

УДК 621.391 : 519.72

© 2025 г. М.В. Бурнашев

**О ФУНКЦИИ КОНЦЕНТРАЦИИ ОДНОЙ СУММЫ СЛУЧАЙНЫХ ВЕЛИЧИН, СВЯЗАННЫХ С ДВОИЧНЫМ СИММЕТРИЧНЫМ КАНАЛОМ<sup>1</sup>**

Рассматривается сумма независимых одинаково распределенных случайных величин специального вида. С помощью такой суммы описываются текущие апостериорные вероятности сообщений для случайно выбранного кода в двоичном симметричном канале. Исследуется функция концентрации этой суммы.

*Ключевые слова:* сумма независимых случайных величин, функция концентрации, двоичный симметричный канал

**DOI:** 10.31857/S0555292325010012, **EDN:** LJWPAV

**§ 1. Основные результаты**

Рассмотрим независимые одинаково распределенные двоичные  $n$ -векторы  $\mathbf{x}_j$ ,  $j = 1, \dots, M$ . При этом каждая координата каждого  $n$ -вектора  $\mathbf{x}_j$  выбирается независимо и равна нулю или единице с вероятностью  $1/2$ . Обозначим через  $w_j = w(\mathbf{x}_j)$ ,  $j = 1, \dots, M$ , вес (т.е. число единиц) двоичного  $n$ -вектора  $\mathbf{x}_j$ . Для  $z > 0$  рассмотрим случайную сумму

$$S(z, M, n) = \sum_{j=1}^M z^{w_j(n)}, \quad z > 0. \quad (1)$$

Ясно, что  $Mz^n \leq S(z, M, n) \leq M$  при  $0 \leq z \leq 1$  и  $M \leq S(z, M, n) \leq Mz^n$  при  $z \geq 1$ .

Суммы типа  $S(z, M, n)$  из (1) возникают в теории информации при исследовании оптимальных характеристик двоичного симметричного канала  $BSC(p)$  с переходной вероятностью  $0 < p < 1/2$  (см. [1]), а также в некоторых задачах теории поиска и планирования экспериментов [2]. В этом случае  $z = p/(1-p) < 1$ . Насколько известно автору, функции распределения (концентрации) случайных сумм  $S(z, M, n)$  ранее не исследовались [3]. Однако эти функции распределения важны при исследовании канала  $BSC(p)$  с обратной связью, так как они позволяют улучшить наилучшие известные результаты для такого канала. В частности, такие результаты были бы полезны в работах [4–6]. При этом желательно, чтобы подобные описания функций распределения случайных величин  $S(z, M, n)$  были с аккуратным исследованием скорости сходимости и равномерности по  $z, M, n$ . Удобнее всего для этого неасимптотические по  $z, M, n$  оценки, чему и посвящена данная статья.

Хотя далее все результаты в статье являются неасимптотическими по  $n, M$ , они в основном ориентированы на случай  $n \rightarrow \infty$  и  $M = e^{Rn}$ ,  $R > 0$ .

Основные результаты статьи представляют теоремы 1 и 2 для случаев  $z \leq 1$  и  $z \geq 1$  соответственно.

<sup>1</sup> Работа выполнена при финансовой поддержке Министерства образования и науки РФ, проект MG-2024-0048.

Теорема 1. Для  $0 < z < 1$  и  $A = z^{bn}$  справедливы следующие границы:

1) Если  $0 \leq b \leq 1/2$ , то

$$\frac{1}{Mn} \ln \mathbf{P}\{S(z, M, n) \geq Mz^{bn}\} = h(b) - \ln 2 + r_1(b, n), \quad (2)$$

где

$$-\frac{\ln(n+1)}{n} - \frac{1}{n} \ln \frac{1-b}{b} - \frac{1}{2n^2b(1-b)} \leq r_1(b, n) \leq \frac{\ln(n+1)}{n}, \quad (3)$$

$$h(x) = -x \ln x - (1-x) \ln(1-x), \quad 0 \leq x \leq 1.$$

2) Если  $1/2 \leq b \leq 1$ , то

$$\frac{1}{Mn} \ln \mathbf{P}\{S(z, M, n) \leq Mz^{bn}\} = \ln 2 - h(b) + r_2(b, n), \quad (4)$$

где

$$-\frac{\ln(n+1)}{n} - \frac{1}{n} \ln \frac{1-b}{b} - \frac{1}{2n^2b(1-b)} \leq r_2(b, n) \leq \frac{\ln(n+1)}{n}. \quad (5)$$

Теорема 2. Для  $z \geq 1$  и  $A = z^{bn}$  справедливы следующие границы:

1) Если  $0 \leq b \leq 1/2$ , то

$$\frac{1}{Mn} \ln \mathbf{P}\{S(z, M, n) \leq Mz^{bn}\} = \ln 2 - h(b) + r_2(1-b, n). \quad (6)$$

2) Если  $1/2 \leq b \leq 1$ , то

$$\frac{1}{Mn} \ln \mathbf{P}\{S(z, M, n) \geq Mz^{bn}\} = h(b) - \ln 2 + r_1(1-b, n). \quad (7)$$

В частности, из (2)–(7) вытекает

Следствие 1. Для любого  $z > 0$  и  $n \geq 10$  справедливо неравенство

$$\mathbf{P}\left\{\left|\ln \frac{S(z, M, n)}{Mz^{n/2}}\right| \geq \sqrt{n \ln(n+1)} |\ln z|\right\} \leq 2(n+1)^{-M}. \quad (8)$$

*Замечание.* Из (8) следует, что если  $M = e^{Rn+o(n)}$  при  $n \rightarrow \infty$ ,  $R > 0$ , то тогда с очень большой вероятностью

$$S(z, M, n) = Mz^{n/2+o(n)}$$

при  $n \rightarrow \infty$  для любого  $z > 0$ .

Далее приводится доказательство теоремы 1. Доказательства теоремы 2 и следствия 1 содержатся в [7].

## § 2. Доказательство теоремы 1

Заметим, что

$$\mathbf{E} e^{\lambda S(z, M, n)} = (\mathbf{E} e^{\lambda z^{w_1(n)}})^M, \quad \mathbf{E} e^{\lambda z^{w_1(n)}} = 2^{-n} \sum_{\ell=0}^n \binom{n}{\ell} e^{\lambda z^\ell}. \quad (9)$$

Далее для биномиальных коэффициентов  $\binom{n}{k}$  используются известные нижние и верхние оценки [8, формула (12.40)]

$$\frac{1}{(n+1)} e^{nh(k/n)} \leq \binom{n}{k} \leq e^{nh(k/n)}, \quad 0 \leq k \leq n, \quad (10)$$

$$h(x) = -x \ln x - (1-x) \ln(1-x).$$

Для удобства обозначим

$$D_1(z, b, n) = \mathbf{P}\{S(z, M, n) \geq Mz^{bn}\}, \quad D_2(z, b, n) = \mathbf{P}\{S(z, M, n) \leq Mz^{bn}\}. \quad (11)$$

Далее, оценивая сверху и снизу вероятности  $D_1(z, b, n)$  и  $D_2(z, b, n)$ , мы получим формулы (2), (3) и формулы (4), (5).

1. Формулы (2), (3). Используя экспоненциальное неравенство Чебышева

$$\mathbf{P}\{S > a\} \leq \inf_{\lambda > 0} \{e^{-\lambda a} \mathbf{E} e^{\lambda S}\} \quad (12)$$

и формулы (9), имеем для любого  $A \geq 0$

$$\begin{aligned} \mathbf{P}\{S(z, M, n) \geq MA\} &\leq \min_{\lambda \geq 0} \{e^{-\lambda MA} \mathbf{E} e^{\lambda S(z, M, n)}\} = \\ &= 2^{-Mn} \min_{\lambda \geq 0} \left\{ e^{-\lambda MA} \left[ \sum_{\ell=0}^n \binom{n}{\ell} e^{\lambda z^\ell} \right]^M \right\}, \end{aligned} \quad (13)$$

откуда в силу (10) при  $\ell = an$ ,  $0 \leq a \leq 1$ , получаем

$$\begin{aligned} \frac{1}{M} \ln D_1(z, b, n) &\leq -n \ln 2 + \min_{\lambda \geq 0} \left\{ -\lambda A + \ln \left[ \sum_{\ell=0}^n \binom{n}{\ell} e^{\lambda z^\ell} \right] \right\} \leq \\ &\leq -n \ln 2 + \ln(n+1) + \min_{\lambda \geq 0} \max_{0 \leq \ell \leq n} \left\{ -\lambda A + \ln \left[ \binom{n}{\ell} e^{\lambda z^\ell} \right] \right\} \leq \\ &\leq -n \ln 2 + \ln(n+1) + \min_{\lambda \geq 0} \max_{0 \leq a \leq 1} f(\lambda, a, z), \end{aligned} \quad (14)$$

где

$$f(\lambda, a, z) = -\lambda A + nh(a) + \lambda z^{an}. \quad (15)$$

Решение  $(\lambda_0, a_0)$  минимаксной задачи в правой части (14) является седловой точкой функции  $f(\lambda, a, z)$  из (15) [9], т.е. определяется условиями

$$\begin{aligned} f'_\lambda(\lambda_0, a_0, z) &= z^{a_0 n} - A = 0, \\ f'_a(\lambda_0, a_0, z) &= n \left( \ln \frac{1-a_0}{a_0} + \lambda_0 z^{a_0 n} \ln z \right) = 0, \end{aligned} \quad (16)$$

или, что равносильно,

$$\begin{aligned} z^{a_0 n} &= A, \\ \ln \frac{1-a_0}{a_0} + \lambda_0 A \ln z &= 0. \end{aligned} \quad (17)$$

При  $A = z^{bn}$ , где  $0 \leq b \leq 1/2$ , система (17) имеет единственное решение  $(\lambda_0, a_0)$  (т.е. функция  $f(\lambda, a, z)$  имеет единственную седловую точку)

$$a_0 = b, \quad \lambda_0 = \frac{\ln[b/(1-b)]}{z^{bn} \ln z} \geq 0, \quad (18)$$

что дает

$$\min_{\lambda \geq 0} \max_{0 \leq a \leq 1} f(\lambda, a, z) = f(\lambda_0, a_0, z) = nh(b). \quad (19)$$

Из (14) и (18), (19) следуют формула (2) и оценка сверху (3).

Для того чтобы получить оценку снизу (3), рассмотрим случай, когда все двоичные  $n$ -векторы  $\{\mathbf{x}_j\}$  в сумме (1) имеют целый вес  $\ell_0$ , такой что  $z^{\ell_0} \geq A$ , т.е.  $\ell_0 \leq bn$ . Тогда в силу (10) для любого  $A = z^{bn} \geq z^n$  имеем

$$\frac{1}{Mn} \ln D_1(z, b, n) \geq \frac{1}{Mn} \ln \left[ 2^{-n} \binom{n}{\ell_0} \right]^M \geq h\left(\frac{\ell_0}{n}\right) - \ln 2 - \frac{\ln(n+1)}{n}. \quad (20)$$

Выбирая максимально возможное целое  $\ell_0$ , имеем

$$\ell_0 \geq bn - 1. \quad (21)$$

Поэтому из (20) и (21) получаем

$$\begin{aligned} \frac{1}{Mn} \ln D_1(z, b, n) &\geq h\left(b - \frac{1}{n}\right) - \ln 2 - \frac{\ln(n+1)}{n} \geq \\ &\geq h(b) - \ln 2 - \frac{\ln(n+1)}{n} - \frac{1}{n} \ln \frac{1-b}{b} - \frac{1}{2n^2b(1-b)}, \end{aligned} \quad (22)$$

где использовался следующий вариант формулы Тейлора (так как  $h^{(3)}(b) \geq 0$ ):

$$h(b - \varepsilon) \geq h(b) - \varepsilon \ln \frac{1-b}{b} - \frac{\varepsilon^2}{2b(1-b)}, \quad 0 < b \leq 1/2, \quad 0 \leq \varepsilon \leq b.$$

Из (22) следует левая часть формулы (3).

**2. Формулы (4), (5).** Формулы (4), (5) доказываются вполне аналогично формулам (2), (3). Используя другой вариант экспоненциального неравенства Чебышева и формулы, аналогичные (12) и (14), для любых  $A \geq 0$ ,  $\lambda \geq 0$  имеем

$$\begin{aligned} \mathbf{P}\{S(z, M, n) \leq MA\} &= \mathbf{P}\{e^{-\lambda S(z, M, n)} \geq e^{-\lambda MA}\} \leq \\ &\leq \min_{\lambda \geq 0} \{e^{\lambda MA} \mathbf{E} e^{-\lambda S(z, M, n)}\} = 2^{-Mn} \min_{\lambda \geq 0} \left\{ e^{\lambda MA} \left[ \sum_{\ell=0}^n \binom{n}{\ell} e^{-\lambda z^\ell} \right]^M \right\}. \end{aligned} \quad (23)$$

Тогда из (23) при  $\ell = an$ ,  $0 \leq a \leq 1$ , аналогично (14) получаем

$$\begin{aligned} \frac{1}{M} \ln D_2(z, b, n) &\leq -n \ln 2 + \min_{\lambda \geq 0} \left\{ \lambda A + \ln \left[ \sum_{\ell=0}^n \binom{n}{\ell} e^{-\lambda z^\ell} \right] \right\} \leq \\ &\leq -n \ln 2 + \ln(n+1) + \min_{\lambda \geq 0} \max_{0 \leq \ell \leq n} \left\{ \lambda A + \ln \left[ \binom{n}{\ell} e^{-\lambda z^\ell} \right] \right\} \leq \\ &\leq -n \ln 2 + \ln(n+1) + \min_{\lambda \geq 0} \max_{0 \leq a \leq 1} g(\lambda, a, z), \end{aligned} \quad (24)$$

где было обозначено

$$g(\lambda, a, z) = \lambda A + nh(a) - \lambda z^{an}. \quad (25)$$

Решение  $(\lambda_0, a_0)$  минимаксной задачи в правой части (24) является седловой точкой функции  $g(\lambda, a, z)$  из (25), т.е. определяется условиями

$$\begin{aligned} g'_\lambda(\lambda_0, a_0, z) &= z^{a_0 n} - A = 0, \\ g'_a(\lambda_0, a_0, z) &= n \left( \ln \frac{1 - a_0}{a_0} - \lambda_0 z^{a_0 n} \ln z \right) = 0, \end{aligned} \quad (26)$$

или, что равносильно,

$$\begin{aligned} z^{a_0 n} &= A, \\ \ln \frac{1 - a_0}{a_0} - \lambda_0 A \ln z &= 0. \end{aligned} \quad (27)$$

При  $A = z^{bn}$ , где  $1/2 \leq b \leq 1$ , система (27) имеет единственное решение  $(\lambda_0, a_0)$  (т.е. функция  $g(\lambda, a, z)$  имеет единственную седловую точку)

$$a_0 = b, \quad \lambda_0 = \frac{\ln[b/(1-b)]}{z^{bn} \ln z} \geq 0, \quad (28)$$

что дает

$$\min_{\lambda \geq 0} \max_{0 \leq a \leq 1} g(\lambda, a, z) = g(\lambda_0, a_0, z) = nh(b). \quad (29)$$

Тогда из (24) и (19) для  $A = z^{bn}$ , где  $1/2 \leq b \leq 1$ , получаем

$$\frac{1}{Mn} \ln \mathbf{P}\{S(z, M, n) \leq MA\} \leq h(b) - \ln 2 + \frac{\ln(n+1)}{n}. \quad (30)$$

Из (30) следует правая часть (3).

Из (24) и (29), (30) следуют формула (4) и оценка сверху (5).

Для того чтобы получить оценку снизу (5), рассмотрим случай, когда все двоичные  $n$ -векторы  $\{\mathbf{x}_j\}$  в сумме (1) имеют целый вес  $\ell_0$ , такой что  $z^{\ell_0} \leq A = z^{bn}$ ,  $1/2 \leq b \leq 1$ , т.е.  $\ell_0 \geq bn \geq n/2$ . Тогда в силу (10) для любого  $A = z^{bn} \geq z^n$ , т.е.  $b \leq 1$ , имеем

$$\frac{1}{Mn} \ln D_2(z, b, n) \geq \frac{1}{Mn} \ln \left[ 2^{-n} \binom{n}{\ell_0} \right]^M \geq h\left(\frac{\ell_0}{n}\right) - \ln 2 - \frac{\ln(n+1)}{n}. \quad (31)$$

Выбирая максимально возможное целое  $\ell_0$ , имеем

$$\ell_0 \geq bn - 1. \quad (32)$$

Поэтому из (31) и (32) аналогично (22) получаем

$$\begin{aligned} \frac{1}{Mn} \ln D_2(z, b, n) &\geq h\left(b - \frac{1}{n}\right) - \ln 2 - \frac{\ln(n+1)}{n} \geq \\ &\geq h(b) - \ln 2 - \frac{\ln(n+1)}{n} - \frac{1}{n} \ln \frac{1-b}{b} - \frac{1}{2n^2 b(1-b)}, \end{aligned} \quad (33)$$

что завершает доказательство оценки снизу (5) и теоремы 1.

## СПИСОК ЛИТЕРАТУРЫ

1. Галлагер Р. Теория информации и надежная связь. М.: Сов. радио, 1974.
2. Альсведе Р., Вегенер И. Задачи поиска. М.: Мир, 1982.
3. Петров В.В. Суммы независимых случайных величин. М.: Наука, 1972.
4. Verlekamp E.R. Block Coding with Noiseless Feedback. PhD Thesis. MIT, Cambridge, USA, 1964. Available at <http://hdl.handle.net/1721.1/14783>.
5. Зигангиров К.Ш. Верхние оценки вероятности ошибки для каналов с обратной связью // Пробл. передачи информ. 1970. Т. 6. № 2. С. 87–92. <http://www.mathnet.ru/ppi1740>
6. Бурнашев М.В. О функции надежности двоичного симметричного канала с обратной связью // Пробл. передачи информ. 1988. Т. 24. № 1. С. 3–10. <http://www.mathnet.ru/ppi681>
7. Бурнашев М.В. On the Distribution of a Statistical Sum Related to the Binary Symmetric Channel // Probl. Inf. Transm. 2025. V. 61. № 1. P. 1–7. <https://doi.org/10.1134/S0032946025010016>
8. Cover T.M., Thomas J.A. Elements of Information Theory. New York: Wiley, 1991.
9. Демьянов В.Ф., Малоземов В.Н. Введение в минимакс. М.: Наука, 1972.

*Бурнашев Марат Валиевич*

Высшая школа современной математики МФТИ, Москва  
[marat.burnashev@mail.ru](mailto:marat.burnashev@mail.ru)

Поступила в редакцию

09.09.2024

После доработки

04.01.2025

Принята к публикации

14.01.2025

---

---

## ON THE CONCENTRATION FUNCTION FOR A SUM OF RANDOM VARIABLES RELATED TO THE BINARY SYMMETRIC CHANNEL

© 2025 M.V. Burnashev

Higher School of Modern Mathematics, MIPT, Moscow  
[marat.burnashev@mail.ru](mailto:marat.burnashev@mail.ru)

A sum of independent identically distributed random variables of a special form is considered. Using this sum, current posterior probabilities of messages for a randomly chosen code in a binary symmetric channel are described. The concentration function of this sum is studied.

*Keywords:* sum of independent random variables, concentration function, binary symmetric channel

**DOI:** 10.31857/S0555292325010012, **EDN:** LJWPAV

Received 09.09.2024

Revised 04.01.2025

Accepted 14.01.2025