ОЦЕНКА СВЕРХУ ДЛЯ БИНОМИАЛЬНЫХ КОЭФФИЦИЕНТОВ В ФОРМЕ МУАВРА – ЛАПЛАСА

С. В. АГИЕВИЧ1)

1)Научно-исследовательский 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.
AN UPPER BOUND ON BINOMIAL COEFFICIENTS IN THE DE MOIVRE – LAPLACE FORM

S. V. AGIEVICH

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 and 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:

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

Данная оценка справедлива при \(n \rightarrow \infty\) и \(k - n/2 = O(\sqrt{n})\), 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:

\[
\binom{n}{k} \leq \binom{en}{k}^k, 1 \leq k \leq n,
\]

или

\[
\frac{2^{H_2(k/n)}}{\sqrt{8k\left(1 - \frac{k}{n}\right)}} \leq \binom{n}{k} \leq \frac{2^{H_2(k/n)}}{\sqrt{2\pi k\left(1 - \frac{k}{n}\right)}}, 1 \leq k \leq n - 1,
\]

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.

**Teorema.** Для натурального \(n\) и \(k \in \{0, 1, \ldots, n\}\) справедлива оценка

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

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, находитя 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 $\mathbb{F}_2^n \rightarrow \mathbb{F}_2$. Для $f \in \mathcal{F}_n$ определена спектральная функция (спектр) Уолша – Адамара:

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

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

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

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

В силу этого тождества $\max_u |\hat{f}(u)| \geq 2^{n/2}$. 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

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

Другими словами, $f$ есть продолжение $g$, если $g$ является сужением $f$ на аффинную плоскость $E = \{(0, \ldots, 0, y_1, \ldots, y_k) : y_i \in \mathbb{F}_2\}$. 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 $|\mathcal{B}_n(g)|$ 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 все возможные сужения $f$ на плоскости, параллельные $E$:

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

От сужений $f_a$ перейдем к их спектрам $\hat{f}_a$, а затем построим функцию

$$f(u, v) = \hat{f}_a(v), \; u \in \mathbb{F}_2^m, \; v \in \mathbb{F}_2^k.$$

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

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

$$f(0, v) = \hat{g}(v).$$
Сразу отметим, что при \( k > \frac{n}{2} \) существуют функции \( g \), не допускающие продолжений: \( |B_n(g)| = 0 \). Примером является функция, которая принимает в точности \( 2^{k-1} + 1 \) нулевых значений, и поэтому \( \hat{g}(0) = 2 \).

Функция \( 2^{(m-k)/2} f(u, 0) \) содержит нечетное или даже дробное значение

\[
2^{(m-k)/2} f(0, 0) = 2^{(m-k)/2} \hat{g}(0) = 2^{(m-k)/2 + 1}
\]

и не может являться спектральной функцией. Следовательно, \( f \) не может быть бент-прямоугольником.

При \( k \leq \frac{n}{2} \) 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 \( n \) и для любой булевой функции \( g \) от \( k n \leq 2 \) переменных множество \( B_n(g) \) непусто. Справедлива оценка

\[
\log_2 |B_n(g)| \leq 2^\gamma \left( 1 - \gamma_{2^{n-k}} \right).
\]

**Доказательство.** Сначала докажем, что \( |B_n(g)| \neq 0 \). Достаточно рассмотреть случай \( k n = 2 \).

Прямоугольник \( f(u, v) = \hat{g}(u + v) \), \( u, v \in \mathbb{F}_2 \), реализует биаффинную конструкцию из [7] и поэтому является бент-прямоугольником. Следовательно, соответствующая \( f \) функция \( f \) лежит в \( B_n \). Более того, первая (при \( u = 0 \)) строка \( f \) совпадает с \( \hat{g} \), и значит, \( f \) является продолжением \( g \). В целом \( f \in B_n(g) \), и, таким образом, \( B_n(g) \) непусто.

Перейдем к оценке \( |B_n(g)| \) сверху. Требуется оценить число бент-прямоугольников \( f(u, v) \) таких, что \( f(0, v) = \hat{g}(v) \). Обозначим \( M = 2^m, K = 2^k, s_v = 2^{(m-k)/2} \hat{g}(v) \).

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

\[
\hat{g}_v(u) = 2^{(m-k)/2} f(u, v), \quad u \in \mathbb{F}_2^m, \quad v \in \mathbb{F}_2^k,
\]

которым соответствуют функции \( g_v \in \mathcal{F}_m \). Исходя из ограничений на \( f \),

\[
\hat{g}_v(0) = 2^{(m-k)/2} f(0, v) = 2^{(m-k)/2} \hat{g}(v) = s_v.
\]

Имеются \( 2^M \) вариантов выбора \( g_v \), и ровно \((M s_v)/(M + s_v)/2\) из них приводят к выполнению равенства \( \hat{g}_v(0) = s_v \). Поэтому искомое число продолжений (число подходящих бент-прямоугольников) есть

\[
|B_n(g)| \leq \prod_{v \in \mathbb{F}_2^k} \left( \frac{M}{(M + s_v)/2} \right).
\]

Логарифмируя обе части этого неравенства и используя оценку теоремы, получаем

\[
\log_2 |B_n(g)| \leq \sum_{v \in \mathbb{F}_2^k} \left( M - \alpha_M s_v^2 - \beta_M \right).
\]

Здесь

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

Воспользовавшись равенством

\[
\sum_{v \in \mathbb{F}_2^k} s_v^2 = 2^{m-k} \sum_{v \in \mathbb{F}_2^k} \hat{g}(v)^2 = 2^{m-k} \cdot 2^{2k} = MK,
\]

69
окончательно получаем
\[ \log_2 |B_n(g)| \leq MK \left( 1 - \alpha_M - \frac{\beta_M}{M} \right) = MK (1 - \gamma_M), \]
что и требовалось доказать.

В доказательстве использовалась следующая форма оценки теоремы:
\[ \left( \frac{M}{M + s} \right)^2 \leq 2^{M - \alpha_M^2 - \beta_M}. \]

По коэффициентам \( \alpha_M \) и \( \beta_M \) была найдена величина \( \gamma_M = \alpha_M + \frac{\beta_M}{M} \), именно она определяла точность оценивания в предложении 1. Оказывается, что \( \alpha_M \) и \( \beta_M \) можно подправить так, чтобы величина \( \gamma_M \) увеличила, 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 \( \gamma_M \) из последнего столбца таблицы можно использовать в предложении 1 вместо указанных там величин \( \gamma_M \).

Решения задачи линейного программирования по нахождению оптимальных значений \( \alpha_M, \beta_M \) и \( \gamma_M \)

| \( M \) | \( \alpha_M \) | \( \beta_M \) | \( \gamma_M \) |
|-------|---------|---------|---------|
| 2     | 1/2     | 1       | 3/4     |
| 4     | 1/6     | 4/3     | 1/2     |
| 8     | 1/12    | 14/3 - \log_2 7 | 2/3 - \log_2 7 = 0,315 7 |

Латинские зависимости

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

Степень зависимости между координатами \( a \) можно оценить по следующей схеме.

Шаг 1. Выбрать случайные независимые \( N \)-наборы \( a^1, \ldots, a^N \) с распределением \( p \).

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

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

Удобно считать, что наборы \( a^i \) образуют строки целочисленной матрицы порядка \( N \), и тогда \( b - \) диагональ матрицы. Вероятность \( P\{b \in \Omega\} \) 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 \( \Omega \) из «разрозненных» координат с распределениями \( p_1, \ldots, p_N \). С увеличением зависимости между координатами \( a \) следует ожидать уменьшения вероятности \( L(p) \). Максимальное значение \( L(p) = 1 \) достигается тогда, когда координаты \( a \) независимы.

Степень латинской зависимости можно вычислить по следующей формуле:
\[ L(p) = \sum_{(h_1, \ldots, h_N) \in \Omega} \prod_{i=1}^{N} p_i(h_i). \]

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


Пусть $N$ четное, $p$ назначает вероятность $\frac{1}{2}$ каждому из $(0, 1)$-наборов длины $N$, в которых в точности $\frac{N}{2}$ единиц. Тогда $p_1(x) = \frac{1}{2}$ для $x \in \{0, 1\}$. Отсюда

$$L(p) = 2^{-N} \left( \frac{N}{(N + x)/2} \right) = \sqrt{\frac{2}{\pi N}}.$$ 

Можно говорить об экспоненциальной зависимости.

Пример 2. Пусть $N$ четное, $p$ назначает вероятность $\frac{1}{2}$ каждому из $(0, 1)$-наборов длины $N$, в которых в точности $\frac{N}{2}$ единиц. Тогда $p_1(x) = \frac{1}{2}$ для $x \in \{0, 1\}$. Отсюда

$$L(p) = 2^{-N} \left( \frac{N}{(N + x)/2} \right) = \sqrt{\frac{2}{\pi N}}.$$ 

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 $\Omega$ состоит из наборов значений спектральных функций $\hat{f}$, соответствующих всевозможным $f \in F_n$, а $p$ задает равномерное распределение на $\Omega$. Тогда

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

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

Степень зависимости координат

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

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

Приложив теорему, имеем

$$L(p) \leq 2^N \max_{(b_1, ..., b_N) \in \Omega} \prod_{i=1}^{N} \sqrt{\frac{2}{\pi N}} \exp \left( -\frac{b_i^2}{2N} + \frac{23}{18N} \right) = \exp \left( \frac{23}{18} \left( \frac{8}{\pi N} \right)^{N/2} \right),$$ 

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 $n$:

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

Функция $r_{s,n}(N)$ является асимптотической интегральной оценкой

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

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

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

71
Предложение 3. Справедлива оценка

\[ \sum_{N=0}^{n^2} r_{s,n}(N) \exp \left( -\frac{N}{n} \right) \geq \left( \frac{\pi n}{2} \right)^{1/2} \exp \left( -\frac{23s}{36n} \right) \]

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

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

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

Сказанное означает, что

\[ 1 = \sum_{-n \leq a_1, \ldots, a_s \leq n} P\left\{ (\xi_1, \ldots, \xi_s) = (2a_1, \ldots, 2a_s) \right\} = \sum_{N=0}^{n^2} \sum_{-n \leq a_1, \ldots, a_s \leq n, \sum a_i^2 = N} r_{s,n}(N) \frac{1}{(\pi n)^{s/2}} \exp \left( -\frac{N}{n} + \frac{23s}{36n} \right) \]

Отсюда следует требуемый результат.

Доказательство теоремы

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

\[ \left\{ \frac{2n}{n+k} \right\} \leq \frac{2^{2n}}{\sqrt{n}} \exp \left( -\frac{k^2}{n} + \frac{23}{36n} \right) \]

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

Для этого случая в [3] найдена оценка

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

в которой

\[ b_{k,n} = n \left\{ \log \left( 1 + \frac{k+1}{n} \right) + \log \left( 1 - \frac{k-1}{n} \right) \right\} \left( \frac{k+1}{n} - \frac{k-1}{n} \right), \]

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

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

72
Пусть \( k_0 = \sqrt{\frac{3n}{2}} \). В области \( k \leq k_0 \) выполняется неравенство

\[
  f(k) > -\frac{k^2}{2n^2} \geq -\frac{k_0^2}{2n^2} = -\frac{c}{n}.
\]

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:

\[
  f'(k) = 2\arctan\left(\frac{k}{n}\right) - \frac{2k}{n^2} + \frac{k}{n^2 - k^2} = 2\arctan x - 2x - \frac{x}{2n(1-x^2)} =
\]

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

Производная последнего выражения имеет вид

\[
  \frac{(1+x^2)(4nx^2(1-x^2)^2-1)}{2n(1-x^2)^2}.
\]

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

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

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

Перейдем к доказательству теоремы. Достаточно рассмотреть случай нечетного \( n = 2m-1 \) и \( k \leq m \).

Имеем

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

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

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 \( t(k) \geq 0 \) в области \( k \in [0; m] \). Производная

\[
  t'(k) = \frac{2k}{2m^2 - m} - \frac{1}{2m-k} = \frac{2(m-k)^2 - m}{(2m^2 - m)(2m-k)},
\]

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

\[
  t(k_0) = \log\left(1 + \frac{1}{\sqrt{2}m}\right) - \frac{1}{1+\sqrt{2}m}.
\]
Обозначим \( x = \sqrt{2m} \). Имеем

\[
I(k_0) \geq \frac{1}{x} - \frac{1}{2x^2} - \frac{1}{1 + x} = \frac{x - 1}{2x^2(x + 1)} > 0,
\]

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. Агиеевич 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*. Amstderdam: 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. Агиеевич 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*. Amstderdam: 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).