УДК 519.716.5 DOI 10.17223/20710410/71/2

ОБ УРОВНЕ СИЛЬНОЙ АФФИННОСТИ БУЛЕВЫХ ФУНКЦИЙ

А. В. Кулагин*, А. В. Тарасов**

*ООО «Центр сертификационных исследований», г. Москва, Россия
**АО «ИТМиВТ», г. Москва, Россия

E-mail: artemcoolag@yandex.ru, alextar1@mail.ru

Изучается такой параметр булевых функций, как уровень сильной аффинности, равный минимальному числу переменных, фиксация которых любыми значениями даёт аффинную функцию. Исследованы основные свойства уровня сильной аффинности и его связь с другими параметрами булевых функций. Доказана асимптотическая максимальность уровня сильной аффинности булевых функций.

Ключевые слова: *булева функция, уровень сильной аффинности, спектральные характеристики, алгебраическая степень, вес, алгебраическая иммунность.*

ON THE STRONG AFFINITY LEVEL OF BOOLEAN FUNCTIONS

A. V. Kulagin*, A. V. Tarasov**

*LLC "Center of Certification Research", Moscow, Russia
**JSC "IPMCE", Moscow, Russia

The paper is devoted to the study of such a parameter of a Boolean function as the strong affinity level $\mathrm{la}_s(f)$, which is equal to the minimum number of variables whose fixation by any values gives an affine function. A criterion for finding the exact value of a strong affinity level has been obtained by searching for the emptiest subgraph in the graph of a Boolean function. A correlation has been found between the level of strong affinity and other parameters of Boolean functions, such as algebraic degree $\deg(f)$, weight $||f||$, and algebraic immunity $\mathrm{Al}(f)$, which are as follows: $\mathrm{la}_s(f) \geqslant \mathrm{Al}(f)$ if the function f is not balanced or does not contain first-degree monomials; $\mathrm{la}_s(f) \geqslant \deg(f) - 1$; $2^{n-\mathrm{la}_s(f)-1} \leqslant ||f|| \leqslant 2^n - 2^{n-\mathrm{la}_s(f)-1}$. It has been proven that symmetric Boolean functions and monotonic Boolean functions that significantly depend on all their variables have the highest possible strong affinity level. Asymptotic maximality of the strong affinity level of Boolean functions has been proven too.

Keywords: *Boolean function, strong affinity level, spectral characteristics, algebraic degree, weight, algebraic immunity.*

Введение

Среди методов решения систем булевых уравнений, возникающих, в том числе, в задачах криптографии, важное место занимают методы, осуществляющие сведение исходной системы к системе линейных булевых уравнений. К ним можно отнести как методы, использующие операции в полиномиальных идеалах [1], так и методы, осуществляющие опробование значений части переменных: метод Жу — Витсе [2], метод локальных аффинностей [3] и т. д.

Очевидно, что эффективность этих методов зависит от свойств булевых функций, встретившихся в исходной системе. В данной работе рассматривается вопрос о свойствах функций, преобразуемых в аффинные путём произвольной фиксации значений некоторого набора переменных. Вводимое понятие уровня сильной аффинности сильнее, чем известное понятие уровня аффинности, ранее изучавшееся в работах В. Г. Рябова, О. А. Логачёва, М. Л. Бурякова и др. [4–7].

Введём необходимые определения и обозначения:

- $\mathbb{F}_2$ — поле из двух элементов;
- V_n — n-мерное векторное пространство над полем $\mathbb{F}_2$;
- $\mathcal{F}_n$ — класс булевых функций от n переменных;
- $||x||$ — вес Хэмминга двоичного вектора $x \in V_n$;
- $||f||$ — вес функции f. Булева функция $f \in \mathcal{F}_n$ называется *сбалансированной*, если $||f|| = 2^{n-1}$;
- $\deg(f)$ — алгебраическая степень булевой функциии f. Булеву функцию f будем называть *квадратичной*, если $\deg(f) \leqslant 2$, и *аффинной*, если $\deg(f) \leqslant 1$;
- $\langle u, x\rangle$ — скалярное произведение векторов из V_n;
- $\mathrm{ev}(f)$ — число существенных переменных функции f;
- $\mathrm{Al}(f)$ — порядок алгебраической иммунности булевой функции f;
- $\mathcal{A}_n$ — класс аффинных булевых функций от n переменных;
- $\mathcal{S}_n$ — класс симметрических булевых функций от n переменных;
- $\mathcal{M}_n$ — класс монотонных булевых функций от n переменных;
- $\mathcal{B}_n$ — класс бент-функций от n переменных;
- $\mathcal{M}_{2k}$ — класс функций Елисеева — Майорана — Макфарланда от $2k$ переменных, то есть функций вида $f(x, y) = \langle x, s(y)\rangle \oplus h(y)$, где s — подстановка на V_k; $h(y)$ — произвольная функция из V_k. Известно, что $\mathcal{M}_{2k} \subset \mathcal{B}_{2k}$.

Для произвольной функции $f \in \mathcal{F}_n$ и произвольного $u \in V_n$ преобразование Уолша — Адамара функции f определяется выражением

$$W_f(u) = \sum_{x \in V_n} (-1)^{f(x) \oplus \langle u, x\rangle}.$$

Набор целых чисел $\{W_f(u) : u \in V_n\}$ называется *спектром* функции f, а каждое число $W_f(u)$ — *спектральным коэффициентом* Уолша — Адамара функции f.

Для наборов $1 \leqslant i_1 < i_2 < \ldots < i_k \leqslant n$, $\mathbf{b} = (b_1, \ldots, b_k) \in V_k$ при $k \leqslant n$ обозначим через $f^{b_1,\ldots,b_k}_{i_1,\ldots,i_k}$ булеву функцию из $\mathcal{F}_{n-k}$, получаемую из f фиксацией переменных $x_{i_1} = b_1, \ldots, x_{i_k} = b_k$ и называемую подфункцией функции f.

Определение 1. Булева функция $f \in \mathcal{F}_n$ называется *k-аффинной*, $1 \leqslant k \leqslant n-1$, если существуют такие наборы $1 \leqslant i_1 < i_2 < \ldots < i_k \leqslant n$, $\mathbf{b} = (b_1, \ldots, b_k) \in V_k$, что $f^{b_1,\ldots,b_k}_{i_1,\ldots,i_k}$ является аффинной, то есть $\deg(f^{b_1,\ldots,b_k}_{i_1,\ldots,i_k}) \leqslant 1$.

Определение 2. *Уровнем аффинности* $\mathrm{la}(f)$ булевой функции $f \in \mathcal{F}_n$ называется минимальное неотрицательное целое число k, для которого функция f является k-аффинной.

Определение 3. Булева функция $f \in \mathcal{F}_n$ называется *сильно k-аффинной*, $1 \leqslant k \leqslant n-1$, если существует такой набор $1 \leqslant i_1 < i_2 < \ldots < i_k \leqslant n$, что подфункция $f^{b_1,\ldots,b_k}_{i_1,\ldots,i_k}$ является аффинной для любого $\mathbf{b} = (b_1, \ldots, b_k) \in V_k$, то есть $\deg(f^{b_1,\ldots,b_k}_{i_1,\ldots,i_k}) \leqslant 1$.

Определение 4. *Уровнем сильной аффинности* $\mathrm{la}_s(f)$ булевой функции $f \in \mathcal{F}_n$ будем называть минимальное неотрицательное целое число k, для которого функция f является сильно k-аффинной.

Замечание 1. Очевидно, что для любой булевой функции $f \in \mathcal{F}_n$ справедливо

$$\mathrm{la}(f) \leqslant \mathrm{la}_s(f) \leqslant \mathrm{ev}(f) - 1 \leqslant n - 1$$

и для любой квадратичной функции $f \in \mathcal{F}_n$

$$\mathrm{la}(f) = \mathrm{la}_s(f).$$

Обозначим через $\mathcal{SA}_n^k$ класс булевых функций от n переменных с уровнем сильной аффинности, равным k, а через $\mathcal{SA}_n^{\leqslant k}$ — класс булевых функций от n переменных с уровнем сильной аффинности, не превосходящим k, где $k \in \{0, \ldots, n-1\}$.

Замечание 2. Для любой аффинной функции как уровень аффинности, так и уровень сильной аффинности равны нулю.

Приведём несколько вспомогательных утверждений, которые пригодятся в дальнейшем.

Утверждение 1 [5]. Для булевой функции $f \in \mathcal{F}_n$ справедливо неравенство

$$\mathrm{la}(f) \geqslant \mathrm{Al}(f) - 1.$$

Утверждение 2 [5]. Для $f \in \mathcal{B}_{2k}$ справедливо соотношение $\mathrm{la}(f) \geqslant k$.

Для $f \in \mathcal{F}_n$ справедливо, что

$$||f|| - \text{нечётен} \Leftrightarrow \deg(f) = n. \tag{1}$$

Для $f \in \mathcal{B}_{2k}$, где $k \geqslant 2$, справедливо соотношение

$$\deg(f) \leqslant k. \tag{2}$$

При $\deg(f) \geqslant 1$ справедливо соотношение

$$2^{n-\deg(f)} \leqslant ||f|| \leqslant 2^n - 2^{n-\deg(f)}. \tag{3}$$

Определение 5. *Обыкновенным графом* называется упорядоченная пара объектов $G = (V, E)$, где V — множество вершин; $E \subseteq V^{[2]}$ — множество рёбер. Под $V^{[2]}$ подразумевается множество всех неупорядоченных пар различных элементов из V.

Если $|V| = n$ и $E = \varnothing$, то такой граф называется *пустым* и обозначается O_n.

Если $|V| = n$ и $E = V^{[2]}$, то такой граф называется *полным* и обозначается K_n.

1. Общие свойства уровня сильной аффинности

Приведём критерии для определения уровня сильной аффинности.

Обозначим через T множество мономов булевой функции $f(x_1, \ldots, x_n)$ при её представлении многочленом Жегалкина.

Теорема 1. Для булевой функции $f(x_1, \ldots, x_n)$ соотношение $\mathrm{la}_s(f) = n - 1$ выполнено тогда и только тогда, когда для любых i, j, $1 \leqslant i < j \leqslant n$, существует такой моном $x_{t_1} \ldots x_{t_{s_{i,j}}} \in T$, $s_{i,j} \in \{2, \ldots, n\}$, что $\{i, j\} \subseteq \{t_1, \ldots, t_{s_{i,j}}\}$.

Доказательство.

Необходимость. Так как $\mathrm{la}_s(f) = n-1$, то $\mathrm{la}_s(f) > n-2$. Значит, для любых $1 \leqslant i_1 < \ldots < i_{n-2} \leqslant n$ существует такой набор $(b_1, \ldots, b_{n-2}) \in V_{n-2}$, что $\deg(f_{i_1,\ldots,i_{n-2}}^{b_1,\ldots,b_{n-2}}) > 1$. Так как это функция от двух переменных, она квадратична и содержит моном $x_{i_{n-1}} x_{i_n}$. Это значит, что исходная функция f содержит некоторый моном $x_{t_1} \ldots x_{t_{s_{i,j}}} \in T$, такой,

что $\{i_{n-1}, i_n\} \subseteq \{t_1, \ldots, t_{s_{i,j}}\}$. Данные рассуждения справедливы для любого набора $1 \leqslant i_1 < \ldots < i_{n-2} \leqslant n$, поэтому любое произведение $x_i x_j$, $1 \leqslant i < j \leqslant n$, содержится в некотором мономе функции f.

Достаточность. Пусть $\mathrm{la}_s(f) \leqslant n-2$. Тогда существует такой набор $1 \leqslant i_1 < \ldots < i_m \leqslant n$, где $m \leqslant n-2$, что для любого вектора $(b_1, \ldots, b_m) \in V_m$ функция $f_{i_1,\ldots,i_m}^{b_1,\ldots,b_m}$ аффинна. Возьмём $i, j \in \{1, \ldots, n\} \setminus \{i_1, \ldots, i_m\}$. Так как ни одна из функций $f_{i_1,\ldots,i_m}^{b_1,\ldots,b_m}$ не содержит произведения $x_i x_j$, то функция f не содержит ни одного монома, содержащего произведение $x_i x_j$, — противоречие. ■

Теорему 1 можно интерпретировать в терминах теории графов для более удобного её понимания и применения на практике.

Для булевой функции $f(x_1, \ldots, x_n)$ построим граф $G_f = (V, E)$, где $V = \{1, \ldots, n\}$, а множество рёбер задается по следующему правилу:

$$\{i, j\} \in E \Leftrightarrow \text{ существует такой моном } x_{i_1} \ldots x_{i_s} \in T, \text{ что } \{i, j\} \subseteq \{i_1, \ldots, i_s\}.$$

Такое сопоставление графа функции является сюръективным, но не биективным, например, функциям $g_1(x_1, x_2, x_3) = x_1 x_2 x_3$ и $g_2(x_1, x_2, x_3) = x_1 x_2 \oplus x_1 x_3 \oplus x_2 x_3$ сопоставляется один и тот же полный граф K_3.

Тогда в терминах теории графов теорема 1 имеет следующую эквивалентную формулировку:

Следствие 1. Для булевой функции $f(x_1, \ldots, x_n)$ соотношение $\mathrm{la}_s(f) = n-1$ выполнено тогда и только тогда, когда граф G_f полный.

Приведём ещё одну эквивалентную формулировку теоремы 1.

Следствие 2. Для булевой функции $f(x_1, \ldots, x_n)$ соотношение $\mathrm{la}_s(f) = n-1$ выполнено тогда и только тогда, когда для любых $1 \leqslant i < j \leqslant n$ выполняется условие

$$f_{i,j}^{1,1} \oplus f_{i,j}^{1,0} \oplus f_{i,j}^{0,1} \oplus f_{i,j}^{0,0} \not\equiv 0.$$

Доказательство. Разложим функцию f по переменным x_i, x_j и преобразуем данное представление:

$$f = x_i x_j f_{i,j}^{1,1} \oplus (x_i \oplus 1) x_j f_{i,j}^{0,1} \oplus x_i (x_j \oplus 1) f_{i,j}^{1,0} \oplus (x_i \oplus 1)(x_j \oplus 1) f_{i,j}^{0,0} =$$
$$= x_i x_j (f_{i,j}^{1,1} \oplus f_{i,j}^{0,1} \oplus f_{i,j}^{1,0} \oplus f_{i,j}^{0,0}) \oplus x_i (f_{i,j}^{1,0} \oplus f_{i,j}^{0,0}) \oplus x_j (f_{i,j}^{0,1} \oplus f_{i,j}^{0,0}) \oplus f_{i,j}^{0,0}.$$

По теореме 1 любое произведение $x_i x_j$, $1 \leqslant i < j \leqslant n$, встречается в некотором мономе функции f при её представлении многочленом Жегалкина, а значит, функция $f_{i,j}^{1,1} \oplus f_{i,j}^{0,1} \oplus f_{i,j}^{1,0} \oplus f_{i,j}^{0,0}$ никогда не равна тождественному нулю. ■

Пример 1. Функция $f_1(x_1, x_2, x_3, x_4, x_5) = x_1 x_2 x_3 \oplus x_1 x_3 x_4 \oplus x_1 x_3 x_5 \oplus x_2 x_4 x_5$ имеет максимальный уровень сильной аффинности, равный 4, так как любое из 10 произведений вида $x_i x_j$, $1 \leqslant i < j \leqslant 5$, является частью некоторого монома многочлена Жегалкина функции $f_1(x_1, \ldots, x_5)$ и граф функции G_{f_1} полный.

Следствие 3. Если для булевой функции $f \in \mathcal{F}_n$ справедливо, что $\deg(f) = n$, то $\mathrm{la}_s(f) = n-1$.

Доказательство. Функция степени n содержит моном $x_1 \ldots x_n$ в её записи в виде многочлена Жегалкина; любое произведение $x_i x_j$, $1 \leqslant i < j \leqslant n$, содержится в этом мономе, значит, по теореме 1 уровень сильной аффинности данной функции максимален. ■

Лемма 1. Если для функции $f \in \mathcal{F}_n$ верно, что $f^{b_1,\ldots,b_k}_{i_1,\ldots,i_k} = c(b_1,\ldots,b_k)$ для любого $(b_1,\ldots,b_k) \in V_k$, где $c(b_1,\ldots,b_k) \in \mathbb{F}_2$, то любая переменная из множества $\{x_1,\ldots,x_n\} \setminus \{x_{i_1},\ldots,x_{i_k}\}$ фиктивна.

Доказательство. Без ограничения общности будем считать, что $i_1 = 1$, $\ldots$, $i_k = k$. Предположим, что для некоторого $t \in \{k+1,\ldots,n\}$ переменная x_t существенна. Тогда найдётся такой набор $(a_1,\ldots,a_{t-1},a_{t+1},\ldots,a_n)$, что $f(a_1,\ldots,a_{t-1},0,a_{t+1},\ldots,a_n) \neq f(a_1,\ldots,a_{t-1},1,a_{t+1},\ldots,a_n)$. Но по условию $f^{a_1,\ldots,a_k}_{i_1,\ldots,i_k} \equiv$ $\equiv$ const, а значит, $f(a_1,\ldots,a_{t-1},0,a_{t+1},\ldots,a_n) = f(a_1,\ldots,a_{t-1},1,a_{t+1},\ldots,a_n)$ — противоречие. ■

Докажем основной критерий точного значения уровня сильной аффинности.

Теорема 2. Для булевой функции $f(x_1,\ldots,x_n)$ соотношение $\mathrm{la}_s(f) = k$, где $k \leqslant n-2$, выполнено тогда и только тогда, когда одновременно выполняются следующие свойства:

1) для некоторого набора $1 \leqslant i_1 < i_2 < \ldots < i_{n-k} \leqslant n$ выполняется следующее условие: ни один моном многочлена Жегалкина функции f не содержит произведение вида $x_{i_j}x_{i_l}$, $1 \leqslant j < l \leqslant n-k$;
2) набора $1 \leqslant i_1 < \ldots < i_t \leqslant n$ длины $t > n-k$ с таким же свойством не существует.

Доказательство.

Достаточность докажем индукцией по параметру k.

Б а з а: $k = 0$. Тогда функция f аффинна и $\mathrm{la}_s(f) = 0$, так как для любых $1 \leqslant i < j \leqslant n$ моном x_ix_j не содержится ни в каком мономе функции f.

Пусть $k = 1$. Тогда существует такой набор $1 \leqslant i_1 < i_2 < \ldots < i_{n-1} \leqslant n$, что никакое произведение x_ix_j, $\{i,j\} \subseteq \{i_1,\ldots,i_{n-1}\}$, не входит в мономы функции f. Без ограничения общности положим $i_1 = 1$, $\ldots$, $i_{n-1} = n-1$. Функция f в этом случае, кроме своей аффинной части, может содержать мономы x_1x_n, x_2x_n, $\ldots$, $x_{n-1}x_n$. Очевидно, что при фиксации переменной x_n любым значением $b \in \mathbb{F}_2$ получим аффинную подфункцию, поэтому $\mathrm{la}_s(f) \leqslant 1$. Случай $\mathrm{la}_s(f) = 0$ невозможен ввиду условия 2, поэтому $\mathrm{la}_s(f) = 1$.

Ш а г: из справедливости утверждения при $k = d-1 \geqslant 1$ докажем его справедливость при $k = d$.

Имеем такой набор $1 \leqslant i_1 < i_2 < \ldots < i_{n-d} \leqslant n$, что ни один моном многочлена Жегалкина функции f не содержит произведения вида $x_{i_j}x_{i_l}$, $1 \leqslant j < l \leqslant n-d$. Без ограничения общности положим $i_1 = 1$, $\ldots$, $i_{n-d} = n-d$. Представим функцию f в виде

$$f(x_1,\ldots,x_n) = x_1x_2g_0(x_3,\ldots,x_n) \oplus x_1g_1(x_3,\ldots,x_n) \oplus x_2g_2(x_3,\ldots,x_n) \oplus g_3(x_3,\ldots,x_n).$$

Так как функция f не содержит мономов, включающих произведение x_1x_2 (в силу того, что $n-d \geqslant 2$), то $g_0 \equiv 0$. По этой же причине функции g_1 и g_2 не содержат переменных $x_3,\ldots,x_{n-d}$ в многочлене Жегалкина и функция $g_3(x_3,\ldots,x_n)$ содержит переменные $x_3,\ldots,x_{n-d}$ только в своей аффинной части, то есть

$$\begin{gathered} g_1(x_3,\ldots,x_n) \equiv h_1(x_{n-d+1},\ldots,x_n), \\ g_2(x_3,\ldots,x_n) \equiv h_2(x_{n-d+1},\ldots,x_n), \\ g_3(x_3,\ldots,x_n) = h_3(x_{n-d+1},\ldots,x_n) \oplus a_3x_3 \oplus \ldots \oplus a_{n-d}x_{n-d}, \end{gathered}$$

где $a_3,\ldots,a_{n-d} \in \mathbb{F}_2$. Таким образом,

$$\begin{gathered} f(x_1,\ldots,x_n) \equiv x_1h_1(x_{n-d+1},\ldots,x_n) \oplus x_2h_2(x_{n-d+1},\ldots,x_n) \oplus \\ \oplus h_3(x_{n-d+1},\ldots,x_n) \oplus a_3x_3 \oplus \ldots \oplus a_{n-d}x_{n-d}. \end{gathered} \tag{4}$$

Теперь очевидно, что, зафиксировав переменные $x_{n-d+1}, \ldots, x_n$ любыми значениями, получим аффинную функцию, то есть $\mathrm{la}_s(f) \leqslant d$.

Предположим, что $\mathrm{la}_s(f) = p < d$. Тогда существует такой набор переменных $\{y_1, \ldots, y_p\} \subsetneq \{x_{n-d+1}, \ldots, x_n\}$, что $f^{b_1,\ldots,b_p}_{y_1,\ldots,y_p}$ аффинна при любых $b_1, \ldots, b_p \in \mathbb{F}_2$. Это означает, что $h_1{}^{b_1,\ldots,b_p}_{y_1,\ldots,y_p}$ и $h_2{}^{b_1,\ldots,b_p}_{y_1,\ldots,y_p}$ — константы при любых $b_1, \ldots, b_p \in \mathbb{F}_2$.

Тогда по лемме 1 все переменные из множества $\{x_{n-d+1}, \ldots, x_n\} \setminus \{y_1, \ldots, y_p\}$ являются фиктивными для функций h_1 и h_2. Рассмотрим произвольный $x_l \in \{x_{n-d+1}, \ldots, x_n\} \setminus \{y_1, \ldots, y_p\} \neq \varnothing$ и набор индексов $1 < 2 < \ldots < n-d < l$ длины $n-d+1$. У функции f в многочлене Жегалкина нет мономов, содержащих произведения x_1x_l, x_2x_l, …, $x_{n-d}x_l$, а значит, для набора $1 < 2 < \ldots < n-d < l$ длины $n-d+1$ верно, что для любых $\{i, j\} \subseteq \{1, \ldots, n-d, l\}$ не существует монома многочлена Жегалкина функции f, содержащего произведение вида x_ix_j. Таким образом, $\mathrm{la}_s(f) = d$.

Необходимость. Докажем первое свойство от противного. Пусть не существует такого набора длины $n-k$, что для любых i, j из этого набора не существует монома многочлена Жегалкина функции f, содержащего произведение вида x_ix_j, то есть данное свойство может выполняться лишь для какого-то набора меньшей длины. Тогда по доказательству достаточности этой теоремы следует, что $\mathrm{la}_s(f) < k$, — противоречие.

Докажем второе свойство также от противного. Пусть существует набор длины $t > n-k$, для которого выполняются вышеуказанные свойства. Тогда по доказательству достаточности этой теоремы следует, что $\mathrm{la}_s(f) > k$, — противоречие.

Таким образом, оба свойства верны. ■

Теорему 2 можно сформулировать в терминах теории графов следующим образом:

Следствие 4. Для булевой функции $f(x_1, \ldots, x_n)$ соотношение $\mathrm{la}_s(f) = k$, где $k \leqslant n-2$, выполнено тогда и только тогда, когда граф G_f содержит подграф O_{n-k} и не содержит подграфа O_t, где $t > n-k$.

Замечание 3. Таким образом, задача определения уровня сильной аффинности сводится к задаче поиска максимально пустого подграфа, которая более известна как задача поиска максимально независимого множества. В общем случае данная задача относится к классу труднорешаемых, вместе с тем существуют приближённые алгоритмы её решения.

Следствие 5. Для булевой функции $f \in \mathcal{F}_n$ соотношение $\mathrm{la}_s(f) = k$, где $k \leqslant n-2$, выполнено тогда и только тогда, когда одновременно выполняются следующие свойства:

1) существует такой набор $1 \leqslant i_1 < i_2 < \ldots < i_{n-k} \leqslant n$, что для любых $\{i, j\} \subseteq \{i_1, \ldots, i_{n-k}\}$ выполняется
$$f^{1,1}_{i,j} \oplus f^{1,0}_{i,j} \oplus f^{0,1}_{i,j} \oplus f^{0,0}_{i,j} \equiv 0;$$
2) набора $1 \leqslant i_1 < \ldots < i_t \leqslant n$ длины $t > n-k$ с таким же свойством не существует.

Доказательство. Достаточно воспользоваться разложением функции f из доказательства следствия 2 и заметить его связь с разложением (4). ■

Следует также отметить, что следствия 2 и 5 являются частными случаями теоремы 7 из работы [8].

Пример 2. Функция $f_2(x_1, \ldots, x_8) = x_2x_3x_4x_7x_8 \oplus x_2x_5x_6x_7x_8 \oplus x_3x_4x_5x_7x_8 \oplus \oplus x_1x_2x_7x_8 \oplus x_1x_3x_4 \oplus x_2x_6x_7 \oplus x_4x_5x_7 \oplus x_1x_7 \oplus x_2x_6 \oplus x_5x_8 \oplus x_6x_7$ имеет уровень сильной аффинности $\mathrm{la}_s(f_2) = 5$, так как граф G_{f_2} содержит подграф O_3.

Замечание 4. Из доказательства теоремы 2 следует, что условие 1 из её формулировки используется для оценки уровня сильной аффинности сверху, а условие 2 — для его оценки снизу, и пересечение этих условий даёт точное значение уровня аффинности. Поэтому укажем важное следствие:

Следствие 6.

1) Если для функции $f(x_1, \ldots, x_n)$ и фиксированного k, $k \leqslant n-2$, существует такой набор $1 \leqslant i_1 < i_2 < \ldots < i_{n-k} \leqslant n$, что ни один моном многочлена Жегалкина функции f не содержит произведения вида $x_{i_j}x_{i_l}$, $1 \leqslant j < l \leqslant n-k$, то $\mathrm{la}_s(f) \leqslant k$.
2) Если для функции $f(x_1, \ldots, x_n)$ и фиксированного k, $k \leqslant n-2$, не существует такого набора $1 \leqslant i_1 < i_2 < \ldots < i_{n-k} \leqslant n$, что ни один моном многочлена Жегалкина функции f не содержит произведения вида $x_{i_j}x_{i_l}$, $1 \leqslant j < l \leqslant n-k$, то $\mathrm{la}_s(f) > k$.

Данное следствие также можно сформулировать в терминах теории графов:

Следствие 7.

1) Если граф G_f функции $f(x_1, \ldots, x_n)$ содержит подграф O_{n-k}, где $k \leqslant n-2$, то $\mathrm{la}_s(f) \leqslant k$.
2) Если граф G_f функции $f(x_1, \ldots, x_n)$ не содержит подграфа O_{n-k}, где $k \leqslant n-2$, то $\mathrm{la}_s(f) > k$.

2. Связь уровня сильной аффинности с другими характеристиками булевых функций

В работе [5] исследована связь уровня аффинности булевой функции с рядом её криптографических параметров.

Теорема 3 [5]. Для коэффициентов Уолша — Адамара функции $f \in \mathcal{F}_n$ выполняется неравенство

$$\max_{u \in V_n} \left|W_f(u)\right| \geqslant 2^{n-\mathrm{la}(f)}.$$

Рассмотрим связь между уровнем сильной аффинности булевой функции и её спектральными характеристиками.

Пусть для булевой функции $f \in \mathcal{F}_n$ справедливо равенство $\mathrm{la}_s(f) = k$ и для набора $1 \leqslant i_1 < i_2 < \ldots < i_k \leqslant n$ подфункция $f^{b_1,\ldots,b_k}_{i_1,\ldots,i_k}$ аффинна для любого $\mathbf{b} = (b_1, \ldots, b_k) \in V_k$. Положим

$$R = \left|\left\{v \in V_{n-k} : f^{b_1,\ldots,b_k}_{i_1,\ldots,i_k} = \langle v, x\rangle \oplus w, (b_1, \ldots, b_k) \in V_k\right\}\right|,$$

где $w \in \mathbb{F}_2$. Очевидно, что $1 \leqslant R \leqslant \min\{2^k, 2^{n-k}\} \leqslant 2^{n/2}$. Известен следующий факт:

Лемма 2 [9]. Для любой функции $f \in \mathcal{F}_n$, произвольного подпространства $L \subseteq V_n$ и произвольных векторов $a, c \in V_n$ справедливо равенство

$$2^{\dim L - n}(-1)^{\langle a,c\rangle} \sum_{x \in L^\perp \oplus c} W_f(x)(-1)^{\langle a,x\rangle} = \sum_{x \in L \oplus a} (-1)^{f(x)\oplus\langle c,x\rangle}. \tag{5}$$

Теорема 4. Существует по крайней мере R различных векторов $u \in V_n$, для каждого из которых выполняется неравенство

$$\left|W_f(u)\right| \geqslant 2^{n-\mathrm{la}_s(f)}.$$

Доказательство. Пусть $\mathrm{la}_s(f) = k$. Тогда найдётся такой набор $1 \leqslant i_1 < i_2 < \ldots < i_k \leqslant n$, что $f^{b_1,\ldots,b_k}_{i_1,\ldots,i_k}(x) = \langle v, x\rangle \oplus w$ для любого $(b_1,\ldots,b_k) \in V_k$, причём $v = v(b_1,\ldots,b_k) \in V_{n-k}$, $w = w(b_1,\ldots,b_k) \in \mathbb{F}_2$.

Аналогично доказательству теоремы 3, для фиксированного $(b_1,\ldots,b_k) \in V_k$ положим:

— $L = \{u \in V_n : u_{i_1} = \ldots = u_{i_k} = 0\}$ — подпространство размерности $\dim L = n - k$ пространства V_n;
— вектор a, такой, что $a_{i_j} = b_j$ для $j \in \{1,\ldots,k\}$ и $a_{i_j} = 0$ для $j \notin \{1,\ldots,k\}$;
— вектор c, такой, что $c_{i_j} = v_{i_j}$ для $j \notin \{1,\ldots,k\}$ и $c_{i_j} = 0$ для $j \in \{1,\ldots,k\}$.

Правая часть равенства (5) в этом случае есть

$$\sum_{x\in L\oplus a} (-1)^{f(x)\oplus\langle c,x\rangle} = \sum_{x\in V_{n-k}} (-1)^{f^{b_1,\ldots,b_k}_{i_1,\ldots,i_k}(x)\oplus\langle v,x\rangle} =$$
$$= \sum_{x\in V_{n-k}} (-1)^{\langle v,x\rangle\oplus w\oplus\langle v,x\rangle} = \sum_{x\in V_{n-k}} (-1)^w = 2^{n-k}(-1)^w.$$

Таким образом, имеем $(-1)^{\langle a,c\rangle} \sum\limits_{x\in L^\perp\oplus c} W_f(x)(-1)^{\langle a,x\rangle} = 2^n(-1)^w$.

Переходя к абсолютным величинам, получим

$$\Big|\sum_{x\in L^\perp\oplus c} W_f(x)(-1)^{\langle a,x\rangle}\Big| = 2^n.$$

Так как число слагаемых в последней сумме равно 2^k, в плоскости $L^\perp \oplus c$ есть такой вектор $u \in V_n$, для которого $|W_f(u)| \geqslant 2^{n-k}$. Так как подпространство $L^\perp$ фиксировано, а вектор $c \in V_n$ пробегает различные R значений, множество $\{L^\perp \oplus c\}$ пробегает R различных непересекающихся плоскостей и в каждой из них найдётся такой вектор $u \in V_n$, что $\big|W_f(u)\big| \geqslant 2^{n-k}$. ■

Утверждение 3 [5]. Для любых $n \geqslant 3$, $2 \leqslant d \leqslant n$, $1 \leqslant k \leqslant n-2$ существует такая функция $f \in \mathcal{F}_n$, что $\deg(f) = d$, $\mathrm{la}(f) = k$.

Следующее утверждение устанавливает связь между уровнем сильной аффинности булевой функции и её алгебраической степенью, что отличает исследуемую характеристику от уровня аффинности (см. утверждение 3).

Утверждение 4. Для булевой функции $f \in \mathcal{F}_n$ справедливо соотношение

$$\mathrm{la}_s(f) \geqslant \deg(f) - 1.$$

Если $f \in \mathcal{B}_n$ и $n \geqslant 4$, то

$$\mathrm{la}_s(f) > \deg(f) - 1.$$

Доказательство. Пусть $\deg(f) = t$. Тогда функция f содержит моном $x_{s_1}\ldots x_{s_t}$, где $1 \leqslant s_1 < \ldots < s_t \leqslant n$, в её представлении в виде многочлена Жегалкина. По теореме 2 ни одна из пар этих индексов не может находиться в наборе $1 \leqslant i_1 < i_2 < \ldots < i_{n-\mathrm{la}_s(f)} \leqslant n$, поэтому максимальная длина этого набора не превышает $n - t + 1$. Таким образом, $n - \mathrm{la}_s(f) \leqslant n - t + 1$, откуда $\mathrm{la}_s(f) \geqslant t - 1 = \deg(f) - 1$.

Второе соотношение следует из (2), утверждения 2 и замечания 1. ■

Следствие 8. Если вес булевой функции $f \in \mathcal{F}_n$ нечётен, то $\mathrm{la}_s(f) = n - 1$.

Доказательство. Следует из (1) и утверждения 4. ■

Отсюда, ввиду утверждения 3, можно вывести связь между уровнем сильной аффинности и весом булевой функции.

Утверждение 5. Для булевой функции $f \in \mathcal{F}_n$, $\deg(f) \geqslant 1$, справедлива оценка

$$2^{n-\mathrm{la}_s(f)-1} \leqslant ||f|| \leqslant 2^n - 2^{n-\mathrm{la}_s(f)-1}, \tag{6}$$

при этом:

1) нижняя оценка достигается только на функциях f вида

$$f(x) = (x_{i_1} \oplus c_1)(x_{i_2} \oplus c_2) \dots (x_{i_k} \oplus c_k) l(x_{i_{k+1}}, x_{i_{k+2}}, \dots, x_{i_n});$$

2) верхняя оценка достигается только на функциях f вида

$$f(x) = (x_{i_1} \oplus c_1)(x_{i_2} \oplus c_2) \dots (x_{i_k} \oplus c_k) l(x_{i_{k+1}}, x_{i_{k+2}}, \dots, x_{i_n}) \oplus 1,$$

где $k = \mathrm{la}_s(f)$, $c_1, \dots, c_k \in \mathbb{F}_2$, $\deg(l) = 1$.

Доказательство. Справедливость оценки следует из (3) и Утверждения 4.

Докажем критерий достижимости нижней оценки в (6).

Достаточность. Для функций такого вида справедливо

$$||f|| = ||x_{i_{k+1}} \oplus x_{i_{k+2}} \oplus \dots \oplus x_{i_n}|| = 2^{n-k-1} = 2^{n-\mathrm{la}_s(f)-1}.$$

Необходимость. По условию $\mathrm{la}_s(f) = k$, значит, существует такой набор $1 \leqslant i_1 < \dots < i_k \leqslant n$, что $f^{b_1,\dots,b_k}_{i_1,\dots,i_k} \in \mathcal{A}_n$ для всех $(b_1, \dots, b_k) \in V_k$. Отсюда

$$||f^{b_1,\dots,b_k}_{i_1,\dots,i_k}|| \in \{0, 2^{n-k-1}, 2^{n-k}\}$$

для всех $(b_1, \dots, b_k) \in V_k$. Очевидно, что

$$||f|| = \sum_{(b_1,\dots,b_k) \in V_k} ||f^{b_1,\dots,b_k}_{i_1,\dots,i_k}|| = 2^{n-k-1}.$$

Отсюда следует, что существует единственный набор $(a_1, \dots, a_k) \in V_k$, такой, что $||f^{a_1,\dots,a_k}_{i_1,\dots,i_k}|| = 2^{n-k-1}$, и $||f^{b_1,\dots,b_k}_{i_1,\dots,i_k}|| = 0$ для всех $(b_1, \dots, b_k) \in V_k \setminus \{(a_1, \dots, a_k)\}$, то есть $f^{b_1,\dots,b_k}_{i_1,\dots,i_k} \equiv 0$ для всех $(b_1, \dots, b_k) \in V_k \setminus \{(a_1, \dots, a_k)\}$ и $\deg(f^{a_1,\dots,a_k}_{i_1,\dots,i_k}) = 1$.

Раскладывая функцию f по переменным $x_{i_1}, \dots, x_{i_k}$, получаем

$$f(x_1, \dots, x_n) = \bigoplus_{(b_1,\dots,b_k) \in V_k} (x_{i_1} \oplus b_1 \oplus 1) \dots (x_{i_k} \oplus b_k \oplus 1) f^{b_1,\dots,b_k}_{i_1,\dots,i_k}(x_{i_{k+1}}, x_{i_{k+2}}, \dots, x_{i_n}) =$$
$$= (x_{i_1} \oplus a_1 \oplus 1) \dots (x_{i_k} \oplus a_k \oplus 1) f^{a_1,\dots,a_k}_{i_1,\dots,i_k}(x_{i_{k+1}}, x_{i_{k+2}}, \dots, x_{i_n}).$$

Для доказательства необходимости остаётся положить $c_1 = a_1 \oplus 1$, …, $c_k = a_k \oplus 1$ и $l(x_{i_{k+1}}, x_{i_{k+2}}, \dots, x_{i_n}) = f^{a_1,\dots,a_k}_{i_1,\dots,i_k}(x_{i_{k+1}}, x_{i_{k+2}}, \dots, x_{i_n})$.

Доказательство верхней оценки аналогично; в этом случае $f^{b_1,\dots,b_k}_{i_1,\dots,i_k} \equiv 1$ для всех $(b_1, \dots, b_k) \in V_k \setminus \{(a_1, \dots, a_k)\}$ и $\deg(f^{a_1,\dots,a_k}_{i_1,\dots,i_k}) = 1$. ■

Из утверждения 1 и замечания 1 следует, что для булевой функции $f \in \mathcal{F}_n$ справедливо соотношение

$$\mathrm{la}_s(f) \geqslant \mathrm{Al}(f) - 1.$$

Данную оценку можно усилить для определённых классов булевых функций.

Утверждение 6 [5]. Для любой булевой функции $f \in \mathcal{F}_n$ справедливо

$$\mathrm{Al}(f) \leqslant \min_{\substack{0 \leqslant s \leqslant \lceil n/2 \rceil \\ 1 \leqslant i_1 < i_2 < \dots < i_s \leqslant n \\ (b_1,\dots,b_s) \in V_s}} \left\{ \deg\left(f^{b_1,\dots,b_s}_{i_1,\dots,i_s}\right) + s \right\}.$$

Утверждение 7. Если булева функция $f \in \mathcal{F}_n$ не является сбалансированной, то

$$\mathrm{la}_s(f) \geqslant \mathrm{Al}(f).$$

Доказательство. Пусть $\mathrm{la}_s(f) = k$. Тогда существует такой набор $1 \leqslant i_1 < \ldots < i_k \leqslant n$, что $f^{b_1,\ldots,b_k}_{i_1,\ldots,i_k} \in \mathcal{A}_n$ для всех $(b_1,\ldots,b_k) \in V_k$. Отсюда

$$||f^{b_1,\ldots,b_k}_{i_1,\ldots,i_k}|| \in \{0, 2^{n-k-1}, 2^{n-k}\}$$

для всех $(b_1,\ldots,b_k) \in V_k$. Если $||f^{b_1,\ldots,b_k}_{i_1,\ldots,i_k}|| = 2^{n-k-1}$ для всех $(b_1,\ldots,b_k) \in V_k$, то

$$||f|| = \sum_{(b_1,\ldots,b_k)\in V_k} ||f^{b_1,\ldots,b_k}_{i_1,\ldots,i_k}|| = 2^k \cdot 2^{n-k-1} = 2^{n-1}$$

— противоречие с несбалансированностью функции f. Поэтому существует такой набор $(a_1,\ldots,a_k) \in V_k$, что $||f^{a_1,\ldots,a_k}_{i_1,\ldots,i_k}|| \in \{0, 2^{n-k}\}$, то есть $f^{a_1,\ldots,a_k}_{i_1,\ldots,i_k} \equiv \mathrm{const}$, а значит, ввиду утверждения 6, получаем

$$\mathrm{Al}(f) \leqslant \deg\left(f^{a_1,\ldots,a_k}_{i_1,\ldots,i_k}\right) + k = k.$$

Утверждение 7 доказано. ■

Представим булеву функцию $f \in \mathcal{F}_n$ в виде

$$f(x_1,\ldots,x_n) = g(x_1,\ldots,x_n) \oplus l(x_1,\ldots,x_n) \oplus a_0,$$

где $a_0 = f(0,\ldots,0)$, функция g содержит только мономы степени 2 и выше, а функция l — только мономы степени 1.

Утверждение 8. Если для булевой функции $f \in \mathcal{F}_n$ справедливо, что $l \equiv 0$, то

$$\mathrm{la}_s(f) \geqslant \mathrm{Al}(f).$$

Доказательство. Пусть $\mathrm{la}_s(f) = k$. Тогда существует такой набор $1 \leqslant i_1 < \ldots < i_k \leqslant n$, что $f^{b_1,\ldots,b_k}_{i_1,\ldots,i_k} \in \mathcal{A}_n$ для всех $(b_1,\ldots,b_k) \in V_k$. Из теоремы 2 следует, что в любом мономе функции f найдётся переменная из множества $\{x_{i_1},\ldots,x_{i_k}\}$. Тогда, зафиксировав каждую переменную из этого множества нулём, получим $f^{0,\ldots,0}_{i_1,\ldots,i_k} = a_0$, а значит, ввиду утверждения 6, $\mathrm{Al}(f) \leqslant \deg\left(f^{0,\ldots,0}_{i_1,\ldots,i_k}\right) + k = k$. ■

3. Уровень сильной аффинности булевых функций из некоторых классов

Обсудим задачу нахождения уровня сильной аффинности для некоторых классов функций. Рассмотрим класс симметрических булевых функций. В работе [10] получена оценка уровня аффинности для функций из этого класса:

Утверждение 9 [10]. Для функции $f \in \mathcal{S}_n$, такой, что $\deg(f) > 1$, справедлива оценка

$$\mathrm{la}(f) > n - \deg(f).$$

Найдём значение уровня сильной аффинности для функций этого класса.

Утверждение 10. Для функции $f \in \mathcal{S}_n$, такой, что $\deg(f) > 1$, справедлива следующая оценка:

$$\mathrm{la}_s(f) = n - 1.$$

Доказательство. Так как $\deg(f) > 1$, то функция f содержит моном степени выше 1, а значит, существует произведение $x_j x_k$, которое является частью некоторого монома функции f при её представлении многочленом Жегалкина. Так как по определению симметрической функции

$$f(x_1, \ldots, x_j, \ldots, x_k, \ldots, x_n) = f(x_{i_1}, \ldots, x_{i_j}, \ldots, x_{i_k}, \ldots, x_{i_n})$$

для любой перестановки $(i_1, \ldots, i_n)$ элементов множества $\{1, \ldots, n\}$, то произведение $x_{i_j} x_{i_k}$ также является частью некоторого монома функции f. Данные рассуждения справедливы для любой перестановки элементов множества $\{1, \ldots, n\}$, значит, для любых $1 \leqslant i < j \leqslant n$ существуют такие $s_{i,j} \in \{2, \ldots, n\}$ и моном $x_{t_1} \ldots x_{t_{s_{i,j}}} \in T$, что $\{i, j\} \subseteq \{t_1, \ldots, t_{s_{i,j}}\}$. Таким образом, из теоремы 1 следует справедливость утверждения 10. ■

Из утверждения 2 и замечания 1 следует, что для булевой функции $f \in \mathcal{B}_{2k}$ справедливо соотношение

$$\mathrm{la}_s(f) \geqslant k. \tag{7}$$

Следствие 9. Для булевой функции $f \in \mathcal{M}_{2k}$ справедливо равенство $\mathrm{la}_s(f) = k$.

Доказательство. При фиксации всех переменных y любыми значениями функция f становится аффинной, т. е. $\mathrm{la}_s(f) \leqslant k$. Ввиду (7) получаем искомое равенство. ■

Рассмотрим класс монотонных булевых функций $\mathcal{M}_n$.

Утверждение 11. Если функция $f \in \mathcal{M}_n$ существенно зависит от всех своих переменных, то

$$\mathrm{la}_s(f) = n - 1.$$

Доказательство. Предположим противное: $\mathrm{la}_s(f) = k \leqslant n-2$. Тогда существует такой набор $1 \leqslant i_1 < \ldots < i_k \leqslant n$, что $f^{b_1,\ldots,b_k}_{i_1,\ldots,i_k} \in \mathcal{A}_{n-k}$. Без ограничения общности положим $i_1 = 1, \ldots, i_k = k$. Тогда для некоторого фиксированного набора $(b_1, \ldots, b_k) \in V_k$ имеем

$$f^{b_1,\ldots,b_k}_{1,\ldots,k}(x_{k+1}, \ldots, x_n) = \langle v, x \rangle \oplus w = v_{k+1} x_{k+1} \oplus \ldots \oplus v_n x_n \oplus w,$$

где $v_{k+1}, \ldots, v_n, w \in \mathbb{F}_2$. Ввиду леммы 1 $v \neq 0$, иначе у функции f были бы фиктивные переменные. Без ограничения общности положим $v_{k+1} \neq 0$. Тогда ввиду монотонности функции f справедливо

$$\begin{gathered} v_{k+2} c_{k+2} \oplus \ldots \oplus v_n c_n \oplus w = f(b_1, \ldots, b_k, 0, c_{k+2}, \ldots, c_n) \leqslant \\ \leqslant f(b_1, \ldots, b_k, 1, c_{k+2}, \ldots, c_n) = 1 \oplus v_{k+2} c_{k+2} \oplus \ldots \oplus v_n c_n \oplus w \end{gathered} \tag{8}$$

для любых $c_{k+2}, \ldots, c_n \in \mathbb{F}_2$. Данное неравенство справедливо лишь в случае, когда $v_{k+2} = \ldots = v_n = w = 0$. Значит, $f^{b_1,\ldots,b_k}_{1,\ldots,k}(x_{k+1}, \ldots, x_n) = v_{k+1} x_{k+1}$, и тогда $f^{b_1,\ldots,b_k,b_{k+1}}_{1,\ldots,k,k+1} = \mathrm{const}$ для любого фиксированного набора $(b_1, \ldots, b_k, b_{k+1}) \in V_{k+1}$. По лемме 1 переменные $x_{k+2}, \ldots, x_n$ фиктивны — противоречие с условием. ■

Следствие 10. Если функция $f \in \mathcal{F}_n$ антимонотонна и существенно зависит от всех своих переменных, то

$$\mathrm{la}_s(f) = n - 1.$$

Доказательство. Аналогично доказательству утверждения 11, за исключением того, что вместо (8) имеет место неравенство

$$\begin{gathered} v_{k+2} c_{k+2} \oplus \ldots \oplus v_n c_n \oplus w = f(b_1, \ldots, b_k, 0, c_{k+2}, \ldots, c_n) \geqslant \\ \geqslant f(b_1, \ldots, b_k, 1, c_{k+2}, \ldots, c_n) = 1 \oplus v_{k+2} c_{k+2} \oplus \ldots \oplus v_n c_n \oplus w \end{gathered}$$

для всех $c_{k+2}, \ldots, c_n \in \mathbb{F}_2$; оно справедливо лишь в случае, когда $w = 1$, $v_{k+2} = \ldots = v_n = 0$. Далее доказательство аналогично. ■

Обобщением утверждения 11 является

Следствие 11. Для функции $f \in \mathcal{M}_n$ справедливо равенство

$$\mathrm{la}_s(f) = \mathrm{ev}(f) - 1.$$

Доказательство. Случай $\mathrm{ev}(f) = n$ доказан в утверждении 11.

Пусть функция f содержит $d < n$ существенных переменных. Без ограничения общности считаем переменные $x_{d+1}, \ldots, x_n$ фиктивными, т. е. в многочлене Жегалкина функции f присутствуют только мономы, содержащие переменные $x_1, \ldots, x_d$. Тогда $\mathrm{la}_s(f) \leqslant d - 1$. Если $\mathrm{la}_s(f) < d - 1$, то аналогично доказательству утверждения 11 получим, что функция f содержит более чем $n - d$ фиктивных переменных, т. е. существенных переменных меньше чем d, — противоречие. Значит, $\mathrm{la}_s(f) = d-1$. ■

Для антимонотонных функций справедливо аналогичное утверждение, доказательство которого аналогично.

Следствие 12. Для антимонотонной функции $f \in \mathcal{F}_n$ справедливо равенство

$$\mathrm{la}_s(f) = \mathrm{ev}(f) - 1.$$

4. Асимптотические оценки уровня сильной аффинности

Будем говорить, что некоторое свойство асимптотически выполняется для почти всех булевых функций, если доля функций в $\mathcal{F}_n$, для которых это свойство выполняется, при $n \to \infty$, стремится к единице.

Асимптотическое поведение уровня аффинности описано В. Г. Рябовым в начале 1980-х и в более общем виде опубликовано в [11]. Для квадратичных форм асимптотическое поведение уровня аффинности изучено в [12].

В работах [6, 7, 13] также исследовано асимптотическое поведение уровня аффинности, в частности, доказана следующая

Теорема 5 [13]. Асимптотически при $n \to \infty$ для почти всех булевых функций $f \in \mathcal{F}_n$ справедливо

$$n - \lfloor \log_2 n \rfloor \leqslant \mathrm{la}(f) \leqslant n - \lceil \log_2 n \rceil + 1.$$

Изучим асимптотическое поведение уровня сильной аффинности. Для этого сначала оценим мощность множества $\mathcal{SA}_n^{\leqslant k}$ для произвольного $k \in \{0, \ldots, n-2\}$.

Утверждение 12. Для произвольного $k \in \{0, \ldots, n-2\}$ справедливо следующее неравенство:

$$2^{(n-k+1)2^k} \leqslant |\mathcal{SA}_n^{\leqslant k}| \leqslant \binom{n}{k} 2^{(n-k+1)2^k}.$$

Доказательство. По определению для $f \in \mathcal{SA}_n^{\leqslant k}$ выполнено $\mathrm{la}_s(f) \leqslant k$. Тогда, воспользовавшись логическим отрицанием п. 2 следствия 6, получим, что существует такой набор $1 \leqslant i_1 < i_2 < \ldots < i_{n-k} \leqslant n$, что ни один моном многочлена Жегалкина функции f не содержит произведения вида $x_{i_j} x_{i_l}$, $1 \leqslant j < l \leqslant n - k$.

Ввиду утверждения 4, $\deg(f) \leqslant k+1$. Ясно, что никакой моном, содержащий две и более переменных из множества $\{x_{i_1}, \ldots, x_{i_{n-k}}\}$, не содержится в многочлене Жегалкина функции $f \in \mathcal{SA}_n^{\leqslant k}$, т. е. среди мономов этого многочлена могут быть мономы, содержащие переменные только из множества $\{x_1, \ldots, x_n\} \setminus \{x_{i_1}, \ldots, x_{i_{n-k}}\} = \{y_1, \ldots, y_k\}$

либо одну переменную из $\{x_{i_1}, \ldots, x_{i_{n-k}}\}$, а остальные из $\{y_1, \ldots, y_k\}$. Такие мономы назовём допустимыми. Посчитав количество допустимых мономов и возведя двойку в степень этого числа, получим количество функций из класса $\mathcal{SA}_n^{\leqslant k}$ с фиксированным набором $1 \leqslant i_1 < i_2 < \ldots < i_{n-k} \leqslant n$, это и будет искомой оценкой снизу:

— число допустимых мономов степени 0: 1;
— число допустимых мономов степени 1: n;
— число допустимых мономов степени 2: $\binom{k}{2} + (n-k)\binom{k}{1}$;
— число допустимых мономов степени 3: $\binom{k}{3} + (n-k)\binom{k}{2}$;
$\ldots$
— число допустимых мономов степени $k-1$: $\binom{k}{k-1} + (n-k)\binom{k}{k-2}$;
— число допустимых мономов степени k: $\binom{k}{k} + (n-k)\binom{k}{k-1}$;
— число допустимых мономов степени $k+1$: $(n-k)\binom{k}{k}$.

Всего допустимых мономов:

$$1 + n + \binom{k}{2} + (n-k)\binom{k}{1} + \binom{k}{3} + (n-k)\binom{k}{2} + \ldots + \binom{k}{k-1} + (n-k)\binom{k}{k-2} +$$
$$+ \binom{k}{k} + (n-k)\binom{k}{k-1} + (n-k)\binom{k}{k} = 1 + n + \sum_{i=2}^{k}\binom{k}{i} + (n-k)\sum_{i=1}^{k}\binom{k}{i} =$$
$$= 1 + n + (2^k - 1 - k) + (n-k)(2^k - 1) = (n-k+1)2^k.$$

Таким образом, доказана оценка снизу. Набор длины $n-k$ можем выбрать $\binom{n}{k}$ способами, откуда следует искомая оценка сверху. ■

Замечание 5. Данная оценка сверху не является достижимой, так как различным наборам длины $n-k$ может соответствовать одна и та же функция. Например, для функции $g(x_1, \ldots, x_6) = x_1x_2x_5x_6 \oplus x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_5x_6$ справедливо $\mathrm{la}_s(g) = 3$ и ей соответствуют два различных набора длины 3: $1 < 2 < 5$ и $1 < 2 < 6$.

Теорема 6. Асимптотически при $n \to \infty$ для почти всех булевых функций $f \in \mathcal{F}_n$ справедливо равенство

$$\mathrm{la}_s(f) = n - 1.$$

Доказательство. Оценим число функций с уровнем сильной аффинности, равным $n-1$.

Так как $|\mathcal{SA}_n^{\leqslant n-1}| = 2^{2^n}$ и по утверждению 12 $|\mathcal{SA}_n^{\leqslant n-2}| \leqslant \binom{n}{2} 2^{3 \cdot 2^{n-2}}$, то

$$|\mathcal{SA}_n^{n-1}| = |\mathcal{SA}_n^{\leqslant n-1}| - |\mathcal{SA}_n^{\leqslant n-2}| \geqslant 2^{2^n} - \binom{n}{2} 2^{3 \cdot 2^{n-2}}.$$

Оценим долю таких функций при $n \to \infty$:

$$\frac{|\mathcal{SA}_n^{n-1}|}{2^{2^n}} \geqslant 1 - \binom{n}{2} 2^{3 \cdot 2^{n-2}} / 2^{2^n} = 1 - \binom{n}{2} 2^{3 \cdot 2^{n-2} - 2^n} = 1 - \frac{n(n-1)}{2^{2^{n-2}+1}} \to 1.$$

Отсюда следует искомое утверждение. ■

ЛИТЕРАТУРА

1. *Ars G., Faugere J.-C., Imai H., et al.* Comparsion between XL and Grobner basis algorithms // LNCS. 2004. V. 3329. P. 148–172.
2. *Joux A. and Vitse V.* A crossbred algorithm for solving Boolean polynomial systems // LNCS. 2018. V. 10737. P. 3–21.
3. *Логачев О. А., Сукаев А. А., Федоров С. Н.* Об одном методе решения систем квадратичных булевых уравнений, использующем локальные аффинности булевых функций // Информ. и её примен. 2019. Т. 13. № 2. С. 37–46.
4. *Буряков М. Л., Логачев О. А.* Об уровне аффинности булевых функций // Дискретная математика. 2005. Т. 17. № 4. С. 98–107.
5. *Буряков М. Л.* О связи уровня аффинности с криптографическими параметрами булевых функций // Дискретная математика. 2008. Т. 20. № 2. С. 3–14.
6. *Буряков М. Л.* Асимптотические оценки уровня аффинности для почти всех булевых функций // Дискретная математика. 2008. Т. 20. № 3. С. 73–79.
7. *Логачев О. А.* Нижняя граница уровня аффинности для почти всех булевых функций // Дискретная математика. 2008. Т. 20. № 4. С. 85–88.
8. *Бабуева А. А., Логачев О. А., Ященко В. В.* О связи локальных аффинностей булевой функции с некоторыми видами ее вырожденности // Дискретная математика. 2022. Т. 34. № 2. С. 7–25.
9. *Логачев О. А., Сальников А. А., Ященко В. В.* Булевы функции в теории кодирования и криптологии. М.: МЦНМО, 2004.
10. *Logachev O. A., Yashchenko V. V., and Denisenko M. P.* Local affinity of Boolean mappings // Boolean Functions in Cryptology and Information Security. V. 18. IOS Press, 2008. P. 148–172.
11. *Рябов В. Г.* О степени ограничений функций q-значной логики на линейные многообразия // Прикладная дискретная математика. 2019. № 45. С. 13–25.
12. *Черемушкин А. В.* Об оценке уровня аффинности квадратичных форм // Дискретная математика. 2017. Т. 29. № 1. С. 114–125.
13. *Логачев О. А.* О значениях уровня аффинности для почти всех булевых функций // Прикладная дискретная математика. 2010. № 3. С. 17–21.

REFERENCES

1. *Ars G., Faugere J.-C., Imai H., et al.* Comparsion between XL and Grobner basis algorithms. LNCS, 2004, vol. 3329, pp. 148–172.
2. *Joux A. and Vitse V.* A crossbred algorithm for solving Boolean polynomial systems. LNCS, 2018, vol. 10737, pp. 3–21.
3. *Logachev O. A., Sukaev A. A., and Fedorov S. N.* Ob odnom metode resheniya sistem kvadratichnykh bulevykh uravneniy, ispol'zuyushchem lokal'nye affinnosti bulevykh funktsiy [On local affinity based method of solving systems of quadratic Boolean equations]. Informatika i Ee Primeneniya, 2019, vol. 13, no. 2, pp. 37–46. (in Russian)
4. *Buryakov M. L. and Logachev O. A.* On the affinity level of Boolean functions. Discrete Math. Appl., 2005, vol. 15, no. 5, pp. 479–488.
5. *Buryakov M. L.* The relationship between the level of affinity and cryptographic parameters of Boolean functions. Discrete Math. Appl., 2008, vol. 18, no. 3, pp. 227–238.
6. *Buryakov M. L.* Asymptotic bounds for the affinity level for almost all Boolean functions. Discrete Math. Appl., 2008, vol. 18, no. 5, pp. 545–551.
7. *Logachev O. A.* A lower bound for the affinity level for almost all Boolean functions. Discrete Math. Appl., 2008, vol. 18, no. 5, pp. 553–556.

8. *Babyeva A. A., Logachev O. A., and Yashchenko V. V.* On the relationship between local affinities of a Boolean function and some types of its degeneracy. Discrete Math. Appl., 2023, vol. 33, no. 6, pp. 339–353.
9. *Logachev O. A., Sal'nikov A. A., and Yashchenko V. V.* Bulevy funktsii v teorii kodirovaniya i kriptologii [Boolean Functions in Coding Theory and Cryptology]. Moscow, MCCME Publ., 2004. (in Russian)
10. *Logachev O. A., Yashchenko V. V., and Denisenko M. P.* Local affinity of Boolean mappings. Boolean Functions in Cryptology and Information Security, vol. 18, IOS Press, 2008, pp. 148–172.
11. *Ryabov V. G.* O stepeni ogranicheniy funktsiy q-znachnoy logiki na lineynye mnogoobraziya [On the degree of restrictions of q-valued logic functions to linear manifolds]. Prikladnaya Diskretnaya Matematika, 2019, no. 45, pp. 13–25. (in Russian)
12. *Cheremushkin A. V.* Estimating the level of affinity of a quadratic form. Discrete Math. Appl., 2017, vol. 27, no. 6, pp. 339–347.
13. *Logachev O. A.* O znacheniyakh urovnya affinnosti dlya pochti vsekh bulevykh funktsiy [On values of affinity level for almost all Boolean functions]. Prikladnaya Diskretnaya Matematika, 2010, no. 3, pp. 17–21. (in Russian)