Дискретная математика и математическая кибернетика

Discrete mathematics and mathematical cybernetics

УДК 519.118

ОЦЕНКА СВЕРХУ ДЛЯ БИНОМИАЛЬНЫХ КОЭФФИЦИЕНТОВ В ФОРМЕ МУАВРА – ЛАПЛАСА

С. В. АГИЕВИЧ[1)]

[1)]*Научно-исследоательский институт прикладных проблем математики и информатики БГУ, пр. Независимости, 4, 220030, г. Минск, Беларусь*

Построена оценка сверху для биномиальных коэффициентов, которая действует на всей области изменения параметров и имеет форму, повторяющую форму аппроксимации Муавра – Лапласа симметричного биномиального распределения. С помощью этой оценки получены ограничения на число продолжений заданной булевой функции до бент-функций, определена степень зависимости в спектрах Уолша – Адамара, найдены ограничения на количество представлений натуральных чисел в виде суммы квадратов целых чисел, ограниченных по модулю.

Ключевые слова: биномиальный коэффициент; теорема Муавра – Лапласа; спектр Уолша – Адамара; бент-функция; представление в виде суммы квадратов.

Образец цитирования:
Агиевич СВ. Оценка сверху для биномиальных коэффициентов в форме Муавра – Лапласа. *Журнал Белорусского государственного университета. Математика. Информатика.* 2022;1:66–74.
https://doi.org/10.33581/2520-6508-2022-1-66-74

For citation:
Agievich SV. An upper bound on binomial coefficients in the de Moivre – Laplace form. *Journal of the Belarusian State University. Mathematics and Informatics.* 2022;1:66–74. Russian.
https://doi.org/10.33581/2520-6508-2022-1-66-74

Автор:
Сергей Валерьевич Агиевич – кандидат физико-математических наук; заведующий научно-исследовательской лабораторией проблем безопасности информационных технологий.

Author:
Sergey V. Agievich, PhD (physics and mathematics); head of the laboratory of IT security.
agievich@bsu.by
https://orcid.org/0000-0002-9413-8574

AN UPPER BOUND ON BINOMIAL COEFFICIENTS IN THE DE MOIVRE – LAPLACE FORM

S. V. AGIEVICH[a]

[a]*Research Institute for Applied Problems of Mathematics and Informatics, Belarusian State University, 4 Niezaliežnasci Avenue, Minsk 220030, Belarus*

We provide an upper bound on binomial coefficients that holds over the entire parameter range an whose form repeats the form of the de Moivre – Laplace approximation of the symmetric binomial distribution. Using the bound, we estimate the number of continuations of a given Boolean function to bent functions, investigate dependencies into the Walsh – Hadamard spectra, obtain restrictions on the number of representations as sums of squares of integers bounded in magnitude.

Keywords: binomial coefficient; de Moivre – Laplace theorem; Walsh – Hadamard spectrum; bent function; sum of squares representation.

Результаты

Теорема Муавра – Лапласа применительно к симметричному биномиальному распределению может быть записана в виде следующей оценки биномиальных коэффициентов:

$$\binom{n}{k} = \frac{2^n}{\sqrt{\frac{\pi n}{2}}} \exp\left(-\frac{2\left(k-\frac{n}{2}\right)^2}{n} \right)\left(1 + O\left(\frac{1}{\sqrt{n}}\right)\right).$$

Данная оценка справедлива при $n \to \infty$ и $\left|k - \frac{n}{2}\right| = O\left(\sqrt{n}\right)$, т. е. в так называемой центральной области изменения параметров.

То, что оценка носит асимптотический характер и справедлива только в центральной области, затрудняет ее применение в ряде случаев (некоторые из них рассмотрены в настоящей работе). Известны неасимптотические оценки, которые справедливы в более широких областях. Например:

$$\left(\frac{n}{k}\right)^k \le \binom{n}{k} \le \left(\frac{en}{k}\right)^k, \ 1 \le k \le n,$$

или

$$\frac{2^{nH_2(k/n)}}{\sqrt{8k\left(1-\frac{k}{n}\right)}} \le \binom{n}{k} \le \frac{2^{nH_2(k/n)}}{\sqrt{2\pi k\left(1-\frac{k}{n}\right)}}, \ 1 \le k \le \boldsymbol{n} - 1,$$

где $H_2(x) = -x\log_2 x - (1-x)\log_2(1-x)$ (см. соответственно [1; 2, chapter 10, lemma 7]). Однако либо эти оценки недостаточно точны, либо их форма оказывается недостаточно удобной.

Автором найдена оценка сверху для биномиальных коэффициентов, в которой сохраняется форма Муавра – Лапласа, и при этом данная оценка справедлива во всей области изменения параметров.

Теорема. *Для натурального n и* $k \in \{0, 1, \ldots, n\}$ *справедлива оценка*

$$\binom{n}{k} \le \frac{2^n}{\sqrt{\frac{\pi n}{2}}} \exp\left(-\frac{2\left(k-\frac{n}{2}\right)^2}{n} + \frac{23}{18n} \right).$$

При ее построении использовался представленный в публикации [3] подход, в свою очередь основанный на ряде предшествующих работ.

Далее в статье обсуждается применение полученной оценки, а именно: оценивается сверху число продолжений заданной булевой функции до бент-функций, определяется степень зависимости координат

спектров Уолша – Адамара, находятся ограничения на количество представлений натуральных чисел в виде суммы квадратов целых чисел, ограниченных по модулю, и приводится доказательство теоремы.

Продолжения до бент-функций

Пусть $\mathbb{F}_2$ – поле из двух элементов (0 и 1), $\mathbb{F}_2^n$ – n-мерное векторное пространство над $\mathbb{F}_2$, $\mathcal{F}_n$ – множество булевых функций от n переменных, т. е. функций $\mathbb{F}_2^n \to \mathbb{F}_2$. Для $f \in \mathcal{F}_n$ определена спектральная функция (спектр) Уолша – Адамара:

$$\hat{f}(\mathbf{u}) = \sum_{\mathbf{x} \in \mathbb{F}_2^n} \chi\big(f(\mathbf{x}) + \mathbf{x} \cdot \mathbf{u}\big),\ \mathbf{u} \in \mathbb{F}_2^n.$$

Здесь χ – нетривиальный аддитивный характер $\mathbb{F}_2$: $\chi(a) = (-1)^a$, а точка обозначает скалярное произведение векторов.

Для спектра $\hat{f}$ справедливо тождество Парсеваля:

$$\sum_{\mathbf{u} \in \mathbb{F}_2^n} \hat{f}(\mathbf{u})^2 = 2^{2n}.$$

В силу этого тождества $\max_{\mathbf{u}} \left|\hat{f}(\mathbf{u})\right| \geq 2^{n/2}$. Если нижняя граница достигается (это возможно только при четных n), то f называется *бент-функцией* [4]. Пусть $\mathcal{B}_n$ – множество бент-функций от n переменных.

Бент-функции являются идеальными объектами в контексте некоторых задач теории кодирования, криптографии, комбинаторики. Несмотря на интенсивные исследования, бент-функции сохраняют статус трудных для изучения, существует множество открытых вопросов, связанных с ними. Один из таких вопросов – оценка числа бент-функций. В [5] для построения оценок сверху предложено оценивать число продолжений булевой функции до бент-функций. Далее остановимся на числе продолжений, раскрывая и детализируя положения [5].

Пусть $k < n$. Функция $f \in \mathcal{F}_n$ является *продолжением* $g \in \mathcal{F}_k$, если

$$g(y_1, \ldots, y_k) = f\left(\underbrace{0, \ldots, 0}_{n-k},\ y_1, \ldots, y_k\right).$$

Другими словами, f есть продолжение g, если g является *сужением* f на аффинную плоскость $E = \left\{(0, \ldots, 0,\ y_1, \ldots, y_k) : y_i \in \mathbb{F}_2\right\}$. Выбор E в нашем случае не имеет принципиального значения: можно зафиксировать любую другую плоскость размерности k.

Пусть $\mathcal{B}_n(g)$ – множество всех функций $f \in \mathcal{B}_n$, которые являются продолжениями g. Далее мы оценим число продолжений $\left|\mathcal{B}_n(g)\right|$ сверху. Используемый метод оценивания основан на представлении бент-функций бент-прямоугольниками. Это представление было введено в [6]. Опишем его.

Пусть $f \in \mathcal{F}_n$ и $n = m + k$, где m и k – натуральные числа. Рассмотрим всевозможные сужения f на плоскости, параллельные E:

$$f_{\mathbf{u}}(\mathbf{y}) = f(\mathbf{u}, \mathbf{y}),\ \mathbf{u} \in \mathbb{F}_2^m,\ \mathbf{y} \in \mathbb{F}_2^k.$$

От сужений $f_{\mathbf{u}}$ перейдем к их спектрам $\hat{f}_{\mathbf{u}}$, а затем построим функцию

$$\overset{\square}{f}(\mathbf{u}, \mathbf{v}) = \hat{f}_{\mathbf{u}}(\mathbf{v}),\ \mathbf{u} \in \mathbb{F}_2^m,\ \mathbf{v} \in \mathbb{F}_2^k.$$

Она называется *прямоугольником f*. По построению сужения $\overset{\square}{f}(\mathbf{u}, \mathbf{v})$ на $\mathbf{v}$ (*строки*) являются спектральными функциями. Если дополнительно сужения $\overset{\square}{f}(\mathbf{u}, \mathbf{v})$ на $\mathbf{u}$ (*столбцы*), домноженные на $2^{(m-k)/2}$, также являются спектральными функциями, то $\overset{\square}{f}$ называется *бент-прямоугольником*. В [6] доказано, что f – бент-функция тогда и только тогда, когда $\overset{\square}{f}$ – бент-прямоугольник.

В терминах бент-прямоугольников задача оценки числа продолжений $\left|\mathcal{B}_n(g)\right|$ сводится к оценке числа бент-прямоугольников $\overset{\square}{f}$, первая строка которых фиксирована:

$$\overset{\square}{f}(\mathbf{0}, \mathbf{v}) = \hat{g}(\mathbf{v}).$$

Сразу отметим, что при $k > \frac{n}{2}$ существуют функции g, не допускающие продолжений: $|\mathcal{B}_n(g)| = 0$. Примером является функция, которая принимает в точности $2^{k-1} + 1$ нулевых значений, и поэтому $\hat{g}(\mathbf{0}) = 2$. Функция $2^{(m-k)/2}\overset{\square}{f}(\mathbf{u}, \mathbf{0})$ содержит нечетное или даже дробное значение

$$2^{(m-k)/2}\overset{\square}{f}(\mathbf{0}, \mathbf{0}) = 2^{(m-k)/2}\hat{g}(\mathbf{0}) = 2^{(m-k)/2+1}$$

и не может являться спектральной функцией. Следовательно, $\overset{\square}{f}$ не может быть бент-прямоугольником.

При $k \le \frac{n}{2}$ ситуация меняется: как показывает следующее предложение, продолжение g до бент-функции всегда существует. С помощью теоремы мы оценим сверху число продолжений.

Предложение 1. *При четном n для любой булевой функции g от* $k \le \frac{n}{2}$ *переменных множество* $\mathcal{B}_n(g)$ *непусто. Справедлива оценка*

$$\log_2|\mathcal{B}_n(g)| \le 2^n\left(1 - \gamma_{2^{n-k}}\right),$$

в которой

$$\gamma_M = \frac{\log_2 e + \log_2 \pi + \log_2 M - 1}{2M} - \frac{23\log_2 e}{18M^2}.$$

Доказательство. Сначала докажем, что $|\mathcal{B}_n(g)| \ne 0$. Достаточно рассмотреть случай $k = \frac{n}{2}$. Прямоугольник

$$\overset{\square}{f}(\mathbf{u}, \mathbf{v}) = \hat{g}(\mathbf{u} + \mathbf{v}),\ \mathbf{u}, \mathbf{v} \in \mathbb{F}_2^k,$$

реализует биаффинную конструкцию из [7] и поэтому является бент-прямоугольником. Следовательно, соответствующая $\overset{\square}{f}$ функция f лежит в $\mathcal{B}_n$. Более того, первая (при $\mathbf{u} = 0$) строка $\overset{\square}{f}$ совпадает с $\hat{g}$, и, значит, f является продолжением g. В целом $f \in \mathcal{B}_n(g)$, и, таким образом, $\mathcal{B}_n(g)$ непусто.

Перейдем к оценке $|\mathcal{B}_n(g)|$ сверху. Требуется оценить число бент-прямоугольников $\overset{\square}{f}(\mathbf{u}, \mathbf{v})$ таких, что $\overset{\square}{f}(\mathbf{0}, \mathbf{v}) = \hat{g}(\mathbf{v})$. Обозначим $M = 2^m$, $K = 2^k$, $s_{\mathbf{v}} = 2^{(m-k)/2}\hat{g}(\mathbf{v})$.

Рассмотрим столбцы $\overset{\square}{f}$, домноженные на $2^{(m-k)/2}$. Речь идет о спектральных функциях

$$\hat{g}_{\mathbf{v}}(\mathbf{u}) = 2^{(m-k)/2}\overset{\square}{f}(\mathbf{u}, \mathbf{v}),\ \mathbf{u} \in \mathbb{F}_2^m,\ \mathbf{v} \in \mathbb{F}_2^k,$$

которым соответствуют функции $g_{\mathbf{v}} \in \mathcal{F}_m$. Исходя из ограничений на $\overset{\square}{f}$,

$$\hat{g}_{\mathbf{v}}(\mathbf{0}) = 2^{(m-k)/2}\overset{\square}{f}(\mathbf{0}, \mathbf{v}) = 2^{(m-k)/2}\hat{g}(\mathbf{v}) = s_{\mathbf{v}}.$$

Имеются 2^M вариантов выбора $g_{\mathbf{v}}$, и ровно $\binom{M}{(M + s_{\mathbf{v}})/2}$ из них приводят к выполнению равенства $\hat{g}_{\mathbf{v}}(\mathbf{0}) = s_{\mathbf{v}}$. Поэтому искомое число продолжений (число подходящих бент-прямоугольников) есть

$$|\mathcal{B}_n(g)| \le \prod_{\mathbf{v} \in \mathbb{F}_2^k}\binom{M}{(M + s_{\mathbf{v}})/2}.$$

Логарифмируя обе части этого неравенства и используя оценку теоремы, получаем

$$\log_2|\mathcal{B}_n(g)| \le \sum_{\mathbf{v} \in \mathbb{F}_2^k}\left(M - \alpha_M s_{\mathbf{v}}^2 - \beta_M\right).$$

Здесь

$$\alpha_M = \frac{\log_2 e}{2M},\ \beta_M = \frac{1}{2}\left(\log_2 \pi + \log_2 M - 1\right) - \frac{23\log_2 e}{18M}.$$

Воспользовавшись равенством

$$\sum_{\mathbf{v} \in \mathbb{F}_2^k} s_{\mathbf{v}}^2 = 2^{m-k}\sum_{\mathbf{v} \in \mathbb{F}_2^k}\hat{g}(\mathbf{v})^2 = 2^{m-k} \cdot 2^{2k} = MK,$$

окончательно получаем

$$\log_2 \left|\mathcal{B}_n(g)\right| \le MK\left(1-\alpha_M-\frac{\beta_M}{M}\right) = MK\left(1-\gamma_M\right),$$

что и требовалось доказать.

В доказательстве использовалась следующая форма оценки теоремы:

$$\binom{M}{(M+s)/2} \le 2^{M-\alpha_M s^2-\beta_M}.$$

По коэффициентам α_M и β_M была найдена величина $\gamma_M = \alpha_M + \frac{\beta_M}{M}$, именно она определяла точность оценивания в предложении 1. Оказывается, что α_M и β_M можно подправить так, чтобы величина γ_M увеличилась, но оценки для биномиальных коэффициентов остались в силе.

При малых M оптимальные тройки $(\alpha_M, \beta_M, \gamma_M)$ можно найти, решив задачу линейного программирования (см. таблицу). Значения γ_M из последнего столбца таблицы можно использовать в предложении 1 вместо указанных там величин γ_M.

Решения задачи линейного программирования по нахождению оптимальных значений α_M, β_M и γ_M

Solutions of the linear programming problem to find the optimal values of α_M, β_M and γ_M

M	α_M	β_M	γ_M
2	$\frac{1}{2}$	1	$\frac{3}{4}$
4	$\frac{1}{6}$	$\frac{4}{3}$	$\frac{1}{2}$
8	$\frac{1}{12}$	$\frac{14}{3}-\log_2 7$	$\frac{2}{3}-\frac{\log_2 7}{8}\approx 0{,}315\,7$

Латинские зависимости

Пусть $\mathbb{Z}^N$ – множество N-наборов целых чисел, Ω – конечное подмножество $\mathbb{Z}^N$, p – распределение вероятностей на Ω, $\mathbf{a} = (a_1, \ldots, a_N)$ – случайный набор Ω с распределением p, p_i – маргинальное распределение i-й координаты набора: $p_i(x) = \mathbf{P}\{a_i = x\}$, $i = 1, \ldots, N$.

Степень зависимости между координатами $\mathbf{a}$ можно оценить по следующей схеме.

Шаг 1. Выбрать случайные независимые N-наборы $\mathbf{a}^1, \ldots, \mathbf{a}^N$ с распределением p.

Шаг 2. Составить набор $\mathbf{b} = (b_1, \ldots, b_N)$, в котором b_i – i-я координата $\mathbf{a}^i$.

Шаг 3. Определить степень зависимости: $L(p) = \mathbf{P}\{\mathbf{b} \in \Omega\}$.

Удобно считать, что наборы $\mathbf{a}^i$ образуют строки целочисленной матрицы порядка N, и тогда $\mathbf{b}$ – диагональ матрицы. Вероятность $\mathbf{P}\{\mathbf{b} \in \Omega\}$ характеризует соблюдение ограничений на диагональ при условии соблюдения ограничений на строки. Похожие ограничения (на строки, столбцы, иногда на диагонали) возникают в латинских квадратах. Поэтому будем называть величину $L(p)$ степенью *латинской* зависимости.

Величина $L(p)$ представляет собой вероятность успешной «сборки» элемента Ω из «разрозненных» координат с распределениями $p_1, \ldots, p_N$. С увеличением зависимости между координатами $\mathbf{a}$ следует ожидать уменьшения вероятности $L(p)$. Максимальное значение $L(p) = 1$ достигается тогда, когда координаты $\mathbf{a}$ независимы.

Степень латинской зависимости можно вычислить по следующей формуле:

$$L(p) = \sum_{(b_1, \ldots, b_N) \in \Omega} \prod_{i=1}^{N} p_i(b_i).$$

Пример 1. Пусть p назначает вероятность $\frac{1}{N!}$ перестановкам чисел от 1 до N и вероятность 0 всем остальным наборам. Тогда $p_i(x) = \frac{1}{N}$ для $x \in \{1, \ldots, N\}$ и $p_i(x) = 0$ в противном случае. Отсюда

$$L(p) = \frac{N!}{N^N} \approx \frac{\sqrt{2\pi N}}{e^N}.$$

Можно говорить об экспоненциальной зависимости.

Пример 2. Пусть N четное, p назначает вероятность $1/\binom{N}{N/2}$ каждому из $(0, 1)$-наборов длины N, в которых в точности $\frac{N}{2}$ единиц. Тогда $p_i(x) = \frac{1}{2}$ для $x \in \{0, 1\}$. Отсюда

$$L(p) = 2^{-N}\binom{N}{N/2} \approx \sqrt{\frac{2}{\pi N}}.$$

Можно говорить о степенной зависимости (точнее, зависимости типа «корень квадратный»).

Покажем, как использовать теорему для оценки степени латинской зависимости в спектрах Уолша – Адамара (см. раздел «Продолжения до бент-функций»).

Предложение 2. *Пусть* Ω *состоит из наборов значений спектральных функций* $\hat{f}$*, соответствующих всевозможным* $f \in \mathcal{F}_n$*, а* p *задает равномерное распределение на* Ω*. Тогда*

$$L(p) \le \exp\left(\frac{23}{18}\right)\left(\frac{8}{\pi e N}\right)^{N/2}, \ N = 2^n.$$

Доказательство. Имеется 2^N функций f, преобразование $f \mapsto \hat{f}$ биективно, поэтому $|\Omega| = 2^N$. Элементы Ω – это N-наборы четных чисел, ограниченных по модулю величиной N. Маргинальные распределения координат наборов $p_i(x) = 2^{-N}\binom{N}{(N+x)/2}$, $x \in \{-N, -N+2, \ldots, N\}$.

Степень зависимости координат

$$L(p) = \sum_{(b_1, \ldots, b_N) \in \Omega} \prod_{i=1}^{N} 2^{-N}\binom{N}{(N+b_i)/2}.$$

Обратим внимание, что в силу тождества Парсеваля $\sum_i b_i^2 = N^2$.

Применяя теорему, имеем

$$L(p) \le 2^N \max_{(b_1, \ldots, b_N) \in \Omega} \prod_{i=1}^{N} \sqrt{\frac{2}{\pi N}} \exp\left(-\frac{b_i^2}{2N} + \frac{23}{18N}\right) =$$

$$= 2^N \left(\frac{2}{\pi N}\right)^{N/2} \exp\left(-\frac{N}{2} + \frac{23}{18}\right) = \exp\left(\frac{23}{18}\right)\left(\frac{8}{\pi e N}\right)^{N/2},$$

что и требовалось доказать.

Как видим, степень латинской зависимости в спектрах Уолша – Адамара асимптотически выше, чем в перестановках. В случае спектров можно говорить о факториальной зависимости.

Представление в виде суммы квадратов

Пусть $r_{s,n}(N)$ – число представлений целого неотрицательного N в виде суммы квадратов s целых чисел, ограниченных по модулю натуральным n:

$$r_{s,n}(N) = \left|\left\{(a_1, \ldots, a_s) \in \mathbb{Z}^s : \sum_{i=1}^{s} a_i^2 = N, \ |a_i| \le n\right\}\right|.$$

Функция $r_{s,n}(N)$ и особенно функция $r_s(N)$, в которой ограничения на модули a_i сняты, давно изучаются в теории чисел. Например, известна асимптотическая интегральная оценка

$$\sum_{N=1}^{R} r_s(N) = \frac{(\pi R)^{s/2}}{\Gamma(s/2+1)} + O\left(R^{(s-1)/2}\right), \ R \to \infty,$$

которая при $s = 2$ известна как круговая теорема Гаусса (см., например, [8]).

С помощью теоремы получаем следующую интегральную оценку для $r_{s,n}(N)$.

Предложение 3. *Справедлива оценка*

$$\sum_{N=0}^{sn^2} r_{s,n}(N)\exp\left(-\frac{N}{n}\right) \geq (\pi n)^{s/2}\exp\left(-\frac{23s}{36n}\right).$$

Доказательство. Набор $(a_1, \ldots, a_s)$ является целой точкой s-мерного вещественного пространства $\mathbb{R}^s$. Эта точка лежит в пределах s-мерного куба со стороной $2n$ и одновременно на окружности с центром в начале координат и радиусом $\sqrt{a_1^2 + \ldots + a_s^2}$. Любая точка внутри куба лежит на окружности какого-то радиуса, причем квадрат этого радиуса является целым неотрицательным числом, не превосходящим sn^2. Воспользуемся этим наблюдением.

Пусть $\xi_1, \ldots, \xi_s$ – случайные величины, каждая из которых получена суммированием $2n$ независимых случайных величин, принимающих значения 1 и –1 с равными вероятностями. Тогда для точек $(a_1, \ldots, a_s)$, лежащих в пределах куба, выполняется соотношение

$$\mathbf{P}\{(\xi_1, \ldots, \xi_s) = (2a_1, \ldots, 2a_s)\} = \prod_{i=1}^{s} 2^{-2n}\binom{2n}{n+a_i} \leq \frac{1}{(\pi n)^{s/2}}\exp\left(-\frac{N}{n} + \frac{23s}{36n}\right).$$

Здесь $N = \sum_i a_i^2$ – квадрат радиуса окружности, на которой лежит точка $(a_1, \ldots, a_s)$.

Сказанное означает, что

$$1 = \sum_{-n \leq a_1, \ldots, a_s \leq n} \mathbf{P}\{(\xi_1, \ldots, \xi_s) = (2a_1, \ldots, 2a_s)\} =$$

$$= \sum_{N=0}^{sn^2} \sum_{\substack{-n \leq a_1, \ldots, a_s \leq n \\ \Sigma a_i^2 = N}} \mathbf{P}\{(\xi_1, \ldots, \xi_s) = (2a_1, \ldots, 2a_s)\} \leq \sum_{N=0}^{sn^2} r_{s,n}(N)\frac{1}{(\pi n)^{s/2}}\exp\left(-\frac{N}{n} + \frac{23s}{36n}\right).$$

Отсюда следует требуемый результат.

Доказательство теоремы

Лемма. *Для натурального n и $k = 0, \pm 1, \ldots, \pm n$ справедлива оценка*

$$\binom{2n}{n+k} \leq \frac{2^{2n}}{\sqrt{\pi n}}\exp\left(-\frac{k^2}{n} + \frac{23}{36n}\right).$$

Доказательство. Оценка очевидно выполняется для $k = \pm n$. Она проверяется прямыми расчетами при $n = 1, 2$. Биномиальные коэффициенты $\binom{2n}{n+k}$ и $\binom{2n}{n-k}$ совпадают. Поэтому остается рассмотреть случай $n \geq 3$ и $0 \leq k < n$.

Для этого случая в [3] найдена оценка

$$\log\left(\binom{2n}{n+k}2^{-2n}\right) \leq \log\frac{1}{\sqrt{\pi n}} - b_{k,n} - \frac{1}{9n},$$

в которой

$$b_{k,n} = n\left(\left(1 + \frac{k+\frac{1}{2}}{n}\right)\log\left(1 + \frac{k}{n}\right) + \left(1 - \frac{k-\frac{1}{2}}{n}\right)\log\left(1 - \frac{k}{n}\right)\right).$$

Остается доказать, что $b_{k,n} > \frac{k^2}{n} - \frac{c}{n}$, где $c = \frac{23}{36} + \frac{1}{9} = \frac{3}{4}$.

Рассмотрим функцию $f(k) = b_{k,n} - \frac{k^2}{n}$. В [3] получено представление

$$f(k) = -\frac{k^2}{2n^2} + \frac{k^4}{2n^3}\left(\frac{1}{3} - \frac{1}{2n}\right) + \frac{k^6}{2n^5}\left(\frac{1}{5} - \frac{1}{2n}\right) + \ldots.$$

Пусть $k_0 = \sqrt{\frac{3n}{2}}$. В области $k \le k_0$ выполняется неравенство

$$f(k) > -\frac{k^2}{2n^2} \ge -\frac{k_0^2}{2n^2} = -\frac{c}{n}.$$

Теперь достаточно доказать, что $f(k)$ как функция вещественного аргумента возрастает в области $k \in [k_0,\ n-1]$.

Обозначим $x = \frac{k}{n}$ и возьмем производную:

$$f'(k) = 2\operatorname{arth}\left(\frac{k}{n}\right) - \frac{2k}{n} + \frac{k}{k^2 - n^2} = 2\operatorname{arth} x - 2x - \frac{x}{2n\left(1-x^2\right)} =$$

$$= \frac{2x^3}{3} + \frac{2x^5}{5} + \frac{2x^7}{7} + \ldots - \frac{x}{2n\left(1-x^2\right)} > \frac{2x^3}{3} + \frac{2x^5}{5} - \frac{x}{2n\left(1-x^2\right)}.$$

Производная последнего выражения имеет вид

$$\frac{\left(1+x^2\right)\left(4nx^2\left(1-x^2\right)^2 - 1\right)}{2n\left(1-x^2\right)^2}.$$

Она положительна в области $x \in \left[x_0,\ \frac{n-1}{n}\right]$, где $x_0 = \frac{k_0}{n}$, и в силу этого $f'(k)$ возрастает в области $k \in [k_0,\ n-1]$. Остается сказать, что

$$f'(k_0) > \frac{2x_0^3}{3} - \frac{x_0}{2n\left(1-x_0^2\right)} = x_0\left(\frac{1}{n} - \frac{1}{2n\left(1-\frac{3}{2n}\right)}\right) \ge 0$$

(с учетом, что $n \ge 3$), и поэтому $f(k)$ также возрастает.

Перейдем к доказательству теоремы. Достаточно рассмотреть случай нечетного $n = 2m - 1$ и $k \le m$. Имеем

$$\binom{2m-1}{k} = \frac{2m-k}{2m}\binom{2m}{k} \le \left(1 - \frac{k}{2m}\right)\frac{2^{2m}}{\sqrt{\pi m}}\exp\left(-\frac{(k-m)^2}{m} + \frac{23}{36m}\right) \le$$

$$\le \frac{2^{2m-1}}{\sqrt{\pi\left(m-\frac{1}{2}\right)}}\exp\left(-\frac{\left(k-m+\frac{1}{2}\right)^2}{m-\frac{1}{2}} + \frac{23}{36\left(m-\frac{1}{2}\right)} + t(k)\right).$$

Здесь

$$t(k) = -\frac{(k-m)^2}{m} + \frac{\left(k-m+\frac{1}{2}\right)^2}{m-\frac{1}{2}} + \log 2 + \log\left(1 - \frac{k}{2m}\right) = \log\left(2 - \frac{k}{m}\right) - \frac{2m^2 - m - 2k^2}{2m(2m-1)}.$$

Достаточно доказать, что $t(k) \ge 0$ в области $k \in [0;\ m]$. Производная

$$t'(k) = \frac{2k}{2m^2 - m} - \frac{1}{2m-k} = \frac{2(m-k)^2 - m}{\left(2m^2 - m\right)(2m-k)},$$

поэтому минимум достигается в точке $k_0 = m - \sqrt{\frac{m}{2}}$, и этот минимум равняется

$$t(k_0) = \log\left(1 + \frac{1}{\sqrt{2m}}\right) - \frac{1}{1+\sqrt{2m}}.$$

Обозначим $x = \sqrt{2m}$. Имеем

$$t(k_0) \geq \frac{1}{x} - \frac{1}{2x^2} - \frac{1}{1+x} = \frac{x-1}{2x^2(x+1)} > 0,$$

что и требовалось доказать.

Библиографические ссылки

1. Odlyzko AM. Asymptotic enumeration methods. In: Graham RL, Grötschel M, Lovász L, editors. *Handbook of combinatorics. Volume 2.* Amsterdam: Elsevier; 1995. p. 1063–1229. Co-published by the «MIT Press».

2. MacWilliams FJ, Sloane NJA. *The theory of error-correcting codes.* 2nd edition. Amsterdam: North-Holland; 1978. XX, 762 p. (North-Holland mathematical library; volume 16).

3. Szabados T. A simple wide range approximation of symmetric binomial distributions. arXiv:1612.01112v1 [Preprint]. 2016 [cited 2021 November 15]: [6 p.]. Available from: https://arxiv.org/abs/1612.01112v1.

4. Rothaus OS. On «bent» functions. *Journal of Combinatorial Theory. Series A.* 1976;20(3):300–305. DOI: 10.1016/0097-3165(76)90024-8.

5. Агиевич СВ. О продолжении до бент-функций и оценке сверху их числа. *Прикладная дискретная математика. Приложение.* 2020;13:18–21. DOI: 10.17223/2226308X/13/4.

6. Agievich S. On the representation of bent functions by bent rectangles. In: Kolchin VF, Kozlov VYa, Mazalov VV, Pavlov YuL, Prokhorov YuV, editors. *Probabilistic methods in discrete mathematics. Proceedings of the Fifth International Petrozavodsk conference; 2000 June 1–6; Petrozavodsk, Russia.* Utrecht: VSP; 2002. p. 121–135.

7. Agievich S. Bent rectangles. In: Preneel B, Logachev OA, editors. *Boolean functions in cryptology and information security. Proceedings of the NATO Advanced Study Institute; 2007 September 8–18; Zvenigorod, Russia.* Amsterdam: IOS Press; 2008. p. 3–22 (NATO science for peace and security series. D: Information and communication security; volume 18).

8. Takloo-Bighash R. *A Pythagorean introduction to number theory. Right triangles, sums of squares, and arithmetic.* Cham: Springer; 2018. XVIII, 279 p. (Undergraduate texts in mathematics).

References

1. Odlyzko AM. Asymptotic enumeration methods. In: Graham RL, Grötschel M, Lovász L, editors. *Handbook of combinatorics. Volume 2.* Amsterdam: Elsevier; 1995. p. 1063–1229. Co-published by the «MIT Press».

2. MacWilliams FJ, Sloane NJA. *The theory of error-correcting codes.* 2nd edition. Amsterdam: North-Holland; 1978. XX, 762 p. (North-Holland mathematical library; volume 16).

3. Szabados T. A simple wide range approximation of symmetric binomial distributions. arXiv:1612.01112v1 [Preprint]. 2016 [cited 2021 November 15]: [6 p.]. Available from: https://arxiv.org/abs/1612.01112v1.

4. Rothaus OS. On «bent» functions. *Journal of Combinatorial Theory. Series A.* 1976;20(3):300–305. DOI: 10.1016/0097-3165(76)90024-8.

5. Agievich SV. On the continuation to bent functions and upper bounds on their number. *Applied Discrete Mathematics. Supplement.* 2020;13:18–21. Russian. DOI: 10.17223/2226308X/13/4.

6. Agievich S. On the representation of bent functions by bent rectangles. In: Kolchin VF, Kozlov VYa, Mazalov VV, Pavlov YuL, Prokhorov YuV, editors. *Probabilistic methods in discrete mathematics. Proceedings of the Fifth International Petrozavodsk conference; 2000 June 1–6; Petrozavodsk, Russia.* Utrecht: VSP; 2002. p. 121–135.

7. Agievich S. Bent rectangles. In: Preneel B, Logachev OA, editors. *Boolean functions in cryptology and information security. Proceedings of the NATO Advanced Study Institute; 2007 September 8–18; Zvenigorod, Russia.* Amsterdam: IOS Press; 2008. p. 3–22 (NATO science for peace and security series. D: Information and communication security; volume 18).

8. Takloo-Bighash R. *A Pythagorean introduction to number theory. Right triangles, sums of squares, and arithmetic.* Cham: Springer; 2018. XVIII, 279 p. (Undergraduate texts in mathematics).

Получена 20.01.2022 / исправлена 21.02.2022 / принята 21.02.2022.
Received 20.01.2022 / revised 21.02.2022 / accepted 21.02.2022.