

УДК 519.7

ПОРОГОВОЕ СВОЙСТВО КВАДРАТИЧНЫХ БУЛЕВЫХ ФУНКЦИЙ ^{*)}

Н. А. Коломеец

Аннотация. Пусть f — булева функция от n переменных такая, что для любого аффинного подпространства L размерности $\lceil n/2 \rceil$ либо f аффинна на всех сдвигах L , либо не аффинна ни на одном. Доказано, что либо степень f не превосходит 2, либо не существует ни одного аффинного подпространства размерности $\lceil n/2 \rceil$, на котором f аффинна.

Ключевые слова: булева функция, квадратичная булева функция, бент-функция.

Введение

В работе рассматривается свойство булевой функции, связанное с её аффинностью на аффинных подпространствах. Это свойство может быть использовано для построения бент-функций по некоторой заданной бент-функции. Бент-функции — булевы функции с максимальной нелинейностью. Конструкции бент-функций важны для криптографических приложений.

Через \mathbb{Z}_2^n обозначим n -мерный булев куб. Отображение $f : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2$ называется *булевой функцией от n переменных*. Степень алгебраической нормальной формы булевой функции называется *алгебраической степенью*, или просто *степенью*. Булева функция называется *аффинной*, если её алгебраическая степень не превосходит 1, и *квадратичной*, если её алгебраическая степень равна 2. Множество $a \oplus D$, где $a \in \mathbb{Z}_2^n$ и $D \subseteq \mathbb{Z}_2^n$, называется *сдвигом* множества D . Множество $U \subseteq \mathbb{Z}_2^n$ называется *аффинным подпространством*, если оно является сдвигом некоторого линейного подпространства в \mathbb{Z}_2^n . *Размерностью* аффинного подпространства называется размерность соответствующего линейного подпространства. Через Ind_D обозначим булеву функцию от n переменных, принимающую значение 1 только на элементах множества $D \subseteq \mathbb{Z}_2^n$. Для

^{*)}Исследование выполнено при финансовой поддержке Российского фонда фундаментальных исследований (проект 12-01-31097) и грантом Президента России для ведущих научных школ НШ-1939.2014.1.

векторов u и v длины n обозначим через $\langle u, v \rangle$ их скалярное произведение $\langle u, v \rangle = u_1v_1 \oplus \dots \oplus u_nv_n$.

Булева функция f от n переменных *аффинна на множестве* $D \subseteq \mathbb{Z}_2^n$, если существуют $a \in \mathbb{Z}_2^n$ и $c \in \mathbb{Z}_2$ такие, что $f|_D(x) = \langle a, x \rangle \oplus c$.

Булевы функции f и g от n переменных *аффинно эквивалентны*, если существует невырожденная двоичная матрица A размера $n \times n$, вектор $b \in \mathbb{Z}_2^n$ и аффинная функция l от n переменных такие, что $g(x) = f(Ax \oplus b) \oplus l(x)$. Под *расстоянием* между двумя булевыми функциями подразумевается расстояние Хэмминга между векторами их значений.

Все квадратичные булевы функции обладают следующим свойством.

Утверждение 1. Пусть f — квадратичная булева функция от n переменных и f аффинна на некотором аффинном подпространстве L размерности $\lceil n/2 \rceil$. Тогда f аффинна на любом сдвиге L .

Доказательство этого утверждения следует из неравенства $\deg(f(x) \oplus f(x \oplus s)) \leq 1$, справедливого для любого $s \in \mathbb{Z}_2^n$.

Утверждение 1 останется верным и без ограничения на размерность подпространства L . Мы рассматриваем размерность $\lceil n/2 \rceil$ по следующим причинам.

Утверждение 2. (i) Пусть f — квадратичная булева функция от n переменных. Тогда существует аффинное подпространство размерности $\lceil n/2 \rceil$, на котором f аффинна.

(ii) Булева функция $f(x_1, \dots, x_{2k}) = x_1x_2 \oplus x_3x_4 \oplus \dots \oplus x_{2k-1}x_{2k}$ не аффинна ни на одном аффинном подпространстве размерности, большей k .

ДОКАЗАТЕЛЬСТВО. П. (i) следует из теоремы Диксона о каноническом представлении квадратичных функций [3], п. (ii) — из того, что f — бент-функция [2]. Утверждение 2 доказано.

Таким образом, $\lceil n/2 \rceil$ — максимальная возможная размерность такая, что любая квадратичная функция аффинна на некотором аффинном подпространстве этой размерности.

Применительно к бент-функциям подпространства данной размерности можно использовать для построения других бент-функций. Булева функция f от чётного числа переменных называется *бент-функцией*, если она находится на максимально возможном расстоянии от множества всех аффинных функций. Бент-функции введены в [8]. Они являются интересными объектами для специалистов в криптографии и теории кодирования, поскольку имеют большое число приложений в этих областях.

Тем не менее до сих пор существует множество нерешённых проблем, связанных с бент-функциями (см., например, [2, 4]).

Из [1] следует, что две бент-функции от $2k$ переменных находятся на минимально возможном расстоянии 2^k тогда и только тогда, когда они различаются на аффинном подпространстве размерности k и обе функции на нём аффинны. Более того, имеет место следующая конструкция. Пусть f — бент-функция от $2k$ переменных и f аффинна на некотором аффинном подпространстве L размерности k . Тогда $g(x) = f(x) \oplus \text{Ind}_L(x)$ также является бент-функцией. Данную конструкцию можно найти в монографии [2].

Также существуют понятия нормальности и слабой нормальности булевой функции. Булева функция f от n переменных называется *нормальной* (*слабо нормальной*), если существует аффинное подпространство размерности $\lceil n/2 \rceil$, на котором f является константой (аффинна). Это определение для чётного числа переменных предложено в [6], а позже обобщено в [5].

Возникает вопрос: существуют ли слабо нормальные булевы функции степени больше 2, для которых аффинность на подпространстве размерности $\lceil n/2 \rceil$ влечёт также аффинность на всех сдвигах этого подпространства? В данной работе доказывается, что таких функций не существует, т. е. степень 2 является порогом для данного свойства.

1. Аффинность булевых функций на объединении граней

Пусть $k, l \in \mathbb{N}$, $y \in \mathbb{Z}_2^l$. Обозначим через L_y^k грань \mathbb{Z}_2^{k+l} размерности k вида $L_y^k = \{(x_1, \dots, x_k, y) \mid x_i \in \mathbb{Z}_2\}$, где $y = (y_1, \dots, y_l)$.

Лемма 1. (i) Пусть $n, m \in \mathbb{N}$ и s_1, s_2 — различные элементы \mathbb{Z}_2^m . Тогда $L_{s_1}^n \cup L_{s_2}^n$ является аффинным подпространством размерности $n+1$.

(ii) Пусть $n, m \in \mathbb{N}$ и s_1, s_2, s_3, s_4 — различные элементы \mathbb{Z}_2^m . Тогда $L_{s_1}^n \cup L_{s_2}^n \cup L_{s_3}^n \cup L_{s_4}^n$ является аффинным подпространством размерности $n+2$ тогда и только тогда, когда $s_1 \oplus s_2 \oplus s_3 \oplus s_4 = 0$.

ДОКАЗАТЕЛЬСТВО. Утверждение (i) очевидно. Докажем (ii). Согласно (i) $L_{s_1}^n \cup L_{s_2}^n$ и $L_{s_3}^n \cup L_{s_4}^n$ являются непересекающимися аффинными подпространствами размерности $n+1$. Таким образом, их объединение является аффинным подпространством тогда и только тогда, когда оба подпространства являются сдвигами одного и того же линейного подпространства. Это означает, что $s_1 \oplus s_2 = s_3 \oplus s_4$. Лемма 1 доказана.

Лемма 2. Пусть $f : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2$ и s_1, s_2 — различные элементы \mathbb{Z}_2^{n-k} , где $0 < k < n$, и $f(x, s_i) = \langle a_i, x \rangle \oplus c_i$, $x \in \mathbb{Z}_2^k$, $i \in \{1, 2\}$, для некоторых

$a_i \in \mathbb{Z}_2^k$, $c_i \in \mathbb{Z}_2$. Тогда функция f аффинна на $L_{s_1}^k \cup L_{s_2}^k$ тогда и только тогда, когда $a_1 = a_2$.

ДОКАЗАТЕЛЬСТВО. Перепишем равенства из условия леммы. Для любых $r_1, r_2 \in \mathbb{Z}_2^{n-k}$

$$f(x, s_i) = \langle (a_i, r_i), (x, s_i) \rangle \oplus \langle r_i, s_i \rangle \oplus c_i.$$

Тем самым функция f аффинна на $L_{s_1}^k \cup L_{s_2}^k$ тогда и только тогда, когда существуют r_1, r_2 такие, что

$$(a_1, r_1) = (a_2, r_2), \quad \langle r_1, s_1 \rangle \oplus c_1 = \langle r_2, s_2 \rangle \oplus c_2,$$

т. е. $a_1 = a_2$, $\langle r_1, s_1 \oplus s_2 \rangle = c_1 \oplus c_2$. Поскольку $s_1 \oplus s_2 \neq 0$, существует r_1 такое, что $\langle r_1, s_1 \oplus s_2 \rangle = c_1 \oplus c_2$. Лемма 2 доказана.

Лемма 3. Пусть $f : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2$ и s_1, s_2, s_3, s_4 — различные элементы \mathbb{Z}_2^{n-k} , $0 < k < n - 1$, такие, что $s_1 \oplus s_2 \oplus s_3 \oplus s_4 = 0$, и для некоторых $a_i \in \mathbb{Z}_2^k$, $c_i \in \mathbb{Z}_2$ верно

$$f(x, s_i) = \langle a_i, x \rangle \oplus c_i, \quad x \in \mathbb{Z}_2^k, \quad i \in \{1, 2, 3, 4\}.$$

Тогда функция f аффинна на $U = L_{s_1}^k \cup L_{s_2}^k \cup L_{s_3}^k \cup L_{s_4}^k$ тогда и только тогда, когда $a_1 = a_2 = a_3 = a_4$ и $c_1 \oplus c_2 \oplus c_3 \oplus c_4 = 0$.

ДОКАЗАТЕЛЬСТВО. Как и в доказательстве леммы 2, перепишем равенства из условия. Для любых $r_1, r_2, r_3, r_4 \in \mathbb{Z}_2^{n-k}$

$$f(x, s_i) = \langle (a_i, r_i), (x, s_i) \rangle \oplus \langle r_i, s_i \rangle \oplus c_i.$$

Функция f аффинна на U тогда и только тогда, когда существуют r_1, r_2, r_3, r_4 такие, что $(a_i, r_i) = (a_j, r_j)$, $\langle r_i, s_i \rangle \oplus c_i = \langle r_j, s_j \rangle \oplus c_j$ для любых i, j . Таким образом, $a_1 = a_2 = a_3 = a_4$ и $r_1 = r_2 = r_3 = r_4$. Обозначим r_1 через r и перепишем оставшиеся уравнения:

$$\langle r, s_2 \rangle \oplus c_2 = \langle r, s_1 \rangle \oplus c_1, \quad \langle r, s_3 \rangle \oplus c_3 = \langle r, s_1 \rangle \oplus c_1, \quad \langle r, s_4 \rangle \oplus c_4 = \langle r, s_1 \rangle \oplus c_1.$$

Заменим последнее уравнение суммой всех уравнений:

$$\langle r, s_2 \rangle \oplus c_2 = \langle r, s_1 \rangle \oplus c_1, \quad \langle r, s_3 \rangle \oplus c_3 = \langle r, s_1 \rangle \oplus c_1,$$

$$\langle r, s_1 \oplus s_2 \oplus s_3 \oplus s_4 \rangle = c_1 \oplus c_2 \oplus c_3 \oplus c_4.$$

Это эквивалентно

$$\langle r, s_1 \oplus s_2 \rangle = c_1 \oplus c_2, \quad \langle r, s_1 \oplus s_3 \rangle = c_1 \oplus c_3, \quad c_1 \oplus c_2 \oplus c_3 \oplus c_4 = 0.$$

Так как все s_i различны, существует r такое, что

$$\langle r, s_1 \oplus s_2 \rangle = c_1 \oplus c_2, \quad \langle r, s_1 \oplus s_3 \rangle = c_1 \oplus c_3.$$

Лемма 3 доказана.

2. Свойство квадратичных булевых функций

Функция $h : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^m$ называется *аффинной*, если $h(x) = Ax \oplus b$ для некоторой двоичной матрицы A размера $m \times n$ и $b \in \mathbb{Z}_2^m$.

Теорема 1. Пусть $f : \mathbb{Z}_2^{2k} \rightarrow \mathbb{Z}_2$ слабо нормальная и для любого аффинного подпространства L размерности k либо f аффинна на всех сдвигах L , либо не аффинна ни на одном. Тогда f либо аффинная, либо квадратичная.

ДОКАЗАТЕЛЬСТВО. Без ограничения общности можем считать, что f представлена в виде

$$f(x, y) = \langle x, \pi(y) \rangle \oplus \varphi(y), \quad (1)$$

где $\pi : \mathbb{Z}_2^k \rightarrow \mathbb{Z}_2^k$, $\varphi : \mathbb{Z}_2^k \rightarrow \mathbb{Z}_2$, поскольку любая булева функция, удовлетворяющая условиям теоремы, аффинно эквивалентна булевой функции в таком виде. Заметим, что это представление похоже на конструкцию Мэйорана — МакФарланда [7], а именно, f является бент-функцией из класса Мэйорана — МакФарланда тогда и только тогда, когда π взаимно однозначна.

Из условия теоремы легко показать, что для любого линейного подпространства U произвольной размерности $t < k$, на котором f аффинна, существует линейное подпространство L размерности k , $U \subseteq L$, на котором f тоже аффинна (например, используя лемму 2 и индукцию по размерности подпространства). Отсюда следует, что свойство функции f справедливо и для подпространств размерности меньше k .

Утверждение $\deg f \leq 2$ для функции (1) эквивалентно выполнению следующих условий:

- (i) π — аффинная функция;
- (ii) $\deg \varphi \leq 2$.

Докажем, что условие (i) выполняется. Используем индукцию по k . Для $k = 1$ утверждение очевидно. Предположим, что для $1, \dots, k-1$ утверждение верно. Покажем, что оно верно и для k .

Рассмотрим значения функции f для всех x таких, что $x_i = 0$ для некоторого $i \in \{1, \dots, k\}$. Для простоты положим $i = k$, т. е. $x_k = 0$. Обозначим через \bar{y} вектор $y \in \mathbb{Z}_2^k$ без последней координаты, т. е. $\bar{y} \in \mathbb{Z}_2^{k-1}$, через $\bar{\pi}(y)$ — вектор $\pi(y)$ без последней координаты. Очевидно, что существуют различные s_1, s_2 такие, что $\bar{\pi}(s_1) = \bar{\pi}(s_2)$. Следовательно, по лемме 2 функция f аффинна на $L_{(0, s_1)}^{k-1} \cup L_{(0, s_2)}^{k-1}$. По условию теоремы функция f аффинна на любом сдвиге $L_{(0, s_1)}^{k-1} \cup L_{(0, s_2)}^{k-1}$. Таким образом, $\bar{\pi}(s_1 \oplus y) = \bar{\pi}(s_2 \oplus y)$ для всех $y \in \mathbb{Z}_2^k$ по лемме 2, что эквивалентно

равенству

$$\bar{\pi}(y) = \bar{\pi}(s_1 \oplus s_2 \oplus y), \quad y \in \mathbb{Z}_2^k.$$

Пусть $s = s_1 \oplus s_2$. Поскольку $s_1 \neq s_2$, s содержит ненулевую координату. Для простоты будем считать, что это последняя координата. Тогда $\bar{\pi}(\bar{y}, 1) = \bar{\pi}(\bar{y} \oplus \bar{s}, 0)$. По предположению индукции $\bar{\pi}(\bar{y}, 0)$ аффинна, следовательно,

$$\bar{\pi}(\bar{y}, y_k) = \bar{\pi}(\bar{y}, 0) \oplus y_k \cdot (\bar{\pi}(\bar{s}, 0) \oplus \bar{\pi}(\mathbf{0}, 0)),$$

где $\mathbf{0}$ — нулевой элемент \mathbb{Z}_2^{k-1} . Таким образом, $\bar{\pi}(y)$ — аффинная функция. Так как любая из координат x_i могла быть фиксирована, π также аффинна. Утверждение (i) доказано.

Докажем, что $\deg \varphi \leq 2$. Так как π аффинна, без ограничения общности будем считать, что $\pi(y) = (y_1, \dots, y_r, (A(y_1, \dots, y_r)^T)^T)^T$ для некоторой матрицы A размера $(k-r) \times r$ (в силу аффинной эквивалентности).

Используя индукцию по k , получаем, что для $k = 1$ и $k = 2$ утверждение верно. Предположим, что для $1, \dots, k-1$ утверждение верно. Докажем, что $\deg \varphi \leq 2$ для k .

Рассмотрим значения функции f для всех x таких, что $x_{k-1} = 0$ и $x_k = 0$. Согласно лемме 3 функция f аффинна на $U = L_{(\mathbf{0}, \mathbf{0}, 0)}^{k-2} \cup L_{(\mathbf{0}, \mathbf{0}, 1)}^{k-2} \cup L_{(\mathbf{0}, 1, 0)}^{k-2} \cup L_{(\mathbf{0}, 1, 1)}^{k-2}$ тогда и только тогда, когда

$$\varphi(\mathbf{0}, 0, 0) \oplus \varphi(\mathbf{0}, 0, 1) \oplus \varphi(\mathbf{0}, 1, 0) \oplus \varphi(\mathbf{0}, 1, 1) = 0. \quad (2)$$

Поскольку $\deg(\varphi(y) \oplus y_{k-1}y_k) \leq 2$ тогда и только тогда, когда $\deg \varphi \leq 2$, достаточно доказать только одно из неравенств. Таким образом, без ограничения общности положим, что справедливо равенство (2). Следовательно, по условию теоремы и лемме 3 имеем

$$\varphi(y, 0, 0) \oplus \varphi(y, 0, 1) \oplus \varphi(y, 1, 0) \oplus \varphi(y, 1, 1) = 0, \quad y \in \mathbb{Z}_2^{k-2}.$$

Разложим φ по последним двум переменным:

$$\begin{aligned} \varphi(y, u, v) &= (u \oplus 1)(v \oplus 1)\varphi(y, 0, 0) \oplus (u \oplus 1)v\varphi(y, 0, 1) \\ &\quad \oplus u(v \oplus 1)\varphi(y, 1, 0) \oplus uv\varphi(y, 1, 1). \end{aligned}$$

Стало быть,

$$\begin{aligned} \varphi(y, u, v) &= (\varphi(y, 0, 0) \oplus \varphi(y, 0, 1) \oplus \varphi(y, 1, 0) \oplus \varphi(y, 1, 1))uv \\ &\quad \oplus (\varphi(y, 0, 0) \oplus \varphi(y, 1, 0))u \oplus (\varphi(y, 0, 0) \oplus \varphi(y, 0, 1))v \oplus \varphi(y, 1, 1) \end{aligned}$$

$$= (\varphi(y, 0, 0) \oplus \varphi(y, 1, 0))u \oplus (\varphi(y, 0, 0) \oplus \varphi(y, 0, 1))v \oplus \varphi(y, 1, 1).$$

Так как $\deg \varphi(y, y_{k-1}, 0) \leq 2$ и $\deg \varphi(y, 0, y_k) \leq 2$ по предположению индукции, имеем

$$\deg(\varphi(y, 0, 0) \oplus \varphi(y, 1, 0)) \leq 1, \quad \deg(\varphi(y, 0, 0) \oplus \varphi(y, 0, 1)) \leq 1.$$

Также по предположению индукции $\deg \varphi(y, 1, 1) \leq 2$. Следовательно, $\deg \varphi \leq 2$. Теорема 1 доказана.

Случай чётного числа переменных обобщается на общий случай очевидным образом (в нечётном случае рассматриваются аффинные подпространства размерности $\lceil n/2 \rceil$, где n — число переменных).

ЛИТЕРАТУРА

1. Коломеец Н. А., Павлов А. В. Свойство бент-функций, находящихся на минимальном расстоянии друг от друга // Прикл. дискрет. математика. — 2009. — № 4. — С. 5–20.
2. Логачев О. А., Сальников А. А., Яценко В. В. Булевы функции в теории кодирования и криптологии. — М.: МЦНМО, 2004. — 470 с.
3. Мак-Вильямс Ф. Д., Слоэн Н. А. Теория кодов, исправляющих ошибки. — М.: Радио и связь, 1979. — 744 с.
4. Токарева Н. Н. Нелинейные булевы функции: бент-функции и их обобщения. — Saarbrücken: LAP LAMBERT Acad. Publ., 2011. — 180 с.
5. Charpin P. Normal Boolean functions // J. Complexity. — 2004. — Vol. 20. — P. 245–265.
6. Dobbertin H. Construction of bent functions and balanced Boolean functions with high nonlinearity // Lect. Notes Comput. Sci. — 1994. — Vol. 1008. — P. 61–74.
7. McFarland R. L. A family of difference sets in non-cyclic groups // J. Combin. Theory. Ser. A. — 1973. — Vol. 15. — P. 1–10.
8. Rothaus O. On bent functions // J. Combin. Theory. Ser. A. — 1976. — Vol. 20, N 3. — P. 300–305.

Коломеец Николай Александрович,
e-mail: nkolomeec@gmail.com

Статья поступила
9 июля 2013 г.

Переработанный вариант —
24 декабря 2013 г.