2010 Теоретические основы прикладной дискретной математики №3(9)

DOI 10.17223/20710410/9/2
УДК 519.7

# О ЗНАЧЕНИЯХ УРОВНЯ АФФИННОСТИ ДЛЯ ПОЧТИ ВСЕХ БУЛЕВЫХ ФУНКЦИЙ[1]

О. А. Логачев

*Институт проблем информационной безопасности,*
*Московский государственный университет им. М. В. Ломоносова, г. Москва, Россия*

**E-mail:** logol@iisi.msu.ru

Рассматривается асимптотическое поведение значений параметра булевой функции, называемого уровнем (обобщенным уровнем) аффинности. Показано, что асимптотически при $n \to \infty$ для почти всех булевых функций от $n$ переменных значения уровня (обобщенного уровня) аффинности принадлежат сегменту $[n - \log_2 n, n - \log_2 n + 1]$.

**Ключевые слова:** *уровень аффинности, обобщенный уровень аффинности, системы булевых уравнений, криптография.*

## Введение

Один из возможных методов линеаризации систем булевых уравнений связан с частичным опробованием некоторого подмножества переменных и сведением исходной системы к линейному следствию. В работах [1, 2] был рассмотрен параметр, называемый уровнем (обобщенным уровнем) аффинности и характеризующий эффективность такой линеаризации. Различные свойства уровня (обобщенного уровня) аффинности изучались в работах [3 – 6]. Систематическое исследование этого параметра было проведено в [7].

## 1. Основные понятия и определения

Пусть $\mathbb{F}_2$ — поле из двух элементов, $V_n = \mathbb{F}_2^n$ — линейное пространство векторов (наборов) длины $n$ над полем $\mathbb{F}_2$. Вес Хэмминга вектора $\mathbf{x} = (x_1, \ldots, x_n) \in V_n$ определяется как $\mathrm{wt}(\mathbf{x}) = \sum\limits_{i=1}^{n} x_i$. Пусть $L$ — некоторое подпространство пространства $V_n$, $\dim L = r$ и $\mathbf{v} \in V_n$. Смежный класс $\pi = L \oplus \mathbf{v}$, где $\oplus$ — сложение по $\bmod 2$, будем называть плоскостью размерности $r$ пространства $V_n$ и писать $\dim \pi = r$. Будем считать, что $\dim \pi = -1$, если $\pi = \varnothing$, и $\dim \pi = 0$, если $\pi = \{\mathbf{u}\}$, $\mathbf{u} \in V_n$. Множество всех плоскостей пространства $V_n$ (включая пустую плоскость) обозначим через $\mathcal{P}(V_n)$.

Через $\mathcal{F}_n$ будем обозначать множество всех булевых функций от $n$ переменных. Любая булева функция $f \in \mathcal{F}_n$ может быть представлена в полиномиальной форме

$$f(\mathbf{x}) = f(x_1, \ldots, x_n) = \bigoplus_{\mathbf{u} \in V_n} g(\mathbf{u}) \mathbf{x}^{\mathbf{u}} = \bigoplus_{(u_1, \ldots, u_n) \in V_n} g(u_1, \ldots, u_n) x_1^{u_1} \cdot \ldots \cdot x_n^{u_n}, \qquad (1)$$

называемой алгебраической нормальной формой (АНФ) этой функции, где $g \in \mathcal{F}_n$ и для любого $1 \leqslant i \leqslant n$

$$x_i^{u_i} = \begin{cases} 1, & u_i = 0, \\ x_i, & u_i = 1. \end{cases}$$

[1]Работа поддержана РФФИ (проекты 09-01-00653-а, 10-01-00475-а).

Алгебраической степенью функции $f$, обозначаемой $\deg f$, является максимальное значение $\mathrm{wt}(\mathbf{u})$ по тем $\mathbf{u} \in V_n$, для которых $g(\mathbf{u}) = 1$. Через $\deg(f, x_i)$ обозначается максимальное значение $\mathrm{wt}(\mathbf{u})$ по тем $\mathbf{u} \in V_n$, для которых $g(\mathbf{u}) = 1$ и $u_i = 1$. Обозначим через $\mathcal{A}_n$ множество аффинных функций, то есть $\mathcal{A}_n = \{f \in \mathcal{F}_n : \deg(f) \leqslant 1\}$.

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

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

**Определение 1** [2]. Уровнем аффинности $\mathrm{la}(f)$ булевой функции $f$ из $\mathcal{F}_n$ называется минимальное число $k$, для которого функция $f$ является $k$-аффинной.

Пусть $f \in \mathcal{F}_n$ и $S$ — произвольное подмножество пространства $V_n$. Ограничением (сужением) $f|_S$ функции $f$ на множество $S$ будем называть отображение $f' \colon S \mapsto \mathbb{F}_2$, такое, что $f'(\mathbf{x}) = f|_S(\mathbf{x}) = f(\mathbf{x})$ для всех $\mathbf{x} \in S$.

Пусть $f \in \mathcal{F}_n$. Плоскость $\pi \in \mathcal{P}(V_n) \setminus \{\varnothing\}$ называется локальной аффинностью булевой функции $f$, если существует аффинная функция $l \in \mathcal{A}_n$, такая, что $f|_\pi = l|_\pi$. Обозначим

$$\tilde{\mathcal{P}}_f(V_n) = \{\pi \in \mathcal{P}(V_n) \setminus \{\varnothing\} : \exists l \in \mathcal{A}_n \ (f|_\pi = l|_\pi)\}$$

— совокупность локальных аффинностей функции $f$.

**Определение 2** [6]. Обобщенным уровнем аффинности $\mathrm{La}(f)$ функции $f \in \mathcal{F}_n$ называется неотрицательное число

$$\mathrm{La}(f) = n - \max_{\pi \in \tilde{\mathcal{P}}_f(V_n)} \dim \pi.$$

**Замечание 1.** При всей близости понятий, введенных в определениях 1 и 2, имеется существенное их различие. Обобщенный уровень аффинности, в отличие от уровня аффинности, является аффинным инвариантом, то есть инвариантом относительно действия на функцию полной аффинной группы (см. [8]).

**Замечание 2.** Очевидно, что

$$\mathrm{La}(f) \leqslant \mathrm{la}(f) \tag{2}$$

для произвольной булевой функции $f$ из $\mathcal{F}_n$.

## 2. Вспомогательные результаты

Асимптотическое поведение уровня (обобщенного уровня) аффинности исследовалось в работах [5 – 7].

Справедлива следующая асимптотическая нижняя оценка для обобщенного уровня аффинности булевых функций.

**Теорема 1** [6]. Пусть $\alpha \in \mathbb{R}, \alpha > 1$ — фиксированная константа. Тогда асимптотически при $n \to \infty$ для почти всех булевых функций $f$ из $\mathcal{F}_n$ справедливо неравенство

$$\mathrm{La}(f) \geqslant n - \alpha \log_2 n.$$

**Следствие 1** [6]. Пусть $\alpha \in \mathbb{R}, \alpha > 1$ — фиксированная константа. Тогда асимптотически при $n \to \infty$ для почти всех булевых функций $f$ из $\mathcal{F}_n$ справедливо неравенство

$$\mathrm{la}(f) \geqslant n - \alpha \log_2(n).$$

Сформулируем утверждение, непосредственно вытекающее из следствия 1 в силу условий, накладываемых на константу $\alpha$.

**Утверждение 1.** Асимптотически при $n \to \infty$ для почти всех булевых функций $f$ из $\mathcal{F}_n$ справедливо неравенство

$$\mathrm{la}(f) \geqslant n - \log_2(n). \tag{3}$$

## 3. Основной результат

Обозначим через $\mathcal{M}_{n,k}$, $1 \leqslant k \leqslant n$, множество функций из $\mathcal{F}_n$, для которых выполняется неравенство $\mathrm{la}(f) \leqslant k$, и $\overline{\mathcal{M}}_{n,k} = \mathcal{F}_n \setminus \mathcal{M}_{n,k}$. Соответствующую долю множества $\mathcal{M}_{n,k}$ в $\mathcal{F}_n$ обозначим $\delta_{n,k} = \mathrm{card}\ \mathcal{M}_{n,k}/2^{2^n}$.

Справедливо следующее утверждение.

**Теорема 2.** Асимптотически при $n \to \infty$ для почти всех булевых функций $f$ из $\mathcal{F}_n$ справедливо неравенство

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

***Доказательство.*** Пусть $f \in \mathcal{F}_n$ и $1 \leqslant k \leqslant n$. Рассмотрим разложение $f$ в сумму ее подфункций по переменным $x_1, \ldots, x_k$ вида

$$f(x_1, \ldots, x_n) = \bigoplus (x_1 \oplus u_1 \oplus 1) \ldots (x_k \oplus u_k \oplus 1) f^{u_1,\ldots,u_k}_{1,\ldots,k}(x_{k+1}, \ldots, x_n). \tag{4}$$

Если $f \in \overline{\mathcal{M}}_{n,k}$, то необходимо, чтобы все подфункции $f^{u_1,\ldots,u_k}_{1,\ldots,k}$ из разложения (4) имели алгебраическую степень не менее 2, то есть не являлись бы аффинными функциями из $\mathcal{A}_{n-k}$. Следовательно,

$$\mathrm{card}\ \overline{\mathcal{M}}_{n,k} \leqslant (2^{2^{n-k}} - 2^{n-k+1})^{2^k}$$

и

$$\mathrm{card}\ \mathcal{M}_{n,k} \geqslant 2^{2^n} - (2^{2^{n-k}} - 2^{n-k+1})^{2^k}.$$

Тогда

$$\delta_{n,k} \geqslant 1 - \left( \frac{2^{2^{n-k}} - 2^{n-k+1}}{2^{2^{n-k}}} \right)^{2^k} = 1 - \alpha_{n,k}. \tag{5}$$

Положим $k = n - \log_2 n + 1$ и устремим $n \to \infty$. Для величины $\alpha_{n,n-\log_2 n+1}$ справедлива следующая цепочка равенств:

$$\alpha_{n,n-\log_2 n+1} = \left( 1 - \frac{2^{n-(n-\log_2 n+1)+1}}{2^{2^{n-(n-\log_2 n+1)}}} \right)^{2^{n-\log_2 n+1}} =$$

$$= \left(1 - \frac{n}{2^{n/2}}\right)^{\frac{2^{n+1}}{n}} = \left( \left( 1 + \frac{-1}{\frac{2^{n/2}}{n}} \right)^{\frac{2^{n/2}}{n}} \right)^{2^{n/2+1}}. \tag{6}$$

Воспользовавшись известным соотношением

$$\lim_{t\to\infty} \left(1 + \frac{d}{t}\right)^t = e^d, d \in \mathbb{R}, \tag{7}$$

совместно с (6), получаем

$$\lim_{n\to\infty} \alpha_{n,n-\log_2 n+1} = 0. \tag{8}$$

Следовательно, соотношения (5) и (8) дают

$$\lim_{n\to\infty} \delta_{n,n-\log_2 n+1} = 1, \tag{9}$$

что и доказывает утверждение теоремы. ■

**Следствие 2.** Асимптотически при $n \to \infty$ для почти всех булевых функций $f$ из $\mathcal{F}_n$ справедливо неравенство

$$\mathrm{La}(f) \leqslant n - \log_2 n + 1.$$

***Доказательство.*** Непосредственно следует из утверждения теоремы 2 и неравенства (2). ■

Поскольку для любой функции $f$ из $\mathcal{F}_n$ значения $\mathrm{la}(f)$ и $\mathrm{La}(f)$ являются неотрицательными целыми числами, то утверждения следствий 1, 2, утверждения 1 и теорем 1, 2 могут быть объединены следующим образом.

**Теорема 3.** Асимптотически при $n \to \infty$ для почти всех булевых функций $f$ из $\mathcal{F}_n$ выполнены условия

$$\begin{array}{l} 1)\ n - \lfloor \log_2 n \rfloor \leqslant \mathrm{la}(f) \leqslant n - \lceil \log_2 n \rceil + 1, \\ 2)\ n - \lfloor \log_2 n \rfloor \leqslant \mathrm{La}(f) \leqslant n - \lceil \log_2 n \rceil + 1. \end{array} \tag{10}$$

Легко видеть, что условия (10) выделяют два возможных случая $n = 2^b$ и $n \neq 2^b$. В случае, когда $n = 2^b$, для почти всех булевых функций имеется два возможных значения уровня (обобщенного уровня) аффинности: $n-b$, $n-b+1$. А в случае, когда $n$ не является степенью 2, для почти всех функций из $\mathcal{F}_n$ имеется одно возможное значение для уровня (обобщенного уровня) аффинности: $n - \lfloor \log_2 n \rfloor = n - \lceil \log_2 n \rceil + 1$.

**Замечание 3.** Воспользовавшись соотношениями (6) и (7), можно легко показать, что в случае $n = 2^b$

$$\lim_{b\to\infty} \delta_{n,n-b} \geqslant 1 - e^{-2}.$$

ЛИТЕРАТУРА

1. *Логачев О. А., Сальников А. А., Ященко В. В.* Корреляционная иммунность и реальная секретность // Математика и безопасность информационных технологий. М.: МЦНМО, 2004. С. 165–170.
2. *Логачев О. А., Сальников А. А., Ященко В. В.* Комбинирующие $k$-аффинные функции // Математика и безопасность информационных технологий. М.: МЦНМО, 2004. С. 176–178.
3. *Буряков М. Л., Логачев О. А.* О распределении уровня аффинности на множестве булевых функций // Математика и безопасность информационных технологий. М.: МЦНМО, 2005. С. 141–146.
4. *Буряков М. Л., Логачев О. А.* Об уровне аффинности булевых функций // Дискретная математика. 2005. Т. 17. Вып. 4. С. 98–107.
5. *Логачев О. А.* Нижняя оценка уровня аффинности для почти всех булевых функций // Там же. 2008. Т. 20. Вып. 4. С. 85–88.
6. *Буряков М. Л.* Асимптотические оценки уровня аффинности для почти всех булевых функций // Там же. 2008. Т. 20. Вып. 3. С. 73–79.

7. *Буряков М. Л.* Алгебраические, комбинаторные и криптографические свойства параметров аффинных ограничений булевых функций: дис. ... канд. физ.-мат. наук. М., 2007.
8. *Логачев О. А., Сальников А. А., Ященко В. В.* Булевы функции в теории кодирования и криптологии. М.: МЦНМО, 2004.