УДК 519.716.32+512.547 DOI 10.17223/20710410/68/2

КРИВИЗНА НЕКОТОРЫХ КЛАССОВ БУЛЕВЫХ ФУНКЦИЙ

А. А. Панпурин

РТУ МИРЭА, г. Москва, Россия

E-mail: aa.panpurin@yandex.ru

Исследуется кривизна различных классов булевых функций, построенных с помощью суперпозиции, симметрических многочленов и бент-функций. Получаются оценки и точные значения для коэффициентов Уолша — Адамара, кривизны и нелинейности рассматриваемых классов булевых функций. Устанавливается связь кривизны и нелинейности произвольных булевых функций.

Ключевые слова: *булевы функции, бент-функции, кривизна булевой функции, нелинейность булевой функции.*

CURVATURE OF SOME CLASSES OF BOOLEAN FUNCTIONS

A. A. Panpurin

MIREA — Russian Technological University, Moscow, Russia

The curvature $\sigma(f)$ of Boolean function f is defined as the sum of the absolute values of its Walsh coefficients. In the paper, the curvature of various classes of Boolean functions constructed using superposition, symmetric polynomials and bent functions is investigated. Estimates and exact values have been obtained for the Walsh coefficients, curvature, and nonlinearity of the classes of Boolean functions under consideration. Let n be an odd number and f be a Boolean function in n variables, constructed according to the rule $f(x_1,\dots,x_n) = x_n\varphi_0(x_1,\dots,x_{n-1}) \oplus \oplus\, \bar{x}_n\varphi_1(x_1,\dots,x_{n-1})$, where φ_0,φ_1 are bent functions in $n-1$ variables. It was shown that for such a function $\sigma(f) = 2^{(3n-1)/2}$. We also examine a function of the form $f = f(x_1,\dots,x_n) = x_n x_{n-1}\varphi(x_1,\dots,x_{n-2})$ with an odd number of variables, where $n \geqslant 6$, φ is a bent function in $n-2$ variables. For this function $\sigma(f) = (2^n-4)2^{(n-2)/2} + 3\cdot 2^{n-1} - 2W_\varphi(0,\dots,0)$, where $W_\varphi(0,\dots,0)$ is the Walsh coefficient of the function φ. Moreover, an inequality is provided that demonstrates the relationship between the curvature and nonlinearity of arbitrary Boolean functions.

Keywords: *Boolean functions, bent functions, curvature of Boolean function, nonlinearity of Boolean function.*

Введение

Пусть n — натуральное число, f — булева функция от n переменных. Всюду далее $\Omega = \{0,1\}$. Коэффициент $W_f(\mathbf{a})$ Уолша — Адамара функции f определяется для каждого вектора $\mathbf{a} = (a_1, a_2, \dots, a_n) \in \Omega^n$ равенством [1]

$$W_f(\mathbf{a}) = \sum_{\mathbf{x}=(x_1,\dots,x_n)\in\Omega^n} (-1)^{f(\mathbf{x})\oplus\langle\mathbf{a},\mathbf{x}\rangle},$$

где $\langle \mathbf{a}, \mathbf{x} \rangle = a_1 x_1 \oplus \ldots \oplus a_n x_n$. Введём обозначение

$$\sigma(f) = \sum_{\mathbf{a} \in \Omega^n} |W_f(\mathbf{a})|$$

и назовём величину $\sigma(f)$ кривизной булевой функции f.

Исследованию величины $\sigma(f)$ посвящена работа [2], где получены следующие оценки, справедливые для каждой булевой функции f от n переменных:

$$2^n \leqslant \sigma(f) \leqslant 2^{3n/2}.$$

Нижняя оценка обращается в равенство тогда и только тогда, когда f — аффинная функция. Верхняя оценка обращается в равенство тогда и только тогда, когда f — бент-функция. Кроме того, в [2] показано, что среднее значение параметра $\sigma(f)$ в классе всех булевых функций от n переменных и в его подклассе из всех сбалансированных булевых функций эквивалентно при $n \to \infty$ величине

$$\sqrt{2/\pi} 2^{3n/2}.$$

В этой же работе приводятся точные значения величин $\sigma(f)$ в случае, когда f — сбалансированная функция, полученная из нормальной бент-функции методом Г. Доббертина [3]. Доказывается, что для этих функций при $n \to \infty$

$$\sigma(f) \sim 2^{3n/2}.$$

В работе [4] получено равенство для кривизны мажоритарной булевой функции $f(x_1, \ldots, x_n)$ от нечётного числа переменных:

$$\sigma(f) = \sigma(n) = 2n \binom{n-1}{(n-1)/2} \sum_{i=0}^{(n-1)/2} \frac{1}{2i+1} \binom{(n-1)/2}{i},$$

а также доказано, что при $n \to \infty$ имеет место соотношение

$$\sigma(f) = \sigma(n) \sim \frac{2}{\sqrt{\pi n}} 2^{3n/2}.$$

Формула для вычисления кривизны $\sigma(f)$ мажоритарной булевой функции $f(x_1, \ldots, x_n)$ от чётного числа переменных получена в работе [5], в которой доказано, что

$$\sigma(f) = \frac{\sigma(n+1)}{2} \sim \frac{2\sqrt{2}}{\sqrt{\pi n}} 2^{3n/2}, \quad n \to \infty.$$

В [6] рассматривается подход к классификации булевых функций на основе равенства их функций автокорреляции. Доказано, что если функции f и g лежат в одном классе рассматриваемой эквивалентности, то $\sigma(f) = \sigma(g)$.

В [7] булевы функции исследуются как точки на гиперсфере в евклидовом пространстве. В ней доказываются свойства кривизны булевой функции с точки зрения геометрии и свойств евклидова пространства. Понятие «кривизна булевой функции» впервые было введено в этой работе.

В работах [8–10] величина $\sigma(f)$ используется для установления оценок частот появлений элементов на отрезках выходных последовательностей фильтрующих и комбинирующих генераторов с функцией усложнения f. Чем меньше значение $\sigma(f)$, тем более точные оценки частот удаётся получить.

В [11] понятие кривизны расширяется на векторные булевы функции и используется для исследования свойств S-боксов.

В данной работе исследуется кривизна различных классов булевых функций, построенных с помощью суперпозиции, симметрических многочленов и бент-функций. В процессе исследований получаются точные значения для коэффициентов Уолша — Адамара, поэтому наряду с кривизной, как правило, приводятся результаты о нелинейности построенных функций. Устанавливается связь кривизны и нелинейности произвольных булевых функций.

1. Кривизна некоторых классов булевых функций

Рассмотрим кривизну классов булевых функций, полученных в результате суперпозиции. Обозначим: $\mathbf{1}^n = (1, \ldots, 1) \in \Omega^n$, $\mathbf{0}^n = (0, \ldots, 0) \in \Omega^n$; $\|\mathbf{u}\|$ — вес Хэмминга вектора $\mathbf{u}$.

Утверждение 1. Пусть $h(x_1, \ldots, x_n)$ — булева функция от n переменных, такая, что $h(x_1, \ldots, x_n) = f(x_1, \ldots, x_k) \oplus g(x_{k+1}, \ldots, x_n)$ для некоторого $k \in \{1, \ldots, n\}$. Тогда

$$\sigma(h) = \sigma(f)\,\sigma(g).$$

Доказательство. Рассмотрим коэффициент Уолша — Адамара функции $h(\mathbf{x})$ на произвольном векторе $\mathbf{u} \in \Omega^n$. Введём обозначения $\mathbf{x}' = (x_1, \ldots, x_k)$, $\mathbf{x}'' = (x_{k+1}, \ldots, x_n)$, $\mathbf{u}' = (u_1, \ldots, u_k)$, $\mathbf{u}'' = (u_{k+1}, \ldots, u_n)$. Тогда $W_h(\mathbf{u}) = W_f(\mathbf{u}')W_g(\mathbf{u}'')$ и для суммы модулей всех рассматриваемых коэффициентов справедливо соотношение

$$\sigma(h) = \sum_{\mathbf{u}\in\Omega^n} |W_h(\mathbf{u})| = \sum_{\mathbf{u}'\in\Omega^k} |W_f(\mathbf{u}')| \sum_{\mathbf{u}''\in\Omega^{n-k}} |W_g(\mathbf{u}'')| = \sigma(f)\,\sigma(g).$$

Утверждение 1 доказано. ■

Утверждение 2. Пусть $h(x_1, \ldots, x_n)$ — булева функция от n переменных, определяемая равенством

$$h(\mathbf{x}) = x_1 \ldots x_{k_1} \oplus x_{k_1+1} \ldots x_{k_1+k_2} \oplus \ldots \oplus x_{k_1+\ldots+k_{t-1}+1} \ldots x_{k_1+\ldots+k_t} \tag{1}$$

для некоторых $k_1, \ldots, k_t \in \{1, \ldots, n\}$, таких, что $k_1 + \ldots + k_t = n$. Тогда

$$\sigma(h) = (3 \cdot 2^{k_1} - 4)(3 \cdot 2^{k_2} - 4) \cdot \ldots \cdot (3 \cdot 2^{k_t} - 4). \tag{2}$$

Доказательство. Найдём кривизну функции $f(x_1, \ldots, x_k) = x_1 \ldots x_k$. Для этого рассмотрим произвольный коэффициент Уолша — Адамара функции f на векторе $\mathbf{u}$:

$$W_f(\mathbf{u}) = \sum_{\mathbf{x}\in\Omega^k} (-1)^{x_1\ldots x_k \oplus \langle \mathbf{x},\mathbf{u}\rangle} = \sum_{\mathbf{x}\in\Omega^k, \mathbf{x}\neq\mathbf{1}^k} (-1)^{\langle \mathbf{x},\mathbf{u}\rangle} - (-1)^{\|\mathbf{u}\|} = \sum_{\mathbf{x}\in\Omega^k} (-1)^{\langle \mathbf{x},\mathbf{u}\rangle} - 2\,(-1)^{\|\mathbf{u}\|}.$$

Тогда

$$W_f(\mathbf{u}) = \begin{cases} 2^k - 2, & \text{если } \mathbf{u} = \mathbf{0}^k, \\ -2\,(-1)^{\|\mathbf{u}\|}, & \text{если } \mathbf{u} \neq \mathbf{0}^k. \end{cases} \tag{3}$$

Отсюда получаем

$$\sigma(f) = \sum_{\mathbf{u}\in\Omega^k} |W_f(\mathbf{u})| = 2^k - 2 + (2^k - 1)\,2 = 3 \cdot 2^k - 4.$$

Из утверждения 1 и определения функции h следует (2). ■

Пусть $h(\mathbf{x})$ — произвольная булева функция от n переменных; $\mathrm{nl}(h)$ — её нелинейность (расстояние до класса аффинных функций). Известно, что при чётном n

$$\mathrm{nl}(h) \leqslant 2^{n-1} - 2^{n/2-1}, \tag{4}$$

а при нечётном n

$$\mathrm{nl}(h) \leqslant 2^{n-1} - 2^{(n-1)/2}. \tag{5}$$

Покажем, что данные оценки достигаются для функций из класса, определённого в утверждении 2.

Утверждение 3. Пусть $h(\mathbf{x})$ — булева функция от n переменных, определяемая равенством (1). Тогда при чётном n неравенство (4) обращается в равенство тогда и только тогда, когда $k_i = 2$ для всех $i \in \{1, \ldots, t\}$. При нечётном n оценка (5) достижима тогда и только тогда, когда $k_j = 1$ для некоторого $j \in \{1, \ldots, t\}$ и $k_i = 2$ для всех $i \neq j$.

Доказательство. Обозначим через $f_i = x_{k_1+\ldots+k_{i-1}+1} \ldots x_{k_i}$ булеву функцию от k_i переменных. Рассмотрим коэффициент Уолша — Адамара функции f_i на произвольном векторе $\mathbf{u} \in \Omega^{k_i}$. Согласно равенству (3), имеем

$$W_{f_i}(\mathbf{u}) = \begin{cases} 2^{k_i} - 2, & \text{если } \mathbf{u} = \mathbf{0}^{k_i}, \\ -2\,(-1)^{\|\mathbf{u}\|}, & \text{если } \mathbf{u} \neq \mathbf{0}^{k_i}. \end{cases}$$

Пусть n — чётное число. При $k_i = 2$ для всех $i \in \{1, \ldots, t\}$ справедливо равенство $h(\mathbf{x}) = x_1x_2 \oplus x_3x_4 \oplus \ldots \oplus x_{n-1}x_n$. Функция h является бент-функцией от n переменных [1] и $\mathrm{nl}(h) = 2^{n-1} - 2^{n/2-1}$. Покажем, что при других k_i, где $i \in \{1, \ldots, t\}$, оценка (4) недостижима. Пусть $k_i \geqslant 3$ для некоторого $i \in \{1, \ldots, t\}$, тогда $|W_{f_i}(0, \ldots, 0)| = 2^{k_i} - 2$. Пусть f' — сумма всех остальных слагаемых. Найдётся $\mathbf{u}' \in \Omega^{n-k_i}$, такой, что $|W_{f'}(\mathbf{u}')| \geqslant 2^{(n-k_i)/2}$; значит, по утверждению 1

$$\max_{\mathbf{u} \in \Omega^n} |W_h(\mathbf{u})| \geqslant (2^{k_i} - 2)2^{(n-k_i)/2} > 2^{n/2},$$

следовательно, оценка (4) не достигается. Предположим, что есть хотя бы два слагаемых степени 1. Без ограничения общности считаем, что $f_1 = x_1 \oplus x_2$, f_2 — сумма остальных слагаемых и $h = f_1 \oplus f_2$. Справедливо равенство $|W_{f_1}(1, 1)| = 4$ и найдётся $\mathbf{u}' \in \Omega^{n-2}$, такой, что $|W_{f_2}(\mathbf{u}')| \geqslant 2^{(n-2)/2}$. Тогда

$$\max_{\mathbf{u} \in \Omega^n} |W_h(\mathbf{u})| \geqslant 4 \cdot 2^{(n-2)/2} = 2^{(n+2)/2} > 2^{\frac{n}{2}},$$

а значит, вновь оценка (4) недостижима.

Пусть n — нечётное число. Покажем, что оценка достигается при $k_j = 1$ для некоторого $j \in \{1, \ldots, t\}$ и $k_i = 2$ для всех $i \neq j$. Без ограничения общности считаем, что $j = t$. Рассмотрим функцию

$$h(\mathbf{x}) = x_1x_2 \oplus x_3x_4 \oplus \ldots \oplus x_{n-2}x_{n-1} \oplus x_n.$$

Нетрудно проверить, что $\mathrm{nl}(h) = 2^{n-1} - 2^{(n-1)/2}$, а значит, неравенство (5) обращается в равенство. Покажем, что для других функций оценка недостижима. Пусть $k_i \geqslant 3$ для некоторого $i \in \{1, \ldots, t\}$. Аналогично случаю чётного n получаем

$$\max_{\mathbf{u} \in \Omega^n} |W_h(\mathbf{u})| \geqslant (2^{k_i} - 2)2^{(n-k_i)/2} > 2^{(n+1)/2}.$$

Пусть в многочлене Жегалкина функции f есть хотя бы три монома степени 1, тогда аналогично случаю чётного n проверяется, что

$$\max_{\mathbf{u}\in\Omega^n}|W_h(\mathbf{u})| \geqslant 2^3\cdot 2^{(n-3)/2} = 2^{(n+3)/2} > 2^{(n+1)/2}.$$

В обоих случаях $\max\limits_{\mathbf{u}\in\Omega^n}|W_h(\mathbf{u})| > 2^{(n+1)/2}$, следовательно, оценка (5) не достигается. ■

Покажем, что аффинные преобразования не меняют кривизну булевой функции.

Утверждение 4. Пусть $f(x_1,\ldots,x_n)$ — булева функция от n переменных; функция $g(x_1,\ldots,x_n)$ получена из f путём следующего преобразования:

$$g(\mathbf{x}) = f(\mathbf{x}A\oplus\mathbf{a})\oplus\langle\mathbf{b},\mathbf{x}\rangle\oplus c.$$

Здесь A — обратимая матрица над полем GF(2); $\mathbf{a},\mathbf{b}\in\Omega^n$; $c\in\Omega$. Тогда $\sigma(g)=\sigma(f)$.

Доказательство. Непосредственно следует из равенства [1]

$$W_g(\mathbf{u}) = (-1)^{\langle(\mathbf{b}\oplus\mathbf{u})(A^{-1})^{\mathrm{T}},\mathbf{a}\rangle\oplus c}\,W_f\big((\mathbf{b}\oplus\mathbf{u})(A^{-1})^{\mathrm{T}}\big).$$

Утверждение 4 доказано. ■

Пусть $n=2k$. Рассмотрим отображение $\Phi:\Omega^k\to\Omega^k$, обладающее следующими свойствами:

1) $\Phi(\mathbf{a})\neq\mathbf{0}^k$ для всех $\mathbf{a}\in\Omega^k$;
2) $\Phi(\mathbf{b})=\Phi(\widehat{\mathbf{b}})=\mathbf{c}$ для некоторых различных элементов $\mathbf{b},\widehat{\mathbf{b}}\in\Omega^k$;
3) отображение $\Phi':\Omega^k\backslash\{\mathbf{b},\widehat{\mathbf{b}}\}\to\Omega^k\backslash\{\mathbf{0}^k,\mathbf{c}\}$, определяемое равенством $\Phi'(\mathbf{x})=\Phi(\mathbf{x})$ для всех $\mathbf{x}\in\Omega^k\setminus\{\mathbf{b},\widehat{\mathbf{b}}\}$, инъективно.

В работе [11] исследована функция $f_\Phi(\mathbf{x},\mathbf{y})=\langle\Phi(\mathbf{x}),\mathbf{y}\rangle$, $\mathbf{x},\mathbf{y}\in\Omega^k$. Рассмотрим усложнение этой функции, прибавив к ней произвольную булеву функцию $h(\mathbf{x})$ от k переменных. В итоге получим конструкцию Елисеева — Мэйорана — МакФарланда [1]. Изучим функцию

$$f_\Phi(\mathbf{x},\mathbf{y}) = \langle\Phi(\mathbf{x}),\mathbf{y}\rangle\oplus h(\mathbf{x}),\ \ \mathbf{x},\mathbf{y}\in\Omega^k. \tag{6}$$

Утверждение 5. Пусть функция $f_\Phi(\mathbf{x},\mathbf{y})$ задана формулой (6). Тогда f_Φ — сбалансированная функция и

$$\sigma(f_\Phi) = 2^{3n/2}-2^n.$$

Доказательство. Коэффициент Уолша — Адамара функции $f_\Phi(\mathbf{x},\mathbf{y})$, соответствующий вектору $(\mathbf{v},\mathbf{w})$, где $\mathbf{v},\mathbf{w}\in\Omega^k$, равен

$$W_{f_\Phi}(\mathbf{v},\mathbf{w}) = \sum_{(\mathbf{x},\mathbf{y})\in\Omega^n}(-1)^{f_\Phi(\mathbf{x},\mathbf{y})\oplus\langle(\mathbf{x},\mathbf{y}),(\mathbf{v},\mathbf{w})\rangle} = \sum_{\mathbf{x}\in\Omega^k}(-1)^{h(\mathbf{x})\oplus\langle\mathbf{x},\mathbf{v}\rangle}\sum_{\mathbf{y}\in\Omega^k}(-1)^{\langle\mathbf{y},\Phi(\mathbf{x})\oplus\mathbf{w}\rangle}.$$

Заметим, что

$$\sum_{\mathbf{y}\in\Omega^k}(-1)^{\langle\mathbf{y},\Phi(\mathbf{x})\oplus\mathbf{w}\rangle} = \begin{cases}0, & \text{если } \Phi(\mathbf{x})\oplus\mathbf{w}\neq\mathbf{0}^k,\\ 2^k, & \text{если } \Phi(\mathbf{x})\oplus\mathbf{w}=\mathbf{0}^k.\end{cases}$$

Значит,

$$W_{f_\Phi}(\mathbf{v},\mathbf{w}) = 2^k\sum_{\mathbf{x}\in\Phi^{-1}(\mathbf{w})}(-1)^{h(\mathbf{x})\oplus\langle\mathbf{x},\mathbf{v}\rangle},$$

где $\Phi^{-1}(\mathbf{w})$ — полный прообраз вектора $\mathbf{w}$ при отображении Φ. Следовательно, получаем

$$W_{f_\Phi}(\mathbf{v},\mathbf{w}) = \begin{cases} 2^k(-1)^{\langle \mathbf{v},\Phi^{-1}(\mathbf{w})\rangle \oplus h(\Phi^{-1}(\mathbf{w}))}, & \text{если } \mathbf{w} \notin \{\mathbf{0}^k, \mathbf{c}\}, \\ 0, & \text{если } \mathbf{w} = \mathbf{0}^k, \\ 2^k((-1)^{\langle \mathbf{v},\mathbf{b}\rangle \oplus h(\mathbf{b})} + (-1)^{\langle \mathbf{v},\widehat{\mathbf{b}}\rangle \oplus h(\widehat{\mathbf{b}})}), & \text{если } \mathbf{w} = \mathbf{c}. \end{cases}$$

Так как $W_{f_\Phi}(\mathbf{0}) = 0$, то функция f_Φ сбалансированная [1].

Рассмотрим, при каких векторах $\mathbf{v}$ выражение $(-1)^{\langle \mathbf{v},\mathbf{b}\rangle \oplus h(\mathbf{b})} + (-1)^{\langle \mathbf{v},\widehat{\mathbf{b}}\rangle \oplus h(\widehat{\mathbf{b}})}$ не равно 0, то есть $\langle \mathbf{v},\mathbf{b}\rangle \oplus h(\mathbf{b}) = \langle \mathbf{v},\widehat{\mathbf{b}}\rangle \oplus h(\widehat{\mathbf{b}})$:

1) если $h(\mathbf{b}) \oplus h(\widehat{\mathbf{b}}) = 0$, то $\langle \mathbf{v}, \mathbf{b} \oplus \widehat{\mathbf{b}}\rangle = 0$ — данное уравнение относительно $\mathbf{v}$ имеет 2^{k-1} различных решений;
2) если $h(\mathbf{b}) \oplus h(\widehat{\mathbf{b}}) = 1$, то $\langle \mathbf{v}, \mathbf{b} \oplus \widehat{\mathbf{b}}\rangle = 1$ — данное уравнение относительно $\mathbf{v}$ также имеет 2^{k-1} различных решений.

Значит,

$$\sigma(f_\Phi) = \sum_{(\mathbf{v},\mathbf{w}) \in \Omega^{2k}} |W_{f_\Phi}(\mathbf{v},\mathbf{w})| = 2^k \cdot 2^k\,(2^k - 2) + 2^{k+1} \cdot 2^{k-1} = 2^{3k} - 2^{2k} = 2^{3n/2} - 2^n.$$

Утверждение 5 доказано. ■

Из доказательства утверждения 5 следует, что для булевой функции $f_\Phi(\mathbf{x},\mathbf{y})$ справедливо равенство

$$\mathrm{nl}(f_\Phi) = 2^{n-1} - 2^{n/2}.$$

Утверждение 6. Пусть $n \geqslant 3$, $f(x_1,\ldots,x_n) = \sigma_{n-1}(x_1,\ldots,x_n)$ — элементарный симметрический многочлен степени $n-1$ от n переменных, определяемый равенством $\sigma_{n-1}(x_1,\ldots,x_n) = \bigoplus\limits_{1 \leqslant i_1 < \ldots < i_{n-1} \leqslant n} x_{i_1} x_{i_2} \ldots x_{i_{n-1}}$. Тогда
при чётном n

$$\sigma(f) = 2^n - 4n + 2n\binom{n}{n/2},$$

а при нечётном n

$$\sigma(f) = 2^n - 4n - 4 + 4n\binom{n-1}{(n-1)/2}.$$

Доказательство. Рассмотрим коэффициент Уолша — Адамара $W_f(\mathbf{a})$ функции $f(\mathbf{x})$ на произвольном векторе $\mathbf{a}$. Разобьём множество Ω^n на подмножества: Ω_1 — множество векторов $\mathbf{x}$, у которых не менее двух координат нулевые; Ω_2 — множество векторов $\mathbf{x}$, у которых ровно одна нулевая координата; $\Omega_3 = \{\mathbf{1}^n\}$.

Нетрудно видеть, что

$$f(\mathbf{x}) = \begin{cases} 0, & \text{если } \mathbf{x} \in \Omega_1, \\ 1, & \text{если } \mathbf{x} \in \Omega_2, \\ n \bmod 2, & \text{если } \mathbf{x} \in \Omega_3. \end{cases}$$

Тогда

$$W_f(\mathbf{a}) = \sum_{\mathbf{x} \in \Omega_1} (-1)^{\langle \mathbf{a},\mathbf{x}\rangle} + \sum_{\mathbf{x} \in \Omega_2} (-1)^{1 \oplus \langle \mathbf{a},\mathbf{x}\rangle} + \sum_{\mathbf{x} \in \Omega_3} (-1)^{n \bmod 2 \oplus \langle \mathbf{a},\mathbf{x}\rangle}.$$

Используя равенство $\Omega_1 = (\Omega^n \setminus \Omega_2) \cup (\Omega^n \setminus \Omega_3)$, получим

$$W_f(\mathbf{a}) = \sum_{\mathbf{x} \in \Omega^n} (-1)^{\langle \mathbf{a},\mathbf{x}\rangle} - 2\sum_{\mathbf{x} \in \Omega_2} (-1)^{\langle \mathbf{a},\mathbf{x}\rangle} - \sum_{\mathbf{x} \in \Omega_3} (-1)^{\langle \mathbf{a},\mathbf{x}\rangle} + \sum_{\mathbf{x} \in \Omega_3} (-1)^{n \oplus \langle \mathbf{a},\mathbf{x}\rangle}.$$

Заметим, что

$$\sum_{\mathbf{x}\in\Omega^n}(-1)^{\langle\mathbf{a},\mathbf{x}\rangle}=\begin{cases}0, & \text{если } \mathbf{a}\neq\mathbf{0}^n,\\ 2^n, & \text{если } \mathbf{a}=\mathbf{0}^n.\end{cases}$$

Значит,

$$W_f(\mathbf{a})=2^n\delta_{\mathbf{a},\mathbf{0}^n}-2\sum_{\mathbf{x}\in\Omega_2}(-1)^{\langle\mathbf{a},\mathbf{x}\rangle}+(-1)^{n\oplus\|\mathbf{a}\|}-(-1)^{\|\mathbf{a}\|},$$

где $\delta_{\mathbf{a},\mathbf{0}^n}$ — символ Кронекера, определённый равенствами

$$\delta_{\mathbf{a},\mathbf{0}^n}=\begin{cases}0, & \text{если } \mathbf{a}\neq\mathbf{0}^n,\\ 1, & \text{если } \mathbf{a}=\mathbf{0}^n.\end{cases}$$

Верно равенство

$$\sum_{\mathbf{x}\in\Omega_2}(-1)^{\langle\mathbf{a},\mathbf{x}\rangle}=\|\mathbf{a}\|(-1)^{\|\mathbf{a}\|+1}+(n-\|\mathbf{a}\|)(-1)^{\|\mathbf{a}\|},$$

и коэффициенты Уолша — Адамара функции f принимают следующий вид:

$$W_f(\mathbf{a})=2^n\delta_{\mathbf{a},\mathbf{0}^n}+(-1)^{\|\mathbf{a}\|}(4\|\mathbf{a}\|-2n-1+(-1)^n).$$

Следовательно,

$$|W_f(\mathbf{a})|=\begin{cases}2^n-2n-1+(-1)^n, & \text{если } \mathbf{a}=\mathbf{0}^n,\\ \big|\,4\|\mathbf{a}\|-2n-1+(-1)^n\big|, & \text{если } \mathbf{a}\neq\mathbf{0}^n.\end{cases}\tag{7}$$

Тогда

$$\sigma(f)=\sum_{\mathbf{a}\in\Omega^n}|W_{\sigma_{n-1}}(\mathbf{a})|=|W_{\sigma_{n-1}}(\mathbf{0})|+\sum_{\mathbf{a}\in\Omega^n\setminus\{\mathbf{0}^n\}}|W_{\sigma_{n-1}}(\mathbf{a})|=$$
$$=2^n-2n-1+(-1)^n+\sum_{\mathbf{a}\in\Omega^n\setminus\{\mathbf{0}^n\}}\big|\,4\|\mathbf{a}\|-2n-1+(-1)^n\big|.$$

Исходя из того, что в множестве Ω^n векторов веса k ровно $\binom{n}{k}$, получаем

$$\sigma(f)=2^n-2n-1+(-1)^n+\sum_{k=1}^{n}\binom{n}{k}|4k-2n-1+(-1)^n|,$$

что при чётных n принимает вид

$$\sigma(f)=2^n-4n+2n\binom{n}{n/2},$$

а при нечётных —

$$\sigma(f)=2^n-4n-4+4n\binom{n-1}{(n-1)/2}.$$

Утверждение 6 доказано. ■

Следствие 1. Пусть $f(x_1,\ldots,x_n)=\sigma_{n-1}(x_1,\ldots,x_n)$, $n\geqslant 4$. Тогда

$$\mathrm{nl}(f)=n+(1-(-1)^n)/2.$$

Доказательство. Покажем, что $\max\limits_{\mathbf{a}\in\Omega^n}|W_f(\mathbf{a})| = |W_f(\mathbf{0}^n)|$. Исходя из равенств (7), $|W_f(\mathbf{a})| = \big|\,4\|\mathbf{a}\| - 2n - 1 + (-1)^n\big|$ при $\mathbf{a} \neq \mathbf{0}^n$. Так как $1 \leqslant \|\mathbf{a}\| \leqslant n$ и $n \geqslant 4$, то

$$0 \leqslant \big|\,4\|\mathbf{a}\| - 2n - 1 + (-1)^n\big| \leqslant 2n - 1 + (-1)^n,$$

а значит, $\max\limits_{\mathbf{a}\in\Omega^n\setminus\{\mathbf{0}^n\}}|W_f(\mathbf{a})| \leqslant 2n - 1 + (-1)^n$. Но $|W_f(\mathbf{0}^n)| = 2^n - 2n - 1 + (-1)^n$ и при $n \geqslant 2$ справедливо неравенство

$$2^n - 2n - 1 + (-1)^n \geqslant 2n - 1 + (-1)^n,$$

следовательно, $|W_f(\mathbf{0}^n)| \geqslant \max\limits_{\mathbf{a}\in\Omega^n\setminus\{\mathbf{0}^n\}}|W_f(\mathbf{a})|$. Тогда

$$\mathrm{nl}(f) = 2^{n-1} - \frac{1}{2}\big(2^n - 2n - 1 + (-1)^n\big) = n + \frac{1-(-1)^n}{2}.$$

Следствие 1 доказано. ■

2. Булевы функции, полученные из бент-функций

Утверждение 7. Пусть n — чётное число, $n \geqslant 4$, $f(x_1,\ldots,x_n)$ — булева функция от n переменных, задаваемая равенством

$$f(x_1,\ldots,x_n) = \sigma_{n-1}(x_1,\ldots,x_n) \oplus \varphi(x_1,\ldots,x_n),$$

где $\varphi(x_1,\ldots,x_n)$ — бент-функция. Тогда

$$2^{3n/2} - n2^{n+1} \leqslant \sigma(f) \leqslant 2^{3n/2}. \tag{8}$$

Доказательство. Рассмотрим коэффициент Уолша — Адамара $W_f(\mathbf{a})$ функции $f(\mathbf{x})$. Используя обозначения из доказательства утверждения 6, запишем

$$W_f(\mathbf{a}) = \sum_{\mathbf{x}\in\Omega_1}(-1)^{\varphi(\mathbf{x})\oplus\langle\mathbf{a},\mathbf{x}\rangle} + \sum_{\mathbf{x}\in\Omega_2}(-1)^{1\oplus\varphi(\mathbf{x})\oplus\langle\mathbf{a},\mathbf{x}\rangle} + \sum_{\mathbf{x}\in\Omega_3}(-1)^{\varphi(\mathbf{x})\oplus\langle\mathbf{a},\mathbf{x}\rangle}.$$

Следовательно,

$$W_f(\mathbf{a}) = \sum_{\mathbf{x}\in\Omega^n}(-1)^{\varphi(\mathbf{x})\oplus\langle\mathbf{a},\mathbf{x}\rangle} - 2\sum_{\mathbf{x}\in\Omega_2}(-1)^{\varphi(\mathbf{x})\oplus\langle\mathbf{a},\mathbf{x}\rangle} + (-1)^{\varphi(\mathbf{1})+\|\mathbf{a}\|} - (-1)^{\varphi(\mathbf{1})+\|\mathbf{a}\|},$$

а значит,

$$W_f(\mathbf{a}) = W_\varphi(\mathbf{a}) - 2\sum_{\mathbf{x}\in\Omega_2}(-1)^{\varphi(\mathbf{x})\oplus\langle\mathbf{a},\mathbf{x}\rangle}.$$

Так как $\varphi(\mathbf{x})$ — бент-функция, то $W_\varphi(\mathbf{a}) = \pm 2^{n/2}$. Тогда

$$2^{n/2} - 2n \leqslant |W_f(\mathbf{a})| \leqslant 2^{n/2} + 2n;$$

отсюда следует (8). ■

Теорема 1. Пусть n — нечетное число, $f(x_1,\ldots,x_n)$ — булева функция от n переменных, определяемая равенством

$$f(x_1,\ldots,x_n) = x_n\varphi_0(x_1,\ldots,x_{n-1}) \oplus \overline{x}_n\varphi_1(x_1,\ldots,x_{n-1}),$$

где $\varphi_0(x_1,\ldots,x_{n-1})$, $\varphi_1(x_1,\ldots,x_{n-1})$ — бент-функции. Тогда $\sigma(f) = 2^{(3n-1)/2}$.

Доказательство. Рассмотрим коэффициент Уолша — Адамара функции $f(\mathbf{x})$, соответствующий вектору $\mathbf{a}$:

$$W_f(\mathbf{a}) = \sum_{\mathbf{x}\in\Omega^n} (-1)^{x_n\varphi_0(x_1,\ldots,x_{n-1})\oplus\overline{x}_n\varphi_1(x_1,\ldots,x_{n-1})\oplus\langle\mathbf{x},\mathbf{a}\rangle}.$$

Введём следующие обозначения: $\mathbf{x}' = (x_1,\ldots,x_{n-1})$; $\mathbf{a}' = (a_1,\ldots,a_{n-1})$. Тогда

$$W_f(\mathbf{a}) = \sum_{\mathbf{x}\in\Omega^n, x_n=1} (-1)^{\varphi_0(\mathbf{x}')\oplus\langle\mathbf{x}',\mathbf{a}'\rangle\oplus a_n} + \sum_{\mathbf{x}\in\Omega^n, x_n=0} (-1)^{\varphi_1(\mathbf{x}')\oplus\langle\mathbf{x}',\mathbf{a}'\rangle}.$$

Следовательно,

$$W_f(\mathbf{a}) = (-1)^{a_n} W_{\varphi_0}(\mathbf{a}') + W_{\varphi_1}(\mathbf{a}').$$

Так как $\varphi_0(\mathbf{x}'), \varphi_1(\mathbf{x}')$ — бент-функции, то $W_f(\mathbf{a}) \in \{0, \pm 2^{(n+1)/2}\}$. Введём обозначения: $\mathbf{a}_1 = (\underbrace{a_1,\ldots,a_{n-1}}_{\mathbf{a}'}, 0)$; $\mathbf{a}_2 = (\underbrace{a_1,\ldots,a_{n-1}}_{\mathbf{a}'}, 1)$. Тогда

$$W_f(\mathbf{a}_1) = W_{\varphi_0}(\mathbf{a}') + W_{\varphi_1}(\mathbf{a}'), \quad W_f(\mathbf{a}_2) = -W_{\varphi_0}(\mathbf{a}') + W_{\varphi_1}(\mathbf{a}').$$

Возможны следующие варианты:

1) $W_f(\mathbf{a}_1) = 0$, $|W_f(\mathbf{a}_2)| = 2^{(n+1)/2}$;
2) $W_f(\mathbf{a}_2) = 0$, $|W_f(\mathbf{a}_1)| = 2^{(n+1)/2}$.

Таким образом, все векторы из Ω^n разбиваются на пары и справедливо соотношение

$$\sigma(f) = \sum_{\mathbf{a}\in\Omega^n} |W_f(\mathbf{a})| = 2^{n-1}(2^{(n+1)/2}) = 2^{(3n-1)/2}.$$

Теорема 1 доказана. ■

Из доказательства следует, что f сбалансирована тогда и только тогда, когда $W_{\varphi_0}(\mathbf{0}^{n-1}) + W_{\varphi_1}(\mathbf{0}^{n-1}) = 0$, то есть, учитывая равенства $\|\varphi_0\| = 2^{n-2} - W_{\varphi_0}(\mathbf{0}^{n-1})/2$ и $\|\varphi_1\| = 2^{n-2} - W_{\varphi_1}(\mathbf{0}^{n-1})/2$, φ_0 и φ_1 — бент-функции разного веса. При этом $\mathrm{nl}(f) = 2^{n-1} - 2^{(n-1)/2}$

Теорема 2. Пусть n — чётное число, $n \geqslant 6$, $f(x_1,\ldots,x_n)$ — булева функция от n переменных, определяемая равенством

$$f(x_1,\ldots,x_n) = x_n x_{n-1}\varphi(x_1,\ldots,x_{n-2}),$$

где $\varphi(x_1,\ldots,x_{n-2})$ — бент-функция. Тогда

$$\sigma(f) = (2^n - 4)\,2^{(n-2)/2} + 3\cdot 2^{n-1} - 2\,W_\varphi(\mathbf{0}^{n-2}).$$

Доказательство. Рассмотрим коэффициент Уолша — Адамара функции $f(\mathbf{x})$, соответствующий вектору $\mathbf{a} = (a_1,\ldots,a_{n-2},a_{n-1},a_n)$. Разобьём множество Ω^n на следующие подмножества: Ω_1 — множество векторов $\mathbf{x}$, для которых $x_{n-1} = 0$, $x_n = 0$; Ω_2 — множество векторов $\mathbf{x}$, для которых $x_{n-1} = 0$, $x_n = 1$; Ω_3 — множество векторов $\mathbf{x}$, для которых $x_{n-1} = 1$, $x_n = 0$; Ω_4 — множество векторов $\mathbf{x}$, для которых $x_{n-1} = 1$, $x_n = 1$. Введём обозначения: $\mathbf{x}' = (x_1,\ldots,x_{n-2})$; $\mathbf{a}' = (a_1,\ldots,a_{n-2})$. Тогда

$$W_f(\mathbf{a}) = \sum_{\mathbf{x}\in\Omega_1} (-1)^{\langle\mathbf{x}',\mathbf{a}'\rangle} + \sum_{\mathbf{x}\in\Omega_2} (-1)^{\langle\mathbf{x}',\mathbf{a}'\rangle\oplus a_n} + \sum_{\mathbf{x}\in\Omega_3} (-1)^{\langle\mathbf{x}',\mathbf{a}'\rangle\oplus a_{n-1}} + \sum_{\mathbf{x}\in\Omega_4} (-1)^{\varphi(\mathbf{x}')\oplus\langle\mathbf{x}',\mathbf{a}'\rangle\oplus a_n\oplus a_{n-1}}.$$

Если $\mathbf{a}' \neq \mathbf{0}^{n-2}$, то $\sum\limits_{\mathbf{x}' \in \Omega^{n-2}} (-1)^{\langle \mathbf{x}', \mathbf{a}' \rangle} = 0$. Тогда $W_f(\mathbf{a}) = (-1)^{a_n \oplus a_{n-1}} W_\varphi(\mathbf{a}')$, а значит, так как $\varphi(\mathbf{x}')$ — бент-функция, верно равенство $|W_f(\mathbf{a})| = |W_\varphi(\mathbf{a}')| = 2^{(n-2)/2}$. Если $\mathbf{a}' = \mathbf{0}^{n-2}$, то $\sum\limits_{\mathbf{x}' \in \Omega^{n-2}} (-1)^{\langle \mathbf{x}', \mathbf{a}' \rangle} = 2^{n-2}$ и справедливо равенство

$$W_f(\mathbf{a}) = 2^{n-2}((-1)^{a_{n-1}} + (-1)^{a_n} + 1) + (-1)^{a_{n-1} \oplus a_n} W_\varphi(\mathbf{a}').$$

Возможны следующие варианты:

1) если $\mathbf{a} = (0, \ldots, 0, 0)$, то $W_f(\mathbf{a}) = 3 \cdot 2^{n-2} + W_\varphi(\mathbf{0}^{n-2})$;
2) если $\mathbf{a} = (0, \ldots, 0, 1)$, то $W_f(\mathbf{a}) = 2^{n-2} - W_\varphi(\mathbf{0}^{n-2})$;
3) если $\mathbf{a} = (0, \ldots, 1, 0)$, то $W_f(\mathbf{a}) = 2^{n-2} - W_\varphi(\mathbf{0}^{n-2})$;
4) если $\mathbf{a} = (0, \ldots, 1, 1)$, то $W_f(\mathbf{a}) = -2^{n-2} + W_\varphi(\mathbf{0}^{n-2})$.

Если $W_\varphi(\mathbf{0}^{n-2}) = 2^{(n-2)/2}$, то

$$\sum_{\mathbf{a} \in \Omega^n, \mathbf{a}' = \mathbf{0}^{n-2}} |W_f(\mathbf{a})| = 6 \cdot 2^{n-2} - 2 \cdot 2^{(n-2)/2} = 3 \cdot 2^{n-1} - 2\, W_\varphi(\mathbf{0}^{n-2}).$$

Если $W_\varphi(\mathbf{0}^{n-2}) = -2^{(n-2)/2}$, то

$$\sum_{\mathbf{a} \in \Omega^n, \mathbf{a}' = \mathbf{0}^{n-2}} |W_f(\mathbf{a})| = 6 \cdot 2^{n-2} + 2 \cdot 2^{(n-2)/2} = 3 \cdot 2^{n-1} - 2\, W_\varphi(\mathbf{0}^{n-2}).$$

Таким образом, получаем

$$\sigma(f) = \sum_{\mathbf{a} \in \Omega^n} |W_f(\mathbf{a})| = \sum_{\mathbf{a} \in \Omega^n, \mathbf{a}' \neq \mathbf{0}^{n-2}} |W_f(\mathbf{a})| + \sum_{\mathbf{a} \in \Omega^n, \mathbf{a}' = \mathbf{0}^{n-2}} |W_f(\mathbf{a})| =$$
$$= (2^n - 4) 2^{(n-2)/2} + 3 \cdot 2^{n-1} - 2\, W_\varphi(\mathbf{0}^{n-2}).$$

Теорема 2 доказана. ■

В работе [2] изучена функция

$$f(x_1, \ldots, x_n) = x_1 x_2 \ldots x_{n-1} \oplus \varphi(x_1, \ldots, x_{n-2}) \oplus x_n,$$

где $\varphi(x_1, \ldots, x_{n-2})$ — бент-функция от $n-2$ переменных; n — чётное число. Рассмотрим некоторое изменение данной функции и исследуем полученный класс.

Утверждение 8. Пусть n — чётное число, $n \geqslant 4$, $f(x_1, \ldots, x_n)$ — булева функция от n переменных, определяемая равенством

$$f(x_1, \ldots, x_n) = x_1 x_2 \ldots x_{n-2} \oplus \varphi(x_1, \ldots, x_{n-2}) \oplus x_{n-1} \oplus x_n,$$

где $\varphi(x_1, \ldots, x_{n-2})$ — бент-функция. Тогда $\sigma(f) = 2^{(3n-2)/2} - 2^{(n+4)/2}$.

Доказательство. Рассмотрим коэффициент Уолша — Адамара функции $f(\mathbf{x})$, соответствующий вектору $\mathbf{a}$. Заметим, что если $a_n = 0$ или $a_{n-1} = 0$, то $W_f(\mathbf{a}) = 0$, поэтому пусть $\mathbf{a} = (a_1, \ldots, a_{n-2}, 1, 1)$. Введём обозначения: $\mathbf{a}' = (a_1, \ldots, a_{n-2})$; $\mathbf{x}' = (x_1, \ldots, x_{n-2})$. Тогда

$$W_f(\mathbf{a}', 1, 1) = \sum_{\mathbf{x} \in \Omega^n} (-1)^{x_1 x_2 \ldots x_{n-2} \oplus \varphi(x_1, \ldots, x_{n-2}) \oplus \langle \mathbf{a}', \mathbf{x}' \rangle} =$$

$$= 4 \left(\sum_{\mathbf{x}' \in \Omega^{n-2} \setminus \{\mathbf{1}^{n-2}\}} (-1)^{\varphi(\mathbf{x}') \oplus \langle \mathbf{a}', \mathbf{x}' \rangle} - (-1)^{\varphi(\mathbf{1}^{n-2}) \oplus \|\mathbf{a}'\|} \right) = 4\, W_\varphi(\mathbf{a}') - 8(-1)^{\varphi(\mathbf{1}^{n-2}) \oplus \|\mathbf{a}'\|}.$$

Рассмотрим бент-функцию $\tilde{\varphi}(\mathbf{x}')$, дуальную к $\varphi(\mathbf{x}')$; для неё справедливо равенство

$$W_\varphi(\mathbf{a}') = (-1)^{\tilde{\varphi}(\mathbf{a}')} 2^{(n-2).2}.$$

Рассмотрим булеву функцию $\psi(\mathbf{x}') = \tilde{\varphi}(\mathbf{x}') \oplus \|\mathbf{x}'\| \oplus \varphi(\mathbf{1}^{n-2})$. Коэффициент Уолша — Адамара функции $\psi(\mathbf{x}')$, соответствующий вектору $\mathbf{0}^{n-2}$, равен

$$W_\psi(\mathbf{0}^{n-2}) = \sum_{\mathbf{x}' \in \Omega^{n-2}} (-1)^{\tilde{\varphi}(\mathbf{x}') \oplus \|\mathbf{x}'\| \oplus \varphi(\mathbf{1}^{n-2})} = (-1)^{\varphi(\mathbf{1}^{n-2})} W_{\tilde{\varphi}}(\mathbf{1}^{n-2}) = 2^{(n-2)/2}.$$

Тогда

$$\|\psi\| = 2^{n-3} - \frac{1}{2} W_\psi(\mathbf{0}^{n-2}) = 2^{n-3} - 2^{(n-4)/2}.$$

Далее заметим, что выполняется соотношение

$$(-1)^{\|\mathbf{a}'\| \oplus \varphi(\mathbf{1}^{n-2})} W_\varphi(\mathbf{a}') = 2^{(n-2)/2} (-1)^{\psi(\mathbf{a}')},$$

следовательно,

$$W_\varphi(\mathbf{a}') = \begin{cases} -2^{(n-2)/2} (-1)^{\|\mathbf{a}'\| \oplus \varphi(\mathbf{1}^{n-2})}, & \text{если } \mathbf{a}' \in N_\psi, \\ 2^{(n-2)/2} (-1)^{\|\mathbf{a}'\| \oplus \varphi(\mathbf{1}^{n-2})}, & \text{если } \mathbf{a}' \notin N_\psi, \end{cases}$$

где $N_\psi = \{\mathbf{a}' \in \Omega^{n-2} : \psi(\mathbf{a}') = 1\}$ — носитель функции ψ. Таким образом, получаем равенство для кривизны

$$\sigma(f) = (2^{n-3} - 2^{(n-4)/2})(4 \cdot 2^{(n-2)/2} + 8) + (2^{n-3} + 2^{(n-4)/2})(4 \cdot 2^{(n-2)/2} - 8) = 2^{(3n-2)/2} - 2^{(n+4)/2}.$$

Утверждение 8 доказано. ■

3. Связь кривизны и нелинейности булевой функции

Утверждение 9. Для произвольной булевой функции $f(x_1, \ldots, x_n)$ от n переменных справедлива оценка

$$\sigma(f) \leqslant S(f)(2^n - 2\,\mathrm{nl}(f)),$$

где $S(f) = |\{\mathbf{a} \in \Omega^n : W_f(\mathbf{a}) \neq 0\}|$ — спектральная сложность функции f.

Доказательство. Заметим, что

$$\max_{\mathbf{a} \in \Omega^n} |W_f(\mathbf{a})| = 2^n - 2\,\mathrm{nl}(f).$$

Тогда

$$\sigma(f) = \sum_{\mathbf{a} \in \Omega^n} |W_f(\mathbf{a})| \leqslant \sum_{\mathbf{a} \in \Omega^n} \max_{\mathbf{b} \in \Omega^n} |W_f(\mathbf{b})| = S(f) \max_{\mathbf{a} \in \Omega^n} |W_f(\mathbf{a})| = S(f)(2^n - 2\,\mathrm{nl}(f)).$$

Утверждение 9 доказано. ■

Оценка из утверждения 9 достигается для бент-функций, аффинных и платовидных функций [1].

Заключение

В работе получены оценки и точные значения кривизны и нелинейности различных классов булевых функций, полученных с помощью суперпозиции булевых функций, симметрических многочленов и бент-функций. Доказано неравенство, связывающее кривизну булевой функции с ее нелинейностью.

ЛИТЕРАТУРА

1. *Логачев О. А., Сальников А. А., Смышляев С. В., Ященко В. В.* Булевы функции в теории кодирования и криптологии. М.: МЦНМО, 2012. 584 с.
2. *Де Ла Крус Хименес Р. А., Камловский О. В.* Суммы модулей коэффициентов Уолша — Адамара булевых функций // Дискретная математика. 2015. Т. 27. Вып. 4. С. 49–66.
3. *Dobbertin H.* Construction of bent functions and balanced Boolean functions with high nonlinearity // LNCS. 1995. V. 1008. P. 61–74.
4. *Камловский О. В.* Суммы модулей коэффициентов Уолша — Адамара некоторых сбалансированных булевых функций // Математические вопросы криптографии. 2017. Т. 8. Вып. 4. С. 75–98.
5. *Тиссин А. С.* Кривизна мажоритарной булевой функции // Дискретная математика. 2021. Т. 33. Вып. 2. С. 155–165.
6. *Fedorov S. N.* On a new classification of Boolean functions // Математические вопросы криптографии. 2019. Т. 10. Вып. 2. С. 159–168.
7. *Логачев О. А., Федоров С. Н., Ященко В. В.* Булевы функции как точки на гиперсфере в евклидовом пространстве //Дискретная математика. 2018. Т. 30. Вып. 1. С. 39–55.
8. *Камловский О. В.* Количество появлений элементов в выходных последовательностях фильтрующих генераторов // Прикладная дискретная математика. 2013. № 3(21). С. 11–25.
9. *Камловский О. В.* Количество появлений векторов на циклах выходных последовательностей двоичных комбинирующих генераторов // Проблемы передачи информации. 2017. Т. 53. Вып. 1. С.92–100.
10. *Тиссин А. С.* Число появлений элементов из заданного подмножества на отрезках усложнений линейных рекуррентных последовательностей // Прикладная дискретная математика. 2023. № 60. С. 30–39.
11. *De la Cruz Jiménez R. A.* On some properties of the curvature and nondegeneracy of Boolean functions // Математические вопросы криптографии. 2022. Т. 13. Вып. 2. С. 65–98.
12. *Камловский О. В.* Спектральный метод оценки числа решений систем нелинейных уравнений с линейными рекуррентными аргументами // Дискретная математика. 2016. Т. 28. Вып. 2. С. 27–43.

REFERENCES

1. *Logachev O. A., Sal'nikov A. A., Smyshlyaev S. V., and Yashchenko V. V.* Bulevy funktsii v teorii kodirovaniya i kriptologii. [Boolean Functions in Coding Theory and Cryptology]. Moscow, MCCME Publ., 2012. 584 p. (in Russian)
2. *De La Krus Khimenes R. A. and Kamlovskii O. V.* The sum of modules of Walsh coefficients of Boolean functions. Discrete Math. Appl., 2016, vol. 26, no. 5, pp. 259–272.
3. *Dobbertin H.* Construction of bent functions and balanced Boolean functions with high nonlinearity. LNCS, 1995, vol. 1008, pp. 61–74.
4. *Kamlovskiy O. V.* Summy moduley koeffitsientov Uolsha — Adamara nekotorykh sbalansirovannykh bulevykh funktsiy [The sum of modules of Walsh coefficients for some balanced Boolean functions]. Matematicheskie Voprosy Kriptografii, 2017, vol. 8, no. 4, pp. 75–98. (in Russian)
5. *Tissin A. S.* Curvature of the Boolean majority function. Discrete Math. Appl., 2022, vol. 32, no. 5, pp. 359–367.
6. *Fedorov S. N.* On a new classification of Boolean functions. Matematicheskie Voprosy Kriptografii, 2019, vol. 10, no. 2, pp. 159–168.

7. *Logachev O. A., Fedorov S. N., and Yashchenko V. V.* Boolean functions as points on the hypersphere in the Euclidean space. Discrete Math. Appl., 2019, vol. 29, no. 2, pp. 89–101.
8. *Kamlovskiy O. V.* Kolichestvo poyavleniy elementov v vykhodnykh posledovatel'nostyakh fil'truyushchikh generatorov [Distribution properties of sequences produced by filtering generators]. Prikladnaya Diskretnaya Matematika, 2013, no. 3(21), pp. 11–25. (in Russian)
9. *Kamlovskii O. V.* Occurrence numbers for vectors in cycles of output sequences of binary combining generators. Problems Inform. Transmission, 2017, vol. 53, no. 1, pp. 84–91.
10. *Tissin A. S.* Chislo poyavleniy elementov iz zadannogo podmnozhestva na otrezkakh uslozhneniy lineynykh rekurrentnykh posledovatel'nostey [The number of occurrences of elements from a given subset on the complication segments of linear recurrence sequences]. Prikladnaya Diskretnaya Matematika, 2023, no. 60, pp. 30–39. (in Russian)
11. *De la Cruz Jiménez R. A.* On some properties of the curvature and nondegeneracy of Boolean functions. Matematicheskiye Voprosy Kriptografii, 2022, vol. 13, no. 2, pp. 65–98.
12. *Kamlovskii O. V.* Estimating the number of solutions of systems of nonlinear equations with linear recurring arguments by the spectral method. Discrete Math. Appl., 2017, vol. 27, no. 4, pp. 199–211.