Math-Net.Ru

Общероссийский математический портал

А. М. Зубков, Моменты весов случайных неравновероятных булевых функций, *Матем. вопр. криптогр.*, 2014, том 5, выпуск 3, 5–15

DOI: <https://doi.org/10.4213/mvk126>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 3.93.64.190

26 апреля 2023 г., 14:13:41

Моменты весов случайных неравновероятных булевых функций

А. М. Зубков

Математический институт им. В. А. Стеклова РАН, Москва

Получено 22.IV.2013

Рассматриваются неравновероятные распределения на множествах булевых функций от n переменных. Получены явные формулы для первых двух моментов веса многочленов Жегалкина с распределением коэффициентов, инвариантным относительно перестановок переменных (и аналогичные формулы для моментов числа мономов в многочлене Жегалкина булевой функции с распределением, инвариантным относительно перестановок переменных).

Ключевые слова: случайные булевы функции, симметричные распределения, многочлены Жегалкина, средние и дисперсии веса функции

Moments of weights of random nonuniform Boolean functions

A. M. Zubkov

Steklov Mathematical Institute of RAS, Moscow

Abstract. Some nonuniform distributions on the Boolean functions of n variables are considered. We obtain explicit formulas for the first two moments of the weight of Zegalkin polynomials having coefficient distributions invariant under permutations of variables (and analogous formulas for the moments of the number of monoms in the Zegalkin polynomial of Boolean function with distribution invariant under permutation of variables).

Keywords: random Boolean functions, symmetrical distributions, Zegalkin polynomials, mean and variance of the weight of a function

1. Формулировки результатов

Различные характеристики случайных булевых функций изучались в большом числе статей и монографий. Например, в [1], [2], [3] изучались свойства распределений, порожденных случайными булевыми формулами, в [4], [5] — свойства спектра Фурье булевых функций, значения которых в разных точках независимы и одинаково распределены, в [6], [7] — свойства случайных булевых функций, зависящих только от числа ненулевых значений аргументов. В настоящей работе получены формулы для первых двух моментов числа ненулевых значений булевой функции, заданной многочленом Жегалкина с независимыми коэффициентами, распределения которых зависят от степеней мономов, соответствующих этим коэффициентам.

Пусть $\mathbb{F}_2 = \{0, 1\}$ — поле из двух элементов, $V_n = \mathbb{F}_2^n = \{\mathbf{x} = (x_1, \dots, x_n) : x_1, \dots, x_n \in \{0, 1\}\}$ — множество n -мерных двоичных векторов. В множестве $\mathbb{F}_2^{V_n}$ булевых функций от n булевых переменных $\mathbf{x} = (x_1, \dots, x_n)$ существует 2^n мономов:

$$1, x_1, \dots, x_n, x_1x_2, x_1x_3, \dots, x_{n-1}x_n, \dots, x_1x_2 \dots x_n.$$

Моном, соответствующий множеству $J \subseteq \{1, \dots, n\}$ номеров входящих в него переменных, будем обозначать через

$$\mathbf{x}^J = \prod_{j \in J} x_j.$$

В дальнейшем будем отождествлять множества $J \subseteq \{1, \dots, n\}$ с элементами $(j_1, \dots, j_n) \in V_n$, считая, что $j_k = 1$, если $k \in J$, и $j_k = 0$, если $j \notin J$ (так что множество $J = \emptyset \subset \{1, \dots, n\}$ отождествляется с $\mathbf{0} \in V_n$); аналогично, векторы $\mathbf{x} = (x_1, \dots, x_n)$ будем отождествлять с подмножествами множества $\{1, \dots, n\}$. Имея в виду такое отождествление, будем в дальнейшем понимать запись вида $J \subset \mathbf{x}$ как условие $x_k = 0 \Rightarrow k \notin J$ для всех $k = 1, \dots, n$.

Булеву функцию $f(\mathbf{x}) \in \mathbb{F}_2^{V_n}$ можно задавать совокупностью ее значений

$$f(\mathbf{x}), \quad \mathbf{x} \in V_n,$$

а также многочленом Жегалкина:

$$f(\mathbf{x}) = \bigoplus_{J \subset \{1, \dots, n\}} f_J \mathbf{x}^J, \quad (1)$$

где $\{f_J \in \{0, 1\} : J \subset \{1, \dots, n\}\}$ — совокупность коэффициентов в представлении функции f многочленом Жегалкина, а $\oplus$ — сложение

в $\mathbb{F}_2$. Если $\{f(\mathbf{x}) : \mathbf{x} \in V_n\}$ или $\{f_J \in \{0, 1\} : J \subset \{1, \dots, n\}\}$ — совокупности случайных величин, то и функция f является случайной.

Эти представления булевой функции тесно связаны. Так как $\mathbf{x}^J = 1$ тогда и только тогда, когда $J \subseteq \mathbf{x}$, то значение функции f в точке $\mathbf{x} \in V_n$ определяется равенством

$$f(\mathbf{x}) = \bigoplus_{J \subseteq \mathbf{x}} f_J. \quad (2)$$

С другой стороны, известно (см., например, [8], теорема 2.10), что

$$f_J = \bigoplus_{\mathbf{x} \subseteq J} f(\mathbf{x}). \quad (3)$$

(Действительно, при любом $J \subset \{1, \dots, n\}$

$$\bigoplus_{\mathbf{x} \subseteq J} f(\mathbf{x}) = \bigoplus_{\mathbf{x} \subseteq J} \bigoplus_{I \subseteq \mathbf{x}} f_I = \bigoplus_{I \subseteq J} f_I \bigoplus_{I \subseteq \mathbf{x} \subseteq J} 1 = f_J,$$

так как число векторов $\mathbf{x}$, удовлетворяющих условиям $I \subseteq \mathbf{x} \subseteq J$, четно, если $I \subset J$ и $I \neq J$, и равно 1 при $I = J$.)

Весом булевой функции $f : \mathbb{F}_2^{V_n} \rightarrow \mathbb{F}_2$ называется число точек, в которых она принимает ненулевые значения:

$$\begin{aligned} \|f\| &= |\{\mathbf{x} \in V_n : f(\mathbf{x}) = 1\}| = \\ &= \sum_{\mathbf{x} \in V_n} \mathbb{I}\{f(\mathbf{x}) = 1\} = \sum_{\mathbf{x} \in V_n} \mathbb{I}\left\{\bigoplus_{J \subseteq \mathbf{x}} f_J = 1\right\}. \end{aligned} \quad (4)$$

Аналогично, *весом Жегалкина* булевой функции $f(\mathbf{x})$ назовем число ненулевых коэффициентов ее многочлена Жегалкина (1):

$$\begin{aligned} \|f\|_{\text{Zeg}} &= |\{J \subseteq \{1, \dots, n\} : f_J = 1\}| = \\ &= \sum_{J \subseteq \{1, \dots, n\}} \mathbb{I}\{f_J = 1\} = \sum_{J \subseteq \{1, \dots, n\}} \mathbb{I}\left\{\bigoplus_{\mathbf{x} \subseteq J} f(\mathbf{x}) = 1\right\}. \end{aligned} \quad (5)$$

Вычисление моментов веса случайной булевой функции в терминах коэффициентов многочлена Жегалкина и моментов веса Жегалкина в терминах значений булевой функции можно провести с помощью следующего утверждения.

Утверждение 1. Для первых двух моментов веса и веса Жегалкина случайной булевой функции $f(\mathbf{x}) \in \mathbb{F}_2^{V_n}$ справедливы формулы

$$\begin{aligned} \mathbf{E}\|f\| &= \sum_{\mathbf{x} \in V_n} b_{\mathbf{x}}, \quad \text{где} \quad b_{\mathbf{x}} = \mathbf{E}f(\mathbf{x}) = \mathbf{P}\left\{\bigoplus_{J \subseteq \mathbf{x}} f_J = 1\right\}, \\ \mathbf{D}\|f\| &= \sum_{\mathbf{x} \in V_n} b_{\mathbf{x}}(1 - b_{\mathbf{x}}) + \sum_{\mathbf{x}_1, \mathbf{x}_2 \in V_n : \mathbf{x}_1 \neq \mathbf{x}_2} b_{\mathbf{x}_1, \mathbf{x}_2}, \end{aligned} \quad (6)$$

где

$$b_{\mathbf{x}_1, \mathbf{x}_2} = \text{cov}(f(\mathbf{x}_1), f(\mathbf{x}_2)) = \mathbf{P} \left\{ \bigoplus_{J \subseteq \mathbf{x}_1} f_J = \bigoplus_{J \subseteq \mathbf{x}_2} f_J = 1 \right\} - b_{\mathbf{x}_1} b_{\mathbf{x}_2},$$

$$\mathbf{E} \|f\|_{\text{Zeg}} = \sum_{J \subseteq \{1, \dots, n\}} c_J, \quad \text{где} \quad c_J = \mathbf{E} f_J = \mathbf{P} \left\{ \bigoplus_{\mathbf{x} \subseteq J} f(\mathbf{x}) = 1 \right\},$$

$$\mathbf{D} \|f\|_{\text{Zeg}} = \sum_{J \subseteq \{1, \dots, n\}} c_J(1 - c_J) + \sum_{J_1, J_2 \subseteq \{1, \dots, n\}: J_1 \neq J_2} c_{J_1, J_2}, \quad (7)$$

где

$$c_{J_1, J_2} = \text{cov}(f_{J_1}, f_{J_2}) = \mathbf{P} \left\{ \bigoplus_{\mathbf{x} \subseteq J_1} f(\mathbf{x}) = \bigoplus_{\mathbf{x} \subseteq J_2} f(\mathbf{x}) = 1 \right\} - c_{J_1} c_{J_2}.$$

Аналогичные (но более громоздкие) формулы справедливы и для моментов более высоких порядков.

Доказательство утверждения 1. Все формулы непосредственно следуют из представлений (4) и (5) веса функции в виде суммы индикаторов и равенств

$$\begin{aligned} \mathbf{E} \sum_{k=1}^M \xi_k &= \sum_{k=1}^M \mathbf{E} \xi_k, \\ \mathbf{D} \sum_{k=1}^M \xi_k &= \mathbf{E} \left(\sum_{k=1}^M (\xi_k - \mathbf{E} \xi_k) \right)^2 = \\ &= \sum_{k=1}^M \mathbf{D} \xi_k + \sum_{k=1}^M \sum_{m \in \{1, \dots, M\} \setminus \{k\}} \text{cov}(\xi_k, \xi_m). \end{aligned}$$

□

В общем случае формулы Утверждения 1 вряд ли можно упростить. При тех или иных дополнительных предположениях о распределении совокупности значений булевой функции f или коэффициентов ее многочлена Жегалкина формулам из Утверждения 1 можно придать более явный вид. Мы будем предполагать, что совместные распределения коэффициентов многочлена Жегалкина (или совместные распределения значений булевой функции) инвариантны относительно перестановок переменных.

Теорема 1. Если коэффициенты $\{f_J : J \subset \{1, \dots, n\}\}$ многочлена Жегалкина булевой функции f независимы и вероятности

$$p_J = \mathbf{P}\{f_J = 1\} = \frac{1}{2} (1 - \Delta_{|J|}), \quad J \subseteq \{1, \dots, n\}, \quad (8)$$

зависят только от числа $|J|$ сомножителей в мономе $\mathbf{x}^J$, то

$$\mathbf{E}\|f\| = 2^{n-1} - \frac{1}{2} \sum_{k=0}^n C_n^k \left(\prod_{r=0}^k \Delta_r^{C_r^k} \right), \quad (9)$$

$$\begin{aligned} \mathbf{D}\|f\| = \frac{1}{4} \left(\sum_{a,b=0}^n \sum_{c=\max\{a+b-n, 0\}}^{\min\{a,b\}} \frac{n! \prod_{r=0}^a \Delta_r^{C_r^a - C_r^c} \prod_{s=0}^b \Delta_s^{C_s^b - C_s^c}}{(a-c)!(b-c)!c!(n-a-b+c)!} - \right. \\ \left. - \left(\sum_{a=0}^n C_n^a \prod_{s=0}^a \Delta_s^{C_s^a} \right)^2 \right). \end{aligned} \quad (10)$$

Формулы (9), (10) справедливы также для $\mathbf{E}\|f\|_{\text{Zeg}}$ и $\mathbf{D}\|f\|_{\text{Zeg}}$, если значения $\{f(\mathbf{x}) : \mathbf{x} \in V_n\}$ булевой функции f независимы и вероятности

$$q_{\mathbf{x}} = \mathbf{P}\{f(\mathbf{x}) = 1\} = \frac{1}{2} (1 - \Delta_{\|\mathbf{x}\|}), \quad \mathbf{x} \in V_n,$$

зависят только от веса $\|\mathbf{x}\|$.

Следствие 1. Если выполнены условия теоремы 1 и $p_J = \frac{1}{2}(1 - \Delta)$, $J \subset \{1, \dots, n\}$, то

$$\begin{aligned} \mathbf{E}\|f\| &= 2^{n-1} - \frac{1}{2} \sum_{k=0}^n C_n^k \Delta^{2^k}, \\ \mathbf{D}\|f\| &= \frac{1}{4} \left(\sum_{a,b=0}^n \sum_{c=\max\{a+b-n, 0\}}^{\min\{a,b\}} \frac{n! \Delta^{2^a + 2^b - 2^c + 1}}{(a-c)!(b-c)!c!(n-a-b+c)!} - \left(\sum_{a=0}^n C_n^a \Delta^{2^a} \right)^2 \right). \end{aligned}$$

Доказательство. Достаточно заметить, что если $\Delta_k = \Delta$ при всех $k = 0, 1, \dots, n$, то

$$\prod_{s=0}^m \Delta^{C_m^s} = \Delta^{2^m}, \quad \prod_{r=0}^m \Delta^{C_m^r - C_j^r} = \Delta^{2^m - 2^j} \quad (0 \leq j \leq m).$$

□

Рис. 1. Математические ожидания (тонкие линии) и среднеквадратические отклонения (жирные линии) весов функций $f(\mathbf{x}) = \bigoplus_{J \subset \{1, \dots, n\}} f_J \mathbf{x}^J$, где f_J независимы и $\mathbf{P}\{f_J = 1\} = p = 1 - \mathbf{P}\{f_J = 0\}$.

Формулы Следствия 1 иллюстрируются рис. 1, где для случаев $n = 5$ и $n = 10$ представлены графики зависимости $\mathbf{E}\|f\|$ и $\sqrt{\mathbf{D}\|f\|}$ от $p = p_J$.

Следствие 2. Если выполнены условия теоремы 1 и при некотором $m \in \{1, \dots, n\}$

$$\Delta_r = \begin{cases} \Delta, & \text{если } r = m, \\ 1, & \text{если } r \neq m, \end{cases}$$

то

$$\begin{aligned} \mathbf{E}\|f\| &= 2^{n-1} - \frac{1}{2} \sum_{k=0}^n C_n^k \Delta_n^{C_k^m}, \\ \mathbf{D}\|f\| &= \frac{1}{4} \left(\sum_{a,b=0}^n \sum_{c=\max\{a+b-n, 0\}}^{\min\{a,b\}} \frac{n! \Delta_n^{C_a^m + C_b^m - 2C_c^m}}{(a-c)!(b-c)!c!(n-a-b+c)!} - \right. \\ &\quad \left. - \left(\sum_{a=0}^n C_n^a \Delta_n^{C_a^m} \right)^2 \right). \end{aligned}$$

Доказательство. Если выполнены условия следствия 2, то

$$\begin{aligned} \prod_{r=0}^a \Delta_r^{C_a^r} &= \begin{cases} 1 = \Delta_n^{C_a^m} & \text{при } a < m, \\ \Delta_n^{C_a^m} & \text{при } a \geq m, \end{cases} \\ \prod_{r=0}^a \Delta_r^{C_a^r - C_c^r} &= \begin{cases} 1 = \Delta_n^{C_a^m - C_c^m} & \text{при } a < m, \\ \Delta_n^{C_a^m - C_c^m} & \text{при } a \geq m. \end{cases} \end{aligned}$$

□

Рис. 2. Математические ожидания (тонкие линии) и среднеквадратические отклонения (жирные линии) весов функций $f(\mathbf{x}) = \bigoplus_{J \subset \{1, \dots, n\}, |J|=m} f_J \mathbf{x}^J$, для $m = 1, 2, 3, 4$, где f_J независимы и $\mathbf{P}\{f_J = 1\} = p = 1 - \mathbf{P}\{f_J = 0\}$.

На рис. 2 представлены графики зависимости $\mathbf{E}\|f\|$ и $\sqrt{\mathbf{D}\|f\|}$ от p для случайных булевых функций от 5 и 10 переменных, являющихся суммами мономов одной и той же степени $m = 1, 2, 3, 4$ с независимыми одинаково распределенными коэффициентами.

Точные формулы для $\mathbf{E}\|f\|$ и $\mathbf{D}\|f\|$ являются многочленами от p довольно высоких степеней, что отражается на виде графиков.

2. Доказательство теоремы 1

Для суммы $\xi_1 \oplus \dots \oplus \xi_m$ независимых индикаторов $\xi_1, \dots, \xi_m$ с

$$\mathbf{P}\{\xi_k = 1\} = \frac{1}{2}(1 - \delta_k), \quad \mathbf{P}\{\xi_k = 0\} = \frac{1}{2}(1 + \delta_k), \quad k = 1, \dots, m,$$

хорошо известны равенства

$$\mathbf{P}\left\{\bigoplus_{k=1}^m \xi_k = 1\right\} = \frac{1}{2} \left(1 - \prod_{k=1}^m \delta_k\right), \quad \mathbf{P}\left\{\bigoplus_{k=1}^m \xi_k = 0\right\} = \frac{1}{2} \left(1 + \prod_{k=1}^m \delta_k\right).$$

Из этих равенств, (6) и предположений (8) следует, что

$$\begin{aligned} b_{\mathbf{x}} &= \mathbf{P}\{f(\mathbf{x}) = 1\} = \mathbf{P}\left\{\bigoplus_{J \subseteq \mathbf{x}} f_J = 1\right\} = \\ &= \mathbf{P}\left\{\bigoplus_{r=0}^{\|\mathbf{x}\|} \bigoplus_{J \subseteq \mathbf{x}, |J|=r} f_J = 1\right\} = \frac{1}{2} \left(1 - \prod_{r=0}^{\|\mathbf{x}\|} \Delta_r^{C_r^{\|\mathbf{x}\|}}\right) \end{aligned} \quad (11)$$

и

$$\mathbf{E}\|f\| = \sum_{\mathbf{x} \in V_n} b_{\mathbf{x}} = \sum_{k=0}^n C_n^k \frac{1}{2} \left(1 - \prod_{r=0}^k \Delta_r^{C_k^r}\right) = 2^{n-1} - \frac{1}{2} \sum_{k=0}^n C_n^k \prod_{r=0}^k \Delta_r^{C_k^r}.$$

Далее, при $\mathbf{x}_1, \mathbf{x}_2 \in V_n$, $\mathbf{x}_1 \neq \mathbf{x}_2$, используя обозначение $\mathbf{x}_1 \mathbf{x}_2 = \mathbf{x}_1 \cap \mathbf{x}_2$, находим:

$$\begin{aligned} &\mathbf{P}\left\{\bigoplus_{J \subseteq \mathbf{x}_1} f_J = \bigoplus_{J \subseteq \mathbf{x}_2} f_J = 1\right\} = \\ &= \mathbf{P}\left\{\bigoplus_{J \subseteq \mathbf{x}_1 \mathbf{x}_2} f_J = 1, \bigoplus_{J \subseteq \mathbf{x}_1 \setminus \mathbf{x}_2} f_J = \bigoplus_{J \subseteq \mathbf{x}_2 \setminus \mathbf{x}_1} f_J = 0\right\} + \\ &+ \mathbf{P}\left\{\bigoplus_{J \subseteq \mathbf{x}_1 \mathbf{x}_2} f_J = 0, \bigoplus_{J \subseteq \mathbf{x}_1 \setminus \mathbf{x}_2} f_J = \bigoplus_{J \subseteq \mathbf{x}_2 \setminus \mathbf{x}_1} f_J = 1\right\} = \\ &= \frac{1}{8} \left(1 - \prod_{r=0}^{\|\mathbf{x}_1 \mathbf{x}_2\|} \Delta_r^{C_r^{\|\mathbf{x}_1 \mathbf{x}_2\|}}\right) \left(1 + \prod_{r=0}^{\|\mathbf{x}_1\|} \Delta_r^{C_r^{\|\mathbf{x}_1\|} - C_r^{\|\mathbf{x}_1 \mathbf{x}_2\|}}\right) \left(1 + \prod_{r=0}^{\|\mathbf{x}_2\|} \Delta_r^{C_r^{\|\mathbf{x}_2\|} - C_r^{\|\mathbf{x}_1 \mathbf{x}_2\|}}\right) + \\ &+ \frac{1}{8} \left(1 + \prod_{r=0}^{\|\mathbf{x}_1 \mathbf{x}_2\|} \Delta_r^{C_r^{\|\mathbf{x}_1 \mathbf{x}_2\|}}\right) \left(1 - \prod_{r=0}^{\|\mathbf{x}_1\|} \Delta_r^{C_r^{\|\mathbf{x}_1\|} - C_r^{\|\mathbf{x}_1 \mathbf{x}_2\|}}\right) \left(1 - \prod_{r=0}^{\|\mathbf{x}_2\|} \Delta_r^{C_r^{\|\mathbf{x}_2\|} - C_r^{\|\mathbf{x}_1 \mathbf{x}_2\|}}\right) = \\ &= \frac{1}{4} \left(1 - \prod_{r=0}^{\|\mathbf{x}_1\|} \Delta_r^{C_r^{\|\mathbf{x}_1\|}} - \prod_{r=0}^{\|\mathbf{x}_2\|} \Delta_r^{C_r^{\|\mathbf{x}_2\|}} + \prod_{r=0}^{\|\mathbf{x}_1\|} \Delta_r^{C_r^{\|\mathbf{x}_1\|} - C_r^{\|\mathbf{x}_1 \mathbf{x}_2\|}} \prod_{s=0}^{\|\mathbf{x}_2\|} \Delta_s^{C_s^{\|\mathbf{x}_2\|} - C_s^{\|\mathbf{x}_1 \mathbf{x}_2\|}}\right). \end{aligned}$$

Поэтому при $\mathbf{x}_1, \mathbf{x}_2 \in V_n$, $\mathbf{x}_1 \neq \mathbf{x}_2$,

$$\begin{aligned}
 b_{\mathbf{x}_1, \mathbf{x}_2} &= \text{cov}(f(\mathbf{x}_1), f(\mathbf{x}_2)) = \mathbf{P} \left\{ \bigoplus_{J \subseteq \mathbf{x}_1} f_J = \bigoplus_{J \subseteq \mathbf{x}_2} f_J = 1 \right\} - b_{\mathbf{x}_1} b_{\mathbf{x}_2} = \\
 &= \frac{1}{4} \left(1 - \prod_{r=0}^{\|\mathbf{x}_1\|} \Delta_r^{C_r^r} - \prod_{r=0}^{\|\mathbf{x}_2\|} \Delta_r^{C_r^r} + \prod_{r=0}^{\|\mathbf{x}_1\|} \Delta_r^{C_r^r - C_r^r} \prod_{s=0}^{\|\mathbf{x}_2\|} \Delta_s^{C_s^s - C_s^s} \right) - \\
 &\quad - \frac{1}{2} \left(1 - \prod_{r=0}^{\|\mathbf{x}_1\|} \Delta_r^{C_r^r} \right) \frac{1}{2} \left(1 - \prod_{s=0}^{\|\mathbf{x}_2\|} \Delta_s^{C_s^s} \right) = \quad (12) \\
 &= \frac{1}{4} \left(\prod_{r=0}^{\|\mathbf{x}_1\|} \Delta_r^{C_r^r - C_r^r} \prod_{s=0}^{\|\mathbf{x}_2\|} \Delta_s^{C_s^s - C_s^s} - \left(\prod_{r=0}^{\|\mathbf{x}_1\|} \Delta_r^{C_r^r} \right) \left(\prod_{s=0}^{\|\mathbf{x}_2\|} \Delta_s^{C_s^s} \right) \right).
 \end{aligned}$$

Теперь, используя общую формулу (6) и равенства (11), (12), находим:

$$\begin{aligned}
 \mathbf{D}\|f\| &= \sum_{\mathbf{x} \in V_n} b_{\mathbf{x}}(1 - b_{\mathbf{x}}) + \sum_{\mathbf{x}_1, \mathbf{x}_2 \in V_n: \mathbf{x}_1 \neq \mathbf{x}_2} b_{\mathbf{x}_1, \mathbf{x}_2} = \\
 &= \frac{1}{4} \sum_{\mathbf{x} \in V_n} \left(1 - \left(\prod_{r=0}^{\|\mathbf{x}\|} \Delta_r^{C_r^r} \right)^2 \right) + \\
 &\quad + \frac{1}{4} \sum_{\mathbf{x}_1, \mathbf{x}_2 \in V_n: \mathbf{x}_1 \neq \mathbf{x}_2} \prod_{r=0}^{\|\mathbf{x}_1\|} \Delta_r^{C_r^r - C_r^r} \prod_{s=0}^{\|\mathbf{x}_2\|} \Delta_s^{C_s^s - C_s^s} - \\
 &\quad - \frac{1}{4} \sum_{\mathbf{x}_1, \mathbf{x}_2 \in V_n: \mathbf{x}_1 \neq \mathbf{x}_2} \left(\prod_{r=0}^{\|\mathbf{x}_1\|} \Delta_r^{C_r^r} \right) \left(\prod_{s=0}^{\|\mathbf{x}_2\|} \Delta_s^{C_s^s} \right) = \\
 &= \frac{1}{4} \left(2^n - \left(\sum_{\mathbf{x} \in V_n} \prod_{r=0}^{\|\mathbf{x}\|} \Delta_r^{C_r^r} \right)^2 + \sum_{\substack{\mathbf{x}_1, \mathbf{x}_2 \in V_n: \\ \mathbf{x}_1 \neq \mathbf{x}_2}} \prod_{r=0}^{\|\mathbf{x}_1\|} \Delta_r^{C_r^r - C_r^r} \prod_{s=0}^{\|\mathbf{x}_2\|} \Delta_s^{C_s^s - C_s^s} \right).
 \end{aligned}$$

Чтобы привести подобные члены в каждой из сумм, достаточно заметить, что число векторов $\mathbf{x} \in V_n$ с $\|\mathbf{x}\| = a$ равно C_n^a , а число $N_n(a, b, c)$ таких пар $\mathbf{x}_1, \mathbf{x}_2 \in V_n$, $\mathbf{x}_1 \neq \mathbf{x}_2$, что $\|\mathbf{x}_1\| = a, \|\mathbf{x}_2\| = b$,

$\|\mathbf{x}_1\mathbf{x}_2\| = c \in \{\max\{a+b-n, 0\}, \dots, \min\{a, b\}\}$, равно

$$N_n(a, b, c) = \begin{cases} \frac{n!}{(a-c)!(b-c)!c!(n-a-b+c)!}, & \text{если } a \neq b \text{ или } a = b \neq c, \\ 0, & \text{если } a = b = c, \end{cases}$$

поэтому формулу для $\mathbf{D}\|f\|$ можно переписать в виде

$$\begin{aligned} \mathbf{D}\|f\| &= \frac{1}{4} \left(2^n - \left(\sum_{a=0}^n C_n^a \prod_{s=0}^a \Delta_s^{C_s^a} \right)^2 + \right. \\ &+ \left. \sum_{a,b=0}^n \sum_{c=\max\{a+b-n, 0\}}^{\min\{a,b\}} \frac{n! \prod_{r=0}^a \Delta_r^{C_r^a - C_r^c} \prod_{s=0}^b \Delta_s^{C_s^b - C_s^c}}{(a-c)!(b-c)!c!(n-a-b+c)!} (1 - \mathbb{I}\{a=b=c\}) \right). \end{aligned}$$

Наконец,

$$\begin{aligned} \sum_{a,b=0}^n \sum_{c=\max\{a+b-n, 0\}}^{\min\{a,b\}} \frac{n! \prod_{r=0}^a \Delta_r^{C_r^a - C_r^c} \prod_{s=0}^b \Delta_s^{C_s^b - C_s^c}}{(a-c)!(b-c)!c!(n-a-b+c)!} \mathbb{I}\{a=b=c\} = \\ = \sum_{a=0}^n \frac{n!}{a!(n-a)!} = 2^n, \end{aligned}$$

и из последних двух формул следует равенство (10).

Вторая часть утверждения теоремы следует из уже доказанного и идентичности формул (6) и (7).

Теорема доказана.

Список литературы

- [1] *Gardy D., Woods A.* And/or tree probabilities of Boolean functions // In: 2005 Intern. Conf. Analysis of Algorithms, volume AD of DMTCS Proceedings. — P. 139–146.
- [2] *Genitrini A., Gittenberger B.* No Shannon effect on probability distributions on Boolean functions induced by Boolean expressions // In: Proc. of Analysis of Algorithms, Wien, Austria, 2010. — P. 303–316.
- [3] *Lefmann H., Savický P.* Some typical properties of large and/or Boolean formulas // Random Struct. Algor. — 1997. — V. 10. — P. 337–351.

-
- [4] *Ивченко Г.И., Медведев Ю.И.* Спектр случайной булевой функции и его производящая функция // Математические вопросы криптографии. — 2011. — Т. 2. Вып. 2. — С. 41–54.
- [5] *Ивченко Г.И., Медведев Ю.И.* Стохастические булевы функции и их спектры // Математические вопросы криптографии. — 2013. — Т. 3. Вып. 3. — С. 21–34.
- [6] *Ивченко Г.И., Медведев Ю.И., Миронова В.А.* Анализ спектра симметрических булевых функций. — Математические вопросы криптографии. — 2013. — Т. 4. Вып.1. — С. 59–76.
- [7] *Ивченко Г.И., Медведев Ю.И., Миронова В.А.* Симметрические булевы функции и их метрические свойства // Математические вопросы криптографии. — 2013. — Т. 4. Вып. 4. — С. 49–63.
- [8] *Логачев О.А., Сальников А.А., Яценко В.В.* Булевы функции в теории кодирования и криптологии. — М. : МЦНМО, 2004.