \mathbb{T}^\pi$ semi-orthogonal if $T_1 \boxplus T_3 \perp T_2 \boxplus T_3, T_3 = T_1 \cap T_2$. Nested spaces ($T_2 \subset T_1$) and orthogonal ones ($T_1 \perp T_2$) are the special cases. We also call two identically chi-square distributed random variables $\sigma_1, \sigma_2 \sim \chi_D^2$ semi-independent [1] if they are representable as

$$\sigma_1 = \tilde{\sigma}_1 + \tilde{\sigma}_0, \sigma_2 = \tilde{\sigma}_2 + \tilde{\sigma}_0, \tilde{\sigma}_0 \sim \chi_d^2, \tilde{\sigma}_1, \tilde{\sigma}_2 \sim \chi_{D-d}^2, \quad (20)$$

for some $0 \leq d \leq D$ and mutually independent $\{\tilde{\sigma}_i\}_{i=0}^2$. Obviously $\text{cor}\{\sigma_1, \sigma_2\} = \frac{d}{D}$.

Corollary 2. Let $T_1, T_2 \subset \mathbb{T}^\pi$ be subspaces of equal dimensions $\dim(T_1) = \dim(T_2)$. Under null hypothesis statistics S_{T_1} and S_{T_2} are asymptotically semi-independent with the asymptotic correlation coefficient

$$\lim \text{cor}\{S_{T_1}, S_{T_2}\} = \frac{\dim(T_1 \cap T_2)}{\dim(T_1)}$$

iff their spaces T_1, T_2 are semi-orthogonal.

Proof. Corollary 1 states bijection between asymptotic joint distribution of a pair (S_{T_1}, S_{T_2}) and relative position of spaces T_1, T_2 . In this bijection representation of the form (20) corresponds to the following representation for spaces:

$$T_1 = \tilde{T}_1 \boxplus \tilde{T}_0, T_2 = \tilde{T}_2 \boxplus \tilde{T}_0, \tilde{T}_1 \perp \tilde{T}_2,$$

which is equivalent to semi-orthogonality of T_1, T_2 .

Proof is complete.

Consider a class of tangent subspaces $T \subset \mathbb{T}^\pi$ to illustrate the above theory. Let us fix some period $\Delta \in \mathbb{N}$. Due to sum (17), the space $\mathbb{T}^\pi\{\Delta\} = \mathbb{T} \otimes \Pi\{\Delta\}$ breaks into a sum

$$\mathbb{T}^\pi\{\Delta\} = \boxplus_{(t,h) \in C_\Delta} \psi^{(t,\Delta)} \otimes \partial T(h), \quad C_\Delta := \mathbb{Z}_\Delta \times \mathbb{N}_0. \quad (21)$$

We call Δ -periodic cell of spatio-temporal index (t, h) (index for brevity, with temporal part t and spatial part h) the summand subspace under $\boxplus$ in formula (21), and we call Δ -periodic cellular space of profile $C \subset C_\Delta, |C| < +\infty$, a partial sum of Δ -periodic cells with indices from the profile C :

$$\mathbb{T}^\pi\{C, \Delta\} := \boxplus_{(t,h) \in C} \psi^{(t,\Delta)} \otimes \partial T(h), \quad \dim(\mathbb{T}^\pi\{C, \Delta\}) =: \dim(C) = \sum_{(t,h) \in C} \gamma[h], \quad (22)$$

where $\dim(\cdot)$ is an unbounded integer-valued dimensionality measure on C_Δ with atomic weights $\gamma[h]$ determined by formula (4).

Example 1. In particular, chi-square statistics (15) and (16) correspond to cellular spaces. Let us show how to get their profiles $C \subset C_\Delta$ by example of FIPS Poker test [7] that corresponds to statistics (15) with $\Delta = 4$ and $s = 0$. The expression in table for tangent subspace $T_{\text{Poker}} \subset \mathbb{T}^\pi$ of Poker test is reduced to the form (22) by breaking $\mathbb{T}(t)$ into sum $\boxplus_{0 \leq \tau \leq t} \partial T(\tau)$. The expression from table, in its turn, is obtained as follows. Space T_{Poker} is a tangent space of u within 15-dimensional Markov model of independent and identically distributed binary 4-blocks. Without loss of generality 4-block starts at zero time: $(x_0, \dots, x_3) \in Y^4$. Let us represent this Markov model as a 4-periodic one of the form (5). Symbol x_0 does not depend on prehistory $\{x_i : i < 0\}$, whence $\omega_0 \in \mathbb{T}(0)$ (zero Markov order). Symbol x_1 under its fixed prehistory $\{x_i : i < 1\}$ conditionally depends only on x_0 , whence $\omega_1 \in \mathbb{T}(1)$ (first Markov order). Similarly $\omega_i \in \mathbb{T}(i), i \in \mathbb{Z}_4$. These conditions are equivalent to representation in table. So the profile of 4-periodic cellular space T_{Poker} is $C = \{(t, h) : 0 \leq h \leq t \in \mathbb{Z}_4\}$, and similarly for statistics (15) with any arbitrary $\Delta \in \mathbb{N}$ and $s = 0$ («stair» shape on fig. 1). Profiles corresponding to statistics (16) have «double-stair» shapes (fig. 2) obtained by set subtraction of two «stair» shapes of different «heights».

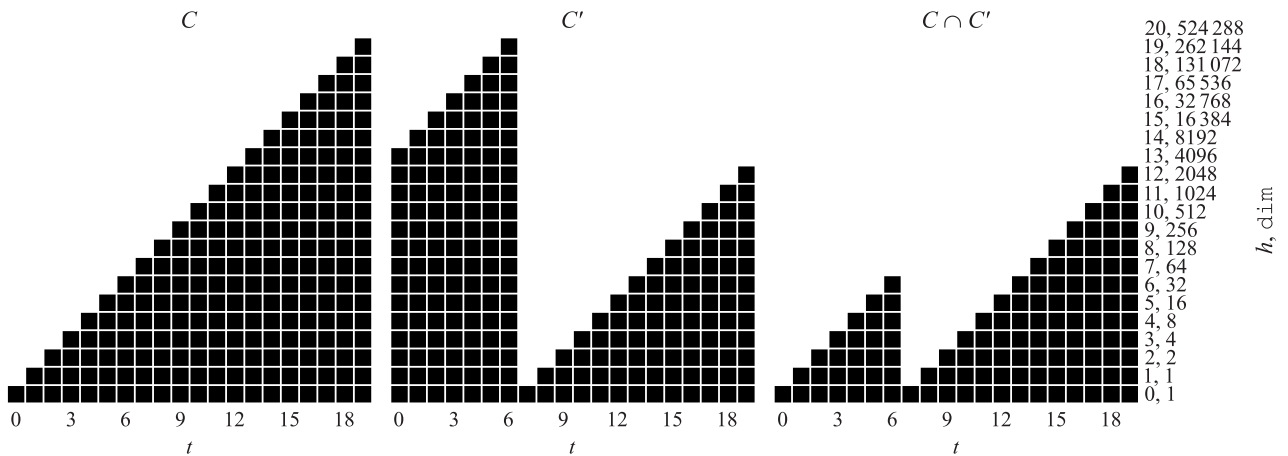


Fig. 1. Illustration to expression (23) for «stair» profile C and its cyclic shift C' ($\Delta = 20$, $\delta = 7$)

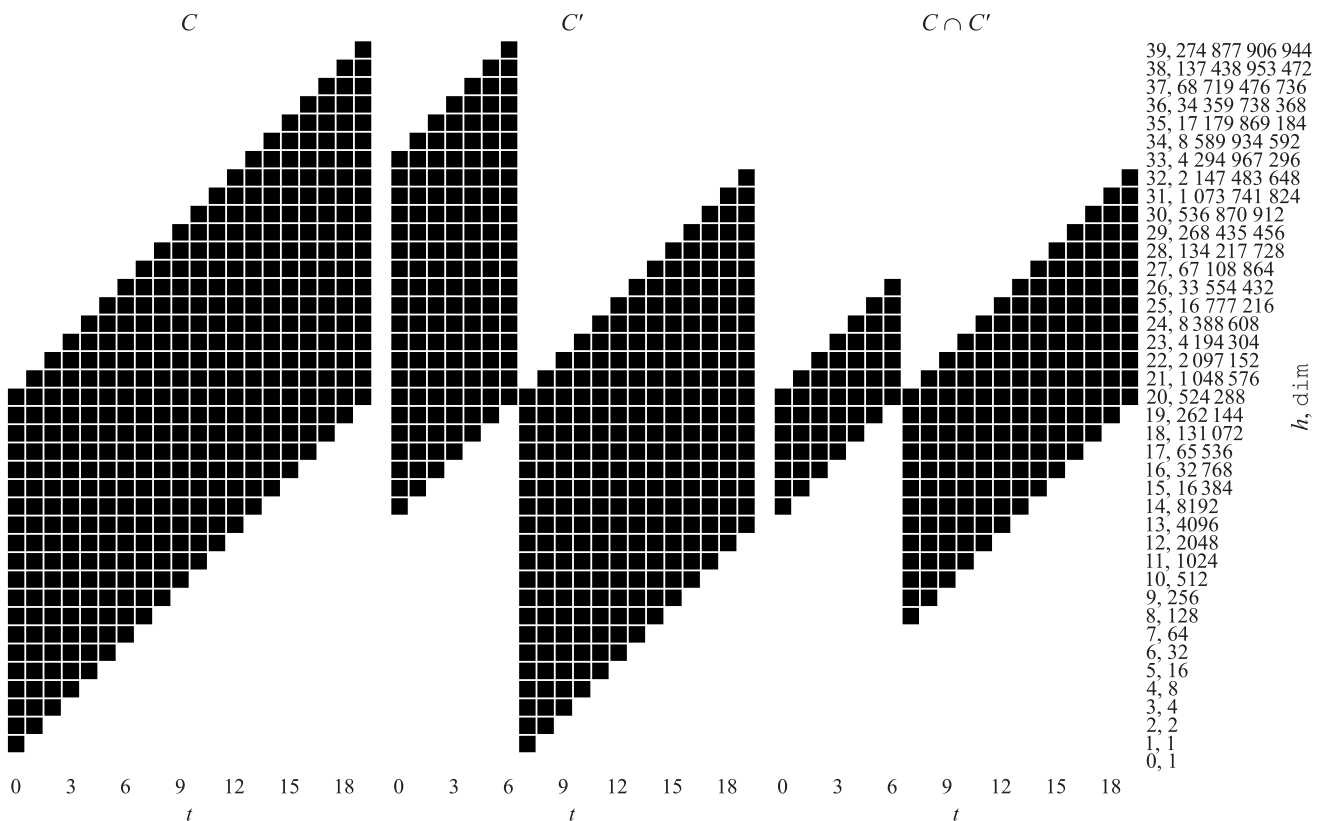


Fig. 2. Illustration to expression (23) for «double-stair» profile C and its cyclic shift C' ($\Delta = 20$, $\delta = 7$)

Due to corollary 2, asymptotic semi-independence of chi-square statistics is equivalent to semi-orthogonality of their tangent subspaces. Let us fix some $\Delta \in \mathbb{N}$ and two profiles $C, C' \subset C_\Delta$ of equal dimensionality measure $d = \dim(C) = \dim(C')$. Corresponding Δ -periodic cellular spaces of equal dimensions d are semi-orthogonal by definition, whence chi-square statistics $S_{\mathbb{T}^\pi\{C, \Delta\}}, S_{\mathbb{T}^\pi\{C', \Delta\}}$ are asymptotically semi-independent, and finding their asymptotic correlation coefficient $\frac{\tilde{d}}{d}$ comes down to calculation of dimensionality measure of intersection profile:

$$\tilde{d} = \dim(\mathbb{T}^\pi\{C, \Delta\} \cap \mathbb{T}^\pi\{C', \Delta\}) = \dim(\mathbb{T}^\pi\{C \cap C', \Delta\}) = \dim(C \cap C').$$

Let us fix now some profile $C \subset C_\Delta$ and consider corresponding chi-square statistics in two versions: undistorted $S_{\mathbb{T}^\pi\{C, \Delta\}}[\mathbf{x}_1^n]$ and δ -distorted $S_{\mathbb{T}^\pi\{C, \Delta\}}[\mathbf{x}_{1+\delta}^n]$ (without the first δ «bits» (see [1, sect. 4])). Reasoning

similarly to example 1, it is easy to show that δ -distortion leads to cyclic δ -shifting of profile along the temporal axis:

$$S_{\mathbb{T}^\pi\{C, \Delta\}} \left[\mathbf{x}_{1+\delta}^n \right] = S_{\mathbb{T}^\pi\{C', \Delta\}} \left[\mathbf{x}_1^n \right], \quad C' = \mathfrak{R}^\delta C,$$

where $\mathfrak{R}^\delta: \mathbf{C}_\Delta \rightarrow \mathbf{C}_\Delta$, $\mathfrak{R}^\delta(t, h) := \left(t + \frac{\Delta}{2}, h \right)$, $(t, h) \in \mathbf{C}_\Delta$. Obviously, dimensionality measure is invariant under this cyclic shift $\dim(C) = \dim(\mathfrak{R}^\delta C)$ as its weight $\gamma[h]$ depends only on the spatial part h of index (t, h) . Finally for chi-square statistics corresponding to Δ -periodic cellular spaces the asymptotic correlation coefficient between the undistorted and δ -distorted versions admits the following expression:

$$\limcor \left\{ S_{\mathbb{T}} \left[\mathbf{x}_1^n \right], S_{\mathbb{T}} \left[\mathbf{x}_{1+\delta}^n \right] \right\} = \frac{\dim(C \cap \mathfrak{R}^\delta C)}{\dim(C)}, \quad \mathbb{T} = \mathbb{T}^\pi\{C, \Delta\}. \quad (23)$$

Below we prove the result presented in article [1] using relation (23) for «stair» and «double-stair» profiles $C \subset \mathbf{C}_\Delta$ (see example 1). For these two types of profiles fig. 1 and 2 illustrate components of the right-hand side fraction (23): original profile C , cyclically shifted one $\mathfrak{R}^\delta C$, and their intersection $C \cap \mathfrak{R}^\delta C$. Weights $\gamma[h]$ of dimensionality measure are plotted on the vertical axis: their sum over profile (black cells) is equal to dimensionality of corresponding cellular space.

Theorem 2. For $0 \leq \delta \leq \Delta$ undistorted and δ -distorted statistics (15) and (16) are asymptotically semi-independent with the following asymptotic correlation coefficients under null hypothesis:

$$\limcor \left\{ M_1^{(s, \Delta)} \left[\mathbf{x}_1^n \right], M_1^{(s, \Delta)} \left[\mathbf{x}_{1+\delta}^n \right] \right\} = \frac{2^\delta + 2^{\delta'} - 2}{2^\Delta - 1}, \quad (24)$$

$$\limcor \left\{ M_2^{(s, \Delta)} \left[\mathbf{x}_1^n \right], M_2^{(s, \Delta)} \left[\mathbf{x}_{1+\delta}^n \right] \right\} = \frac{(2^\delta + 2^{\delta'})(2^\Delta + 1) - 2^{2+\Delta}}{(2^\Delta - 1)^2}, \quad (25)$$

where $\delta' = \Delta - \delta$.

Proof. «Stair» profile for $M_1^{(s, \Delta)}$ is

$$C = C_1^{(s, \Delta)} = \{(t, h) : 0 \leq h \leq s\Delta + t, t \in \mathbb{Z}_\Delta\}. \quad (26)$$

Corresponding δ -shifted profile in expression (23) is

$$C' = \{(t, h) : 0 \leq h \leq s\Delta + \tilde{t}, t \in \mathbb{Z}_\Delta\}, \quad \tilde{t} = \left(t + \frac{\Delta}{2} \right).$$

The following sums are used below:

$$\begin{aligned} \sum_{t \in \mathbb{Z}_\Delta} 2^{\min\{t, \tilde{t}\}} &= \sum_{\tau=0}^{\delta-1} 2^\tau + \sum_{\tau=0}^{\delta'-1} 2^\tau = 2^\delta + 2^{\delta'} - 2, \\ \sum_{t \in \mathbb{Z}_\Delta} 2^{\max\{t, \tilde{t}\}} &= \sum_{t \in \mathbb{Z}_\Delta} \left(2^t + 2^{\tilde{t}} - 2^{\min\{t, \tilde{t}\}} \right) = 2^{1+\Delta} - 2^\delta - 2^{\delta'}. \end{aligned} \quad (27)$$

Using formulas (4) and (27), dimensionality measure for intersection

$$\dim(C \cap C') = \sum_{t \in \mathbb{Z}_\Delta} \sum_{h=0}^{s\Delta + \min\{t, \tilde{t}\}} \gamma[h] = 2^{s\Delta} \sum_{t \in \mathbb{Z}_\Delta} 2^{\min\{t, \tilde{t}\}} = 2^{s\Delta} (2^\delta + 2^{\delta'} - 2).$$

We put this and $\dim(C) = D_1^{(s, \Delta)} = 2^{s\Delta} (2^\Delta - 1)$ into expression (23) and get asymptotic correlation coefficient (25).

«Double-stair» profile for $M_2^{(s, \Delta)}$ is a set subtraction of two adjacent «stair» profiles (26):

$$C = C_2^{(s, \Delta)} = C_1^{(s, \Delta)} \setminus C_1^{(s-1, \Delta)} = \{(t, h) : (s-1)\Delta + t < h \leq s\Delta + t, t \in \mathbb{Z}_\Delta\}.$$

Corresponding δ -shifted profile is

$$C' = \{(t, h) : (s-1)\Delta + \tilde{t} < h \leq s\Delta + \tilde{t}, t \in \mathbb{Z}_\Delta\}.$$

Using formula (27), dimensionality measure for intersection

$$\begin{aligned} \dim(C \cap C') &= \sum_{t \in \mathbb{Z}_\Delta} \sum_{h=1+(s-1)\Delta+\max\{t, \tilde{t}\}}^{s\Delta+\min\{t, \tilde{t}\}} \gamma[h] = \sum_{t \in \mathbb{Z}_\Delta} \left(2^{s\Delta+\min\{t, \tilde{t}\}} - 2^{(s-1)\Delta+\max\{t, \tilde{t}\}} \right) = \\ &= 2^{s\Delta} (2^\delta + 2^{\delta'} - 2) - 2^{(s-1)\Delta} (2^{1+\Delta} - 2^\delta - 2^{\delta'}). \end{aligned}$$

Put this and $\dim(C) = D_2^{(s, \Delta)} = 2^{(s-1)\Delta} (2^\Delta - 1)^2$ into expression (23) and get asymptotic correlation coefficient (25) after simplification.

Proof is complete.

Note that the values (24) and (25) do not depend on parameter s . Their plots for $\Delta = 7$ are presented in fig. 3. These plots are very close to each other, and they indeed are asymptotically equivalent (i. e. ratio goes to unity) uniformly over $0 \leq \delta \leq \Delta$ as $\Delta \rightarrow +\infty$. The plots are minimal at half-period $\delta = \frac{\Delta}{2}$ ($\delta = \frac{\Delta \pm 1}{2}$ for odd Δ) and maximal at full period $\delta \in \{0, \Delta\}$. The minimal values have asymptotics $\text{cor}_{\min} \sim R \cdot 2^{-\frac{\Delta}{2}}$, where $R = 2$ for even Δ and $R = \frac{3\sqrt{2}}{2}$ for odd Δ . In the neighbourhood of half-period the plots tend to the scaled hyperbolic cosine. In the neighbourhood of full period adjacent values differ approximately twofold for large Δ .

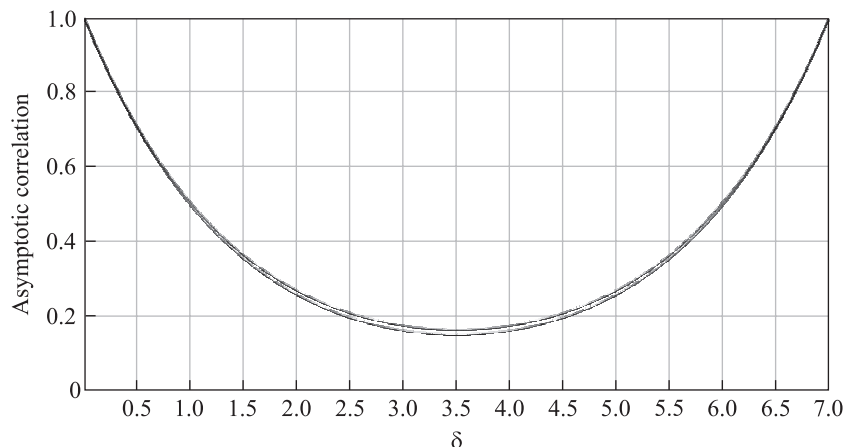


Fig. 3. Asymptotic correlation coefficients (24) and (25) plotted against δ ($\Delta = 7$)

Consider now joint asymptotic distribution of a pair $\left(S_{\mathbb{T}^\pi\{C, \Delta\}}, S_{\mathbb{T}^\pi\{C', \Delta'\}} \right)$ of chi-square statistics corresponding to cellular spaces of two arbitrary periods $\Delta, \Delta' \in \mathbb{N}$. In the case $\Delta \neq \Delta'$ there is no more guaranteed semi-orthogonality of cellular spaces, and as a consequence, asymptotic semi-independence of chi-square statistics. Therefore, we need more general corollary 1 to describe joint asymptotic distribution of chi-square statistics. The following trivial factorisation lemma is also used.

Lemma 1. Let two sums $T_1 = \bigoplus_{j \in J} T_{1,j}$, $T_2 = \bigoplus_{k \in K} T_{2,k}$ of tangent subspaces satisfy diagonality property $T_{1,j} \perp T_{2,k}$ for any $j \neq k$. Then their Jordan multiset breaks into union

$$\Lambda(T_1, T_2) = \bigcup_{j \in J \cap K} \Lambda(T_{1,j}, T_{2,j}).$$

Let us break $\gamma[h]$ -dimensional Δ -periodic cell of index $(t, h) \in C_\Delta$ into a sum of one-dimensional orthogonal subspaces:

$$\Psi^{(t, \Delta)} \otimes \partial \mathbb{T}(h) = \bigoplus_{Q \in \Upsilon^+[h]} \text{span} \left\{ \Psi^{(t, \Delta)} \otimes \chi^{(Q)} \right\}. \quad (28)$$

By analogy with Δ -periodic cells, we call Δ -periodic atom of spatio-temporal index (index for brevity) $(t, Q) \in \mathbf{A}_\Delta := \mathbb{Z}_\Delta \times \Upsilon^+$ the summand subspace under $\bigoplus$ in formula (28): Q is a spatial part of atom's index. Rewrite cellular space (22) as a sum of atoms, grouping summands by spatial parts Q :

$$\mathbb{T}^\pi\{C, \Delta\} = \bigoplus_{(t, h) \in C} \bigoplus_{Q \in \mathbb{Y}^+[h]} \text{span}\{\psi^{(t, \Delta)} \otimes \chi^{(Q)}\} = \bigoplus_{h \in \mathbf{h}^{(C)}} \bigoplus_{Q \in \mathbb{Y}^+[h]} \chi^{(Q)} \otimes \Pi\{\mathbf{t}_h^{(C)}, \Delta\}, \quad (29)$$

$$\Pi\{\mathbf{t}, \Delta\} := \text{span}\{\psi^{(t, \Delta)} : t \in \mathbf{t}\} \subset \Pi\{\Delta\},$$

$$\mathbf{t}_h^{(C)} := \{t : (t, h) \in C\} \subset \mathbb{Z}_\Delta, \quad \mathbf{h}^{(C)} := \{h : \exists (t, h) \in C\} \subset \mathbb{N}_0. \quad (30)$$

Here $\mathbf{t}_h^{(C)}$ is a «temporal slice» of profile C at the spacial level h ; $\mathbf{h}^{(C)}$ is a «spatial projection» of profile C ; $\Pi\{\mathbf{t}, \Delta\}$ is a canonic subspace of $\Pi\{\Delta\}$ corresponding to «temporal profile» $\mathbf{t}$.

Theorem 3. *Jordan multiset of two arbitrary cellular spaces is as follows:*

$$\Lambda(\mathbb{T}^\pi\{C, \Delta\}, \mathbb{T}^\pi\{C', \Delta'\}) = \left\{ \left(\frac{|\mathbf{t}_{h, \tau}^{(C)}| |\mathbf{t}_{h, \tau}^{(C')}|}{aa'} \right)^{\times \gamma[h]} : h \in \mathbf{h}^{(C)} \cap \mathbf{h}^{(C')}, \tau \in \left(\frac{\mathbf{t}_h^{(C)}}{\kappa \mathbb{Z}} \right) \cap \left(\frac{\mathbf{t}_h^{(C')}}{\kappa \mathbb{Z}} \right) \right\}, \quad (31)$$

where notation (30) is used, and also $\lambda^{\times \mu}$ means element λ of multiset taken with multiplicity μ ; $\kappa = \gcd(\Delta, \Delta')$; $a = \frac{\Delta}{\kappa}$; $a' = \frac{\Delta'}{\kappa}$; $\mathbf{t}_{h, \tau}^{(C)} = \left\{ t \in \mathbf{t}_h^{(C)} : t \equiv \tau \right\}$.

Proof. Consider a similar sum (29) for cellular space $\mathbb{T}^\pi\{C', \Delta'\}$. Diagonality property of lemma 1 holds for these sums over Q : it follows from formula (9) and characters orthogonality. Hence

$$\begin{aligned} \Lambda(\mathbb{T}^\pi\{C, \Delta\}, \mathbb{T}^\pi\{C', \Delta'\}) &= \bigcup_{h \in \mathbf{h}^{(C)} \cap \mathbf{h}^{(C')}, Q \in \mathbb{Y}^+[h]} \Lambda(\chi^{(Q)} \otimes \Pi\{\mathbf{t}_h^{(C)}, \Delta\}, \chi^{(Q)} \otimes \Pi\{\mathbf{t}_h^{(C')}, \Delta'\}) = \\ &= \bigcup_{h \in \mathbf{h}^{(C)} \cap \mathbf{h}^{(C')}} \Lambda^{\times \gamma[h]}(\Pi\{\mathbf{t}_h^{(C)}, \Delta\}, \Pi\{\mathbf{t}_h^{(C')}, \Delta'\}), \end{aligned} \quad (32)$$

where $\Lambda^{\times \mu}$ means multiset Λ taken with multiplicity μ . Denote $\mathbf{t} = \mathbf{t}_h^{(C)}$, $\mathbf{t}' = \mathbf{t}_h^{(C')}$ for brevity. From formulas (8) and (10) we get

$$\langle \psi^{(t, \Delta)}, \psi^{(t', \Delta')} \rangle = 1 \left\{ t \equiv t' \right\} (aa')^{-\frac{1}{2}}, \quad t \in \mathbb{Z}_\Delta, \quad t' \in \mathbb{Z}_{\Delta'}. \quad (33)$$

In other words, $\langle \psi^{(t, \Delta)}, \psi^{(t', \Delta')} \rangle \equiv 0$ for $t \not\equiv t'$. Let us break $\Pi\{\mathbf{t}, \Delta\}$ into a sum over integers modulo κ :

$$\Pi\{\mathbf{t}, \Delta\} = \bigoplus_{\tau \in \frac{\mathbf{t}}{\kappa \mathbb{Z}}} \Pi\{\mathbf{t}_\tau, \Delta\}, \quad \mathbf{t}_\tau = \left\{ t \in \mathbf{t} : t \equiv \tau \right\},$$

and similarly for $\Pi\{\mathbf{t}', \Delta'\}$. These sums satisfy diagonality property of lemma, whence

$$\Lambda(\Pi\{\mathbf{t}, \Delta\}, \Pi\{\mathbf{t}', \Delta'\}) = \bigcup_{\tau \in \left(\frac{\mathbf{t}}{\kappa \mathbb{Z}} \right) \cap \left(\frac{\mathbf{t}'}{\kappa \mathbb{Z}} \right)} \Lambda(\Pi\{\mathbf{t}_\tau, \Delta\}, \Pi\{\mathbf{t}'_\tau, \Delta'\}). \quad (34)$$

Due to formula (33), projection operator $\text{proj}(\Pi\{\mathbf{t}_\tau, \Delta\} | \Pi\{\mathbf{t}'_\tau, \Delta'\})$ is represented by a matrix $|\mathbf{t}_\tau| \times |\mathbf{t}'_\tau|$ of all equal entries $(aa')^{-\frac{1}{2}}$. This matrix has a single non-zero singular number $\sqrt{\frac{|\mathbf{t}_\tau| |\mathbf{t}'_\tau|}{aa'}}$, whence formula (34) takes the form

$$\Lambda(\Pi\{\mathbf{t}, \Delta\}, \Pi\{\mathbf{t}', \Delta'\}) = \left\{ \frac{|\mathbf{t}_\tau| |\mathbf{t}'_\tau|}{aa'} : \tau \in \left(\frac{\mathbf{t}}{\kappa \mathbb{Z}} \right) \cap \left(\frac{\mathbf{t}'}{\kappa \mathbb{Z}} \right) \right\}. \quad (35)$$

Combining formulas (32) and (35), we get multiset (31).

Proof is complete.

Theorem 3 means, in particular, that Jordan multiset of any two cellular spaces of periods $\Delta, \Delta' \in \mathbb{N}$ contains only rational numbers of the form $\frac{bb'}{aa'}$, $1 \leq b \leq a, 1 \leq b' \leq a'$, where $\frac{a}{a'}$ is an irreducible fraction equals to $\frac{\Delta}{\Delta'}$.

From theorem 3 we also derive the following semi-orthogonality criterion for cellular spaces (i. e. criterion for Jordan multiset of all units).

Corollary 3. *In the notation of theorem 3 cellular spaces $\mathbb{T}^\pi\{C, \Delta\}$ and $\mathbb{T}^\pi\{C', \Delta'\}$ are semi-orthogonal iff for each simultaneously non-empty equivalence classes*

$$\mathbf{t}_{h,\tau}^{(C)}, \mathbf{t}_{h,\tau}^{(C')} \neq \emptyset, h \in \mathbf{h}^{(C)} \cap \mathbf{h}^{(C')}, \tau \in \left(\frac{\mathbf{t}_h^{(C)}}{\kappa\mathbb{Z}} \right) \cap \left(\frac{\mathbf{t}_h^{(C')}}{\kappa\mathbb{Z}} \right),$$

these classes are both maximal:

$$|\mathbf{t}_{h,\tau}^{(C)}| = a, |\mathbf{t}_{h,\tau}^{(C')}| = a'.$$

This criterion obviously holds for $\Delta = \Delta'$ as $a = a' = 1$ and non-emptiness is equivalent to maximality. Introduce piecewise linear functions [1], satisfying finite difference relation (fig. 4):

$$\rho_1(x) = \max\{0, 1 - \max\{0, x\}\}, \rho_2(x) = \max\{0, 1 - |x|\} = \rho_1(x) - \rho_1(x+1), x \in \mathbb{R}. \quad (36)$$

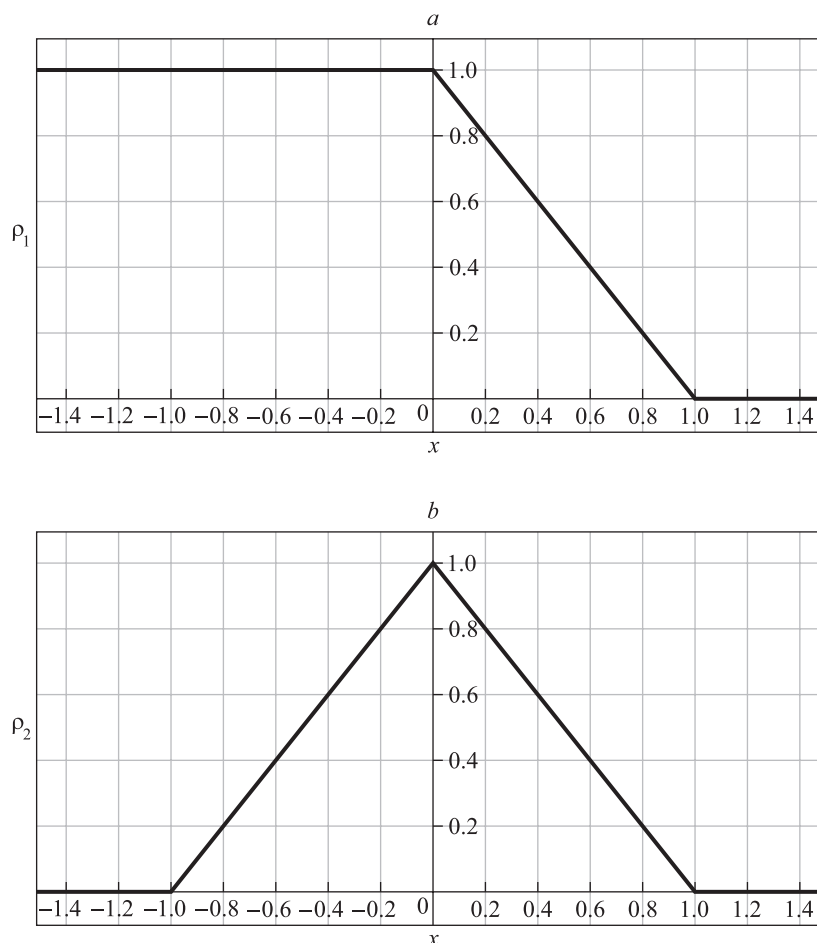


Fig. 4. Functions $\rho_1(x)$ (a) and $\rho_2(x)$ (b)

Below we prove the result presented in article [1], applying theorem 3 to «stair» and «double-stair» profiles.

Theorem 4. *Let $(i, j) \in \{(2, 2), (1, 2), (1, 1)\}$. In the notation of theorem 3 and functions (36) asymptotic covariances of statistics (15) and (16) under null hypothesis are as follows:*

$$\lim_{\text{cov}} \left\{ M_i^{(s, \Delta)}, M_j^{(s', \Delta')} \right\} = R + 2 \frac{(2^\kappa - 1)^2}{2^\kappa} \sum_{\mu=\mu_-}^{\mu_+} \rho_i \left(\frac{\mu}{a} - s \right) \rho_j \left(\frac{\mu}{a'} - s' \right) 2^{\mu\kappa}, \quad (37)$$

where $R = 2(2^\kappa - 1)$ for $(i, j) = (1, 1)$ and $R = 0$ otherwise; $\mu_+ = \min \{(s+1)a, (s'+1)a'\} - 1$;

$$\mu_- = \begin{cases} \max \{(s-1)a, (s'-1)a'\} + 1, & (i, j) = (2, 2), \\ (s'-1)a' + 1, & (i, j) = (1, 2), \\ 1, & (i, j) = (1, 1). \end{cases}$$

Proof. The cases $(i, j) = (2, 2)$ and $(i, j) = (1, 2)$ follow from the case $(i, j) = (1, 1)$, finite difference relations (16) and (36), and linearity of covariance with regard to its arguments. Thus, it is enough to prove asymptotic covariances (37) for $(i, j) = (1, 1)$, which, due to expression (19), is reduced to the summation of the elements over Jordan multiset (31) for «stair» profiles $C = C_1^{(s, \Delta)}$, $C' = C_1^{(s', \Delta')}$ of the form (26).

Let us fix some $\tau \in \mathbb{Z}_\kappa$ and find a part of sum corresponding to it (removing restrictions from the range of «stair heights» h adds zeros to Λ_τ without affecting the resulting sum):

$$\Sigma_\tau = \sum_{\lambda \in \Lambda_\tau} \lambda, \quad \Lambda_\tau = \left\{ \left(\frac{|\mathbf{t}_{h,\tau}^{(C)}| |\mathbf{t}_{h,\tau}^{(C')}|}{aa'} \right)^{\gamma[h]} : h \in \mathbb{N}_0 \right\}. \quad (38)$$

Break $\mathbb{N}_0$ into disjunctive intervals $I_\mu = [\max \{0, (\mu-1)\kappa + \tau + 1\} : \mu\kappa + \tau]$, $\mu \in \mathbb{N}_0$. For $h \leq s\Delta$ we have $\mathbf{t}_h^{(C)} = [0 : \Delta - 1]$. For $s\Delta < h < (s+1)\Delta$, $\mathbf{t}_h^{(C)} = [h - s\Delta : \Delta - 1]$. For $h \geq (s+1)\Delta$, $\mathbf{t}_h^{(C)} = \emptyset$. Finally it is easy to check the following relation for the number $|\mathbf{t}_{h,\tau}^{(C)}|$ of elements in $\mathbf{t}_h^{(C)}$ that equal τ modulo κ :

$$\frac{|\mathbf{t}_{h,\tau}^{(C)}|}{a} = \rho_1 \left(\frac{\mu}{a} - s \right), \quad h \in I_\mu, \quad \mu \in \mathbb{N}_0. \quad (39)$$

Putting expression (39) and similar relation for C' into formula (38) leads to the following expression (formula (4) is used):

$$\begin{aligned} \Sigma_\tau &= \sum_{\mu \in \mathbb{N}_0} \sum_{h \in I_\mu} \gamma[h] \frac{|\mathbf{t}_{h,\tau}^{(C)}| |\mathbf{t}_{h,\tau}^{(C')}|}{aa'} = \sum_{\mu \in \mathbb{N}_0} \rho_1 \left(\frac{\mu}{a} - s \right) \rho_1 \left(\frac{\mu}{a'} - s' \right) \sum_{h \in I_\mu} \gamma[h] = \\ &= \sum_{h \in I_0} \gamma[h] + \sum_{\mu \in \mathbb{N}} \rho_1 \left(\frac{\mu}{a} - s \right) \rho_1 \left(\frac{\mu}{a'} - s' \right) \sum_{h \in I_\mu} \gamma[h] = 2^\tau + 2^{\tau-\kappa} (2^\kappa - 1) \sum_{\mu \in \mathbb{N}} 2^{\mu\kappa} \rho_1 \left(\frac{\mu}{a} - s \right) \rho_1 \left(\frac{\mu}{a'} - s' \right). \end{aligned} \quad (40)$$

Summation of expressions (40) over $\tau \in \mathbb{Z}_\kappa$ with doubling (see expression (19)) gives asymptotic covariances (37) for $(i, j) = (1, 1)$, where the upper limit μ_+ of summation over μ «cuts off» zero summands at $\mu > \mu_+$.

Proof is complete.

Thus, asymptotic covariances of statistics (15) and (16) are expressed as some weighted dot products over integer lattice of «shifts and stretchings» of functions (36).

References

1. Voloshko VA. Local information geometry for high-order binary Markov chains and its applications. In: Kharin YuS, Zubkov AM, Kharin AYU, Maltsev MV, Palukha UYu, editors. *Computer data analysis and modeling: stochastics and data science. Proceedings of the 14th International conference; 2025 September 24–27; Minsk, Belarus*. Minsk: Belarusian State University; 2025. p. 266–271.
2. Amari S, Nagaoka H. *Methods of information geometry*. Harada D, translator. Oxford: Oxford University Press; 2000. 206 p. (Translations of mathematical monographs; volume 191).

3. Luong B. *Fourier analysis on finite Abelian groups*. Boston: Birkhauser; 2009. XVI, 159 p. (Applied and numerical harmonic analysis).
4. Voloshko VA, Kharin YuS, Trubey AI. On power comparison for some tests on pure randomness under Markov high-order dependencies. In: Kharin YuS, Zubkov AM, Kharin AYu, Maltsev MV, Palukha UYu, editors. *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.
5. Voloshko VA. [On asymptotic properties for a family of χ^2 -tests of pure randomness of binary sequence]. In: Kharin YuS, editor. *Teoreticheskaya i prikladnaya kriptografiya. Materialy II Mezhdunarodnoi nauchnoi konferentsii; 19–20 oktyabrya 2023 g.; Minsk, Belarus* [Theoretical and applied cryptography. Proceedings of the 2nd International conference; 2023 October 19–20; Minsk, Belarus]. Minsk: Belarusian State University; 2023. p. 15–43. Russian.
6. Hayashi M, Watanabe S. Information geometry approach to parameter estimation in Markov chains. *Annals Statistics*. 2016;44(4):1495–1535. DOI: 10.1214/15-AOS1420.
7. National Institute of Standards and Technology. *Security requirements for cryptographic modules*. Gaithersburg: National Institute of Standards and Technology; 2001. 64 p. (Federal information processing standards publications; FIPS PUB 140-2). DOI: 10.6028/NIST.FIPS.140-2.
8. Rukhin A, Soto J, Nechvatal J, Smid M, Barker E, Leigh S, et al. *A statistical test suite for random and pseudorandom number generators for cryptographic applications*. Gaithersburg: National Institute of Standards and Technology; 2010. [131] p. (NIST special publications; SP 800-22 revision 1a).
9. Jordan C. Essai sur la geometrie a n dimensions. *Bulletin de la societe mathematique de France*. 1875;3:103–174.

Received 24.12.2025 / revised 19.01.2026 / accepted 29.01.2026.