

## СОВМЕСТНОЕ РАСПРЕДЕЛЕНИЕ НЕКОТОРЫХ СТАТИСТИК СЛУЧАЙНОЙ БИТОВОЙ ПОСЛЕДОВАТЕЛЬНОСТИ

**Аннотация.** Для конечной последовательности, состоящей из независимых одинаково распределенных случайных величин, принимающих значение нуль или единица, установлены двумерные и трехмерные распределения некоторых специальных статистик, характеризующих расположение ее элементов. Приведены таблицы, иллюстрирующие применение указанных распределений для последовательности длины 32 в предположении, что ее элементы принимают значения нуль или единица с равными вероятностями.

**Ключевые слова:** многомерная статистика, случайная последовательность, s-цепочки, стеганография, статистическое тестирование.

### ВВЕДЕНИЕ

Факт наличия шифрата является одним из недостатков криптозащиты информации, поскольку дает повод «противнику» предполагать существование в ней скрытых данных. Устранение указанного недостатка можно осуществить, используя, например, методы стеганографии [1]. Построение (в рамках цифровой стеганографии) математических моделей вкрапления одной битовой информации в другую битовую последовательность не исключает статистического анализа ее локальных участков на предмет выявления особенностей расположения в них нулей и единиц.

В настоящей статье, являющейся продолжением работы [2], получены явные функции совместного распределения 2-цепочек и 3-цепочек специального вида.

### ПОСТАНОВКА ЗАДАЧИ

Рассмотрим случайные величины

$$\gamma_1, \gamma_2, \dots, \gamma_n, \quad (1)$$

где  $\gamma_i \in \{0, 1\}$ ,  $i = 1, 2, \dots, n$ ,  $n > 0$ , в предположении следующего условия.

**Условие 1.** Последовательность (1) состоит из  $n$ ,  $n > 0$ , независимых одинаково распределенных случайных величин; вероятности событий  $\{\gamma_i = 1\}$ ,  $\{\gamma_i = 0\}$  известны и имеют вид

$$P\{\gamma_i = 1\} = p, \quad P\{\gamma_i = 0\} = q, \quad (2)$$

где  $p + q = 1$ ,  $i = 1, 2, \dots, n$ .

Подпоследовательность  $\gamma_j, \gamma_{j+1}, \dots, \gamma_{j+s-1}$  последовательности (1) называют  $s$ -цепочкой,  $j = 1, 2, \dots, n - s + 1$ ,  $s = 1, 2, \dots, n$ . Обозначим  $\eta(t_1, t_2, \dots, t_s)$  число  $s$ -цепочек, совпадающих с  $t_1, t_2, \dots, t_s$ , где  $t_i \in \{0, 1\}$ ,  $i = 1, 2, \dots, s$ . Например, последовательность типа 1001011100100011 имеет две 4-цепочки типа 1001,  $\eta(1001) = 2$ ; четыре 2-цепочки типа 00,  $\eta(00) = 4$ ; одну 3-цепочку типа 111,  $\eta(111) = 1$  и т.д.

**Теорема 1.** Пусть выполняются условия (2) и целые числа  $n, k_1, k_2, k_3, t, t^*$  такие, что  $k_1 \geq k_2 \geq 0$ ,  $k_3 \geq 0$ ,  $t \in \{0, 1\}$ ,  $t^* = 1 - t$ . Тогда:

• вероятность совместного осуществления событий  $\{\eta(tt) = k_1\}$ ,  $\{\eta(ttt) = k_2\}$  и  $\{\eta(tt^*t) = k_3\}$  имеет вид

$$\begin{aligned}
& P \{ \eta(tt) = k_1, \eta(ttt) = k_2, \eta(tt^*t) = k_3 \} = \\
& = \sum_{m_1=0}^n p^{m_1} q^{m_0} \left\{ \binom{m_t - k_1}{k_1 - k_2} \binom{m_t - k_1 - 1}{k_3} \binom{m_t^* - m_t + k_1 + 2}{m_t - k_1 - k_3} \times \right. \\
& \quad \left. \times Z(k_1; k_1 - k_2) \chi(m_t \geq 1) + \chi(m_t = k_1 = k_2 = k_3 = 0) \right\}, \quad (3)
\end{aligned}$$

где  $m_0 = n - m_1$ ,  $\chi(E)$  — индикатор события  $E$ ,

$$Z(a; b) = \begin{cases} \binom{a-1}{b-1}, & \text{если } a \geq b \geq 1, \\ 1, & \text{если } a = b = 0, \\ 0 & \text{в остальных случаях;} \end{cases}$$

• вероятность совместного осуществления событий  $\{ \eta(tt) = k_1 \}$  и  $\{ \eta(ttt) = k_2 \}$ , если целые числа  $k_1, k_2, t$  такие, что  $k_1 \geq k_2 \geq 0, t \in \{0, 1\}$ , имеет вид

$$\begin{aligned}
& P \{ \eta(tt) = k_1, \eta(ttt) = k_2 \} = \\
& = \sum_{m_1=0}^n p^{m_1} q^{m_0} \left\{ \binom{m_t - k_1}{k_1 - k_2} \binom{m_t^* + 1}{m_t - k_1} Z(k_1; k_1 - k_2) \right\}; \quad (4)
\end{aligned}$$

• вероятность совместного осуществления событий  $\{ \eta(tt) = k_1 \}$  и  $\{ \eta(tt^*t) = k_2 \}$  имеет вид

$$\begin{aligned}
& P \{ \eta(tt) = k_1, \eta(tt^*t) = k_2 \} = \sum_{m_1=0}^n p^{m_1} q^{m_0} \left\{ \binom{m_t - 1}{k_1} \binom{m_t - k_1 - 1}{k_2} \times \right. \\
& \quad \left. \times \binom{m_t^* - m_t + k_1 + 2}{m_t - k_1 - k_2} \chi(m_t \geq 1) + \chi(m_t = k_1 = k_2 = 0) \right\}; \quad (5)
\end{aligned}$$

• вероятность совместного осуществления событий  $\{ \eta(tt) = k_1 \}$  и  $\{ \eta(ttt) + \eta(tt^*t) = k_2 \}$  имеет вид

$$\begin{aligned}
& P \{ \eta(tt) = k_1, \eta(ttt) + \eta(tt^*t) = k_2 \} = \sum_{m_1=0}^n p^{m_1} q^{m_0} \times \\
& \times \sum_{\delta + \delta^* = k_2 + m_t - 2k_1} \left\{ \binom{m_t - k_1}{\delta} \binom{m_t - k_1 - 1}{\delta^*} \binom{m_t^* - m_t + k_1 + 2}{m_t - k_1 - \delta - \delta^*} \times \right. \\
& \quad \left. \times Z(k_1; m_t - k_1 - \delta) \chi(m_t \geq 1) + \chi(m_t = k_1 = k_2 = 0) \right\}. \quad (6)
\end{aligned}$$

**Доказательство.** Обоснуем соотношение (3). В силу условия (2) количество единиц (обозначим его  $\nu$ ) в последовательности (1) имеет биномиальное распределение с параметрами  $(n, p)$ :

$$P \{ \nu = m \} = C_n^m p^m q^{n-m}, \quad m = 1, 2, \dots, n. \quad (7)$$

Используя формулу полной вероятности, получаем

$$P\{E_1, E_2, E_3\} = \sum_{m=0}^n P\{v=m\}P\{E_1, E_2, E_3 / v=m\}, \quad (8)$$

где  $E_1 = \{\eta(tt) = k_1\}$ ,  $E_2 = \{\eta(ttt) = k_2\}$  и  $E_3 = \{\eta(tt^*t) = k_3\}$ .

Покажем, что имеет место соотношение

$$P\{E_1, E_2, E_3 / v = m_1\} = (C_n^{m_1})^{-1} C_{m_1-k_1}^{k_1-k_2} C_{k_1-1}^{k_2} C_{m_1-k_1-1}^{k_3} C_{m_1^*-m_1+k_1+2}^{m_1-k_1-k_3}. \quad (9)$$

Для этого введем обозначения:

- $\Omega(n, m_1)$  — совокупность всех  $(0, 1)$ -последовательностей длины  $n$ , каждая из которых содержит  $m_1$  единиц и  $m_0$  нулей,  $m_0 + m_1 = n$ ,  $n \geq 3$ ;
- $Q$  — число всех векторов  $\bar{v}, \bar{v} \in \Omega(n, m_1)$ , для каждого из которых имеют место события  $E_1, E_2, E_3$ .

Для произвольного вектора  $\bar{v}, \bar{v} \in \Omega(n, m_1)$ , состоящего из  $m_t (m_{t^*})$   $t$ -элементов ( $t^*$ -элементов),  $m_t + m_{t^*} = n$ ,  $t \in \{0, 1\}$ , имеем:

- при условии  $E_1$  вектор  $\bar{v}$  состоит из  $m_t - k_1$   $t$ -серий;
- среди  $m_t - k_1 - 1$  промежутков, образованных этими  $t$ -сериями,  $k_3$  позиций заняты (при условии  $E_3$ ) в точности одним  $t^*$ -элементом;
- число  $\delta_t$   $t$ -серий длины единица в векторе  $\bar{v}$  (при условиях  $E_1$  и  $E_2$ ) составляет

$$\delta_t = k_2 + m_t - 2k_1. \quad (10)$$

Данный вектор  $\bar{v}$  определяется однозначно (при условиях  $E_1, E_2, E_3$ ), если зафиксировать:

- одно из  $R_{1,t} (R_{1,t^*})$  всех возможных попарно различных размещений  $t$ -серий ( $t^*$ -серий) длины единица на  $m_t - k_1$  ( $m_t - k_1 - 1$ ) позициях;
- одно из  $R_{2,t} (R_{2,t^*})$  всех возможных разбиений оставшихся  $m_t - \delta_t$   $t$ -элементов ( $m_{t^*} - k_3$   $t^*$ -элементов) на  $t$ -серии ( $t^*$ -серии) подходящей длины.

С учетом (10) получаем

$$R_{1,t} = C_{m_t-k_1}^{k_1-k_2}. \quad (11)$$

В свою очередь,

$$R_{1,t^*} = C_{m_t-k_1-1}^{k_3}. \quad (12)$$

Число  $R_{2,t}$ , равное количеству всех возможных разбиений  $m_t - \delta_t$   $t$ -элементов на  $t$ -серии, длина каждой из которых не менее двух, удовлетворяет (при условии  $k_1 > k_2$ ) соотношению

$$R_{2,t} = C_{k_1-1}^{k_2} \chi(k_1 > k_2). \quad (13)$$

Число  $R_{2,t^*}$ , равное количеству всех возможных разбиений  $m_{t^*} - k_3$   $t^*$ -элементов на  $t^*$ -серии таких, что длина каждой  $t^*$ -серии, расположенной на любой из всех возможных позиций  $m_t - k_1 - k_3 - 1$ , не менее двух, а остальные  $t^*$ -серии имеют произвольную допустимую длину при условии  $m_t - k_1 - k_3 - 1 \geq 2$ , определяется выражением

$$R_{2,t^*} = C_{m_{t^*}-m_t+k_1+2}^{m_t-k_1-k_3} \chi(m_t - k_1 - k_2 \geq 2). \quad (14)$$

Заметим, что равенству  $m_t - k_1 - k_3 = 1$  соответствует ситуация, при которой между произвольными двумя соседними  $t$ -сериями находится в точности один  $t^*$ -элемент, а первая и последняя  $t^*$ -серии вектора  $\vec{v}$  содержат в сумме  $m_{t^*} - k_3$   $t^*$ -элементов. Число вариантов, для которых эта сумма может реализоваться, составляет

$$m_{t^*} - k_3 + 1 = C_{m_{t^*} + k_1 - m_t + 2}^{m_t - k_1 - k_3} \chi(m_t - k_1 - k_3 = 1). \quad (15)$$

Из сказанного следует, что для  $k_1 > k_2$  имеем  $Q = R_{1,t} R_{2,t} R_{1,t^*} R_{2,t^*}$ , откуда с учетом (11)–(15) получаем

$$Q = C_{m_t - k_1}^{k_1 - k_2} C_{k_1 - 1}^{k_2} C_{m_t - k_1 - 1}^{k_3} C_{m_{t^*} - m_t + k_1 + 2}^{m_t - k_1 - k_3} \chi(k_1 > k_2). \quad (16)$$

В принятых обозначениях вероятность  $P\{E_1, E_2, E_3 / \nu = m_1\}$  совместного осуществления событий  $E_1, E_2, E_3$  при условии, что  $\nu = m_1$ , имеет вид

$$P\{E_1, E_2, E_3 / \nu = m_1\} = (|\Omega(n, m_1)|)^{-1} Q. \quad (17)$$

Используя (16), (17) и равенство

$$|\Omega(n, m_1)| = C_n^{m_1}, \quad (18)$$

получаем (9).

Соотношение  $k_1 = k_2$  возможно (при условиях  $E_1$  и  $E_2$ ) тогда и только тогда, когда  $k_1 = k_2 = 0$  и, таким образом, все  $t$ -серии в векторе  $\vec{v}$  имеют длину единица (при условии  $m_t \geq 1$ ). В этом случае положим

$$R_{1,t} = R_{2,t} = \chi(k_1 = k_2 = 0), \quad (19)$$

а для  $R_{1,t^*}$  и  $R_{2,t^*}$  находим

$$R_{1,t^*} = C_{m_t - 1}^{k_3}, \quad (20)$$

$$R_{2,t^*} = C_{m_{t^*} - m_t + 2}^{m_t - k_3}. \quad (21)$$

Следовательно, если  $k_1 = k_2$  и  $m_t \geq 1$ , то в силу (19)–(21) имеем число  $Q$ :

$$Q = C_{m_t - 1}^{k_3} C_{m_{t^*} - m_t + 2}^{m_t - k_3} \chi(k_1 = k_2 = 0, m_t \geq 1). \quad (22)$$

С учетом (17), (18) и (22) получаем соотношение

$$P\{E_1, E_2, E_3 / \nu = m_1\} = (C_n^{m_1})^{-1} C_{m_t - 1}^{k_3} C_{m_{t^*} - m_t + 2}^{m_t - k_3} \times \\ \times \chi(k_1 = k_2 = k_3 = m_t = 0). \quad (23)$$

Если  $k_1 = k_2 = m_t = 0$ , то для положительных значений параметра  $k_3, k_3 > 0$ , число  $Q = 0$ , а для  $k_3 = 0$  имеем соотношение  $Q = \chi(k_1 = k_2 = k_3 = m_t = 0)$ , поэтому

$$P\{E_1, E_2, E_3 / \nu = m_1\} = (C_n^{m_1})^{-1} \chi(k_1 = k_2 = k_3 = m_t = 0). \quad (24)$$

Формулы (7)–(9), (17) и (24) доказывают равенство (3).

Теорема доказана.

Аналогично доказательству (3) проверяются формулы (4)–(6).

**ПРИМЕРЫ К ТЕОРЕМЕ 1**

В примерах рассмотрен случай для  $p = q = 1/2$  и малой выборки  $n$ ,  $n = 32$ .

**Пример использования равенства (6).** В табл. 1 приведены соотношения из (6) для  $n = 32$  и некоторых значений  $k_1$  и  $k_2$ . В первом и втором столбцах помещены все возможные варианты значений  $k_1$  и  $k_2$ , для которых имеем вероятность  $P \{ \eta(tt) = k_1, \eta(ttt) + \eta(tt^*t) = k_2 \} \geq 0.02$ . В третьем столбце даны вероятности (в неубывающем порядке)  $P \{ \eta(tt) = k_1, \eta(ttt) + \eta(tt^*t) = k_2 \}$  для пар чисел  $(k_1, k_2)$ , указанных в первом и втором столбцах соответственно. В четвертом столбце дана сумма накопленных вероятностей  $P_c$  до реализации события  $\{ \eta(tt) = k_1, \eta(ttt) + \eta(tt^*t) = k_2 \}$ .

**Таблица 1.** Значения вероятности осуществления события для чисел  $k$  с использованием равенства (6)

$k_1$	$k_2$	$P$	$P_c$
7	8	0.02005	0.721063
9	7	0.02006	0.741119
6	7	0.02043	0.761554
5	5	0.02081	0.782367
9	9	0.02095	0.803314
8	6	0.02107	0.824389
6	5	0.02348	0.847872
9	8	0.02377	0.87164
8	8	0.02453	0.896168
6	6	0.02491	0.921081
7	7	0.02612	0.947201
8	7	0.02637	0.973573
7	6	0.02643	1

На рис. 1 представлена пузырьковая диаграмма реализации соотношения (6) для  $n = 32$ . Здесь первый параметр (горизонтальная ось) представляет возможные значения  $k_1$ , второй параметр (вертикальная ось) представляет возможные значения  $k_2$ , третий параметр (размер пузырька) представляет определенную вероятность осуществления события  $\{ \eta(tt) = k_1, \eta(ttt) + \eta(tt^*t) = k_2 \}$ , выраженную в процентах. Например, при  $k_1 = 6$  и  $k_2 = 6$  вероятность осуществления события  $\{ \eta(tt) = k_1, \eta(ttt) + \eta(tt^*t) = k_2 \}$  составляет 2.49 %.

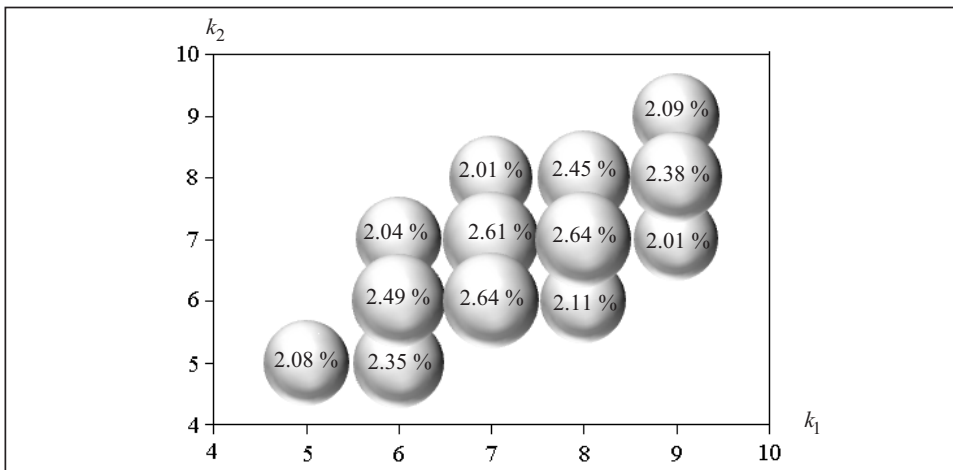


Рис. 1

**Пример использования равенства (4).** В табл. 2 приведены соотношения из (4) для  $n = 32$  и некоторых значений  $k_1$  и  $k_2$ . В первом и втором столбцах помещены все возможные варианты значений  $k_1$  и  $k_2$ , для которых вероятность  $P \{ \eta(tt) = k_1, \eta(ttt) = k_2 \} \geq 0.03$ . В третьем столбце даны значения вероятности (в неубывающем порядке)  $P \{ \eta(tt) = k_1, \eta(ttt) = k_2 \}$  для пар чисел  $(k_1, k_2)$ , указанных в первом и втором столбцах соответственно. В четвертом столбце пред-

ставлена сумма накопленных вероятностей  $P_c$  до реализации события  $\{\eta(tt) = k_1, \eta(ttt) = k_2\}$ .

На рис. 2 представлена пузырьковая диаграмма реализации соотношения (4) для  $n = 32$ . Здесь первый параметр (горизонтальная ось) представляет возможные значения  $k_1$ , второй параметр (вертикальная ось) представляет возможные значения  $k_2$ , третий параметр (размер пузырька) представляет определенную вероятность осуществления события  $P\{\eta(tt) = k_1, \eta(ttt) = k_2\}$ , выраженную в процентах. Например, при  $k_1 = 7$  и  $k_2 = 3$  вероятность осуществления события  $P\{\eta(tt) = k_1, \eta(ttt) = k_2\}$  составляет 5.01%.

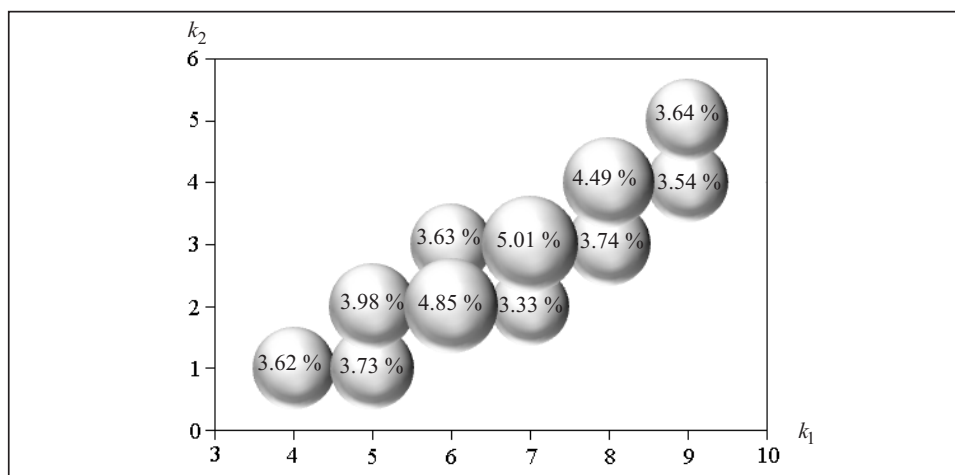


Рис. 2

**Пример использования равенства (5).** В табл. 3 приведены соотношения из (5) для  $n = 32$  и некоторых значений  $k_1$  и  $k_2$ . В первом и втором столбцах помещены все возможные варианты значений  $k_1$  и  $k_2$ , для которых имеем вероятность  $P\{\eta(tt) = k_1, \eta(tt^*t) = k_2\} \geq 0.02$ . В третьем столбце даны значения вероятности (в неубывающем порядке)  $P\{\eta(tt) = k_1, \eta(tt^*t) = k_2\}$  для пар чисел  $(k_1, k_2)$ , указанных в первом и втором столбцах. В четвертом столбце помещена сумма накопленных вероятностей  $P_c$  до реализации события  $\{\eta(tt) = k_1, \eta(tt^*t) = k_2\}$ .

**Таблица 2.** Значения вероятности осуществления события для чисел  $k$  с использованием равенства (4)

$k_1$	$k_2$	$P$	$P_c$
7	2	0.033341	0.597797
9	4	0.035397	0.633194
4	1	0.036205	0.669399
6	3	0.036262	0.705662
9	5	0.036379	0.74204
5	1	0.037323	0.779364
8	3	0.03736	0.816724
5	2	0.039788	0.856512
8	4	0.044858	0.90137
6	2	0.048534	0.949904
7	3	0.050096	1

**Таблица 3.** Значения вероятности осуществления события для чисел  $k$  с использованием равенства (23)

$k_1$	$k_2$	$P$	$P_c$
8	5	0.020082	0.737322
5	4	0.02016	0.757482
7	5	0.020578	0.778061
5	3	0.020824	0.798885
9	3	0.02306	0.821945
9	4	0.023135	0.84508
6	4	0.024607	0.869687
6	3	0.02502	0.894708
8	4	0.025917	0.920625
8	3	0.025982	0.946607
7	4	0.026605	0.973213
7	3	0.026787	1

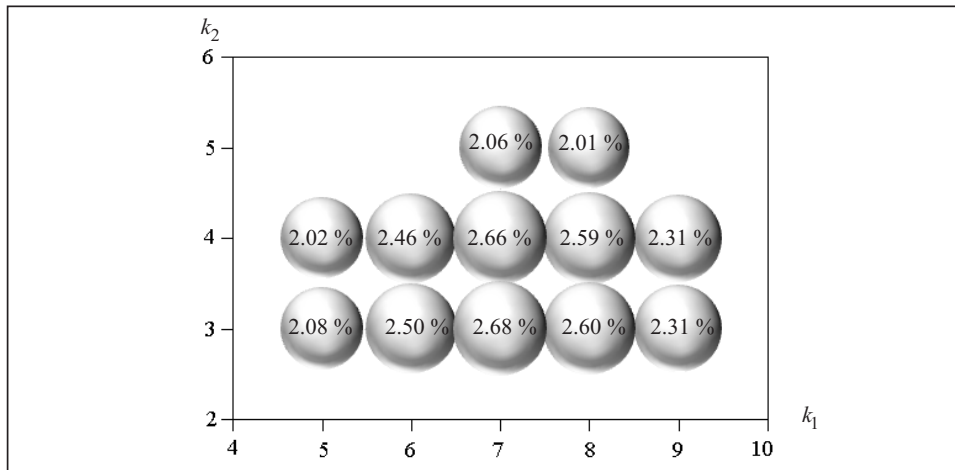


Рис. 3

На рис. 3 представлена пузырьковая диаграмма реализации соотношения (5) для  $n = 32$ . Здесь первый параметр (горизонтальная ось) представляет возможные значения  $k_1$ , второй параметр (вертикальная ось) представляет возможные значения  $k_2$ , третий параметр (размер пузырька) представляет определенную вероятность осуществления события  $P \{ \eta(tt) = k_1, \eta(tt^*t) = k_2 \}$ , выраженную в процентах. Например, при  $k_1 = 7$  и  $k_2 = 4$  вероятность осуществления события  $P \{ \eta(tt) = k_1, \eta(tt^*t) = k_2 \}$  составляет 2.66%.

**Пример использования равенства (3).** В табл. 4 приведены соотношения из (3) для  $n = 32$  и некоторых значений  $k_1, k_2$  и  $k_3$ . В первом, втором и третьем столбцах даны все возможные варианты значений  $k_1, k_2$  и  $k_3$ , для которых вероятность  $P \{ \eta(tt) = k_1, \eta(ttt) = k_2, \eta(tt^*t) = k_3 \} \geq 0.01$ . В четвертом столбце даны значения вероятности (в неубывающем порядке)  $P \{ \eta(tt) = k_1, \eta(ttt) = k_2, \eta(tt^*t) = k_3 \}$  для чисел  $(k_1, k_2, k_3)$ , указанных в первом, втором и третьем столбцах соответственно. В пятом столбце помещена сумма накопленных вероятностей  $P_c$  до реализации события  $\{ \eta(tt) = k_1, \eta(ttt) = k_2, \eta(tt^*t) = k_3 \}$ .

**Таблица 4.** Значения вероятности осуществления события для чисел  $k$  с использованием равенства (3)

$k_1$	$k_2$	$k_3$	$P$	$P_c$
6	2	3	0.010131	0.968497
6	2	4	0.01019	0.978687
7	3	4	0.010539	0.989226
7	3	3	0.010774	1

#### ЗАКЛЮЧЕНИЕ

Изучаются совместные распределения числа 2-цепочек и числа 3-цепочек фиксированного вида в конечной битовой последовательности, состоящей из независимых одинаково распределенных случайных величин. В соотношениях (3)–(6) рассматриваются цепочки вида  $tt, ttt, tt^*t$ , для которых устанавливаются явные выражения функций распределений таких событий:  $\{ \eta(tt) = k_1, \eta(ttt) = k_2, \eta(tt^*t) = k_3 \}$ ,  $\{ \eta(tt) = k_1, \eta(ttt) = k_2 \}$ ,  $\{ \eta(tt) = k_1, \eta(tt^*t) = k_2 \}$ ,  $\{ \eta(tt) = k_1, \eta(ttt) + \eta(tt^*t) = k_2 \}$ , где  $\eta(t_1, t_2, \dots, t_s)$  — число  $s$ -цепочек вида  $t_1$ ,

$t_2, \dots, t_s$  в исходной  $n$ -мерной  $(0, 1)$ -последовательности;  $t^* = 1 - t$ ;  $k_1, k_2, k_3$  — подходящие целые неотрицательные числа. Доказательства формул для функций распределений указанных событий построены на подсчете числа соответствующих благоприятных событий при условии, что  $(0, 1)$ -последовательность содержит фиксированное количество нулей и единиц. В качестве примеров использования явных выражений функций распределений приведены таблицы, в которых помещены значения вероятностей перечисленных выше событий для  $(0, 1)$ -последовательности длины  $n$ ,  $n = 32$ , и некоторых значений параметров  $k_1, k_2$  и  $k_3$  при ограничении, что нули и единицы появляются равновероятно. Установленные формулы могут представлять интерес для задач тестирования локальных участков, формирующихся на выходе генераторов псевдослучайных чисел, а также в иных сферах, где возникает необходимость в анализе битовых последовательностей.

#### СПИСОК ЛИТЕРАТУРЫ

1. Задірака В.К., Сергієнко І.В., Коваленко І.М., Андон П.І. Комп'ютерна стеганографія. В кн.: Алексєєв В.А., Алішов Н.І., Андон П.І., Анісімов А.В., Баран Л.Б., Белов В.М., Боюн В.П., Булавацький В.М., Бунін С.Г., Валах В.Я. *Стан та перспективи розвитку інформатики в Україні*. Київ: Наук. думка, 2010. С. 736–747.
2. Masol V.I., Popereshnyak S.V. Checking the randomness of bits disposition in local segments of the  $(0, 1)$ -sequence. *Cybernetics and Systems Analysis*. 2020. Vol. 56, N 3. P. 513–520. <https://doi.org/10.1007/s10559-020-00267-0>.

Надійшла до редакції 06.08.2020

#### **В.І. Масол, С.В. Поперешняк**

##### **СУМІСНИЙ РОЗПОДІЛ ДЕЯКИХ СТАТИСТИК ВИПАДКОВОЇ БІТОВОЇ ПОСЛІДОВНОСТІ**

**Анотація.** Для скінченної послідовності, що складається з незалежних однаково розподілених випадкових величин, які набувають значень нуль або одиниця, визначено двовимірні та тривимірні розподіли деяких спеціальних статистик, що характеризують розташування її елементів. Наведено таблиці, які ілюструють застосування зазначених розподілів для послідовності довжини 32 у припущенні, що її елементи набувають значень нуль або одиниця з однаковими ймовірностями.

**Ключові слова:** багатовимірна статистика, випадкова послідовність,  $s$ -ланцюжки, стеганографія, статистичне тестування.

#### **V. Masol, S. Popereshnyak**

##### **JOINT DISTRIBUTION OF SOME STATISTICS OF RANDOM BIT SEQUENCES**

**Abstract.** For a finite sequence consisting of independent equally distributed random variables, taking the value zero or one, two-dimensional and three-dimensional distributions of some special statistics characterizing the location of its elements are obtained. The tables that illustrate the application of these distributions to a sequence of length 32 whose elements are assumed to take values of zero or one with equal probabilities are presented.

**Keywords:** multidimensional statistic, random sequence,  $s$ -chains, steganography, statistical testing.

#### **Масол Владимир Иванович,**

доктор физ.-мат. наук, профессор Киевского национального университета имени Тараса Шевченко, e-mail: vimasol@ukr.net.

#### **Поперешняк Светлана Владимировна,**

кандидат физ.-мат. наук, доцент Киевского национального университета имени Тараса Шевченко, e-mail: spopereshnyak@gmail.com.