Math-Net.Ru

Общероссийский математический портал

А. А. Серов, Среднее и дисперсия числа подфункций случайной булевой функции, близких к множеству аффинных функций, *Дискрет. матем.*, 2015, том 27, выпуск 3, 108–122

DOI: <https://doi.org/10.4213/dm1338>

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: 54.84.234.179

26 апреля 2023 г., 15:58:51

Среднее и дисперсия числа подфункций случайной булевой функции, близких к множеству аффинных функций

© 2015 г. А. А. Серов*

Для случайных равновероятных булевых функций изучается распределение количеств подфункций от заданного числа переменных, близких к множеству аффинных булевых функций. Показано, например, что для булевых функции от n переменных математическое ожидание числа подфункций от $s \geq 3 + \log_2 n$ переменных, расстояние Хэмминга от которых до множества аффинных функций меньше 2^{s-2} , стремится к 0 при $n \rightarrow \infty$.

Ключевые слова: случайная булева функция, подфункция, аффинные булевы функции, расстояние Хэмминга.

1. Формулировки основных результатов

Пусть $V_n = \text{GF}(2)^n$ — линейное n -мерное пространство над полем $\text{GF}(2)$, $\mathbb{F}_2^{V_n}$ и $\mathbb{A}_n$ — множества всех булевых и всех аффинных функций от n булевых переменных соответственно. Обозначим через $\rho(f, g)$ расстояние Хэмминга между булевыми функциями $f, g \in \mathbb{F}_2^{V_n}$, которое определяется как число значений аргумента $x \in V_n$, при которых $f(x) \neq g(x)$, и через $\rho(f, B) = \min\{\rho(f, g) : g \in B\}$ расстояние Хэмминга от булевой функции $f \in \mathbb{F}_2^{V_n}$ до множества $B \subseteq \mathbb{F}_2^{V_n}$. Пусть $\mathbb{F}_2^{V_n}(r) \subseteq \mathbb{F}_2^{V_n}$ — множество булевых функций, расстояние Хэмминга от которых до множества $\mathbb{A}_n$ не превосходит r (см., например, [4]).

Пусть $f = f(x_1, \dots, x_n) \in \mathbb{F}_2^{V_n}$. Элементы множества $I_n^s \subset \{1, \dots, n\}$, $|I_n^s| = s$, и его дополнения $\mathfrak{I}_n^{n-s} = \{1, \dots, n\} \setminus I_n^s$ при $s \in \{1, \dots, n-1\}$ будем обозначать через $\{i_1 < \dots < i_s\}$, $\{j_1 < \dots < j_{n-s}\}$ соответственно. Множеству I_n^s и набору констант $C_{n-s} = \{c_{j_t} \in \mathbb{F}_2, t = 1, \dots, n-s\}$ соответствует подфункция $g(f, \mathfrak{I}_n^{n-s}, C_{n-s}; y_1, \dots, y_s) = f(z_1, \dots, z_n) \in \mathbb{F}_2^D$ булевой функции $f(x_1, \dots, x_n)$, где

$$z_j = \begin{cases} c_{j_m} & \text{при } j = j_m \in \mathfrak{I}_n^{n-s}, \\ y_k & \text{при } j = i_k \in I_n^s, \end{cases} \quad j = 1, \dots, n, \quad m = 1, \dots, n-s, \quad k = 1, \dots, s \text{ и}$$

$$D = \left\{ (z_1, z_2, \dots, z_n) : z_j = \begin{cases} c_{j_m} \in C_{n-s} & \text{при } j = j_m \in \mathfrak{I}_n^{n-s}, \\ y_k \in \mathbb{F}_2 & \text{при } j = i_k \in I_n^s. \end{cases} , j \in \{1, 2, \dots, n\} \right\} —$$

область определения подфункции изоморфная V_s .

*Место работы: Математический институт им. В. А. Стеклова РАН,
e-mail: serov@mi.ras.ru

Введём индикатор

$$\chi(f, \mathfrak{S}_n^{n-s}, C_{n-s}, r) = \begin{cases} 0, & \text{если } g \notin \mathbb{F}_2^{V_s}(r), \\ 1, & \text{если } g \in \mathbb{F}_2^{V_s}(r), \end{cases}$$

где $g = g(f, \mathfrak{S}_n^{n-s}, C_{n-s}; y_1, \dots, y_s)$. Для функции $f \in \mathbb{F}_2^n$ обозначим через $\nu(f, s, r)$ число ее подфункций от s переменных, находящихся в r -окрестности множества $\mathbb{A}_s$, т.е. число таких пар $(\mathfrak{S}_n^{n-s}, C_{n-s})$, что $g(f, \mathfrak{S}_n^{n-s}, C_{n-s}; y_1, \dots, y_s) \in \mathbb{F}_2^{V_s}(r)$:

$$\nu(f, s, r) = \sum_{\substack{\{(\mathfrak{S}_n^{n-s}, C_{n-s})\}: \\ \mathfrak{S}_n^{n-s} \subset \{1, \dots, n\}, C_{n-s} \in \text{GF}(2)^{n-s}}} \chi(f, \mathfrak{S}_n^{n-s}, C_{n-s}, r). \quad (1)$$

Утверждение 1. Если f — случайная булева функция, имеющая равномерное распределение на $\mathbb{F}_2^n$, то при $r < 2^{s-2}$

$$\mathbf{E} \nu(f, s, r) = 2^{n-2^s+1} \binom{n}{s} \sum_{j=0}^r \binom{2^s}{j}. \quad (2)$$

Утверждение 2. При $r < 2^{s-2}$ справедливы грубые оценки

$$2^{n-2^s+1} \binom{n}{s} \binom{2^s}{r} \leq \mathbf{E} \nu(f, s, r) \leq 3 \cdot 2^n \binom{n}{s} \left(\frac{2}{3}\right)^{2^s-2} \quad (3)$$

и уточнённые двусторонние оценки

$$2^{n+1} C(s, r) \binom{n}{s} \leq \mathbf{E} \nu(f, s, r) \leq 2^{n+1} C(s, r+1) \binom{n}{s},$$

где $C(s, 0) = \left(\frac{1}{2}\right)^{2^s}$, $C(s, r) = \Phi\left(-\sqrt{2^{s+1} H\left(\frac{r}{2^s}\right)}\right)$, $H(x) = x \ln 2x + (1-x) \ln 2(1-x)$.

Замечание 1. При $n \rightarrow \infty$ левая часть в (3) стремится к бесконечности, если $s = s(n) \leq \log_2 n$, а правая часть стремится к 0, если $s = s(n) \geq \log_2 n + 3$. Таким образом, при $n \rightarrow \infty$ «пороговыми» являются значения s , лежащие в интервале от $[\log_2 n]$ до $[\log_2 n] + 3$.

Утверждение 3. а) При $n \geq 72$ максимумы верхней и нижней оценок $\mathbf{E} \nu(f, s, 2^{s-2} - 1)$ по s достигаются в одной из точек

$$\{t-1, t, t+1\},$$

где $t = [\log_2 \ln n + 3]$.

б) При $r < 2^{s-2}$ неравенство

$$\mathbf{E} \nu(f, s, r) < 1$$

справедливо для всех $n > 8$ при $s \geq [\log_2 n] + 5$.

Теорема 1. Пусть f — случайная булева функция, имеющая равномерное распределение на $\mathbb{F}_2^{V_n}$, тогда при $r < 2^{s-3}$ справедлива оценка

$$\mathbf{D}\nu(f, s, r) < \mathbf{E}\nu(f, s, r) + \frac{3s \cdot \binom{n}{s} \cdot 2^{2n + \frac{7}{2}s - 2}}{\pi\sqrt{\pi}} \cdot \exp\left\{\frac{-3 \cdot 2^{2s-4}}{2^s + 2}\right\} (1 + o(1)). \quad (4)$$

Замечание 2. Последнее слагаемое оценки сверху (4) дисперсии случайной величины $\nu(f, s, r)$ при $s \rightarrow \infty$ стремится к 0.

В таблице 1 представлены результаты вычислений математического ожидания $\mathbf{E}\nu(f, s, r)$, дисперсии $\mathbf{D}\nu(f, s, r)$ (точная формула представлена в доказательстве теоремы 1) и среднеквадратичного отклонения $\sqrt{\mathbf{D}\nu(f, s, r)}$ случайной величины $\nu(f, s, r)$ для различных значений параметров n , s и r .

Таблица 1

n	s	r	$\mathbf{E}\nu(f, s, r)$	$\mathbf{D}\nu(f, s, r)$	$\sqrt{\mathbf{D}\nu(f, s, r)}$
16	6	4	$3.9 \cdot 10^{-5}$	$3.9 \cdot 10^{-5}$	$6.2 \cdot 10^{-3}$
		11	53	77	8.8
		15	12787	612662	782
16	7	13	$1.1 \cdot 10^{-12}$	$1.1 \cdot 10^{-12}$	$1.0 \cdot 10^{-6}$
		26	$5.8 \cdot 10^{-3}$	$5.9 \cdot 10^{-3}$	$7.7 \cdot 10^{-2}$
		31	3.1	3.6	1.9
128	8	63	$7.8 \cdot 10^{34}$	$1.3 \cdot 10^{35}$	$3.6 \cdot 10^{17}$
128	9	127	$2.1 \cdot 10^{21}$	$2.1 \cdot 10^{21}$	$4.6 \cdot 10^{10}$
128	10	255	$1.5 \cdot 10^{-7}$	$1.5 \cdot 10^{-7}$	$3.9 \cdot 10^{-4}$
256	7	5	$2.5 \cdot 10^{60}$	$2.5 \cdot 10^{60}$	$1.6 \cdot 10^{30}$
		25	$3 \cdot 10^{78}$	$1.4 \cdot 10^{82}$	$1.2 \cdot 10^{41}$
		31	$6.3 \cdot 10^{81}$	$1.0 \cdot 10^{89}$	$3.2 \cdot 10^{44}$
256	8	56	$1.7 \cdot 10^{72}$	$1.8 \cdot 10^{72}$	$1.3 \cdot 10^{36}$
		62	$2.5 \cdot 10^{75}$	$8.1 \cdot 10^{76}$	$2.9 \cdot 10^{38}$
		63	$7.6 \cdot 10^{75}$	$8.0 \cdot 10^{77}$	$8.9 \cdot 10^{38}$
256	9	127	$4.3 \cdot 10^{62}$	$4.3 \cdot 10^{62}$	$2.1 \cdot 10^{31}$

2. Доказательства утверждений

Доказательство утверждения 1. Для любых аффинных функций $l_1, l_2 \in \mathbb{A}_s$, $l_1 \neq l_2$, расстояние $\rho(l_1, l_2) \geq 2^{s-1}$, поэтому множества $\{h \in \mathbb{F}_2^{V_s} : \rho(h, l_1) \leq r\}$ и $\{h \in \mathbb{F}_2^{V_s} : \rho(h, l_2) \leq r\}$ не содержат общих элементов, если $r < 2^{s-2}$. Так как мощность множества $\mathbb{A}_s$ равна 2^{s+1} , то при $r < 2^{s-2}$

$$\left| \mathbb{F}_2^{V_s}(r) \right| = 2^{s+1} \sum_{j=0}^r \binom{2^s}{j}.$$

Значит, при $r < 2^{s-2}$ вероятность того, что подфункция $g(f, \mathfrak{S}_n^{n-s}, C_{n-s}; y_1, \dots, y_s)$ случайной равновероятной функции $f \in \mathbb{F}_2^{V_n}$ принадлежит множеству $\mathbb{F}_2^{V_s}(r)$, равна

$$\mathbf{P} \left\{ g(f, \mathfrak{S}_n^{n-s}, C_{n-s}; y_1, \dots, y_s) \in \mathbb{F}_2^{V_s}(r) \right\} = \frac{|\mathbb{F}_2^{V_s}(r)|}{2^{2^s}} = 2^{s+1-2^s} \sum_{j=0}^r \binom{2^s}{j}. \quad (5)$$

Учитывая, что при фиксированных n, s число различных пар $(\mathfrak{S}_n^{n-s}, C_{n-s})$ есть $2^{n-s} \binom{n}{s}$ и согласно (1) математическое ожидание случайной величины $\nu(f, s, r)$ можно записать в виде суммы математических ожиданий $\chi(f, \mathfrak{S}_n^{n-s}, C_{n-s})$, получим

$$\begin{aligned} \mathbf{E}\nu(f, s, r) &= \\ &= \sum_{\left\{ \begin{array}{c} (\mathfrak{S}_n^{n-s}, C_{n-s}) : \\ \mathfrak{S}_n^{n-s} \subset \{1, \dots, n\}, C_{n-s} \in \text{GF}(2)^{n-s} \end{array} \right\}} \mathbf{E}\chi(f, \mathfrak{S}_n^{n-s}, C_{n-s}, r) = 2^{n+1-2^s} \binom{n}{s} \sum_{j=0}^r \binom{2^s}{j}. \end{aligned}$$

Утверждение 1 доказано.

Доказательство утверждения 2. Используя при $0 \leq j < 2^{s-2} - 1$ неравенства $\frac{\binom{2^s}{j}}{\binom{2^s}{j+1}} = \frac{j+1}{2^s-j} \leq \frac{2^{s-2}-1}{2^s-2^{s-2}} < \frac{1}{3}$, оценим сумму в правой части (2) при $r = 2^{s-2} - 1$:

$$\begin{aligned} \sum_{j=0}^{2^{s-2}-1} \binom{2^s}{j} &\leq \sum_{j=0}^{2^{s-2}-1} \binom{2^s}{2^{s-2}-1} \left(\frac{1}{3}\right)^{2^{s-2}-1-j} < \\ &< \binom{2^s}{2^{s-2}-1} \left(\frac{1}{1-\frac{1}{3}}\right) < \frac{3}{2} \binom{2^s}{2^{s-2}}. \end{aligned}$$

Значит, при $r < 2^{s-2}$ верхняя оценка математического ожидания случайной величины $\nu(f, s, r)$ имеет вид

$$\begin{aligned} \mathbf{E}\nu(f, s, r) &\leq \mathbf{E}\nu(f, s, 2^{s-2} - 1) = \\ &= 2^{n-2^s+1} \binom{n}{s} \sum_{j=0}^{2^{s-2}-1} \binom{2^s}{j} < 3 \cdot 2^{n-2^s} \binom{n}{s} \binom{2^s}{2^{s-2}}. \quad (6) \end{aligned}$$

Из оценки сверху биномиального коэффициента

$$\binom{2^s}{2^{s-2}} \leq \frac{2^{s2^s}}{2^{(s-2)2^{s-2}} (3 \cdot 2^{s-2})^{3 \cdot 2^{s-2}}} = \frac{2^{2^{s+1}}}{3^{3 \cdot 2^{s-2}}} = \left(\frac{4}{3^{3/4}}\right)^{2^s}$$

(неравенство $\binom{N}{k} \leq \frac{N^N}{k^k (N-k)^{N-k}}$ доказывается индукцией по N) следует, что

$$\mathbf{E}\nu(f, s, 2^{s-2} - 1) < 3 \cdot 2^n \binom{n}{s} \left(\frac{16}{27}\right)^{2^{s-2}} < 3 \cdot 2^n \binom{n}{s} \left(\frac{2}{3}\right)^{2^{s-2}}$$

и корректность (3).

Далее, согласно [3] для любого $1 \leq r < 2^s$ справедлива двусторонняя оценка

$$C(s, r) \leq \frac{1}{2^{2^s}} \sum_{j=0}^r \binom{2^s}{j} \leq C(s, r+1),$$

и, в частности,

$$C(s, 2^{s-2} - 1) \leq \frac{1}{2^{2^s}} \sum_{j=0}^{2^{s-2}-1} \binom{2^s}{j} \leq C(s, 2^{s-2}), \quad (7)$$

где монотонно возрастающие последовательности $\{C(s, r)\}_{r=0}^{2^s}$ определяются формулами $C(s, 0) = (\frac{1}{2})^{2^s}$, $C(s, 2^s) = 1 - (\frac{1}{2})^{2^s}$,

$$C(s, r) = \Phi\left(\operatorname{sgn}\left(\frac{r}{2^s} - \frac{1}{2}\right) \sqrt{2^{s+1} H\left(\frac{r}{2^s}\right)}\right), \quad (8)$$

$H(x) = x \ln 2x + (1-x) \ln 2(1-x)$, $\operatorname{sgn}(x) = x/|x|$ при $x \neq 0$ и $\operatorname{sgn}(0) = 0$. Значит, имеет место двусторонняя оценка математического ожидания

$$2^{n+1} C(s, r) \binom{n}{s} \leq \mathbf{E} \nu(f, s, r) \leq 2^{n+1} C(s, r+1) \binom{n}{s}.$$

Утверждение 2 доказано.

Доказательство утверждения 3 п. а).

Из (7), (8) и неравенств для функции стандартного нормального распределения ([5], гл. 7, § 1):

$$\frac{e^{-x^2/2}}{\sqrt{2\pi}} \left(\frac{1}{x} - \frac{1}{x^3} \right) < \Phi(-x) = 1 - \Phi(x) < \frac{e^{-x^2/2}}{\sqrt{2\pi}} \frac{1}{x}, \quad x > 0,$$

следует, что

$$\begin{aligned} \binom{n}{s} \frac{e^{-2^s H\left(\frac{2^{s-2}-1}{2^s}\right)}}{\sqrt{2^{s+2} \pi H\left(\frac{2^{s-2}-1}{2^s}\right)}} \left(1 - \frac{1}{2^{s+1} H\left(\frac{2^{s-2}-1}{2^s}\right)} \right) &\leq \\ &\leq \frac{\mathbf{E} \nu(f, s, 2^{s-2} - 1)}{2^{n+1}} \leq \binom{n}{s} \frac{e^{-2^s H\left(\frac{1}{4}\right)}}{\sqrt{2^{s+2} \pi H\left(\frac{1}{4}\right)}}. \end{aligned} \quad (9)$$

Обозначим левую часть (9) через $LowEst(n, s)$, а его правую часть через $UppEst(n, s)$.

Исследуем отношения

$$\frac{UppEst(n, s)}{UppEst(n, s+1)} = \sqrt{2} e^{2^s H\left(\frac{1}{4}\right)} \frac{s+1}{n-s} = e^{2^s H\left(\frac{1}{4}\right) + \ln(s+1) - \ln(n-s) + \frac{1}{2} \ln 2}$$

и

$$\frac{LowEst(n, s)}{LowEst(n, s+1)} = \frac{s+1}{n-s} \exp \left\{ 2^{s+1} H \left(\frac{2^{s-1}-1}{2^{s+1}} \right) - 2^s H \left(\frac{2^{s-2}-1}{2^s} \right) \right\} \cdot \sqrt{\frac{8H^3 \left(\frac{2^{s-1}-1}{2^{s+1}} \right) 2^{s+1} H \left(\frac{2^{s-2}-1}{2^s} \right) - 1}{H^3 \left(\frac{2^{s-2}-1}{2^s} \right) 2^{s+2} H \left(\frac{2^{s-1}-1}{2^{s+1}} \right) - 1}}.$$

Обозначим $\ln \frac{UppEst(n, s)}{UppEst(n, s+1)}$ через $b(n, s)$ при $n > s > 0$. Так как

$$\frac{\partial}{\partial s} (b(n, s))' = 2^s H \left(\frac{1}{4} \right) \ln 2 + \frac{1}{s+1} + \frac{1}{n-s} > 0,$$

то отношение $\frac{UppEst(n, s)}{UppEst(n, s+1)}$ строго возрастает по s при любом фиксированном n .

Найдём такое минимальное натуральное s_* при котором $b(n, s_*) > 0$. Так как $H \left(\frac{1}{4} \right) \approx 0.131$, то при $n \geq 72$

$$b(n, \log_2 \ln n + 2) = 4H \left(\frac{1}{4} \right) \ln n - \ln(n - \log_2 \ln n - 2) + \ln(\log_2 \ln n + 3) + \frac{1}{2} \ln 2 < 0,$$

$$b(n, \log_2 \ln n + 3) = 8H \left(\frac{1}{4} \right) \ln n - \ln(n - \log_2 \ln n - 3) + \ln(\log_2 \ln n + 4) + \frac{1}{2} \ln 2 > 0.$$

Значит, $s_* \in \{t-1, t, t+1\}$, где $t = \lfloor \log_2 \ln n + 3 \rfloor$.

Аналогично, обозначив $\ln \left(\frac{LowEst(n, s)}{LowEst(n, s+1)} \right)$ через $e(n, s)$ и заметив, что при $n \geq 40$

$$e(n, \log_2 \ln n + 2) < 0 \text{ и } e(n, \log_2 \ln n + 3) > 0,$$

убеждаемся в том, что минимальное натуральное s_{**} при котором $e(n, s_{**}) > 0$ принадлежит множеству $\{t-1, t, t+1\}$, где $t = \lfloor \log_2 \ln n + 3 \rfloor$.

Значит, при $n \geq 72$ максимумы верхней и нижней оценок $\mathbf{E} \nu(f, s, 2^{s-2}-1)$ достигаются в одной из точек

$$\{t-1, t, t+1\},$$

где $t = \lfloor \log_2 \ln n + 3 \rfloor$.

Утверждение 3 п. а) доказано.

Доказательство утверждения 3 п. б).

Из оценки снизу $s! > \sqrt{2\pi s} \left(\frac{s}{e}\right)^s$ (см., например, [5; с. 67]) и неравенства $\binom{n}{s} < \frac{n^s}{s!}$ следует, что

$$\binom{n}{s} < \frac{1}{\sqrt{2\pi s}} \left(\frac{ne}{s}\right)^s.$$

Значит, при $r < 2^{s-2}$

$$\mathbf{E} \nu(f, s, r) < 2^{n+1} \frac{1}{\sqrt{2\pi s}} \frac{(ne)^s}{s^s} \frac{e^{-2^s H \left(\frac{1}{4} \right)}}{\sqrt{2^{s+2} \pi H \left(\frac{1}{4} \right)}} = \exp \left\{ (n+1) \ln 2 - 2^s H \left(\frac{1}{4} \right) + \right. \\ \left. + s(\ln n - \ln s + 1) - \frac{1}{2} \left(\ln(2\pi s) + (s+2) \ln 2 + \ln \left(\pi H \left(\frac{1}{4} \right) \right) \right) \right\}.$$

Так как $\frac{x}{2} < 2^{\lceil \log_2 x \rceil}$, при $s \geq \lceil \log_2 n \rceil + 5$

$$n \ln 2 - 2^s H\left(\frac{1}{4}\right) < n \ln 2 - n 2^4 H\left(\frac{1}{4}\right) < -1.39 \cdot n$$

и максимальное по s значение $(n + \ln 2)$ функция $s(\ln n - \ln s + 1) + \ln 2$ принимает при $s = n$, то при $s \geq \lceil \log_2 n \rceil + 5$ и $n \geq 9$

$$\mathbf{E} \nu(f, s, r) < 1.$$

Утверждение 3 доказано.

Доказательство теоремы 1. Из (1) следует, что

$$\begin{aligned} \mathbf{D} \nu(f, s, r) = & \sum_{\left\{ \begin{smallmatrix} (\mathfrak{S}_n^{n-s}, C_{n-s}) : \\ \mathfrak{S}_n^{n-s} \subset \{1, \dots, n\}, C_{n-s} \in \text{GF}(2)^{n-s} \end{smallmatrix} \right\}} \mathbf{D} \chi(f, \mathfrak{S}_n^{n-s}, C_{n-s}, r) + \\ + & \sum_{\left\{ \begin{smallmatrix} (\mathfrak{S}_n^{n-s}, C_{n-s}) \neq (\tilde{\mathfrak{S}}_n^{n-s}, \tilde{C}_{n-s}) : \\ \mathfrak{S}_n^{n-s}, \tilde{\mathfrak{S}}_n^{n-s} \subset \{1, \dots, n\}, C_{n-s}, \tilde{C}_{n-s} \in \text{GF}(2)^{n-s} \end{smallmatrix} \right\}} \text{cov} \left(\chi(f, \mathfrak{S}_n^{n-s}, C_{n-s}, r), \chi(f, \tilde{\mathfrak{S}}_n^{n-s}, \tilde{C}_{n-s}, r) \right). \end{aligned} \quad (10)$$

Так как а) $f \in \mathbb{F}_2^{V_n}$ — случайная равновероятная функция, б) число подфункций от s переменных булевой функции от n переменных, совпадающее с мощностью множества $\left\{ \begin{smallmatrix} (\mathfrak{S}_n^{n-s}, C_{n-s}) : \\ \mathfrak{S}_n^{n-s} \subset \{1, \dots, n\}, C_{n-s} \in \text{GF}(2)^{n-s} \end{smallmatrix} \right\}$, равно $2^{n-s} \binom{n}{s}$ и в) для любой пары $(\mathfrak{S}_n^{n-s}, C_{n-s})$ из такого множества

$$\begin{aligned} \mathbf{D} \chi(f, \mathfrak{S}_n^{n-s}, C_{n-s}, r) &= \mathbf{E} \chi^2(f, \mathfrak{S}_n^{n-s}, C_{n-s}, r) - (\mathbf{E} \chi(f, \mathfrak{S}_n^{n-s}, C_{n-s}, r))^2 = \\ &= 2^{s+1-2^s} \sum_{j=0}^r \binom{2^s}{j} \left(1 - 2^{s+1-2^s} \sum_{j=0}^r \binom{2^s}{j} \right), \end{aligned}$$

то первое слагаемое в правой части (10) имеет вид

$$\begin{aligned} & \sum_{\left\{ \begin{smallmatrix} (\mathfrak{S}_n^{n-s}, C_{n-s}) : \\ \mathfrak{S}_n^{n-s} \subset \{1, \dots, n\}, C_{n-s} \in \text{GF}(2)^{n-s} \end{smallmatrix} \right\}} \mathbf{D} \chi(f, \mathfrak{S}_n^{n-s}, C_{n-s}, r) = \\ &= 2^{n+1-2^s} \binom{n}{s} \sum_{j=0}^r \binom{2^s}{j} \left(1 - 2^{s+1-2^s} \sum_{j=0}^r \binom{2^s}{j} \right). \end{aligned} \quad (11)$$

Ковариации индикаторов $\chi(f, \mathfrak{S}_n^{n-s}, C_{n-s}, r)$ и $\chi(f, \tilde{\mathfrak{S}}_n^{n-s}, \tilde{C}_{n-s}, r)$, входящие во второе слагаемое правой части (10) и соответствующие независимым подфункциям, равны 0. Осталось разобраться когда подфункции случайной равновероятной булевой функции, входящие в пару, зависимы, каково число таких пар и вероятность

того, что обе функции из такой пары содержатся в r окрестности множества $\mathbb{A}_s$. Тем самым мы определим второе слагаемое правой части (10).

Без ограничения общности будем считать, что $g_1 = g_1(f, \mathfrak{S}_n^{n-s}, C_{n-s}; y_1, \dots, y_s) \in \mathbb{F}_2^{D_1}$, $g_2 = g_2(f, \tilde{\mathfrak{S}}_n^{n-s}, \tilde{C}_{n-s}; \tilde{y}_1, \dots, \tilde{y}_s) \in \mathbb{F}_2^{D_2}$ — различные подфункции функции $f \in \mathbb{F}_2^{V_n}$, где

$$D_1 = \left\{ (z_1, z_2, \dots, z_n) : z_j = \begin{cases} c_{j_m} \in C_{n-s} & \text{при } j = j_m \in \mathfrak{S}_n^{n-s}, \\ y_k \in \mathbb{F}_2 & \text{при } j = i_k \in I_n^s. \end{cases}, j \in \{1, 2, \dots, n\} \right\},$$

$$D_2 = \left\{ (z_1, z_2, \dots, z_n) : z_j = \begin{cases} c_{j_m} \in \tilde{C}_{n-s} & \text{при } j = j_m \in \tilde{\mathfrak{S}}_n^{n-s}, \\ y_k \in \mathbb{F}_2 & \text{при } j = i_k \in \tilde{I}_n^s. \end{cases}, j \in \{1, 2, \dots, n\} \right\}$$

области определения функций g_1, g_2 . Пусть

$$B = \mathfrak{S}_n^{n-s} \cap \tilde{\mathfrak{S}}_n^{n-s}$$

— множество номеров переменных функции f , зафиксированных одновременно как в g_1 так и в g_2 .

Очевидно, что

$$\max\{0, n - 2s\} \leq |B| \leq n - s$$

и $|B| = 0$, если g_1, g_2 получены с помощью фиксации различных переменных функции f , что возможно только при $s > \frac{n-1}{2}$. Если $|B| > 0$ и существует переменная x_j , $j \in B$, функции f , зафиксированная противоположными значениями в подфункциях g_1, g_2 , то индикаторы $\chi(f, \mathfrak{S}_n^{n-s}, C_{n-s}, r)$, $\chi(f, \tilde{\mathfrak{S}}_n^{n-s}, \tilde{C}_{n-s}, r)$ независимы и

$$\begin{aligned} & \mathbf{P} \left\{ \chi(f, \mathfrak{S}_n^{n-s}, C_{n-s}, r) = \chi(f, \tilde{\mathfrak{S}}_n^{n-s}, \tilde{C}_{n-s}, r) = 1 \right\} = \\ & = \mathbf{P} \left\{ \chi(f, \mathfrak{S}_n^{n-s}, C_{n-s}, r) = 1 \right\} \mathbf{P} \left\{ \chi(f, \tilde{\mathfrak{S}}_n^{n-s}, \tilde{C}_{n-s}, r) = 1 \right\} = 2^{2s+2-2^{s+1}} \left(\sum_{j=0}^r \binom{2^s}{j} \right)^2. \end{aligned} \quad (12)$$

Индикаторы $\chi(f, \mathfrak{S}_n^{n-s}, C_{n-s}, r)$, $\chi(f, \tilde{\mathfrak{S}}_n^{n-s}, \tilde{C}_{n-s}, r)$ зависимы тогда и только тогда, когда $B = \emptyset$, $|B| = 0$, или когда переменные подфункций g_1 и g_2 с номерами из B зафиксированы одинаково. В таком случае при $|B| = b$ существует общая подфункция

$$w = g(f, \mathfrak{S}_n^{n-s} \cup \tilde{\mathfrak{S}}_n^{n-s}, C_{n-s} \cup \tilde{C}_{n-s}, z_1, \dots, z_d) \in \mathbb{F}_2^{W_d} \quad (13)$$

подфункций $g_1(f, \mathfrak{S}_n^{n-s}, C_{n-s}; y_1, \dots, y_s)$, $g_2(f, \tilde{\mathfrak{S}}_n^{n-s}, \tilde{C}_{n-s}; \tilde{y}_1, \dots, \tilde{y}_s) \in \mathbb{F}_2^{V_s}$, определённая на координатном подпространстве

$$W_d = \left\{ (z_1, z_2, \dots, z_n) : z_j = \begin{cases} c_{j_m} & \text{при } j = j_m \in \mathfrak{S}_n^{n-s}, \\ \tilde{c}_{j_k} & \text{при } j = j_k \in \tilde{\mathfrak{S}}_n^{n-s}, \\ y_p & \text{при } j = i_p \in \{1, 2, \dots, n\} \setminus \{\mathfrak{S}_n^{n-s} \cup \tilde{\mathfrak{S}}_n^{n-s}\}. \end{cases} \right\}$$

пространства V_n , где $d = n - (2(n - s) - b) = 2s - n + b$. Значит, число таких упорядоченных пар различных зависимых индикаторов или число упорядоченных пар $g_1, g_2 \in \mathbb{F}_2^{V_s}$, $g_1 \neq g_2$, с общей подфункцией при $|B| = b = n + d - 2s$, $B = \mathfrak{S}_n^{n-s} \cap \tilde{\mathfrak{S}}_n^{n-s}$, есть

$$2^{n-d} \binom{n}{n-s} \binom{n-s}{b} \binom{s}{n-s-b}, \quad (14)$$

так как $\binom{n}{n-s}$ — количество возможных способов выбора множества $\mathfrak{S}_n^{n-s}$ и $\binom{n-s}{b}$ — число различных вариантов выбора множества B , $\binom{s}{n-s-b}$ — число разных способов выбора множества $\{\tilde{\mathfrak{S}}_n^{n-s} \setminus B\}$, 2^{n-d} — число различных вариантов фиксации переменных с номерами из множества $\{\mathfrak{S}_n^{n-s} \cup \tilde{\mathfrak{S}}_n^{n-s}\}$, причем $d \in \{\max\{0, 2s - n\}, \dots, s\}$. Заметим, что $w = g_1 = g_2$ при $d = s$ и ковариации индикаторов, соответствующих паре одинаковых подфункций, не входят в последнюю сумму правой части (10), а также что в силу случайности и равновероятности булевой функции f на $\mathbb{F}_2^{V_n}$ совместные вероятности

$$\begin{aligned} & \mathbf{P} \left\{ g_1(f, \mathfrak{S}_n^{n-s}, C_{n-s}; y_1, \dots, y_s), g_2(f, \tilde{\mathfrak{S}}_n^{n-s}, \tilde{C}_{n-s}; \tilde{y}_1, \dots, \tilde{y}_s) \in \mathbb{F}_2^{V_s}(r) : w = \right. \\ & \left. = g(f, \mathfrak{S}_n^{n-s} \cup \tilde{\mathfrak{S}}_n^{n-s}, C_{n-s} \cup \tilde{C}_{n-s}, z_1, \dots, z_d) \in \mathbb{F}_2^{W_d} \right\} = \mathbf{P} \left\{ g_1, g_2 \in \mathbb{F}_2^{V_s}(r) : w \in \mathbb{F}_2^{W_d} \right\}, \end{aligned}$$

а значит, и ковариации $\text{cov}(\chi(f, \mathfrak{S}_n^{n-s}, C_{n-s}, r), \chi(f, \tilde{\mathfrak{S}}_n^{n-s}, \tilde{C}_{n-s}, r))$, зависят лишь от размерности координатного подпространства W_d .

Резюмируя вышесказанное, приходим к точной записи второго слагаемого в правой части (10)

$$\begin{aligned} & \sum_{d=\max\{0, 2s-n\}}^{s-1} 2^{n-d} \binom{n}{s} \binom{n-s}{n+d-2s} \binom{s}{s-d} \times \\ & \times \left(\mathbf{P} \left\{ g_1, g_2 \in \mathbb{F}_2^{V_s}(r) : w \in \mathbb{F}_2^{W_d} \right\} - \mathbf{P} \left\{ g_1 \in \mathbb{F}_2^{V_s}(r) \right\} \mathbf{P} \left\{ g_2 \in \mathbb{F}_2^{V_s}(r) \right\} \right), \quad (15) \end{aligned}$$

где g_1, g_2 и w определены выше. Вероятность события вида $\{g_1 \in \mathbb{F}_2^{V_s}(r)\}$ зависит лишь от числа переменных s в подфункции и радиуса окрестности r , определена в (5). Далее мы определим и оценим сверху совместную вероятность

$$\mathbf{P} \left\{ g_1, g_2 \in \mathbb{F}_2^{V_s}(r) : w \in \mathbb{F}_2^{W_d} \right\}.$$

Обозначим через $|_{W_d}$ ограничение булевой функции на подпространство W_d . Количество упорядоченных пар булевых функций от s переменных, совпадающих на координатном подпространстве W_d , есть

$$2^{2^s} \cdot 2^{2^s - 2^d} = \left| \left\{ g_1, g_2 \in \mathbb{F}_2^{V_s} : g_1|_{W_d} = g_2|_{W_d} = w \in \mathbb{F}_2^{W_d} \right\} \right|,$$

так как первая функция выбирается произвольно, а вторая с учётом того, что она совпадает с уже выбранной по крайней мере на $(2^s - 2^d)$ значениях аргументов.

Значит,

$$\mathbf{P} \left\{ g_1, g_2 \in \mathbb{F}_2^{V_s}(r) : w \in \mathbb{F}_2^{W_d} \right\} = \frac{\left| \left\{ g_1, g_2 \in \mathbb{F}_2^{V_s}(r) : g_1|_{W_d} = g_2|_{W_d} = w \in \mathbb{F}_2^{W_d} \right\} \right|}{2^{2^s} \cdot 2^{2^s - 2^d}}.$$

Далее, используя обозначения введённые ранее, определим мощность множества стоящего в числителе дроби, определяющую исследуемую вероятность, или, что то же самое, число таких пар различных булевых функций от s переменных, имеющих общую подфункцию от d аргументов, что обе функции лежат в r -окрестности $\mathbb{A}_s$, при $r < 2^{s-2}$.

Итак, расстояния Хэмминга от функций $g_1, g_2 \in \mathbb{F}_2^{V_s}$ с общей подфункцией $w \in \mathbb{F}_2^{W_d}$ до некоторой пары аффинных функций $l_1, l_2 \in \mathbb{A}_s$, где $\mathbb{A}_s = \{h \in \mathbb{F}_2^{V_s} : h(x_1, \dots, x_s) = \alpha_0 \oplus \alpha_1 x_1 \oplus \dots \oplus \alpha_s x_s, \alpha_0, \dots, \alpha_s \in \mathbb{F}_2\}$, зависят от расстояний между w и $l_1|_{W_d}, l_2|_{W_d}$, которые, в свою очередь, зависят от расстояния между ограничениями $l_1|_{W_d}$ и $l_2|_{W_d}$. Из определения аффинных функций следует, что при фиксированном d , произвольных $l_1, l_2 \in \mathbb{A}_s$ и W_d расстояние между ограничениями $l_1|_{W_d}$ и $l_2|_{W_d}$ имеет вид

$$\rho(l_1|_{W_d}, l_2|_{W_d}) = \begin{cases} 0, & \text{если } l_1|_{W_d} \oplus l_2|_{W_d} = 0, \\ 2^d, & \text{если } l_1|_{W_d} \oplus l_2|_{W_d} = 1, \\ 2^{d-1}, & \text{если } l_1|_{W_d} \oplus l_2|_{W_d} \neq \text{const.} \end{cases} \quad (16)$$

Очевидно, W_d — общее координатное подпространство D_1 и D_2 . Рассмотрим каждый из трёх возможных случаев, обозначенных в (16):

- (1) Пусть $U_1 = \{(l_1, l_2) : l_1|_{W_d} \oplus l_2|_{W_d} = 0, l_1, l_2 \in \mathbb{A}_s\}$ — множество упорядоченных пар аффинных функций, совпадающих на координатном подпространстве W_d . Мощность U_1 равна

$$|U_1| = 2^{d+1} \cdot (2^{s-d})^2 = 2^{2s-d+1}.$$

Обозначим через

$$Z_1(l_1, l_2, s, d, w, r) = \left\{ (g_1, g_2) \mid \rho(g_1, l_1) \leq r, \rho(g_2, l_2) \leq r, g_1, g_2 \in \mathbb{F}_2^{V_s}, \right. \\ \left. g_1|_{W_d} = g_2|_{W_d} = w, (l_1, l_2) \in U_1 \right\}$$

множество таких пар функций $g_1, g_2 \in \mathbb{F}_2^{V_s}$ с общей подфункцией w от d аргументов, что расстояния $\rho(g_1, l_1)$ и $\rho(g_2, l_2)$ не превосходят r . Сопоставим функциям g_1, g_2 величины

$$\begin{aligned} k_1 &= |\{x \in W_d \mid g_1|_{W_d}(x) \neq l_1|_{W_d}(x)\}|, \\ k_2 &= |\{x \in D_1 \setminus W_d \mid g_1|_{D_1 \setminus W_d}(x) \neq l_1|_{D_1 \setminus W_d}(x)\}|, \\ k_3 &= |\{x \in W_d \mid g_2|_{W_d}(x) \neq l_2|_{W_d}(x)\}|, \\ k_4 &= |\{x \in D_2 \setminus W_d \mid g_2|_{D_2 \setminus W_d}(x) \neq l_2|_{D_2 \setminus W_d}(x)\}|. \end{aligned}$$

Число упорядоченных пар $(g_1, g_2) \in Z_1(l_1, l_2, s, d, w, r)$ с фиксированными значениями k_1, k_2, k_3 и k_4 равно, очевидно, $C_{2^d}^{k_1} C_{2^s-2^d}^{k_2} C_{2^s-2^d}^{k_4}$. Далее,

$$\rho(g_1, l_1) = k_1 + k_2 \text{ и } \rho(g_2, l_2) = k_3 + k_4,$$

т. е. при $r < 2^{s-2}$ и $d = 2s - n + b$ условия

$$\left\{ \rho(g_1, l_1) \leq r, \rho(g_2, l_2) \leq r, g_1, g_2 \in \mathbb{F}_2^{V_s}, (l_1, l_2) \in U_1 \right\}$$

эквивалентны условиям

$$\begin{cases} 0 \leq k_1 \leq \min\{2^d, r\}, \\ 0 \leq k_2 \leq 2^s - 2^d, \\ 0 \leq k_3 \leq \min\{2^d, r\}, \\ 0 \leq k_4 \leq 2^s - 2^d, \\ k_1 + k_2 \leq r, \quad k_3 + k_4 \leq r, \\ k_1 = k_3, \end{cases} \Leftrightarrow \begin{cases} 0 \leq k_1 \leq \min\{2^d, r\}, \\ 0 \leq k_2 \leq 2^s - 2^d, \\ 0 \leq k_4 \leq 2^s - 2^d, \\ k_1 \leq r - k_2, \\ k_1 \leq r - k_4. \end{cases}$$

Значит,

$$|Z_1(l_1, l_2, s, d, w, r)| = \sum_{k_1=0}^{\min\{2^d, r\}} \binom{2^d}{k_1} \sum_{k_2=0}^{r-k_1} \binom{2^s - 2^d}{k_2} \sum_{k_4=0}^{r-k_1} \binom{2^s - 2^d}{k_4}. \quad (17)$$

- (2) Пусть $U_2 = \{(l_1, l_2) : l_1|_{W_d} \oplus l_2|_{W_d} = 1, l_1, l_2 \in \mathbb{A}_s\}$ — множество упорядоченных пар аффинных функций, противоположных на W_d . Мощность U_2 равна мощности U_1 . Обозначим через

$$Z_2(l_1, l_2, s, d, w, r) = \{(g_1, g_2) \mid \rho(g_1, l_1) \leq r, \rho(g_2, l_2) \leq r, g_1, g_2 \in \mathbb{F}_2^{V_s}, \\ g_1|_{W_d} = g_2|_{W_d} = w, (l_1, l_2) \in U_2\},$$

множество таких пар различных функций $g_1 = g_1(f, \mathfrak{S}_n^{n-s}, C_{n-s}; y_1, \dots, y_s)$, $g_2 = g_2(f, \tilde{\mathfrak{S}}_n^{n-s}, \tilde{C}_{n-s}; \tilde{y}_1, \dots, \tilde{y}_s) \in \mathbb{F}_2^{V_s}$ с общей подфункцией $w = g(f, \mathfrak{S}_n^{n-s} \cup \tilde{\mathfrak{S}}_n^{n-s}, C_{n-s} \cup \tilde{C}_{n-s}, z_1, \dots, z_d) \in \mathbb{F}_2^{W_d}$ от d аргументов, что расстояния $\rho(g_1, l_1)$ и $\rho(g_2, l_2)$ не превосходят r . Запишем систему неравенств, определяющую такое множество:

$$\begin{cases} 0 \leq k_1 \leq \min\{2^d, r\}, \\ 0 \leq k_2 \leq 2^s - 2^d, \\ 0 \leq k_3 \leq \min\{2^d, r\}, \\ 0 \leq k_4 \leq 2^s - 2^d, \\ k_1 + k_2 \leq r, \quad k_3 + k_4 \leq r, \\ k_1 = 2^d - k_3, \end{cases} \Leftrightarrow \begin{cases} 0 \leq k_1 \leq \min\{2^d, r\}, \\ 0 \leq k_2 \leq 2^s - 2^d, \\ 0 \leq k_4 \leq 2^s - 2^d, \\ 2^d + k_4 - r \leq k_1 \leq r - k_2, \end{cases}$$

где $d = 2s - n + b$.

Значит,

$$|Z_2(l_1, l_2, s, d, w, r)| = \sum_{k_1=\max\{2^d-r, 0\}}^{\min\{2^d, r\}} \binom{2^d}{k_1} \sum_{k_2=0}^{r-k_1} \binom{2^s - 2^d}{k_2} \sum_{k_4=0}^{r-2^d+k_1} \binom{2^s - 2^d}{k_4}.$$

Очевидно, что $|Z_2(l_1, l_2, s, d, w, r)| = 0$ при $r < 2^{d-1}$.

(3) Пусть

$$U_3 = \{(l_1, l_2) : l_1|_{W_d} \oplus l_2|_{W_d} \neq \text{const}, l_1, l_2 \in \mathbb{A}_s\}$$

— множество упорядоченных пар аффинных функций, отличающихся на координатном подпространстве W_d ровно в половине значений аргументов. Ясно, что мощность U_3 есть

$$|U_3| = 2^{2(s+1)} - |U_1| - |U_2| = 2^{2(s+1)} - 2^{2s-d+2}.$$

Обозначим через

$$Z_3(l_1, l_2, s, d, w, r) = \{(g_1, g_2) \mid \rho(g_1, l_1) \leq r, \rho(g_2, l_2) \leq r, g_1, g_2 \in \mathbb{F}_2^{V_s}, \\ g_1|_{W_d} = g_2|_{W_d} = w, (l_1, l_2) \in U_3\},$$

— множество пар функций $g_1, g_2 \in \mathbb{F}_2^{V_s}$ с общей подфункцией от d аргументов, расстояния от которых до соответствующих аффинных функций $(l_1, l_2) \in U_3$ не превосходят r и положим

$$m_0 = |\{x \in W_d : g_1|_{W_d}(x) \neq l_1|_{W_d}(x), l_1|_{W_d}(x) = l_2|_{W_d}(x)\}|, \\ m_1 = |\{x \in W_d : g_1|_{W_d}(x) \neq l_1|_{W_d}(x), l_1|_{W_d}(x) \neq l_2|_{W_d}(x)\}|.$$

При $s > d \geq 1$ запишем систему неравенств, эквивалентную определению множества $Z_3(l_1, l_2, s, d, w, r)$:

$$\begin{cases} 0 \leq m_0, m_1 \leq \min\{2^{d-1}, r\}, \\ 0 \leq m_0 + m_1 \leq \min\{2^d, r\}, \\ 0 \leq k_2 \leq 2^s - 2^d, \\ 0 \leq m_0 + (2^{d-1} - m_1) \leq 2^d, \\ 0 \leq k_4 \leq 2^s - 2^d, \\ m_0 + m_1 + k_2 \leq r, \\ m_0 + (2^{d-1} - m_1) + k_4 \leq r, \end{cases} \Leftrightarrow \begin{cases} 0 \leq m_0, m_1 \leq \min\{2^{d-1}, r\} \\ 0 \leq m_0 \leq \min\{2^d, r\} - m_1, \\ 0 \leq k_2 \leq 2^s - 2^d, \\ m_0 - 2^{d-1} \leq m_1 \leq 2^{d-1} + m_0, \\ 0 \leq k_4 \leq 2^s - 2^d, \\ m_1 \leq r - m_0 - k_2, \\ m_1 \geq m_0 + k_4 + 2^{d-1} - r. \end{cases}$$

Значит,

$$|Z_3(l_1, l_2, s, d, w, r)| = \sum_{m_0=0}^{\min\{2^{d-1}, r\}} \binom{2^{d-1}}{m_0} \sum_{m_1=\max\{0, m_0+2^{d-1}-r\}}^{\min\{2^{d-1}, r-m_0\}} \binom{2^{d-1}}{m_1} \times \\ \times \sum_{k_2=0}^{r-(m_0+m_1)} \binom{2^s-2^d}{k_2} \sum_{k_4=0}^{r-(m_0+2^{d-1}-m_1)} \binom{2^s-2^d}{k_4}.$$

Очевидно, что $|Z_3(l_1, l_2, s, d, w, r)| = 0$, если $r < 2^{d-2}$.

Следовательно, если подфункции $g_1 = g_1(f, \mathfrak{Z}_n^{n-s}, C_{n-s}; y_1, \dots, y_s)$, $g_2 = g_2(f, \tilde{\mathfrak{Z}}_n^{n-s}, \tilde{C}_{n-s}; \tilde{y}_1, \dots, \tilde{y}_s) \in \mathbb{F}_2^{V_s}$ имеют общую подфункцию w от d аргументов

и $r < 2^{s-2}$, то

$$\begin{aligned} \mathbf{P} \left\{ g_1, g_2 \in \mathbb{F}_2^{V_s}(r) : w \in \mathbb{F}_2^{W_d} \right\} = \\ = \frac{|U_1||Z_1(l_1, l_2, s, d, w, r)| + |U_2||Z_2(l_1, l_2, s, d, w, r)| + |U_3||Z_3(l_1, l_2, s, d, w, r)|}{2^{2^{s+1}-2^d}}. \end{aligned} \quad (18)$$

Из (10), (11) и (15) следует, что

$$\begin{aligned} D\nu(f, s, r) = 2^{n+1-2^s} \binom{n}{s} \sum_{j=0}^r \binom{2^s}{j} \left(1 - 2^{s+1-2^s} \sum_{j=0}^r \binom{2^s}{j} \right) + \\ + \sum_{d=\max\{0, 2s-n\}}^{s-1} 2^{n-d} \binom{n}{s} \binom{n-s}{n+d-2s} \binom{s}{s-d} \times \\ \times \left(\mathbf{P} \left\{ g_1, g_2 \in \mathbb{F}_2^{V_s}(r) : w \in \mathbb{F}_2^{W_d} \right\} - \left(\mathbf{P} \left\{ g_1 \in \mathbb{F}_2^{V_s}(r) \right\} \right)^2 \right). \end{aligned} \quad (19)$$

Заметим, что при фиксированных r и d из определений множеств $Z_1(l_1, l_2, s, d, w, r)$, $Z_2(l_1, l_2, s, d, w, r)$, $Z_3(l_1, l_2, s, d, w, r)$ следует, что

$$|Z_1(l_1, l_2, s, d, w, r)| \geq |Z_3(l_1, l_2, s, d, w, r)| \geq |Z_2(l_1, l_2, s, d, w, r)|$$

и, значит, при $r < 2^{s-2}$ справедлива следующая оценка вероятности того, что подфункции g_1, g_2 с общей подфункцией w лежат в r -окрестности множества $\mathbb{A}_s$:

$$\mathbf{P} \left\{ g_1, g_2 \in \mathbb{F}_2^{V_s}(r) : w \in \mathbb{F}_2^{W_d} \right\} < \frac{3 \cdot 2^{2(s+1)}}{2^{2^{s+1}-2^d}} |Z_1(l_1, l_2, s, d, w, r)|. \quad (20)$$

Оценку сверху мощности множества $Z_1(l_1, l_2, s, d, w, r)$ получим, оценив каждое слагаемое в суммах в правой части (17) максимальными входящими в них биномиальными коэффициентами и учитывая, что $2^s - 2^d \geq 2^{s-1}$, $r - k_1 \leq 2^{s-2}$:

$$\begin{aligned} |Z_1(l_1, l_2, s, d, w, r)| = \sum_{k_1=0}^{\min\{2^d, r\}} \binom{2^d}{k_1} \left(\sum_{k_2=0}^{r-k_1} \binom{2^s - 2^d}{k_2} \right)^2 < \\ < 2^{2(s-2)} \sum_{k_1=0}^{\min\{2^d, r\}} \binom{2^d}{k_1} \binom{2^s - 2^d}{r - k_1}^2. \end{aligned}$$

Кроме того, для отношений биномиальных коэффициентов справедливы цепочки неравенств при $1 \leq k_1 \leq 2^{d-1}$:

$$\frac{\binom{2^d}{k_1-1}}{\binom{2^d}{k_1}} = 1 - \frac{2^d - 2k_1 + 1}{2^d - k_1 + 1} < 1 - \frac{2(2^{d-1} - k_1)}{2^d + 1} \leq \exp \left\{ -\frac{2(2^{d-1} - k_1)}{2^d + 1} \right\}$$

и при $2^{d-1} \leq k_1 \leq 2^d - 1$:

$$\frac{\binom{2^d}{k_1+1}}{\binom{2^d}{k_1}} = \frac{2^d - k_1}{k_1 + 1} = 1 - \frac{2k_1 - 2^d + 1}{k_1 + 1} < 1 - \frac{2k_1 - 2^d}{2^d + 1} \leq \exp \left\{ -\frac{2(k_1 - 2^{d-1})}{2^d + 1} \right\}.$$

Из них при любом $0 \leq k_1 \leq 2^d$ последовательно следуют оценки

$$\begin{aligned} \binom{2^d}{k_1} &\leq \binom{2^d}{2^{d-1}} \cdot \exp \left\{ -\frac{2}{2^d + 1} \sum_{i=k_1+1}^{2^{d-1}} (2^{d-1} - i) \right\} = \\ &= \binom{2^d}{2^{d-1}} \cdot \exp \left\{ -\frac{(2^{d-1} - k_1)(2^{d-1} - k_1 - 1)}{2^d + 1} \right\} \end{aligned}$$

и

$$\begin{aligned} |Z_1(l_1, l_2)| &< 2^{2(s-2)} \binom{2^d}{2^{d-1}} \left(\binom{2^s - 2^d}{2^{s-1} - 2^{d-1}} \right)^2 (\min\{2^d, r\} + 1) \times \\ &\max_{0 \leq k_1 \leq \min\{2^d, r\}} \left\{ \exp \left\{ -\frac{(2^{d-1} - k_1)(2^{d-1} - k_1 - 1)}{2^d + 1} - 2 \frac{(2^{s-1} - 2^{d-1} - r + k_1)(2^{s-1} - 2^{d-1} - r + k_1 - 1)}{2^s - 2^d + 1} \right\} \right\}. \end{aligned} \quad (21)$$

Обозначим показатель экспоненты в правой части (21) через $A(s, d, k_1, r)$ и, выполнив элементарные преобразования, запишем его в виде

$$\begin{aligned} A(s, d, k_1, r) &= -\frac{(k_1 - 2^{d-1})(k_1 - 2^{d-1} + 1)}{2^d + 1} - \\ &- 2 \frac{(k_1 + 2^{s-1} - 2^{d-1} - r)(k_1 + 2^{s-1} - 2^{d-1} - r - 1)}{2^s - 2^d + 1}. \end{aligned}$$

Частная производная $A(s, d, k_1, r)$ по k_1 имеет вид

$$\frac{\partial}{\partial k_1} A(s, d, k_1, r) = -\frac{2k_1 - 2^d + 1}{2^d + 1} - \frac{2(2k_1 + 2^s - 2^d - 2r - 1)}{2^s - 2^d + 1} < 0.$$

Решением уравнения $\frac{\partial}{\partial k_1} A(s, d, k_1, r) = 0$ является

$$k_1^* = \frac{4(1 + 2^d)(r + 1) - (2^d + 3)(2^s - 2^d + 1)}{2(2^s + 2^d + 3)}.$$

Заметим, что $k_1^* < 0$ для любого $d \in \{0, 1, \dots, s-1\}$ при $r \leq 2^{s-3} - 1$; значит, при таких значениях d и r максимум $A(s, d, k_1, r)$ по k_1 достигается в точке $k_1 = 0$ и равен

$$A(s, d, 0, r) = -\frac{2^d - 2}{4 + 2^{2-d}} - \frac{(2^s - 2^d - 2r)(2^s - 2^d - 2r - 2)}{2(2^s - 2^d + 1)}. \quad (22)$$

Из (22) и условия $d \leq s-1$ следует, что $A(s, d, 0, r)$ принимает максимальное значение

$$\frac{-3 \cdot 2^{2s-3} - 4r(r+1) + 2^{s-1}(4r+3)}{2^s + 2} = A(s, s-1, 0, r) \quad (23)$$

при $d = s - 1$.

Из (19), (20), (21), (23) заключаем, что при $r \leq 2^{s-3} - 1$

$$\begin{aligned} \mathbf{D}\nu(f, s, r) &< 2^{n+1-2^s} \binom{n}{s} \sum_{j=0}^r \binom{2^s}{j} \left(1 - 2^{s+1-2^s} \sum_{j=0}^r \binom{2^s}{j} \right) + \\ &+ \sum_{d=\max\{0, 2s-n\}}^{s-1} 2^{n-d} \binom{n}{s} \binom{n-s}{n+d-2s} \binom{s}{s-d} \frac{3 \cdot 2^{2(s+1)}}{2^{2s} (2^{2s-2d} - 1)} \times \\ &\times 2^{2(s-2)} \binom{2^d}{2^{d-1}} \left(\binom{2^s - 2^d}{2^{s-1} - 2^{d-1}} \right)^2 (\min\{2^d, r\} + 1) e^{A(s, s-1, 0, r)}. \end{aligned}$$

Учитывая, что

$$\begin{aligned} \binom{n-s}{n+d-2s} &< 2^{n-s}, \quad \binom{s}{d} < 2^s, \\ \binom{2^d}{2^{d-1}} &= \frac{2^{2^d}}{\sqrt{\pi 2^{d-1}}} (1 + o(1)), \quad \binom{2^s - 2^d}{2^{s-1} - 2^{d-1}} = \frac{2^{2^s - 2^d}}{\sqrt{\pi (2^{s-1} - 2^{d-1})}} (1 + o(1)), \quad d \rightarrow \infty, \end{aligned}$$

получим оценку

$$\begin{aligned} \mathbf{D}\nu(f, s, r) &< \left(1 - 2^{s+1-2^s} \sum_{j=0}^r \binom{2^s}{j} \right) \mathbf{E}\nu(f, s, r) + \\ &+ \frac{3s \cdot \binom{n}{s} \cdot 2^{2n+5s-5}}{\pi \sqrt{\pi 2^{s-2} 2^{s-2}}} \exp \{A(s, s-1, 0, r)\} (1 + o(1)). \quad (24) \end{aligned}$$

Оценка сверху $A(s, s-1, 0, r)$ при $0 \leq r \leq 2^{s-3} - 1$

$$A(s, s-1, 0, r) = \frac{-(2^{s-1} - (2r+1))^2 - \frac{1}{2}(2^{s-1} - 1)^2 + \frac{3}{2}}{2^s + 2} \leq \frac{-3 \cdot 2^{2s-4}}{2^s + 2}$$

завершает доказательство теоремы 1.

Автор признателен А.М. Зубкову за внимание к работе.

Список литературы

1. Зубков А. М., Серов А. А., “Оценка числа булевых функций, имеющих аффинные приближения заданной точности”, *Дискрет. матем.*, **22**:4 (2010), 3–19.
2. Серов А.А., “Оценка числа булевых функций, имеющих квадратичные приближения заданной точности”, *Дискрет. матем.*, **24**:3 (2012), 90–107.
3. Зубков А. М., Серов А. А., “Полное доказательство универсальных неравенств для функции распределения биномиального закона”, *Теория вероятн. и ее примен.*, **57**:3 (2012), 597–602.
4. Логачев О.А., Сальников А.А., Яценко В.В., *Булевы функции в теории кодирования и криптологии*, М.: МЦНМО, 2004.
5. Феллер В., *Введение в теорию вероятностей и её приложения*, **1**, М.: Мир, 1984.

Статья поступила 17.02.2015.