

УДК 519.21

М.М. Савчук

ВЕКТОРНІ ВИПАДКОВІ ПРОЦЕСИ І СТАТИСТИЧНІ ТЕСТИ ДЛЯ БІНАРНИХ ПОСЛІДОВНОСТЕЙ

Вступ

Випадкові та псевдовипадкові послідовності і генератори таких послідовностей мають різноманітні застосування в технічних пристроях, при статистичному моделюванні, обчисленнях, реалізації алгоритмів, а також є невід'ємною складовою будь-якої системи криптографічного захисту інформації. Зрештою, кожен потоковий шифр можна розглядати як генератор псевдовипадкових послідовностей, від якості якого залежить стійкість алгоритму шифрування. Оцінювання якості випадкових (псевдовипадкових) послідовностей та можливостей їх використання в різних застосуваннях є одним із найактуальніших питань, зокрема захисту інформації. Нині використовуються кілька наборів тестів для перевірки властивостей випадкових послідовностей. Найбільш відомі тести NIST [1]. Але існуючі критерії не вирішують усіх питань проблеми генерування та оцінки властивостей випадкових чисел і послідовностей.

Постановка задачі

У даній статті пропонуються та досліджуються нові статистичні тести перевірки якості випадкових послідовностей, що базуються на функціональних граничних теoreмах теорії випадкових процесів. Застосування добре розробленого апарату граничних теорем теорії випадкових процесів дає можливість отримувати теоретичні асимптотичні розподіли статистик та розраховувати критичні області, рівні значущості та інші характеристики критеріїв. Для цих цілей використовуються теореми про слабку збіжність у просторі функцій без розриву 2-го роду векторних випадкових процесів у схемах розміщення частинок по комірках, які побудовано певним чином за послідовністю, що тестується.

Побудова випадкових процесів за послідовністю

Нехай задана послідовність $\bar{\varepsilon} = \varepsilon_1 \varepsilon_2 \dots \varepsilon_s$, $\varepsilon_i \in \{0, 1\}$, $i = 1, \dots, s$, яку розглядаємо як реалізацію деякого випадкового дискретного процесу. Необхідно перевірити гіпотезу H_0 : послідовність ε є реалізацією послідовності незалежних рівномірних двійкових знаків, інакше кажучи, випадкові величини ε_i незалежні в сукупності і $\forall i = 1, \dots, s \quad P(\varepsilon_i = 1) = 1 - P(\varepsilon_i = 0) = 1/2$.

Нехай у послідовності $\bar{\varepsilon} = \varepsilon_1 \varepsilon_2 \dots \varepsilon_s$ $s = nN$, де n і N — деякі натуральні числа. Позначимо $\bar{\varepsilon}_i = \varepsilon_{(i-1)N+1}, \dots, \varepsilon_{iN}$, $i = 1, \dots, n$, $\tilde{N} = 2^N$. Будемо розглядати $\bar{\varepsilon}_i$ як двійкове число, $\bar{\varepsilon}_i \in \{0, 1, \dots, \tilde{N} - 1\}$.

Для деякого дійсного $T > 0$, такого, що $n = [T\tilde{N}]$, де $[x]$ — ціла частина дійсного числа x , введемо випадкові процеси на $[0, T]$:

$$X_N^j(t) = \sum_{l=0}^{\tilde{N}-1} \delta(j, \sum_{i=1}^{[t\tilde{N}]} \delta(i, \bar{\varepsilon}_i)),$$

$$\mu_N^j(t) = \tilde{N}^{-1/2} (X_N^j(t) - M X_N^j(t)), \quad j = 0, \dots, n,$$

де $\delta(i, j)$ — символ Кронекера, який дорівнює 1, коли $i = j$, і 0 при $i \neq j$; $t \in [0, T]$.

$$\text{При цьому } \sum_{j=0}^{[t\tilde{N}]} j X_N^j(t) = [\tilde{N}t], \quad \sum_{j=0}^{[t\tilde{N}]} X_N^j(t) = \tilde{N}.$$

Коли $j > [t\tilde{N}]$, то випадковий процес $X_N^j(u) = 0$ для будь-якого $u, 0 \leq u \leq t$. Якщо виконується гіпотеза H_0 , то математичне сподівання становитиме $M X_N^j(t) = C_{[t\tilde{N}]}^j \frac{1}{\tilde{N}^j} \left(1 - \frac{1}{\tilde{N}}\right)^{[t\tilde{N}]-j} \tilde{N}$, $0 \leq t \leq T$ [2].

Введемо для довільного r , $0 \leq r \leq n$, векторні випадкові процеси на $[0, T]$:

$$\mu_N(t) = (\mu_N^0(t), \mu_N^1(t), \dots, \mu_N^r(t)). \quad (1)$$

Побудуємо за послідовністю $\bar{\varepsilon} = \varepsilon_1 \varepsilon_2 \dots \varepsilon_s$ випадкові процеси на інтервалі $[0, 1]$:

$$Y_N^i(t) = \sum_{l=0}^{[(\tilde{N}-1)t]} \delta(i, \sum_{m=1}^n \delta(l, \bar{\varepsilon}_m)), \quad i = 0, \dots, n, \quad t \in [0, 1],$$

$$\sum_{i=0}^n Y_N^i(t) = [\tilde{N}t],$$

$$\xi_N^i(t) = \tilde{N}^{-1/2}(Y_N^i(t) - MY_N^i(t)), i = 0, \dots, n, t \in [0, 1],$$

$$Z_N(t) = \sum_{l=0}^{[(\tilde{N}-1)t]} \sum_{m=1}^n \delta(l, \bar{\varepsilon}_m), \quad (2)$$

$$\chi_N(t) = \tilde{N}^{-1/2}(Z_N(t) - MZ_N(t)),$$

$$\xi_N(t) = (\chi_N(t), \xi_N^0(t), \xi_N^1(t), \dots, \xi_N^r(t)).$$

Якщо виконується гіпотеза H_0 , то математичні сподівання становитимуть $MY_N^i(t) = C_n^i \frac{1}{\tilde{N}^i} \left(1 - \frac{1}{\tilde{N}}\right)^{n-1} [t\tilde{N}]$, $0 \leq t \leq 1$; $MZ_N(t) = [tN]$, $0 \leq t \leq 1$ [2].

Таким чином, $\mu_N(t), \xi_N(t)$ — центровані векторні випадкові процеси з нульовими математичними сподіваннями.

Доведення слабкої збіжності багатовимірних випадкових процесів

Теорема 1. Якщо $\bar{\varepsilon} = \varepsilon_1 \varepsilon_2 \dots \varepsilon_s$ — послідовність незалежних рівномірних двійкових знаків, $N \rightarrow \infty$, $r = \text{const} \geq 0$, $T = \text{const} > 0$, то послідовність випадкових процесів

$$\mu_N(t) = (\mu_N^0(t), \mu_N^1(t), \dots, \mu_N^r(t)) \quad (3)$$

слабко збігається на відрізку $[0, T]$ в $(r+1)$ -вимірному просторі D^{r+1} функцій без розриву 2-го роду з топологією Скорохода до неперервного з ймовірністю 1 гауссівського дифузійного процесу $\mu(t) = (\mu^0(t), \mu^1(t), \dots, \mu^r(t))$ з нульовим математичним сподіванням та матрицею кореляційних функцій

$$K_1(t, s) = \|k_{ij}(t, s)\|_0^r,$$

де при $t \geq s$, $i, j = 0, 1, \dots, r$ $k_{ij}(t, s) = p_j(s) \left\{ p_{i-j}(t-s) - p_i(t) \left[1 + \frac{(t-i)(s-j)}{t} \right] \right\}$, $p_m(t) = t^m e^{-t}/m!$, коли $m = 0, 1, 2, \dots$, та $p_m(t) = 0$ при $m < 0$, тобто $m = -1, -2, \dots$

Доведення. Сформулюємо задачу в термінах випадкового розміщення частинок по комірках. Випадкові величини $\bar{\varepsilon}_i$, $i = 1, 2, \dots, n$, за умовою задачі незалежні та з однаковою

ймовірністю набувають будь-якого значення з множини $\{0, 1, \dots, \tilde{N} - 1\}$. Будемо вважати цю множину множиною комірок, занумерованих від 0 до $\tilde{N} - 1$, а реалізацію випадкових величин $\bar{\varepsilon}_i$ — влучанням i -ї частинки в комірку з номером $\bar{\varepsilon}_i$. Тоді для послідовності випадкових векторних процесів (1) $\mu_N(t) = (\mu_N^0(t), \mu_N^1(t), \dots, \mu_N^r(t))$, які побудовані за послідовністю $\bar{\varepsilon} = \varepsilon_1 \varepsilon_2 \dots \varepsilon_s$ як описано вище, згідно з твердженням теореми 1 будуть виконуватись також умови теореми 7.2.1 із праці [2] з числом комірок $\tilde{N}$ і $\lambda = 1/\tilde{N}$. Згідно з цією теоремою матиме місце слабка збіжність випадкових процесів (3) у просторі D^{r+1} до неперервного з ймовірністю 1 гауссівського дифузійного процесу з нульовим математичним сподіванням та наведеною у формулюванні теореми 1 матрицею кореляційних функцій.

Теорема 2. Якщо $\bar{\varepsilon} = \varepsilon_1 \varepsilon_2 \dots \varepsilon_s$ — послідовність незалежних рівномірних двійкових знаків, $N \rightarrow \infty$ та $n/\tilde{N} \rightarrow \alpha < \infty$, то для будь-якого цілого $r \geq 0$ послідовність випадкових процесів

$$\xi_N(t) = (\chi_N(t), \xi_N^0(t), \xi_N^1(t), \dots, \xi_N^r(t)) \quad (4)$$

слабко збігається на відрізку $[0, 1]$ в $(r+2)$ -вимірному просторі D^{r+2} функцій без розриву 2-го роду з топологією Скорохода до неперервного з ймовірністю 1 гауссівського дифузійного процесу $\xi(t) = (\chi(t), \xi^0(t), \xi^1(t), \dots, \xi^r(t))$ з нульовим математичним сподіванням та матрицею кореляційних функцій

$$K_2(t, s) = \|k_{ij}(t, s)\|_1^n,$$

де при $t \geq s$ $k_{11} = \alpha s(1-t)$, $k_{1,i+2}(t, s) = k_{i+2,1}(t, s) = (i-\alpha)p_i(\alpha)s(1-t)$, $i = 0, 1, \dots, r$; $p_m(\alpha) = \alpha^m e^{-\alpha}/m!$; $k_{i+2,j+2}(t, s) = p_i(\alpha)s[\delta(i, j) - p_j(\alpha)\{1 + t\alpha^{-1}(i-\alpha) \times (j-\alpha)\}]$, $i, j = 0, 1, \dots, r$.

Доведення вказаної збіжності випадкових процесів (4) аналогічно доведенню теореми 1 зводиться до відповідної задачі про випадкове розміщення частинок по комірках. Випадкові величини $\bar{\varepsilon}_i$, $i = 1, 2, \dots, n$, за умовою задачі незалежні та з однаковою ймовірністю набувають будь-якого значення з множини $\{0, 1, \dots, \tilde{N} - 1\}$, яка інтерпретується як множина занумерована

них від 0 до $\tilde{N} - 1$ комірок, а реалізація випадкових величин $\bar{\varepsilon}_i$ — влучанням i -ї частинки в комірку з номером $\bar{\varepsilon}_i$. Тоді при виконанні умов теореми 2 для послідовності випадкових векторних процесів (2), (4), а саме $\xi_N(t) = (\chi_N(t), \xi_N^0(t), \xi_N^1(t), \dots, \xi_N^r(t))$, які побудовані за послідовністю $\bar{\varepsilon} = \varepsilon_1 \varepsilon_2 \dots \varepsilon_s$, будуть виконуватись умови теореми 7.3.2 з праці [2] з числом комірок $\tilde{N}$ та кількістю частинок n , відповідно до якої матиме місце слабка збіжність цих випадкових процесів у просторі D^{r+2} до неперервного з ймовірністю 1 гауссівського дифузійного процесу з нульовим математичним сподіванням та описаною у формулюванні теореми 2 матрицею кореляційних функцій.

Таким чином, для будь-якого фіксованого t , $0 < t \leq T$, в теоремі 1 та, відповідно, для будь-якого фіксованого t , $0 < t \leq T$, в теоремі 2 асимптотичний розподіл випадкового вектора $\mu_N(t) = (\mu_N^0(t), \mu_N^1(t), \dots, \mu_N^r(t))$ та, відповідно, асимптотичний розподіл випадкового вектора $\xi_N(t) = (\chi_N(t), \xi_N^0(t), \xi_N^1(t), \dots, \xi_N^r(t))$, що побудовані за послідовністю незалежних біт $\bar{\varepsilon}_i$, $i = 1, 2, \dots, n$ з ймовірністю $p = 1/2$ появи 1 (гіпотеза H_0), є невідродженим гауссівським розподілом з нульовим математичним сподіванням та кореляційною матрицею $K_1(t, t) = K_1(t)$ і, відповідно, $K_2(t, t) = K_2(t)$. Існує невідроджена матриця $A_i(t)$, $i \in \{1, 2\}$, така, що $A_i(t)A_i'(t) = K_i(t)$, де $A_i'(t)$ — транспонована матриця, $i \in \{1, 2\}$. Тоді $\mu(t) = A_1(t)\eta^{(1)}(t)$ і $\xi(t) = A_2(t)\eta^{(2)}(t)$, де $\mu(t)$, $\xi(t)$ і $\eta^{(i)}(t)$, $i \in \{1, 2\}$, — вектори-стовпці; $\eta^{(1)}(t) = (\eta_1^{(1)}(t), \eta_2^{(1)}(t), \dots, \eta_{r+1}^{(1)}(t))$ і $\eta^{(2)}(t) = (\eta_1^{(2)}(t), \eta_2^{(2)}(t), \dots, \eta_{r+2}^{(2)}(t))$ — випадкові вектори, що мають стандартний гауссівський розподіл, тобто координатні випадкові величини $\eta_j^{(i)}(t)$, $i \in \{1, 2\}$, незалежні і мають нормальний розподіл з параметрами (0;1) [3]. Відомо, що випадкова величина $\zeta^{(i)}(t) = (\eta_1^{(i)}(t))^2 + (\eta_2^{(i)}(t))^2 + \dots + (\eta_{r+i}^{(i)}(t))^2$ має χ^2 -розподіл з $r+i$ ступенями вільності $i = 1, 2$, а випадкова величина $\sqrt{\zeta^{(i)}}(t)$ має χ -розподіл з $r+i$ ступенями вільності. Існують обернені матриці $A_i^{-1}(t)$, $i \in \{1, 2\}$, і вектори $\eta^{(i)}(t)$

можна записати у вигляді $\eta^{(1)}(t) = A_1^{-1}(t)\mu(t)$ і $\eta^{(2)}(t) = A_2^{-1}(t)\xi(t)$. Враховуючи результати граничних теорем 1 і 2, останні співвідношення можна записати у вигляді асимптотичних рівностей $\eta^{(1)}(t) = A_1^{-1}(t)\mu_N(t)$ і $\eta^{(2)}(t) = A_2^{-1}(t)\xi_N(t)$. Доведені твердження та наведені результати (див. [3, 4]) використовуються далі для побудови статистичних критеріїв перевірки якості випадкових бінарних послідовностей. Алгоритм обчислення матриць $A_i(t)$, $i \in \{1, 2\}$, що задовольняють умову $A_i(t)A_i'(t) = K_i(t)$, наведено, наприклад, у статті [5], де запропоновано багатовимірний статистичний тест для двійкових послідовностей іншого типу.

Статистичні критерії

Побудова багатовимірних критеріїв 1 і 2 тестування послідовностей. 1. Нехай задано послідовність $\varepsilon' = \varepsilon_1 \varepsilon_2 \dots \varepsilon_v$, $\varepsilon_i \in \{0, 1\}$. Вибираємо параметри алгоритму n, N , $s \in Z^+$ так, що $n = \left\lceil \frac{v}{N} \right\rceil$, $s = nN$. Далі розглядаємо послідовність $\bar{\varepsilon} = \varepsilon_1 \varepsilon_2 \dots \varepsilon_s$, $\varepsilon_i \in \{0, 1\}$. Задамо рівень значущості критерію згоди α , $0 < \alpha < 1$, фіксуємо деяке $t \in (0, T]$ для критерію 1 і деяке $t \in (0, 1]$ для критерію 2.

2. За послідовністю $\bar{\varepsilon} = \varepsilon_1 \varepsilon_2 \dots \varepsilon_s$ будуюмо випадкові величини і вектори для критерію 1:

$$X_N^j(t) = \sum_{l=0}^{\tilde{N}-1} \delta(j, \sum_{i=1}^{\lfloor t\tilde{N} \rfloor} \delta(l, \bar{\varepsilon}_i)),$$

$$\mu_N^j(t) = \tilde{N}^{-1/2} (X_N^j(t) - M X_N^j(t)),$$

$$\mu_N(t) = (\mu_N^0(t), \mu_N^1(t), \dots, \mu_N^r(t)),$$

а також випадкові величини і вектори для побудови критерію 2:

$$Y_N^i(t) = \sum_{l=0}^{[(\tilde{N}-1)t]} \delta(i, \sum_{m=1}^n \delta(l, \bar{\varepsilon}_m)),$$

$$Z_N(t) = \sum_{l=0}^{[(\tilde{N}-1)t]} \sum_{m=1}^n \delta(l, \bar{\varepsilon}_m),$$

$$\xi_N^i(t) = \tilde{N}^{-1/2} (Y_N^i(t) - M Y_N^i(t)),$$

$$\chi_N(t) = \tilde{N}^{-1/2} (Z_N(t) - M Z_N(t)),$$

$$\xi_N(t) = (\chi_N(t), \xi_N^0(t), \xi_N^1(t), \dots, \xi_N^r(t)).$$

3. Знаходимо матриці $A_i(t)$, $i=1,2$, такі, що $A_i(t)A_i'(t) = K_i(t)$, де $A_i'(t)$ – транспонована матриця, а також обернені матриці $A_i^{-1}(t)$.

4. Знаходимо вибіркові асимптотичні значення гауссівських векторів із стандартним $(r+i)$ -вимірним розподілом: $\eta^{(1)} = A_1^{-1}\mu_N(t)$ і $\eta^{(2)} = A_2^{-1}\xi_N(t)$.

5. Підраховуємо значення статистик $\zeta^{(1)}(t) = \eta_1^2(t) + \eta_2^2(t) + \dots + \eta_{r+2}^2(t)$ і $\zeta^{(2)}(t) = \eta_1^2(t) + \eta_2^2(t) + \dots + \eta_{r+2}^2(t)$. Знаходимо квантилі $Z_{1-\alpha}^i$ рівня $1-\alpha$ χ^2 -розподілу з $r+i$ ступенями вільності, $i \in \{1,2\}$ [4].

6. Якщо значення статистики $\zeta^{(1)}(t)$ більше $Z_{1-\alpha}^1$, то гіпотеза H_0 про те, що послідовність $\bar{\epsilon}$ є реалізацією послідовності незалежних двійкових знаків, що з ймовірністю $p=1/2$ набувають значень 0 і 1, за критерієм 1 відхиляється. Якщо $\zeta^{(1)}(t) \leq Z_{1-\alpha}^1$, то гіпотеза H_0 справджується і не суперечить даній послідовності за критерієм 1.

Якщо значення статистики $\zeta^{(2)}(t)$ більше $Z_{1-\alpha}^2$, то гіпотеза H_0 про те, що послідовність $\bar{\epsilon}$ є реалізацією послідовності незалежних двійкових знаків, що з ймовірністю $p=1/2$ набувають значень 0 і 1, за критерієм 2 відхиляється. Якщо $\zeta^{(2)}(t) \leq Z_{1-\alpha}^2$, то гіпотеза H_0 справджується і не суперечить даній послідовності за критерієм 2.

Критерії 3 і 4 (узагальнення багатовимірних критеріїв 1 і 2). 1. Нехай задано послідовність $\epsilon' = \epsilon_1\epsilon_2\dots\epsilon_v$. Вибираємо параметри алгоритму n, N , $s \in Z^+$ так, що $n = \left\lceil \frac{v}{N} \right\rceil$, $s = nN$.

Далі розглядаємо послідовність $\bar{\epsilon} = \epsilon_1\epsilon_2\dots\epsilon_s$. Задамо рівень значущості критерію згоди α , $0 < \alpha < 1$. Виберемо k моментів часу $0 < t_1 < t_2 < \dots < t_k \leq T$ для критерію 3 і k моментів часу $0 < t_1 < t_2 < \dots < t_k \leq 1$ для критерію 4.

2. За послідовністю $\epsilon' = \epsilon_1\epsilon_2\dots\epsilon_v$ будемо випадкові вектори для критерію 3

$$\mu_N(t_j) = (\mu_N^0(t_j), \mu_N^1(t_j), \mu_N^2(t_j), \dots, \mu_N^r(t_j)),$$

$$j = 1, 2, \dots, k,$$

$$\mu_N(t_1, \dots, t_k) = (\mu_N(t_1), \mu_N(t_2), \dots, \mu_N(t_k)),$$

а також випадкові вектори для критерію 4

$$\xi_N(t_j) = (\chi_N(t_j), \xi_N^0(t_j), \xi_N^1(t_j), \xi_N^2(t_j), \dots,$$

$$\xi_N^r(t_j)), \quad j = 1, 2, \dots, k,$$

$$\xi_N(t_1, \dots, t_k) = (\xi_N(t_1), \xi_N(t_2), \dots, \xi_N(t_k)).$$

Для $i \in \{1,2\}$ $(r+i)k$ -вимірні вектори $\mu_N(t_1, \dots, t_k) = (\mu_N(t_1), \mu_N(t_2), \dots, \mu_N(t_k))$ і $\xi_N(t_1, \dots, t_k) = (\xi_N(t_1), \xi_N(t_2), \dots, \xi_N(t_k))$ мають $((r+i)k \times (r+i)k)$ -матрицю коваріацій $\Sigma_i = \|K_i(t_l, t_m)\|$, $l, m = 1, 2, \dots, k$, що утворена k^2 блоками, кожен з яких є відповідною $(r+i) \times (r+i)$ -матрицею.

3. Знаходимо $((r+i)k \times (r+i)k)$ -матриці A_i , такі, що $A_i A_i' = \Sigma_i$, і обернені матриці A_i^{-1} , $i \in \{1,2\}$.

4. Знаходимо вибіркові значення асимптотично гауссівських векторів із стандартним $(r+i)k$ -вимірним розподілом $\eta^{(1)}(t_1, \dots, t_k) = A_1^{-1} \times \mu_N(t_1, \dots, t_k)$ і $\eta^{(2)}(t_1, \dots, t_k) = A_2^{-1} \xi_N(t_1, \dots, t_k)$.

5. Підраховуємо значення статистики $\zeta^{(i)}(t_1, \dots, t_k) = \eta_1^2 + \eta_2^2 + \dots + \eta_{(r+i)k}^2$, де η_j , $j = 1, \dots, (r+i)k$, – координати вектора $\eta^{(i)}(t_1, \dots, t_k)$, $i \in \{1,2\}$. Знаходимо квантилі $Z_{1-\alpha}^i$, $i \in \{1,2\}$, рівня $1-\alpha$ χ^2 -розподілу з $(r+i)k$ ступенями вільності.

6. Якщо значення статистики $\zeta^{(i)}(t_1, \dots, t_k)$ більше $Z_{1-\alpha}^i$, то гіпотеза H_0 про те, що послідовність ϵ є реалізацією послідовності незалежних двійкових знаків, що з ймовірністю $p=1/2$ набувають значень 1, відхиляється за критерієм 3 для $i=1$ і за критерієм 4 при $i=2$.

Якщо $\zeta^{(i)}(t_1, \dots, t_k) \leq Z_{1-\alpha}^i$, $i \in \{1,2\}$, то гіпотеза H_0 справджується і не суперечить даній послідовності за критеріями 3 і 4, відповідно.

Експериментальні дослідження показують, що критерії 1–4 при правильному виборі пара-

метрів ефективні для перевірки якості також досить коротких бінарних послідовностей.

Висновки

У статті запропоновано та обґрунтовано статистичні тести перевірки якості випадкових та псевдовипадкових двійкових послідовностей, що базуються на використанні функціональних граничних теорем для векторних випадкових

процесів. Дані тести дають можливість ефективно аналізувати випадкові й псевдовипадкові бітові послідовності і орієнтовані на роботу з послідовностями короткої та середньої довжини. Наведені багатовимірні критерії можуть краще "працювати" при інших параметрах послідовностей, ніж, наприклад, відомі тести NIST [1], або краще відхиляти певні типи альтернативних гіпотез.

М.Н. Савчук

ВЕКТОРНЫЕ СЛУЧАЙНЫЕ ПРОЦЕССЫ И СТАТИСТИЧЕСКИЕ ТЕСТЫ ДЛЯ БИНАРНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Построены многомерные статистические критерии проверки качества случайных последовательностей. С использованием слабой сходимости векторных случайных процессов найдены асимптотические распределения статистик.

M.M. Savchuk

VECTORIAL RANDOM PROCESSES AND STATISTICAL TESTS FOR BINARY SEQUENCES

We construct the multidimensional statistical criteria of quality check of casual sequences. By using the weak convergence of vector casual processes, we discover asymptotic distributions of statistics.

1. *A Statistical Test Suite for The Validation of Random Number Generators and Pseudo Random Number Generators for Cryptographic Applications. Special Publication 800-22 Revision 1.* <http://csrc.nist.gov/publications/nistpubs/800-22-rev1/SP800-22rev1.pdf>
2. *Коваленко И.Н., Левитская А.А., Савчук М.Н.* Избранные задачи вероятностной комбинаторики. — К.: Наук. думка, 1986. — 224 с.
3. *Афифи А., Эйзен С.* Статистический анализ. Подход с использованием ЭВМ. — М.: Мир, 1982. — 488 с.
4. *Ивченко Г.И., Медведев Ю.И.* Математическая статистика: Учеб. пособие для вузов. — М.: Высш. шк., 1984. — 248 с.
5. *Савчук М., Шапанов В.* Многомерный статистический тест для двоичных последовательностей // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. — 2009. — № 1(18). — С. 65–72.

Рекомендована Радою
Фізико-технічного інституту
НТУУ "КПІ"

Надійшла до редакції
2 червня 2010 року