

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

DOI 10.17223/20710410/12/1

УДК 519.7

О НЕКОТОРЫХ МЕРАХ НЕЛИНЕЙНОСТИ БУЛЕВЫХ ФУНКЦИЙ¹

Е. К. Алексеев

*Московский государственный университет им. М. В. Ломоносова, г. Москва, Россия***E-mail:** geni-cmc@mail.ru

Рассматривается расстояние до алгебраически вырожденных функций как мера нелинейности булевых функций. Устанавливаются соотношения между этим расстоянием и некоторыми ранее предложенными мерами нелинейности булевых функций. Исследуется порядок алгебраической вырожденности тех функций, которые наилучшим образом аппроксимируют данную.

Ключевые слова: *нелинейность булевых функций, алгебраически вырожденные функции, пространство линейных структур, криптография.*

Введение

Одним из приемов современного криптоанализа является использование близости (относительно некоторой метрики) криптографических отображений к отображениям, позволяющим свести исходную криптографическую задачу к менее трудоемкой. Яркими примерами этого являются корреляционный [1] и линейный [2] методы криптоанализа. Одна из возможных характеристик, показывающая эффективность этих методов, была названа нелинейностью булевой функции [3]. Однако могут быть использованы не только линейные (аффинные) приближения. В работе [3] также рассматривались меры близости к другим «слабым» с криптографической точки зрения классам функций. Множество алгебраически вырожденных функций в этом плане представляет определенный практический и теоретический интерес.

В данной работе рассматривается расстояние до алгебраически вырожденных функций. Устанавливаются соотношения между этим расстоянием и некоторыми ранее предложенными мерами нелинейности булевых функций. Рассматривается также степень алгебраической вырожденности тех функций, которые наилучшим образом аппроксимируют данную функцию.

1. Основные определения и обозначения

Пусть F_2 — конечное поле из двух элементов. Пусть $V_n = \underbrace{F_2 \times \dots \times F_2}_n$ — векторное пространство наборов длины n с компонентами из F_2 . Булевой функцией от n переменных будем называть отображение из V_n в F_2 . Множество всех булевых функций от n переменных будем обозначать $\mathcal{F}_n$. Носителем функции $f \in \mathcal{F}_n$ называется множество $1_f = \{x \in V_n : f(x) = 1\}$. Весом $\text{wt}(f)$ булевой функции $f \in \mathcal{F}_n$ называется мощность ее носителя 1_f .

¹Работа поддержана РФФИ (проект № 09-01-00653-а).

В дальнейшем будем придерживаться следующих обозначений: $x^{(i)}$ — i -й вектор из некоторой совокупности векторов; x_j — j -я компонента вектора x . Если n — натуральное число, а $c \in \{0, 1\}$, то через c^n будем обозначать вектор длины n , все компоненты которого равны c . Константные булевы функции будем обозначать через $\bar{0}$ и $\bar{1}$.

Пусть L — подмножество пространства V_n . Тот факт, что L является подпространством пространства V_n , будем обозначать так: $L < V_n$. Для произвольного линейного подпространства $L < V_n$ через L^* будем обозначать множество $L \setminus \{0^n\}$. Плоскостями в V_n будем называть смежные классы по подпространствам этого пространства.

Индикаторной функцией множества $S \subseteq V_n$ называется такая функция $I_S \in \mathcal{F}_n$, что $I_S(x) = 1$ тогда и только тогда, когда $x \in S$.

Для булевой функции f от n переменных и вектора $u \in V_n$ будем обозначать через f^u функцию $f^u(x) = f(x \oplus u)$. *Производной булевой функции* f по направлению $u \in V_n^*$ называется функция $D_u f = f \oplus f^u$. Через $J(f)$ будем обозначать подпространство $\{u \in V_n : f^u = f\}$ пространства V_n .

Пусть A — $(n \times k)$ -матрица над F_2 , а g — булева функция от k переменных. Через g^A будем обозначать функцию от n переменных $g^A(x) = g(xA)$.

Утверждение 1 [4]. Любая функция $f \in \mathcal{F}_n$ представима в виде

$$f = \bigoplus_{i=1}^{2^{n-\dim J(f)}} \varepsilon_i I_{J(f) \oplus z^{(i)}},$$

где $\varepsilon_i \in \{0, 1\}$; $z^{(i)} \in V_n$.

Определение 1 [5]. *Порядком алгебраической вырожденности* $AD(f)$ булевой функции $f \in \mathcal{F}_n$ называется максимально возможное значение $n - k$, где для целого числа k , $0 \leq k \leq n$, существуют такие функция $g \in \mathcal{F}_k$ и $(n \times k)$ -матрица D над F_2 , что выполнено равенство $f = g^D$. Функции, для которых $AD(f) > 0$, называются *алгебраически вырожденными*. Множество всех алгебраически вырожденных функций от n переменных обозначим через

$$DG(n) = \{f \in \mathcal{F}_n : AD(f) > 0\}.$$

Определение 2. Булева функция $f \in \mathcal{F}_n$ обладает нетривиальной *линейной структурой*, если существует такой вектор $u \in V_n^*$, что $D_u f \in \{\bar{0}, \bar{1}\}$. Подпространство $L_f = \{u \in V_n : D_u f \in \{\bar{0}, \bar{1}\}\}$ называется *пространством линейных структур* функции f .

Множество булевых функций $f \in \mathcal{F}_n$, имеющих нетривиальную линейную структуру, обозначается через $\mathcal{F}_n^0$ [6]. Легко показать, что если для $f \in \mathcal{F}_n^0$ существует такой вектор $u \in V_n^*$, что $D_u f = \bar{1}$, то $L_f = J(f) \cup (J(f) \oplus u)$.

Определение 3. *Преобразование Уолша — Адамара* булевой функции f называется целочисленная функция на V_n , определяемая следующим равенством:

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

(суммирование производится в действительной области). Для каждого $u \in V_n$ значение $W_f(u)$ называется *коэффициентом Уолша — Адамара*.

Определение 4. Пусть $f \in \mathcal{F}_n$. Целочисленная функция

$$\Delta_f(u) = \sum_{x \in V_n} (-1)^{f(x) \oplus f(x \oplus u)},$$

определенная на пространстве V_n , называется *автокорреляционной функцией*, или *автокорреляцией* булевой функции f .

Справедлива следующая теорема о связи автокорреляционной функции с преобразованием Уолша — Адамара.

Теорема 1 [6]. Пусть $f \in \mathcal{F}_n$. Тогда для любого вектора $v \in V_n$ справедливы соотношения

$$W_f^2(v) = \sum_{u \in V_n} \Delta_f(u) (-1)^{\langle u, v \rangle},$$

$$\Delta_f(v) = 2^{-n} \sum_{u \in V_n} W_f^2(u) (-1)^{\langle u, v \rangle}.$$

Определение 5. Булева функция $f \in \mathcal{F}_n$ называется *корреляционно-иммунной* порядка m , $0 < m \leq n$, если для любого вектора $u \in V_n$, такого, что $1 \leq \text{wt}(u) \leq m$, выполнено равенство $W_f(u) = 0$.

Корреляционно-иммунная порядка m функция является корреляционно-иммунной любого меньшего порядка, поэтому введем обозначение

$$\text{cor} f = \max\{m \in \mathbb{N} : f - \text{корреляционно-иммунна порядка } m\}.$$

Справедливо следующее соотношение между порядком корреляционной иммунности $\text{cor} f$ булевой функции f и ее алгебраической степенью $\deg f$.

Теорема 2 (неравенство Зигенталера). Для любой функции $f \in \mathcal{F}_n$ справедливо неравенство $\deg f + \text{cor} f \leq n$.

Определение 6. Функция $f \in \mathcal{F}_n$ называется *бент-функцией*, если все ее коэффициенты Уолша — Адамара равны $\pm 2^{n/2}$.

Определение 7. Булева функция f от n переменных называется *уравновешенной*, если $\text{wt}(f) = 2^{n-1}$. Уравновешенная корреляционно-иммунная порядка d функция $f \in \mathcal{F}_n$ называется *d -устойчивой*.

Теорема 3 (критерий Ротхауза). Булева функция $f \in \mathcal{F}_n$ является бент-функцией тогда и только тогда, когда ее производная $D_u f$ по каждому ненулевому направлению $u \in V_n^*$ уравновешена.

Определение 8. Пусть $f \in \mathcal{F}_n$. Если существует такое натуральное число $r \in \mathbb{N}$, $0 \leq r \leq n$, что квадрат каждого коэффициента Уолша — Адамара равен либо 2^{2n-2r} , либо 0, то функция f называется *платовидной функцией порядка $2r$* .

Лемма 1. Пусть $f \in \mathcal{F}_n$, $\deg f = d \geq 1$. Тогда

$$2^{n-d} \leq \text{wt}(f) \leq 2^n - 2^{n-d}.$$

2. Невырожденность булевых функций

Рассмотрим соотношение между параметром $AD(f)$ и подпространством $J(f)$.

Утверждение 2. Для любой булевой функции $f \in \mathcal{F}_n$ справедливо равенство

$$AD(f) = \dim J(f).$$

Доказательство. Пусть $\dim J(f) = n - k$. Пусть $C = J(f)$ и $u^{(1)}, \dots, u^{(k)}$ — базис пространства $C^\perp$. Пусть D — $(n \times k)$ -матрица, столбцами которой являются векторы

$u^{(1)}, \dots, u^{(k)}$. По утверждению 1 функция f может быть представлена следующим образом: $f = I_{C \oplus z^{(1)}} \oplus \dots \oplus I_{C \oplus z^{(t)}}$, где $t \leq 2^k$. Пусть функция $g \in \mathcal{F}_k$ такова, что $g(x) = 1$ тогда и только тогда, когда существует номер $i = 1, \dots, t$, что $x = z^{(i)}D$.

Покажем, что $f(x) = g(xD)$ для любого вектора $x \in V_n$. Поскольку множество 1_f представимо в виде объединения смежных классов $C \oplus z^{(1)}, \dots, C \oplus z^{(t)}$, то для векторов $x \in 1_f$ и только для них справедливо представление $x = z^{(i)} \oplus c$, где $i \in \{1, \dots, t\}$, $c \in C$. Поэтому верно соотношение $g(xD) = g(z^{(i)}D \oplus cD) = g(z^{(i)}D) = 1 = f(x)$. Таким образом, $AD(f) \geq \dim J(f)$.

Пусть $AD(f) = n - k$ и D — такая $(n \times k)$ -матрица ранга k , столбцами которой являются векторы $u^{(1)}, u^{(2)}, \dots, u^{(k)}$ пространства V_n , что $f(x) = g(xD)$. Пусть C — линейное подпространство пространства V_n с базисом $u^{(1)}, \dots, u^{(k)}$. Тогда для любого $u \in C^\perp$ и любого $x \in V_n$ выполнено $f(x \oplus u) = g((x \oplus u)D) = g(xD \oplus uD) = g(xD) = f(x)$. Таким образом, $C^\perp \subseteq J(f)$ и $AD(f) = \dim C^\perp \leq \dim J(f)$.

Учитывая ранее доказанное обратное неравенство, получаем $AD(f) = \dim J(f)$. ■

В работе [3] были введены следующие меры нелинейности булевых функций:

$$\begin{aligned} \text{nl}(f) &= \text{dist}(f, \mathcal{A}_n) = 2^{n-1} - \frac{1}{2} \max_{u \in V_n} |W_f(u)|; \\ \delta(f) &= \text{dist}(f, \mathcal{F}_n^0) = 2^{n-2} - \frac{1}{4} \max_{u \in V_n^*} |\Delta_f(u)|. \end{aligned}$$

Будем называть *невыврожденностью* функции $f \in \mathcal{F}_n$ значение

$$\rho(f) = \text{dist}(f, DG(n)).$$

Заметим, что параметры $AD(f)$, $\text{nl}(f)$, $\delta(f)$ и $\rho(f)$ являются аффинными инвариантами.

Утверждение 3. Пусть $f \in \mathcal{F}_n$ и u — произвольный вектор из V_n^* . Если функция $g \in DG(n)$ такова, что $u \in J(g)$ и $\text{dist}(f, g) = \min_{g': u \in J(g')} \text{dist}(f, g')$, то g представима в виде $g = f \cdot f^u \oplus h$, где для функции $h \in \mathcal{F}_n$ выполняется условие $D_u f \cdot h = h$ и $u \in J(h)$.

Доказательство. Покажем, что $1_g \subseteq 1_{f \vee f^u}$ и $1_{f \cdot f^u} \subseteq 1_g$.

Пусть $h_1 = g((f \vee f^u) \oplus \bar{1})$. Тогда $u \in J(h_1)$. Но $\text{dist}(g \oplus h_1, f) \leq \text{dist}(g, f)$ и $u \in J(g \oplus h_1)$. Поэтому $h_1 = \bar{0}$, т. е. $1_g \subseteq 1_{f \vee f^u}$.

Пусть $h_2 = (g \oplus \bar{1})(f \cdot f^u)$. Тогда $u \in J(h_2)$ и $u \in J(g \oplus h_2)$. Но $\text{dist}(g \oplus h_2, f) \leq \text{dist}(g, f)$. Поэтому $h_2 = \bar{0}$, т. е. $1_{f \cdot f^u} \subseteq 1_g$.

Поскольку $1_{f \cdot f^u} \subseteq 1_g$, то g представима в виде $g = f \cdot f^u \oplus h$, где $h \cdot f \cdot f^u = \bar{0}$ и $u \in J(h)$. Поскольку $1_g \subseteq 1_{f \vee f^u}$, а $f \vee f^u = f \cdot f^u \oplus D_u f$, то для функции h выполнено $h \cdot D_u f = h$. Показанные соотношения доказывают утверждение. ■

Следствие 1. Для любой булевой функции $f \in \mathcal{F}_n$ справедливо соотношение

$$\rho(f) = \min_{u \in V_n^*} \frac{\text{wt}(D_u f)}{2} = 2^{n-2} - \frac{1}{4} \max_{u \in V_n^*} \Delta_f(u).$$

Доказательство. Из определения параметра ρ следует, что справедливо равенство $\rho(f) = \min_{u \in V_n^*} \min_{g': u \in J(g')} \text{dist}(f, g')$. Вычислим $\text{dist}(f, g)$ для тех функций g , для которых существует ненулевой вектор $u \in J(g)$ и $\text{dist}(f, g) = \min_{g': u \in J(g')} \text{dist}(f, g')$. Из утверждения 3 следует, что $g = f \cdot f^u \oplus h$, где $u \in J(h)$ и $h \cdot D_u f = h$. Для функции h

выполняется равенство $h = h_1 \oplus h_2$, где $h_1 \cdot h_2 = \bar{0}$, $h_1^u = h_2$ и справедливы соотношения $h_1(f \oplus f \cdot f^u) = h_1$ и $h_2(f \oplus f \cdot f^u) = \bar{0}$. Поэтому $\text{dist}(f, g) = \text{wt}(f \oplus f \cdot f^u \oplus h_1 \oplus h_2) = \text{wt}(f) - \text{wt}(f \cdot f^u) - \text{wt}(h_1) + \text{wt}(h_2) = \text{wt}(D_u f)/2$. Это соотношение доказывает первое равенство. Второе равенство следует из первого и из того, что

$$\Delta_f(u) = W_{D_u f}(0^n) = 2^n - 2 \text{dist}(D_u f, \bar{0}) = 2^n - 2 \text{wt}(D_u f).$$

Следствие доказано. ■

Следствие 2. Пусть $f \in \mathcal{F}_n$. Если $g \in DG(n)$ и $\text{dist}(f, g) = \rho(f)$, то для любого вектора $u \in J^*(g)$ справедливо равенство $\Delta_f(u) = \max\{\Delta_f(v) : v \in V_n^*\}$.

Доказательство. Пусть u — произвольный вектор из $J^*(g)$. Тогда, по утверждению 3, функция g представима в виде $g = f \cdot f^u \oplus h_u$. Отсюда и из следствия 1 получаем, что

$$\text{dist}(f, g) = \frac{\text{wt}(D_u f)}{2} = 2^{n-2} - \frac{1}{4} \Delta_f(u) = \rho(f) = 2^{n-2} - \frac{1}{4} \max_{v \in V_n^*} \Delta_f(v).$$

Следовательно, $\Delta_f(u) = \max_{v \in V_n^*} \Delta_f(v)$. ■

Утверждение 4. Для любой булевой функции f от $n \geq 2$ переменных справедливо неравенство $\rho(f) \leq 2^{n-2}$.

Доказательство. Предположим, что для некоторой функции $f \in \mathcal{F}_n$ и для любого ненулевого вектора $u \in V_n$ справедливо $\Delta_f(u) < 0$, а поскольку числа $\Delta_f(u)$ четны, то $\Delta_f(u) \leq -2$.

Из равенства $\sum_{u \in V_n} \Delta_f(u) = W_f^2(0^n)$ следует $\sum_{u \in V_n} \Delta_f(u) \geq 0$. Но $\Delta_f(0^n) = 2^n$, а по предположению $\Delta_f(u) \leq -2$, поэтому

$$\sum_{u \in V_n} \Delta_f(u) \leq 2^n - 2(2^n - 1) = 2 - 2^n.$$

Следовательно, $\sum_{u \in V_n} \Delta_f(u) < 0$ при $n \geq 2$. Полученное противоречие показывает, что существует такой ненулевой вектор $u \in V_n$, что $\Delta_f(u) \geq 0$, а значит, $\rho(f) \leq 2^{n-2}$. ■

Заметим, что поскольку выполнены включения $\mathcal{A}_n \subset DG(n) \subset \mathcal{F}_n^0$, то

$$\text{nl}(f) \geq \rho(f) \geq \delta(f).$$

Следующий пример показывает, что высокая нелинейность не гарантирует высокой невырожденности булевой функции.

Пример 1. Рассмотрим функцию $f_{10,2}^4 \in \mathcal{F}_{10}$, построенную в работе [7]:

$$\begin{aligned} f_{10,2}^4(x) = & (x_9 \oplus x_{10} \oplus 1)(x_1 x_3 \oplus x_1 x_4 \oplus x_2 x_3 \oplus x_2 x_4 \oplus x_1 \oplus x_3 \oplus x_5 \oplus x_6 \oplus x_7 \oplus x_8) \oplus \\ & \oplus (x_9 \oplus x_{10})(x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_5 x_7 \oplus x_5 x_8 \oplus x_6 x_7 \oplus x_6 x_8 \oplus x_5 \oplus x_7) \oplus x_9. \end{aligned}$$

Функция $f_{10,2}^4$ является 6-устойчивой булевой функцией, нелинейность которой равна $2^9 - 2^7 = 384$. Однако $\rho(f_{10,2}^4) = \delta(f_{10,2}^4) = 0$, т. е. функция является алгебраически вырожденной, причем $AD(f_{10,2}^4) = 3$, а $\dim L_{f_{10,2}^4} = 4$.

Рассмотрим вопрос достижимости параметром ρ своего максимального значения 2^{n-2} . Из критерия Ротхауза следует, что для любой бент-функции f справедливо соотношение $\rho(f) = 2^{n-2}$. Для нечетного числа переменных справедлива

Теорема 4. Пусть n нечетно, функция $f \in \mathcal{F}_n$ является платовидной функцией порядка $n - 1$ и $\{u \in V_n : W_f(u) \neq 0\} = \{u \in V_n : \langle u, w \rangle = 1\}$ для некоторого ненулевого вектора w . Тогда $\rho(f) = 2^{n-2}$.

Доказательство. Рассмотрим соотношение между автокорреляционными коэффициентами и коэффициентами Уолша — Адамара функции f для ненулевого вектора u . Поскольку функция f является платовидной функцией порядка $n - 1$, то в том случае, когда $W_f^2(u) \neq 0$, справедливо равенство $W_f^2(u) = 2^{2n-(n-1)} = 2^{n+1}$. Следовательно,

$$\Delta_f(u) = \frac{1}{2^n} \sum_{v \in V_n} W_f^2(v) (-1)^{\langle u, v \rangle} = \frac{2^{n+1}}{2^n} \sum_{v: \langle v, w \rangle = 1} (-1)^{\langle u, v \rangle} = \begin{cases} 0, & \text{если } u \neq w, \\ -2^n, & \text{если } u = w. \end{cases}$$

Таким образом, $\max_{u \in V_n^*} \Delta_f(u) = 0$ и $\rho(f) = 2^{n-2}$. ■

В работе [8] было показано, что функции, удовлетворяющие условиям теоремы 4, представимы в виде $f = g^B$, где B — некоторая невырожденная $(n \times n)$ -матрица над F_2 и $g(x) = x_n \oplus h(x_1, \dots, x_{n-1})$, где h — бент-функция от $n - 1$ переменных.

Заметим, что проблема исчерпывающего описания множества функций, для которых параметр ρ достигает своего максимума, пока не решена.

3. Порядок алгебраической вырожденности наилучших аппроксимаций

Будем обозначать множество алгебраически вырожденных функций, наилучшим образом приближающих некоторую булеву функцию f , через

$$DG(f) = \{g \in DG(n) : \text{dist}(f, g) = \rho(f)\}.$$

Множество функций, имеющих нетривиальную линейную структуру и наилучшим образом приближающих функцию f , обозначим через

$$\mathcal{F}_n^0(f) = \{g \in \mathcal{F}_n^0 : \text{dist}(f, g) = \delta(f)\}.$$

Рассмотрим следующие функционалы:

$$\begin{aligned} \pi_\rho(f) &= \max_{g \in DG(f)} \dim J(g) = \max_{g \in DG(f)} AD(g); \\ \pi_\delta(f) &= \max_{g \in \mathcal{F}_n^0(f)} \dim L_g. \end{aligned}$$

Алгебраически вырожденные функции, наилучшим образом аппроксимирующие данную функцию f , находятся от нее на расстоянии $\rho(f)$. Однако на этом расстоянии могут находиться функции с разными значениями порядка алгебраической вырожденности. С точки зрения криптоанализа нужно аппроксимировать функцию f с помощью наиболее алгебраически вырожденной функции. Максимальное значение порядка алгебраической вырожденности тех функций, которые находятся от f на расстоянии $\rho(f)$, отражает параметр $\pi_\rho(f)$. Содержательный смысл параметра $\pi_\delta(f)$ аналогичен.

Определение 9. Пусть $f \in \mathcal{F}_n$; π_ρ -функцией для f назовем функцию $g_\rho \in DG(f)$, для которой $AD(g_\rho) = \pi_\rho(f)$.

Аналогично определяется понятие π_δ -функции для f .

Используя введенные понятия, можно следующим образом описать связь параметров δ , π_δ , ρ , π_ρ .

Утверждение 5. Если $\rho(f) = \delta(f)$, то $\pi_\delta(f) \in \{\pi_\rho(f), \pi_\rho(f)+1\}$. Если $\rho(f) > \delta(f)$, то $\pi_\delta(f) = 1$.

Доказательство. Пусть функции g_ρ и g_δ являются соответственно π_ρ -функцией и π_δ -функцией для f .

Пусть $\rho(f) = \delta(f)$. Тогда $\pi_\delta(f) \geq \pi_\rho(f)$, так как иначе $\dim L_{g_\rho} > \dim L_{g_\delta}$, что противоречит условию. Заметим также, что $\dim J(g_\delta) \leq \dim J(g_\rho)$. Тот факт, что для любой функции h справедливо $\dim L_h \in \{\dim J(h), \dim J(h) + 1\}$, показывает справедливость первой импликации.

Если же $\rho(f) > \delta(f)$, то $\dim J(g_\delta) = 0$, а $L_{g_\delta} = \{0^n, u\}$, где $D_u g_\delta = \bar{1}$, т. е. $\pi_\delta(f) = 1$. Утверждение доказано. ■

Заметим, что для функции $f_{10,2}^4$ из примера 1 справедливы соотношения

$$\rho(f_{10,2}^4) = \delta(f_{10,2}^4) \quad \text{и} \quad \pi_\delta(f_{10,2}^4) = \pi_\rho(f_{10,2}^4) + 1,$$

а для функции f , удовлетворяющей условиям теоремы 4, справедливы равенства

$$\delta(f) = 0 \quad \text{и} \quad \pi_\delta(f) = 1.$$

Исходя из доказанного утверждения, можно сказать, что при равенстве значений $\rho(f)$ и $\delta(f)$, вычислив один из параметров π_δ и π_ρ , можно достаточно точно оценить значение второго. Однако когда $\rho(f) \neq \delta(f)$, значение $\pi_\delta(f)$ равно 1, тогда как $\pi_\rho(f)$ необходимо вычислять. В связи с этим далее большее внимание будет уделяться именно параметру π_ρ .

Утверждение 6. Пусть $f \in \mathcal{F}_n$. Если $|\text{wt}(f) - 2^{n-1}| > \rho(f)$, то $\rho(f) = \delta(f)$ и $\pi_\rho(f) = \pi_\delta(f)$.

Доказательство. Непосредственно следует из того факта, что любая функция h , для которой существует вектор $u \in V_n^*$, такой, что $D_u h = \bar{1}$, является уравновешенной, и из определений соответствующих функционалов. ■

Теорема 5. Для любой булевой функции $f \in \mathcal{F}_n$, для которой $\rho(f) > 0$, справедливо соотношение

$$\log_2 \rho(f) + \pi_\rho(f) \leq n.$$

Доказательство. Пусть g — некоторая π_ρ -функция для f . Тогда справедливо соотношение $f = g \oplus h$, где $\text{wt}(h) = \rho(f)$. Предположим, что для некоторого вектора $u \in J(g)$ справедливо $h \cdot h^u \neq \bar{0}$. Тогда, переписав соотношение для функции f в виде $f = (g \oplus h \cdot h^u) \oplus (h \oplus h \cdot h^u)$, можно заметить, что

$$\text{dist}(f, g \oplus h \cdot h^u) = \text{wt}(h \oplus h \cdot h^u) < \text{wt}(h) = \rho(f).$$

Но это противоречит условию, поскольку функция $g \oplus h \cdot h^u$ является алгебраически вырожденной.

Получаем, что $\text{wt}(D_u h) = 2\text{wt}(h)$ для любого ненулевого вектора $u \in J(g)$. Но максимальный вес такой функции h совпадает с мощностью фактор-пространства $V_n/J(g)$. Следовательно, $\rho(f) = \text{wt}(h) \leq 2^{n-AD(g)} = 2^{n-\pi_\rho(f)}$. Утверждение теоремы получается путем логарифмирования обеих частей неравенства. ■

Заметим, что если сравнивать полученное неравенство с неравенством Зигенталера с точки зрения оптимизации криптографических параметров, то можно заметить следующее различие. С точки зрения стойкости криптографических примитивов нужно

максимизировать и $\deg(f)$, и $\text{cor}(f)$. Неравенство Зигенталера показывает, что эти два параметра вступают в противоречие друг с другом. Исходя из тех же соображений, необходимо максимизировать $\rho(f)$, но минимизировать $\pi_\rho(f)$. Полученное в теореме 5 неравенство показывает, что эти два параметра в каком-то смысле согласованы.

Следствие 3. Пусть функция $f \in \mathcal{F}_n$ такова, что $\text{nl}(f) = \rho(f)$. Тогда справедливо неравенство $\text{nl}(f) = \rho(f) \leq 2$.

Доказательство. Если $\text{nl}(f) = \rho(f)$, то существует такая аффинная функция g , что $\text{dist}(f, g) = \rho(f)$. Для этой функции справедливо соотношение $AD(g) \geq n - 1$. Отсюда $\pi_\rho(f) \geq n - 1$. Из утверждения теоремы 5 заключаем, что $\log_2 \rho(f) \leq 1$, т. е. $\rho(f) \leq 2$. ■

Следующие две леммы описывают некоторые классы булевых функций, для которых в неравенстве теоремы 5 достигается равенство.

Лемма 2. Пусть функция $f \in \mathcal{F}_n$ такова, что $\pi_\rho(f) = k > n/2$. Тогда для функции f выполнено равенство $\log_2 \rho(f) + \pi_\rho(f) = n$ тогда и только тогда, когда f представима в виде $f = g \oplus h$, где $AD(g) = k$, $\text{wt}(h) = 2^{n-k}$ и для любых различных векторов $u, v \in 1_h$ справедливо $u \oplus v \notin J(g)$.

Доказательство. Необходимость. Доказательство аналогично теореме 5.

Достаточность. Пусть $J(g) = L$. Заметим, что для любого вектора $u \in L^*$ справедливо $\text{wt } D_u f = \text{wt } (D_u g \oplus D_u h) = \text{wt } D_u h = 2 \cdot 2^{n-k} < 2 \cdot 2^{\frac{n}{2}}$.

Пусть $u \in V_n \setminus L$. Тогда $\text{wt } D_u f = \text{wt } (D_u g \oplus D_u h) \geq \text{wt } D_u g - \text{wt } D_u h$. Поскольку $\text{wt } D_u g \geq 2 \cdot 2^k$, а $\text{wt } D_u h \leq 2 \cdot 2^{n-k}$, то

$$\text{wt } D_u f \geq 2(2^k - 2^{n-k}) > 2(2 \cdot 2^{\frac{n}{2}} - 2^{\frac{n}{2}}) > 2 \cdot 2^{\frac{n}{2}}.$$

Учитывая неравенство, полученное для векторов из L^* , получаем, что для любых векторов $u \in L^*$ и $v \in V_n \setminus L$ справедливо $\text{wt } D_u f < \text{wt } D_v f$. Таким образом,

$$\rho(f) = \frac{1}{2} \text{wt } D_u f = 2^{n-k} = \text{dist}(f, g).$$

Тот факт, что $\pi_\rho(f) = AD(g) = k$, следует из неравенства $\log_2 \rho(f) + \pi_\rho(f) \leq n$. ■

Лемма 3. Пусть натуральные числа n и k удовлетворяют условиям $n \geq 3$, $2 \leq k \leq n/2$. Пусть $A - (n \times (n-k))$ -матрица над F_2 ранга $n-k$ и L — подпространство пространства V_n , ортогональное к подпространству, порожденному набором из $n-k$ столбцов матрицы A . Пусть если число $(n-k)$ четно, то g является бент-функцией от $n-k$ переменных, иначе пусть функция $g \in \mathcal{F}_{n-k}$ удовлетворяет условиям теоремы 4. Пусть функция $h \in \mathcal{F}_n$ такова, что $\text{wt}(h) = 2^{n-k}$ и носитель 1_h является такой плоскостью пространства V_n , что для любых двух ненулевых векторов $u, v \in 1_h$ справедливо соотношение $u \oplus v \notin L$. Тогда для функции $f = g^A \oplus h$ справедливы соотношения

$$\rho(f) = 2^{n-k}, \quad \pi_\rho(f) = k.$$

Доказательство. Пусть $(n-k)$ четно. Если $u \in L^*$, то

$$\text{wt } D_u f = \text{wt } (D_u g^A \oplus D_u h) = \text{wt } D_u h = 2 \cdot \text{wt}(h) = 2 \cdot 2^{n-k}.$$

Пусть теперь $u \in V_n \setminus L$. Если $u \in J(h)$, то

$$\text{wt } D_u f = \text{wt } (D_u g^A \oplus D_u h) = \text{wt } D_u g^A = 2^{n-1}.$$

Последнее равенство справедливо, поскольку функция g является бент-функцией от $n - k$ переменных и $D_u g^A = (D_v g)^A$ для некоторого $v \in V_{n-k}$.

Если же $u \notin J(h)$, то

$$\text{wt } D_u f = \text{wt}(D_u g^A \oplus D_u h) = \text{wt } D_u g^A + \text{wt } D_u h - 2 \cdot \text{wt}(D_u g^A \cdot D_u h).$$

Заметим, что для любого $z \in V_n \setminus L$ справедливо равенство $\text{wt}(I_{L \oplus z} \cdot D_u h) = 2$. Поэтому $\text{wt}(D_u g^A \cdot D_u h) = 2^{n-1-k} \cdot 2$ и

$$\text{wt } D_u f = 2^{n-1} + 2^{n-k+1} - 2 \cdot 2^{n-k} = 2^{n-1}.$$

Получили, что

$$\text{wt } D_u f = \begin{cases} 2^{n-1}, & \text{если } u \notin L, \\ 2^{n-k+1}, & \text{если } u \in L^*. \end{cases}$$

Следовательно, $\rho(f) = 2^{n-k}$. А поскольку $\rho(f) = \text{dist}(f, g)$ и $AD(g) = k$, то из теоремы 5 следует, что $\pi_\rho(f) = k$.

Пусть теперь число $(n - k)$ нечетно. Поскольку функция g удовлетворяет условиям теоремы 4, то справедливо соотношение $\text{wt}(D_u g^A) \in \{0, 2^{n-1}, 2^n\}$ для любого вектора $u \in V_n^*$. Пусть вектор $u \in V_n^*$ таков, что $\text{wt}(D_u g^A) = 2^n$. Тогда $\text{wt}(D_u f) \geq 2^n - 2^{n-k+1} \geq 2^{n-k+1}$. Рассмотрение оставшихся случаев аналогично случаю, когда $(n - k)$ четно. В результате получаем, что $\rho(f) = 2^{n-k}$ и $\pi_\rho(f) = k$. ■

Пример 2. Примером использования конструкции леммы 3 может служить функция f_8 от 8 переменных, которая задается в виде алгебраической нормальной формы следующим образом:

$$\begin{aligned} f_8(x) = & x_5 x_6 x_7 x_8 \oplus x_7 x_8 \oplus x_5 x_6 x_8 \oplus x_5 x_6 x_7 \oplus x_5 x_8 \oplus x_5 x_7 x_8 \oplus x_6 x_7 \oplus x_6 x_7 x_8 \oplus \\ & \oplus x_1 x_2 \oplus x_3 x_4 \oplus x_6 x_8 \oplus x_5 x_7 \oplus x_5 x_6 \oplus x_3 \oplus x_8 \oplus x_7 \oplus x_5 \oplus x_6 \oplus 1. \end{aligned}$$

Параметры функции f_8 имеют значения

$$\deg(f_8) = 4, \quad \text{nl}(f_8) = 100, \quad \rho(f_8) = \delta(f_8) = 16, \quad \pi_\rho(f_8) = 4, \quad \text{wt}(f_8) = 100.$$

Функция f_8 представима в виде $f_8 = g^A \oplus h$. Функция $g = x_2 \oplus x_1 x_2 \oplus x_3 x_4$ является бент-функцией от 4 переменных. Носитель функции h является подпространством пространства V_8 размерности 4 с базисом $u^{(1)} = (00000001)$, $u^{(2)} = (00000010)$, $u^{(3)} = (00000100)$, $u^{(4)} = (00001000)$. Эти же векторы являются столбцами (8×4) -матрицы A .

Рассмотрим теперь некоторые соотношения, которые связывают параметры ρ и π_ρ булевой функции с другими ее важными характеристиками.

Теорема 6. Для любой функции $f \in \mathcal{F}_n$, такой, что $\pi_\rho(f) > n/2$, существует такое целое число T , $0 \leq T \leq 2^{n-\pi_\rho(f)}$, что справедливо неравенство

$$T(2^{\pi_\rho(f)} - 1) \leq \text{wt}(f) \leq T(2^{\pi_\rho(f)} - 1) + 2^{n-\pi_\rho(f)}.$$

Доказательство. Пусть g — некоторая π_ρ -функция для f . Тогда для любого смежного класса $J(g) \oplus z$ справедливо $|1_f \cap J(g) \oplus z| \in \{0, 1, 2^{\pi_\rho(f)} - 1, 2^{\pi_\rho(f)}\}$. Вес функции f получается суммированием мощностей множеств $|1_f \cap J(g) \oplus z|$ по всем различным смежным классам $J(g) \oplus z$. Утверждение теоремы следует из того, что количество различных смежных классов по подпространству $J(g)$ равно $2^{n-\pi_\rho(f)}$. ■

Теорема 7. Пусть $f \in \mathcal{F}_n$. Если $\pi_\rho(f) > \log_2 \rho(f)$, то $\deg f \geq \pi_\rho(f)$.

Доказательство. Пусть функция $f \in \mathcal{F}_n$ представима в виде $f = g \oplus h$, где $AD(g) = \pi_\rho(f) > \log_2 \text{wt}(h) = \log_2 \rho(f)$. Тогда справедливы неравенства

$$2^{n-\deg h} \leq \text{wt}(h) \leq 2^n - 2^{n-\deg h} \quad \text{и} \quad \deg g \leq n - \pi_\rho(f).$$

Отсюда получаем $\deg h \geq n - \log_2 \rho(f)$ и $n - \pi_\rho(f) \geq \deg g$. Складывая эти два неравенства, получим, что $\deg h - \deg g \geq \pi_\rho(f) - \log_2 \rho(f) > 0$, т. е. $\deg h > \deg g$.

Поскольку $\deg f = \max(\deg g, \deg h)$ при $\deg g \neq \deg h$, то $\deg f = \deg h \geq n - \log_2 \rho(f) \geq \pi_\rho(f)$. ■

Неравенство, полученное в теореме 6 и связывающее вес функции со значением параметра π_ρ , схоже с двусторонним неравенством из леммы 1. Комбинирование этих двух неравенств позволяет получать соотношения между различными параметрами булевой функции.

4. Свойства π_ρ -функций и вычисление параметра π_ρ

Рассмотрим свойства π_ρ -функций для некоторой функции f .

Теорема 8. Пусть $f \in \mathcal{F}_n$ и $g \in DG(f)$. Если существуют два таких различных вектора $u, v \in V_n^*$, что $u, v \in J(g)$, то функция g представима в виде

$$g = f \cdot f^u \oplus f \cdot f^v \oplus f^u \cdot f^v.$$

Доказательство. Поскольку $f^u \cdot f^v = (f \cdot f^{u \oplus v})^v$, то из следствия 2 следует, что $\text{wt}(f \cdot f^u) = \text{wt}(f \cdot f^v) = \text{wt}(f^u \cdot f^v)$. Из утверждения 3 следует, что функция g представима в виде

$$\begin{aligned} g &= f \cdot f^u \oplus h_u \oplus h_u^u, \quad \text{где } h_u \cdot f = h_u \text{ и } h_u^u \cdot f = \bar{0}, \\ g &= f \cdot f^v \oplus h_v \oplus h_v^v, \quad \text{где } h_v \cdot f = h_v \text{ и } h_v^v \cdot f = \bar{0}. \end{aligned}$$

Умножим обе части первого равенства на функцию $f \cdot f^v \oplus f \cdot f^u \cdot f^v$:

$$g(f \cdot f^v \oplus f \cdot f^u \cdot f^v) = f \cdot f^v \oplus f \cdot f^u \cdot f^v = (f \cdot f^v \oplus f \cdot f^u \cdot f^v) h_u.$$

Отсюда получаем, что $\text{wt}(h_u) \geq \text{wt}(f \cdot f^v \oplus f \cdot f^u \cdot f^v)$.

Воспользовавшись вторым представлением функции g , получим

$$g \cdot h_u^u = h_u^u = h_v \cdot h_u^u \oplus h_u^u \cdot h_v^v = h_v \cdot f \cdot h_u^u \oplus h_u^u \cdot h_v^v \cdot f^v = h_u^u \cdot f^v \cdot h_v^v.$$

Таким образом, справедливо равенство $h_u^u = h_u^u \cdot f^v$. Теперь умножим обе части первого представления функции g на функцию $f^u \cdot f^v \oplus f \cdot f^u \cdot f^v$:

$$g(f^u \cdot f^v \oplus f \cdot f^u \cdot f^v) = h_u^u \cdot f^u \cdot f^v \oplus h_u^u \cdot f \cdot f^u \cdot f^v = h_u^u \cdot f^v = h_u^u.$$

Отсюда получаем $\text{wt}(f^u \cdot f^v \oplus f \cdot f^u \cdot f^v) \geq \text{wt}(h_u^u)$. Поскольку $\text{wt}(h_u^u) = \text{wt}(h_u)$ и $\text{wt}(f^u \cdot f^v \oplus f \cdot f^u \cdot f^v) = \text{wt}(f \cdot f^v \oplus f \cdot f^u \cdot f^v)$, то $\text{wt}(h_u) = \text{wt}(f \cdot f^v \oplus f \cdot f^u \cdot f^v)$, а значит, верны равенства $h_u = f \cdot f^v \oplus f \cdot f^u \cdot f^v$, $h_u^u = f^u \cdot f^v \oplus f \cdot f^u \cdot f^v$.

Переписав первое представление для функции g , учитывая полученные соотношения, получим $g = f \cdot f^u \oplus f \cdot f^v \oplus f^u \cdot f^v$. ■

Таким образом, вычисление значения $\pi_\rho(f)$ можно проводить по следующему принципу. Необходимо вычислить значение $\Delta_f^* = \max_{u \in V_n^*} \Delta_f(u)$, одновременно сформировав

множество $A = \{u \in V_n^* : \Delta_f(u) = \Delta_f^*\}$. Вычислить значение $\pi_\rho(f)$ можно с помощью множества $B = \{g = f \cdot f^u \oplus f \cdot f^v \oplus f^u \cdot f^v : u, v \in A, u \neq v, \text{dist}(f, g) = \rho(f)\}$ по формуле

$$\pi_\rho(f) = \max\{1, \max_{g \in B} \dim J(g)\}.$$

5. Вырожденность бент-функций

Рассмотрим свойства параметров ρ и π_ρ для случая, когда f является бент-функцией.

Лемма 4. Пусть $f \in \mathcal{F}_n$ является бент-функцией и $g \in DG(f)$. Если существуют два различных ненулевых вектора $u, v \in V_n$, такие, что $u, v \in J(g)$, то функция g представима в виде $g = D_u(f \cdot f^v)$.

Доказательство. По теореме 8 справедливо равенство $g = f \cdot f^u \oplus f \cdot f^v \oplus f^u \cdot f^v$. По условию $g = g^u$. Используя представление функции g , получим равенство

$$f \cdot f^v \oplus f^u \cdot f^v = f^u \cdot f^{u \oplus v} \oplus f \cdot f^{u \oplus v}.$$

Преобразовав его, получаем $D_u f (D_u f)^v = \bar{0}$. Учитывая, что производная бент-функции по любому направлению уравновешена, это соотношение можно переписать в виде $D_u f \oplus \bar{1} = (D_u f)^v$. Умножая обе части на f , получаем $f(\bar{1} \oplus f \oplus f^u) = (f^v \oplus f^{u \oplus v})f$, $f \cdot f^u \oplus f \cdot f^v \oplus f \cdot f^{u \oplus v} = \bar{0}$. Используя представление функции g , запишем $g = f \cdot f^{u \oplus v} \oplus (f \cdot f^{u \oplus v})^u = D_u(f \cdot f^{u \oplus v})$. После переобозначения векторов имеем требуемое соотношение. ■

Теорема 8 и лемма 4 показывают, что π_ρ -функции для функции f легко выражаются через функции вида $f \cdot f^u$. Некоторые свойства функций вида $f \cdot f^u$ для случая, когда функция f является бент-функцией, отражены в следующем утверждении.

Утверждение 7. Для любой бент-функции $f \in \mathcal{F}_n$, где $n \geq 4$, и любого ненулевого вектора $u \in V_n$ справедливо соотношение $AD(f \cdot f^u) = 1$.

Доказательство. По критерию Ротхауза, производная функции f по любому ненулевому направлению уравновешена. Из соотношения $\text{wt}(f \cdot f^u) = \text{wt}(f) - \text{wt}(D_u f) = 2^{n-2} \pm 2^{\frac{n}{2}-1}$ получаем, что для любых ненулевых векторов $u, v \in V_n$ справедливо равенство $\text{wt}(f \cdot f^u) = \text{wt}(f \cdot f^v)$.

Предположим, что утверждение не верно, т.е. $AD(f \cdot f^u) > 1$. Поскольку справедливо $AD(f \cdot f^u) = \dim J(f \cdot f^u)$, то это означает, что существует такой ненулевой вектор $v \in V_n$, отличный от u , что $(f \cdot f^u)^v = f \cdot f^u$. Учитывая равенство весов $\text{wt}(f \cdot f^u) = \text{wt}(f \cdot f^v)$, получаем $f \cdot f^u = f \cdot f^v = f \cdot f^{u \oplus v} = (f \cdot f^{u \oplus v})^u = f^u \cdot f^v$.

Используя полученные ранее равенства, имеем $f(f^u \oplus f^v) = \bar{0}$, откуда $f(D_{u \oplus v} f)^u = (f^u \cdot D_{u \oplus v} f)^u = \bar{0}$. Таким образом, выполнено соотношение $f^u \cdot D_{u \oplus v} f = \bar{0}$. Заменяя в рассуждениях вектор u на v , получаем $f^v \cdot D_{u \oplus v} f = \bar{0}$.

Рассмотрим два случая. Если $\text{wt}(f) = 2^{n-1} + 2^{\frac{n}{2}-1}$, то ни одно из полученных ранее соотношений не может быть выполнено, так как производная бент-функции по любому ненулевому направлению уравновешена.

Если же $\text{wt}(f) = 2^{n-1} - 2^{\frac{n}{2}-1}$, то для выполнения двух полученных равенств необходимо, чтобы выполнялось неравенство $\text{wt}(f^u) + \text{wt}(f^v) - \text{wt}(f^u \cdot f^v) + 2^{n-1} \leq 2^n$. Так как $f^u \cdot f^v = (f \cdot f^{u \oplus v})^u$, то $\text{wt}(f^u \cdot f^v) = 2^{n-2} - 2^{\frac{n}{2}-1}$. Подставляя значения весов функций в неравенство, получаем

$$2^n + 2^{n-1} - 2^{n-2} - 2^{\frac{n}{2}-1} \leq 2^n,$$

$$2^{n-2} - 2^{\frac{n}{2}-1} \leq 0.$$

Но для $n \geq 4$ это неравенство не выполняется. Получили противоречие, которое доказывает утверждение. ■

Для бент-функций параметр ρ достигает своего максимального значения 2^{n-2} . С помощью конструкции, описанной в лемме 3, можно строить бент-функции, для которых в неравенстве теоремы 5 достигается равенство, т. е. бент-функции с $\pi_\rho(f) = 2$. Для этого достаточно задать четное число переменных n и положить $k = 2$.

Пример 3. Функция b_8 является бент-функцией от восьми переменных и задается следующим образом:

$$b_8(x) = x_4x_5x_6 \oplus x_2x_3x_5 \oplus x_1x_3x_4 \oplus x_7x_8 \oplus x_1x_5 \oplus x_3x_4 \oplus x_2x_4 \oplus x_1x_4 \oplus x_2x_3 \oplus x_1x_3 \oplus x_3x_6 \oplus x_8 \oplus x_7 \oplus 1.$$

Параметры функции b_8 имеют следующие значения:

$$\deg(b_8) = 3, \quad \text{nl}(b_8) = 120, \quad \rho(b_8) = \delta(b_8) = 64, \quad \pi_\rho(b_8) = 2, \quad \text{wt}(b_8) = 120.$$

Функция b_8 представима в виде $b_8 = g^A \oplus h$. Функция

$$g(x) = x_2x_6 \oplus x_3x_6 \oplus x_1x_2x_3 \oplus x_4x_6 \oplus x_1x_4 \oplus x_3x_4 \oplus x_3x_4x_6 \oplus x_3x_5 \oplus x_4x_5 \oplus x_2x_4x_5$$

является бент-функцией от шести переменных. Векторы $u^{(1)} = (00000001)$, $u^{(2)} = (00000010)$, $u^{(3)} = (00000100)$, $u^{(4)} = (00001000)$, $u^{(5)} = (00010000)$, $u^{(6)} = (00100000)$ являются столбцами (8×6) -матрицы A , а также образуют базис подпространства, которое является носителем функции h .

ЛИТЕРАТУРА

1. *Siegenthaler T.* Decrypting a class of stream cipher using ciphertext only // IEEE Trans. Computers. 1985. V. C-34. No. 1. P. 81–85.
2. *Matsui M.* Linear cryptanalysis method for DES cipher // LNCS. 1993. V. 765. P. 386–397.
3. *Meier W. and Staffelbach O.* Nonlinearity criteria for cryptographic functions // LNCS. 1990. V. 434. P. 549–562.
4. *Алексеев Е. К.* О некоторых алгебраических и комбинаторных свойствах корреляционно-иммунных булевых функций // Дискретная математика. 2010. Т. 22. № 3. С. 110–126.
5. *Dawson E. and Wu C. K.* Construction of correlation immune boolean functions // LNCS. 1997. V. 1334. P. 170–180.
6. *Логачев О. А., Сальников А. А., Яценко В. В.* Булевы функции в теории кодирования и криптологии. М.: МЦНМО, 2004.
7. *Таранников Ю. В.* О корреляционно-иммунных и устойчивых булевых функциях // Математические вопросы кибернетики. Вып. 11. М.: Физматлит, 2002. С. 91–148.
8. *Zhang X. M. and Zheng Y.* Characterizing the structures of cryptographic functions satisfying the propagation criterion for almost all vectors // Design Codes Cryptography. 1996. No. 7 (1/2). P. 111–134.