М. В. Бурнашев

О РАСПРЕДЕЛЕНИИ ОДНОЙ СТАТИСТИЧЕСКОЙ СУММЫ, СВЯЗАННОЙ С ДВОИЧНЫМ СИММЕТРИЧНЫМ КАНАЛОМ [1]

Исследуется функция распределения суммы независимых, одинаково распределенных случайных величин специального вида. С помощью этой суммы описываются текущие апостериорные вероятности сообщений для случайно выбранного кода в двоичном симметричном канале. Такие апостериорные вероятности полезны при исследовании каналов с обратной связью. Получены близкие между собой неасимптотические оценки снизу и сверху для этой функции распределения.

Ключевые слова: статистическая сумма, двоичный симметричный канал.

§ 1. Введение и основные результаты

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

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

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

Суммы типа $S(z, M, n)$ из (1) возникают в теории информации при исследовании оптимальных характеристик двоичного симметричного канала BSC(p) с переходной вероятностью $0 < p < 1/2$ [1], а также в некоторых задачах теории поиска и планировании экспериментов [2]. В этом случае $z = p/(1-p) < 1$. Насколько известно автору, функции распределения 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 весьма полезны в работах [4], [5], [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 работа.

[1]Поддержано МОН, проект MG-2024-0048.

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

Основные результаты работы представляют теоремы 1 и 2 для случаев $z \le 1$ and $z \ge 1$, соответственно.

Т е о р е м а 1. *Для* $0 < z < 1$ *и* $A = z^{bn}$ *справедливы следующие границы:*

1) *Если* $0 \le b \le 1/2$, *то*

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

где

$$\begin{gathered} -\frac{\ln(n+1)}{n} - \frac{1}{n}\ln\frac{1-b}{b} - \frac{1}{2n^2 b(1-b)} \le r_1(b,n) \le \frac{\ln(n+1)}{n}, \\ h(x) = -x\ln x - (1-x)\ln(1-x), \quad 0 \le x \le 1. \end{gathered} \tag{3}$$

2) *Если* $1/2 \le b \le 1$, *то*

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

где

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

Т е о р е м а 2. *Для* $z \ge 1$ *и* $A = z^{bn}$ *справедливы следующие границы*

1) *Если* $0 \le b \le 1/2$, *то*

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

2) *Если* $1/2 \le b \le 1$, *то*

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

В частности, из (2)-(7) следует

С л е д с т в и е 1. *Для любого* $z > 0$ *и* $n \ge 10$ *справедливо неравенство*

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

Замечание. Из (8) следует, что если $M = e^{Rn+o(n)}$, $R > 0$ при $n \to \infty$, то тогда с очень большой вероятностью $S(z,M,n) = Mz^{n/2+o(n)}$ при $n \to \infty$ для любого $z > 0$.

§ 2. Доказательства

1. Доказательство теоремы 1. Заметим, что

$$\mathbf{E}e^{\lambda S(z,M,n)} = \left(\mathbf{E}e^{\lambda z^{w_1(n)}}\right)^M, \qquad \mathbf{E}e^{\lambda z^{w_1(n)}} = 2^{-n}\sum_{l=0}^{n}\binom{n}{l}e^{\lambda z^l}. \tag{9}$$

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

$$\begin{gathered}\frac{1}{(n+1)}e^{nh(k/n)} \le \binom{n}{k} \le e^{nh(k/n)}, \quad 0 \le k \le n,\\ h(x) = -x\ln x - (1-x)\ln(1-x).\end{gathered} \tag{10}$$

Для удобства обозначим

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

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

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

$$\mathbf{P}\{S > a\} \le \inf_{\lambda>0}\left\{e^{-\lambda a}\mathbf{E}e^{\lambda S}\right\} \tag{12}$$

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

$$\begin{aligned}\mathbf{P}\{S(z,M,n) \ge MA\} &\le \min_{\lambda\ge0}\left\{e^{-\lambda MA}\mathbf{E}e^{\lambda S(z,M,n)}\right\} =\\ &= 2^{-Mn}\min_{\lambda\ge0}\left\{e^{-\lambda MA}\left[\sum_{l=0}^{n}\binom{n}{l}e^{\lambda z^l}\right]^M\right\},\end{aligned} \tag{13}$$

откуда в силу (10) с $l = an$, $0 \le a \le 1$ получаем

$$\begin{aligned}\frac{1}{M}\ln D_1(z,b,n) &\le -n\ln 2 + \min_{\lambda\ge0}\left\{-\lambda A + \ln\left[\sum_{l=0}^{n}\binom{n}{l}e^{\lambda z^l}\right]\right\} \le\\ &\le -n\ln 2 + \ln(n+1) + \min_{\lambda\ge0}\max_{0\le l\le n}\left\{-\lambda A + \ln\left[\binom{n}{l}e^{\lambda z^l}\right]\right\} \le\\ &\le -n\ln 2 + \ln(n+1) + \min_{\lambda\ge0}\max_{0\le a\le1} f(\lambda,a,z),\end{aligned} \tag{14}$$

где

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

Решение (λ_0, a_0) минимаксной задачи в правой части (14) является седловой точкой функции $f(\lambda,a,z)$ из (15) [9], т.е. определяется условиями

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

или, эквивалентно,

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

При $A = z^{bn}$ с $0 \le b \le 1/2$ система (17) имеет единственное решение (λ_0, a_0) (т.е. функция $f(\lambda, a, z)$ имеет единственную седловую точку)

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

что дает

$$\min_{\lambda\ge 0}\max_{0\le a\le 1} f(\lambda, a, z) = f(\lambda_0, a_0, z) = nh(b). \tag{19}$$

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 $\{\boldsymbol{x}_j\}$ в сумме (1) имеют целый вес l_0 такой, что $z^{l_0} \ge A$, т.е. $l_0 \le bn$. Тогда в силу (10) имеем для любого $A = z^{bn} \ge z^n$

$$\frac{1}{Mn}\ln D_1(z,b,n) \ge \frac{1}{Mn}\ln\left[2^{-n}\binom{n}{l_0}\right]^M \ge h\left(\frac{l_0}{n}\right) - \ln 2 - \frac{\ln(n+1)}{n}. \tag{20}$$

Выбирая максимально возможное целое l_0, имеем

$$l_0 \ge bn - 1. \tag{21}$$

Поэтому из (20) и (21) получаем

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

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

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

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

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

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

Тогда из (23) с $l = an$, $0 \le a \le 1$, аналогично (14) получаем

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

где было обозначено

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

Решение (λ_0, a_0) минимаксной задачи в правой части (24) является седловой точкой функции $g(\lambda,a,z)$ из (25), т.е. определяется условиями

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

или, эквивалентно,

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

При $A = z^{bn}$ с $1/2 \le b \le 1$ система (27) имеет единственное решение (λ_0, a_0) (т.е. функция $g(\lambda,a,z)$ имеет единственную седловую точку)

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

что дает

$$\min_{\lambda\ge 0}\max_{0\le a\le 1} g(\lambda,a,z) = g(\lambda_0,a_0,z) = nh(b). \tag{29}$$

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

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

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 $\{\boldsymbol{x}_j\}$ в сумме (1) имеют целый вес l_0 такой, что $z^{l_0} \le A = z^{bn}$, $1/2 \le b \le 1$, т.е. $l_0 \ge bn \ge n/2$. Тогда в силу (10) имеем для любого $A = z^{bn} \ge z^n$, т.е. $b \le 1$

$$\frac{1}{Mn}\ln D_2(z,b,n) \ge \frac{1}{Mn}\ln\left[2^{-n}\binom{n}{l_0}\right]^M \ge h\left(\frac{l_0}{n}\right) - \ln 2 - \frac{\ln(n+1)}{n}. \tag{31}$$

Выбирая максимально возможное целое l_0, имеем

$$l_0 \geq bn - 1. \tag{32}$$

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

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

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

2. Доказательство теоремы 2. Заметим, что для любых $z > 0$ и $j = 1, \ldots, M$ случайные величины $z^{w_j(n)}$ и $z^{n-w_j(n)}$ имеют одинаковые функции распределения. Поэтому случайные суммы $S(z,M,n)$ и $z^n S(1/z,M,n)$ также имеют одинаковые функции распределения. Тогда в силу соотношений (2) имеем для $z \geq 1$ и $A = z^{bn}$, $1/2 \leq b \leq 1$

$$\begin{gathered}\frac{1}{Mn}\ln \mathbf{P}\{S(z,M,n) \geq Mz^{bn}\} = \frac{1}{Mn}\ln \mathbf{P}\{S(1/z,M,n) \geq Mz^{(b-1)n}\} = \\ = h(b) - \ln 2 + r_1(1-b,n),\end{gathered} \tag{34}$$

откуда следует формула (7). Аналогично доказывается формула (6).

3. Доказательство следствия 1. Для $0 \leq z \leq 1$ положим в (2) $A = z^{n(1/2-\varepsilon)}$, $0 \leq \varepsilon \leq 1/2$. Тогда $a_0 = 1/2 - \varepsilon$ и

$$\begin{gathered}\frac{1}{Mn}\ln \mathbf{P}\left\{\ln\frac{S(z,M,n)}{Mz^{n/2}} \geq -\varepsilon n \ln z\right\} \leq h(1/2-\varepsilon) - \ln 2 + \frac{\ln(n+1)}{n} \leq \\ \leq -2\varepsilon^2 + \frac{\ln(n+1)}{n},\end{gathered} \tag{35}$$

так как $h(1/2-\varepsilon) \leq \ln 2 - 2\varepsilon^2$ для $|\varepsilon| \leq 1/2$. Аналогично, полагая в (3) $A = z^{n(1/2+\varepsilon)}$, для $0 \leq \varepsilon \leq 1/2$ имеем

$$\frac{1}{Mn}\ln \mathbf{P}\left\{\ln\frac{S(z,M,n)}{Mz^{n/2}} \leq \varepsilon n \ln z\right\} \leq -2\varepsilon^2 + \frac{\ln(n+1)}{n}. \tag{36}$$

Положим

$$\varepsilon = \sqrt{\frac{\ln(n+1)}{n}}, \quad n \geq 10, \tag{37}$$

и тогда из (35) -(37) получаем (8) для $0 \leq z \leq 1$.

Для $z \geq 1$ положим в (4) $A = z^{n(1/2+\varepsilon)}$, $0 \leq \varepsilon \leq 1/2$. Тогда $b = 1/2 + \varepsilon$ и аналогично (35) имеем

$$\begin{gathered}\frac{1}{Mn}\ln \mathbf{P}\left\{\ln\frac{S(z,M,n)}{Mz^{n/2}} \geq \varepsilon n \ln z\right\} \leq \\ \leq h(1/2-\varepsilon) - \ln 2 + \frac{\ln(n+1)}{n} \leq -2\varepsilon^2 + \frac{\ln(n+1)}{n}.\end{gathered} \tag{38}$$

Аналогично, полагая в (7) $A = z^{n(1/2-\varepsilon)}$, для $0 \le \varepsilon \le 1/2$ также имеем

$$\frac{1}{Mn}\ln \mathbf{P}\left\{\ln\frac{S(z,M,n)}{Mz^{n/2}} \le -\varepsilon n \ln z\right\} \le -2\varepsilon^2 + \frac{\ln(n+1)}{n}. \tag{39}$$

Положим

$$\varepsilon = \sqrt{\frac{\ln(n+1)}{n}}, \quad n \ge 10, \tag{40}$$

и тогда из (38) -(40) получаем (8) для $z \ge 1$.

СПИСОК ЛИТЕРАТУРЫ

1. *Gallager R. G.* Information theory and reliable communication. Wiley, NY, 1968. (*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. *Berlekamp E. R.*, Block Coding with Noiseless Feedback, Ph. D. Thesis, MIT, Dept. Electrical Enginering, 1964.

5. *Зигангиров К.Ш.* Верхние оценки вероятности ошибки для каналов с обратной связью // Пробл. передачи информ. 1970. Т. 6, № 2. С. 87–92.

6. *Бурнашев М. В.* О функции надежности двоичного симметричного канала с обратной связью // Пробл. передачи информ. 1988. Т. 24, № 1. С. 3–10.

7. *Бурнашев М. В.* О функции концентрации одной суммы случайных величин, связанных с двоичным симметричным каналом // Пробл. передачи информ. 2025.

8. *Cover T. M., Thomas J.A.* Elements of Information Theory. Wiley, NY, 1991.

9. *Демьянов В.Ф., Малоземов В.Н.* Введение в минимакс. М.: Наука, 1972.

Бурнашев Марат Валиевич
Высшая школа современной математики МФТИ. Москва Климентовский пер. 1.
marat.burnashev@mail.ru