ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ
Январь—февраль 2013. Том 20, № 1. С. 77–92

УДК 519.7

СУЩЕСТВЕННАЯ ЗАВИСИМОСТЬ БЕНТ-ФУНКЦИЙ КАСАМИ ОТ ПРОИЗВЕДЕНИЙ ПЕРЕМЕННЫХ *)

А. А. Фролова

Аннотация. Исследуются бент-функции Касами, которые являются наиболее сложными по своим свойствам в классе алгебраических конструкций бент-функций. Доказано, что функции Касами степени t имеют ненулевые $(t-2)$-кратные производные при $4 \leqslant t \leqslant (n+3)/3$ и ненулевые $(t-3)$-кратные производные при $(n+3)/3 < t \leqslant n/2$. Установлено, что порядок существенной зависимости бент-функций Касами равен либо $t-2$, либо $t-3$.

Ключевые слова: булева функция Касами, бент-функция, алгебраическая нормальная форма, производная булевой функции.

Введение

Булевы функции, отстоящие на максимально возможное расстояние от множества всех аффинных булевых функций (при чётном числе переменных — *бент-функции*), возникают в приложениях различных областей математики, таких как криптография, теория кодирования и т. д. (см. подробнее [2]). Рассматриваемые в данной работе бент-функции Касами, например, используются также в системе спутникового наблюдения ГЛОНАСС для построения специальных кодов, обладающих хорошей структурой.

Конструкция булевых функций Касами описана в [5]. Там же показано, что при определенных условиях мономиальные булевы функции с показателем Касами являются бент-функциями. В дальнейшем исследован ряд интересных свойств бент-функций Касами: они не аффинно эквивалентны бент-функциям из классов PS и Майорана — МакФарланда [3, 8], а также своим дуальным функциям [7]. Кроме того, известно, что в классе бент-функций Касами существуют функции, не являющиеся нормальными [3], т. е. тождественно равными константе на некотором аффинном подпространстве размерности $n/2$, где n — число переменных функции.

*) Исследование выполнено при финансовой поддержке Российского фонда фундаментальных исследований (проекты 11–01–00997 и 12–01–31097).

Налицо сложность этих функций по своим свойствам, при том что они имеют довольно простое алгебраическое описание через функцию следа в конечном поле. В данной работе рассматриваются комбинаторные свойства бент-функций Касами, а именно, свойство зависимости алгебраической нормальной формы (АНФ) функции от произведений переменных. Вводится следующее понятие: булеву функцию назовём *k-существенно зависимой*, если для любого произведения из k различных переменных в АНФ функции существует слагаемое, содержащее это произведение. Доказана теорема о том, что булевы функции Касами степени t являются $(t-2)$-существенно зависимыми при $4 \leqslant t \leqslant (n+3)/3$, а также $(t-3)$-существенно зависимыми при $(n+3)/3 < t \leqslant n/2$.

1. Базовые определения

Пусть $\mathbb{Z}_2^n$ — множество двоичных векторов длины n и $x, y \in \mathbb{Z}_2^n$. *Весом Хэмминга* двоичного вектора x называется количество единиц, содержащихся в x. Пусть символ $\oplus$ обозначает сложение по модулю два. *Скалярным произведением* двоичных векторов x, y называется число $\langle x, y\rangle = x_1 y_1 \oplus \ldots \oplus x_n y_n$.

Булевой функцией от n переменных называется функция, действующая из $\mathbb{Z}_2^n$ в $\mathbb{Z}_2$. *Расстоянием Хэмминга* между булевыми функциями f и g называется число $d(f,g) = \big|\{x \mid f(x) \neq g(x), x \in \mathbb{Z}_2^n\}\big|$. Пусть $\mathcal{M}_n$ — некоторое множество булевых функций от n переменных. Тогда расстояние от функции g до множества функций $\mathcal{M}_n$ определяется как $d(g, \mathcal{M}_n) = \min\limits_{f \in \mathcal{M}_n} d(f,g)$.

Любую булеву функцию можно записать в *алгебраической нормальной форме* (АНФ), т. е. представить в виде

$$f(y_1, \ldots, y_n) = \bigoplus_{k=1}^{n} \bigoplus_{i_1, \ldots, i_k} a_{i_1, \ldots, i_k} y_{i_1} \ldots y_{i_k} \oplus a_0,$$

где $\{i_1, \ldots, i_k\} \subseteq \{1, \ldots, n\}$ и $a_{i_1,\ldots,i_k},\ a_0 \in \mathbb{Z}_2$. *Степенью* $\deg(f)$ булевой функции f называется количество переменных в самом длинном слагаемом, встречающемся в АНФ функции.

Булева функция степени 1, т. е. вида $f(y) = \langle a, y\rangle \oplus a_0$, $a \in \mathbb{Z}_2^n$, $a_0 \in \mathbb{Z}_2$, называется *аффинной*. В случае $a_0 = 0$ она называется *линейной*.

Для любой булевой функции f *производная по направлению* a, где $a \in \mathbb{Z}_2^n$, определяется следующим образом: $D_a f(y) = f(y) \oplus f(y \oplus a)$.

Любое натуральное число m представимо в виде $m = \sum\limits_{i=0}^{\ell} m_i 2^i$, где $m_i \in \{0, 1\}$ и ℓ — натуральное число. *Весом Хэмминга* $\mathrm{wt}(m)$ числа m

называется количество ненулевых коэффициентов из $m_0, \ldots, m_\ell$. *Отношение предшествования* на множестве натуральных чисел определяется следующим образом: $m \preceq m'$, если для всех i выполнено $m_i \leqslant m'_i$. Если к тому же $m \neq m'$, то говорят, что предшествование *строгое*, и пишут $m \prec m'$. Для любого целого числа m обозначим через $[m]$ наименьшее натуральное число, сравнимое с m по модулю $2^n - 1$.

Через S_m будем обозначать симметрическую группу степени m, а через π — произвольный элемент S_m.

2. Алгебраическое описание булевых функций

Пусть $GF(2)$ — конечное поле характеристики 2 из двух элементов и $GF(2^n)$ — расширение степени n поля $GF(2)$. Через $GF^*(2^n)$ обозначим множество обратимых элементов поля. Любой элемент $\beta \in GF(2^n)$ можно представить в виде многочлена от формального символа x степени не выше $n-1$: $\beta = \beta(x) = \beta_0 + \beta_1 x + \ldots + \beta_{n-1}x^{n-1}$, где $\beta_0, \ldots, \beta_{n-1} \in GF(2)$. В данной работе в случае, когда для элемента поля β используется представление в виде многочлена, будем обозначать его через $\beta(x)$. Напомним, что операции в поле $GF(2^n)$ определяются следующим образом:

$$\begin{aligned} &\beta + \beta' = d, \quad d(x) = \beta(x) + \beta'(x), \\ &\beta \cdot \beta' = d, \quad d(x) = \beta(x) \cdot \beta'(x) (\mathrm{mod}\ g(x)), \end{aligned}$$

где под сложением многочленов понимаем их сложение над полем $GF(2)$, а $g(x)$ — произвольный фиксированный неприводимый над $GF(2)$ многочлен степени n. В дальнейшем для краткости вместо записи $\beta \cdot \beta'$ будем использовать $\beta\beta'$.

Любую булеву функцию из $\mathbb{Z}_2^n$ в $\mathbb{Z}_2$ можно также рассматривать как функцию, действующую из $GF(2^n)$ в $GF(2)$, так как между $\mathbb{Z}_2^n$ и $GF(2^n)$ существует взаимно однозначное соответствие, а именно, элементу β из $GF(2^n)$, представленному в виде многочлена $\beta(x)$, однозначно соответствует вектор $\beta = (\beta_1, \ldots, \beta_n) \in \mathbb{Z}_2^n$

Функция *след*, действующая из $GF(2^n)$ в $GF(2^n)$, определяется следующим образом: $\mathrm{tr}(\beta) = \beta + \beta^2 + \beta^{2^2} + \ldots + \beta^{2^{n-1}}$.

Отметим важные свойства функции следа:

(i) для любого элемента $\beta \in GF(2^n)$ значение $\mathrm{tr}(\beta)$ лежит в $GF(2)$;

(ii) для любого натурального числа r и любого элемента $\beta \in GF(2^n)$ выполнено $\mathrm{tr}(\beta^{2^r}) = \mathrm{tr}(\beta)$;

(iii) функция следа линейна, т. е. $\mathrm{tr}(\beta_1 + \beta_2) = \mathrm{tr}(\beta_1) + \mathrm{tr}(\beta_2)$ для любых $\beta_1, \beta_2 \in GF(2^n)$.

Циклотомическим классом по модулю $2^n - 1$ с представителем t называется множество $C(t) = \{[2^j t] \mid 0 \leqslant j < n\}$. Отметим два свойства циклотомического класса:

(a) мощность $C(t)$ является делителем числа n;

(b) для любого числа s из циклотомического класса с представителем t справедливо равенство $\mathrm{tr}(\beta^s) = \mathrm{tr}(\beta^t)$ (оно следует из свойства (ii) функции следа).

Обозначим через CS множество наименьших представителей всех циклотомических классов по модулю $2^n - 1$. Тогда любую булеву функцию от n переменных можно описать с помощью следа [4]:

$$f(\beta) = \mathrm{tr}\Big(\sum_{j \in CS} a_j \beta^j\Big), \text{ где } a_j \in GF(2^n).$$

Функция, заданная выражением $f(\beta) = \mathrm{tr}(\lambda\beta^k)$, называется *мономиальной*. В частности [1], множество функций вида $f(\beta) = \mathrm{tr}(\lambda\beta)$, когда λ пробегает всё поле $GF(2^n)$, совпадает с множеством всех линейных функций.

3. Бент-функции Касами

Максимально нелинейной называется булева функция от n переменных, расстояние Хэмминга от которой до множества $\mathcal{A}_n$ всех аффинных функций от n переменных является максимально возможным. В случае чётного n такую функцию также называют *бент-функцией*.

Класс бент-функций от n переменных не описан при $n \geqslant 8$, не известно даже количество таких функций. Предложены лишь некоторые конструкции бент-функций, часть из которых является алгебраическими, в том числе и бент-функции, рассматриваемые в данной работе.

Определение 1. Булева функция от n переменных (n чётное) вида $f(\beta) = \mathrm{tr}(\lambda\beta^k)$ называется *булевой функцией Касами*, если выполнено условие

(i) $k = 2^{2d} - 2^d + 1$, где НОД$(n, d) = 1,\ 0 < d < n$.

Если к тому же выполнено условие

(ii) λ не принадлежит множеству $\{\gamma^3 \mid \gamma \in GF(2^n)\}$,

то f является бент-функцией и называется *бент-функцией Касами*.

В [6] доказано, что при выполнении условия (ii) булева функция Касами является бент-функцией, однако впервые это показано в [5], но только для случая, когда число переменных n не делится на 3.

Известно следующее свойство функций Касами, которое для полноты приведём с доказательством.

Утверждение 1. *Степень булевой функции Касами от n переменных равна $d+1$ при $0 < d < n/2$ и $n-d+1$ при $n/2 < d < n$.*

Доказательство. Воспользуемся тем (см. [4]), что степень любой мономиальной булевой функции $f(\beta) = \mathrm{tr}(\lambda\beta^k)$ от n переменных равна весу Хэмминга числа $[k]$. В случае, когда $0 < d < n/2$, имеем

$$[k] = [2^{2d} - 2^d + 1] = [2^{2d-1} + 2^{2d-2} + \ldots + 2^d + 2^0] = 2^{2d-1} + 2^{2d-2} + \ldots + 2^d + 2^0,$$

где последнее равенство справедливо, так как $2d-1 < n-1$. Из полученного представления заключаем, что вес Хэмминга числа $[k]$ равен $d+1$.

В случае, когда $n/2 < d < n$, поделим k на $2^n - 1$ с остатком:

$$\begin{aligned} k &= 2^{2d-1} + 2^{2d-2} + \ldots + 2^d + 2^0 \\ &= (2^n - 1)(2^{2d-n-1} + 2^{2d-n-2} + \ldots + 2^0) + 2^{n-1} + 2^{n-2} + \ldots + 2^d + 2^0. \end{aligned}$$

Нетрудно убедиться, что в этом случае вес Хэмминга числа $[k]$, т. е. вес Хэмминга остатка от деления числа k на $2^n - 1$, равен $n - d + 1$. Утверждение 1 доказано.

4. Вспомогательные утверждения

Приведём вспомогательные леммы, которые потребуются для получения основного результата.

Для любого чётного числа n и целого числа d определим число k_d:

$$k_d = [2^{2d} - 2^d + 1].$$

Лемма 1 [8]. *Если $0 < d < n/2$, то $k_{n-d} = 2^r k_d$ при $r = n - 2d$.*

Рассмотрим целые числа $t = 2^{2d-1} + 2^{2d-2} + 2^{2d-3} + \ldots + 2^d + 1$ и $t' = 2^{2d-s} + 2^{2d-s-1} + 2^{2d-s-2} + \ldots + 2^d + 1$, где $1 < s < d < n/2$ и n чётное, и определим множества

$$S(t) = \{\ell \in \mathbb{N} \mid \ell \prec t\}, \quad M(t') = \{[2^j t'] \mid 0 < j < n\}.$$

В приведённых обозначениях сформулируем и докажем две леммы, обобщающие леммы из [8].

Лемма 2. *Множества $S(t)$ и $M(t')$ не пересекаются.*

Доказательство. Покажем, что любой элемент из множества $M(t')$ не лежит в $S(t)$, т. е. число

$$[2^j t'] = [2^{2d-s+j} + 2^{2d-s-1+j} + 2^{2d-s-2+j} + \ldots + 2^{d+j} + 2^j]$$

не предшествует числу t при всех j, $0 < j < n$. Рассмотрим три случая.

Случай 1: $0 < j < d$. Если $2d - s + j \leqslant n - 1$, то число

$$[2^j t'] = 2^{2d-s+j} + 2^{2d-s-1+j} + 2^{2d-s-2+j} + \ldots + 2^{d+j} + 2^j$$

не может предшествовать t, поскольку слагаемое 2^j есть в разложении $[2^j t']$, но отсутствует в разложении t.

Если $2d - s + j > n - 1$, то поделим $[2^j t']$ на $2^n - 1$ с остатком:

$$2^j t' = (2^n - 1)(2^{2d-n-s+j} + 2^{2d-n-s-1+j} + \ldots + 2^0) + 2^{n-1} + 2^{n-2} + \ldots + 2^{d+j} + 2^j + 2^{2d-n-s+j} + 2^{2d-n-s-1+j} + \ldots + 2^0.$$

Полученный остаток не предшествует t за счёт наличия в его разложении 2^j и того, что $2d - n - s + j < j$ (так как $2d - n - s < 0$), т. е. $2^j \neq 2^{2d-n-s+j}$.

Случай 2: $d \leqslant j \leqslant n - d - 1$. Тогда $2d \leqslant d + j \leqslant n - 1$. Аналогично случаю 1 получаем, что $[2^j t']$ не предшествует t, поскольку 2^{d+j} будет присутствовать в разложении $[2^j t']$ и отсутствовать в разложении t (где все показатели степеней основания два строго меньше $2d$).

Случай 3: $n - d \leqslant j < n$. Для начала рассмотрим $j = n - d$:

$$2^{n-d} t' = 2^{n+d-s} + 2^{n+d-s-1} + 2^{n+d-s-2} + \ldots + 2^n + 2^{n-d}.$$

Поделим полученное на $2^n - 1$ с остатком:

$$(2^n - 1)(2^{d-s} + 2^{d-s-1} + 2^{d-s-2} + \ldots + 2^0) + 2^{n-d} + 2^{d-s} + 2^{d-s-1} + \ldots + 2^0.$$

Остаток не предшествует t, так как в разложении $[2^j t']$ присутствует 2^{d-s} и $0 < d - s < d$, а в разложении t таких показателей основания два нет.

Теперь если $n - d < j < n$, то $j = n - d + j'$, где $0 < j' < d$. Получаем

$$[2^j t'] = [(2^{n-d} t') 2^{j'}] = [2^{n-d+j'} + 2^{d-s+j'} + 2^{d-s-1+j'} + \ldots + 2^{j'}].$$

Так как $n - d + j' < n$ и $d - s + j' < 2d - s < n - s$, число

$$[2^j t'] = 2^{n-d+j'} + 2^{d-s+j'} + 2^{d-s-1+j'} + \ldots + 2^{j'}$$

не предшествует t за счёт наличия $2^{j'}$ в разложении $[2^j t']$.

Итак, рассмотрев все случаи, т. е. все возможные значения j такие, что $0 < j < n$, получаем, что элементы $[2^j t']$, пробегающие всё множество $M(t')$, не могут принадлежать множеству $S(t)$, т. е. $S(t) \cap M(t') = \varnothing$. Лемма 2 доказана.

Лемма 3. *Мощность циклотомического класса $C(t')$ по модулю $2^n - 1$ равна n.*

Доказательство. От противного. Предположим, что $|C(t')| < n$. Тогда найдётся по крайней мере одно число j, $0 < j < n$, такое, что $[2^j t'] = t'$, а следовательно, $t' \in M(t')$. Кроме того, как нетрудно заметить, $t' \prec t$, т. е. $t' \in S(t)$. Но $S(t) \cap M(t') = \varnothing$ по лемме 2; противоречие. Таким образом, $|C(t')| = n$. Лемма 3 доказана.

Рассмотрим целое число $t'' = 2^d + 1$, где $0 < d < n/2$, n чётное.

Лемма 4. *Для t'' справедливы следующие утверждения*:
(i) $|C(t'')| = n$;
(ii) *множества $S(t)$ и $M(t'')$ не пересекаются при $d \leqslant n/3$.*

Доказательство. (i) От противного. Предположим, что мощность класса $C(t'')$ равна r, где $r < n$. По свойству (a) циклотомического класса $r|n$, т. е. r делит n. Тогда $2^r t'' \equiv t'' (\bmod\ (2^n - 1))$ или

$$(2^r - 1)t'' \equiv 0 \ (\bmod\ (2^n - 1)).$$

Получаем, что $(2^n - 1)|(2^r - 1)t''$. Так как $r|n$ и $r < n$, то $r \leqslant n/2$. К тому же $d < n/2$, а следовательно, $t'' < 2^{n/2} + 1$. Получаем противоречие, поскольку $(2^n - 1)$ не делит $(2^r - 1)t'' < (2^{n/2} - 1)(2^{n/2} + 1) = (2^n - 1)$.

(ii) Рассмотрим элементы множества $M(t'')$:

$$[2^i t''] = [2^{d+i} + 2^i] = \begin{cases} 2^{d+i} + 2^i & \text{при } 0 < i < n - d, \\ 2^i + 1 & \text{при } i = n - d, \\ 2^{d+i-n} + 2^i & \text{при } n - d < i < n. \end{cases}$$

Аналогично доказательству леммы 3 нетрудно убедиться, что элементы множества $M(t'')$ не лежат в $S(t)$ при $i \neq n - d$, т. е. не предшествуют t. Рассмотрим случай $i = n - d$: число $2^{n-d} + 1$ не предшествует t, только если $n - d \geqslant 2d$, т. е. $n \geqslant 3d$, или $n - d < d$, т. е. $n < 2d$, что противоречит выбору d, поскольку рассматриваем $d < n/2$. Таким образом, при $d \leqslant n/3$ множества $M(t'')$ и $S(t)$ не пересекаются. Лемма 4 доказана.

Лемма 5. *Пусть $a_1, \ldots, a_m$ — произвольные ненулевые попарно различные элементы поля $GF(2^n)$, p — целое число такое, что $0 < p \leqslant m$, и $r_1, \ldots, r_p$ — целые числа. Для суммы*

$$A = \sum_{1 \leqslant i \leqslant m} a_i^{2^{r_1}+\ldots+2^{r_p}} + \sum_{1 \leqslant i < j \leqslant m} (a_i + a_j)^{2^{r_1}+\ldots+2^{r_p}} + \ldots + (a_1 + \ldots + a_m)^{2^{r_1}+\ldots+2^{r_p}}$$

справедливы следующие утверждения:

(i) *A тождественно равно нулю при $p < m$*;

(ii) $A = \sum\limits_{\pi \in S_m} a_1^{2^{r_1\pi}} a_2^{2^{r_2\pi}} \ldots a_m^{2^{r_m\pi}}$ *при $p = m$.*

Доказательство. Используя равенство $(\beta_1+\beta_2)^{2^r} = \beta_1^{2^r}+\beta_2^{2^r}$, справедливое для любых элементов $\beta_1, \beta_2 \in GF(2^n)$ и целого числа r, перепишем сумму A следующим образом:

$$A = \sum_{1 \leqslant i \leqslant m} a_i^{2^{r_1}+\ldots+2^{r_p}} + \sum_{1 \leqslant i < j \leqslant m} \prod_{1 \leqslant \ell \leqslant p} \left(a_i^{2^{r_\ell}} + a_j^{2^{r_\ell}}\right) + \ldots + \prod_{1 \leqslant \ell \leqslant p} \left(a_1^{2^{r_\ell}} + \ldots + a_m^{2^{r_\ell}}\right).$$

Нетрудно заметить, что в каждом произведении, стоящем под суммой, при перемножении все слагаемые различны. Посчитаем сколько раз встречаются различные слагаемые в сумме A:

$$\begin{aligned}
&a_i^{2^{r_1}+\ldots+2^{r_p}} : && 1 + C_{m-1}^1 + \ldots + C_{m-1}^{m-1} = 2^{m-1},\\
&a_{j_1}^{2^{r_1\pi}+\ldots+2^{r_k\pi}} a_{j_2}^{2^{r_{(k+1)\pi}}+\ldots+2^{r_p\pi}} : && 0 + 1 + C_{m-2}^1 + \ldots + C_{m-2}^{m-2} = 2^{m-2},\\
&\qquad\qquad \ldots &&\\
&a_{j_1}^{2^{r_1\pi}+\ldots+2^{r_{k_1}\pi}} \ldots a_{j_p}^{2^{r_{(k_{p-1}+1)\pi}}+\ldots+2^{r_p\pi}} : && 0 + 0 + 0 + \ldots + C_{m-p}^{m-p} = 2^{m-p}.
\end{aligned}$$

Таким образом, все возможные слагаемые рассмотрены, при $p < m$ каждое из этих слагаемых встречается чётное число раз, а следовательно, по модулю 2 сокращается. Если же $p = m$, то остаются лишь слагаемые вида $a_1^{2^{r_1\pi}} \ldots a_m^{2^{r_m\pi}}$, которые встречаются в сумме A ровно по одному разу для любой перестановки $\pi \in S_m$, что обеспечивает справедливость (ii). Лемма 5 доказана.

Лемма 6. *Для произвольных элементов $a_1, \ldots, a_m$ поля $GF(2^n)$ справедливо равенство*

$$\sum_{\pi\in S_m} a_1^{2^{m-1\pi}} a_2^{2^{m-2\pi}} \ldots a_m^{2^{m-m\pi}} = (a_1 + \ldots + a_m) \times \prod_{1\leqslant i_1<\ldots<i_{m-1}\leqslant m} (a_{i_1} + \ldots + a_{i_{m-1}}) \ldots \prod_{1\leqslant i_1<i_2\leqslant m} (a_{i_1} + a_{i_2}) \prod_{1\leqslant i\leqslant m} a_i.$$

Доказательство. Рассмотрим произвольное слагаемое, получаемое при раскрытии скобок в правой части равенства: $a_{1\pi}^{k_1} a_{2\pi}^{k_2} \ldots a_m^{k_m}$, где π — произвольная фиксированная перестановка и $k_1 \geqslant \ldots \geqslant k_m$. Нетрудно заметить, что $1 \leqslant k_i \leqslant 2^{m-1}$ для всех i от 1 до m, а также $\sum\limits_{i=1}^{m} k_i = 2^m - 1$. Покажем, что рассматриваемое слагаемое встречается нечётное число раз (т. е. сравнимое с 1 в поле характеристики 2) только при $k_i = 2^{m-i}$ для всех i от 1 до m и чётное число раз (т. е. сравнимое с 0 в поле характеристики 2) при любых других $k_1, \ldots, k_m$.

Подсчитаем, сколько раз встречается такое слагаемое: выбираем его $K = C_{2^{m-1}}^{k_1} \cdot N(k_1)$ способом, где первый биномиальный коэффициент отвечает за выбор $a_{1\pi}^{k_1}$, а $N(k_1)$ — за выбор $a_{2\pi}^{k_2} \ldots a_{m\pi}^{k_m}$ в зависимости от k_1. Тем самым K нечётно, если $N(k_1)$ нечётно и $C_{2^{m-1}}^{k_1} \equiv 1 \pmod 2$, что выполняется только при $k_1 \preceq 2^{m-1}$. Следовательно, для нечётного K необходимо, чтобы k_1 равнялось 2^{m-1}. После того как выбрали 2^{m-1} скобку с элементом $a_{1\pi}$ из правой части равенства, выбираем из оставшихся скобок k_2 скобки с $a_{2\pi}$, их осталось ровно 2^{m-2}. Таким образом,

$$K = C_{2^{m-1}}^{k_1} C_{2^{m-2}}^{k_2} \cdot N(k_1, k_2).$$

Аналогичными рассуждениями получаем, что $k_2 = 2^{m-2}$. Продолжая данный процесс, выводим требуемое, а именно, что K нечётно только при $k_i = 2^{m-i}$ для всех i.

Итак, в произведении в правой части при раскрытии скобок остаются только слагаемые вида $a_{1\pi}^{2^{m-1}} a_{2\pi}^{2^{m-2}} \ldots a_{m\pi}^{2^0}$ для произвольной перестановки $\pi \in S_m$, что с точностью до переобозначения совпадает с суммой из левой части равенства. Лемма 6 доказана.

5. Кратные производные булевых функций Касами

В [8] исследована вторая производная булевых функций Касами и доказана

Теорема 1. *Для любой функции Касами f от n переменных, где n чётное и $n \geqslant 8$, такой, что $\deg(f) \geqslant 4$, вторая производная $D_a D_b f$ тождественно не равна нулю для любых ненулевых $a, b \in GF(2^n)$, $a \neq b$.*

Следствием этой теоремы в [8] являлось то, что произвольная не квадратичная бент-функция Касами аффинно не эквивалентна бент-функциям из класса Майорана — МакФарланда.

В данной работе исследуются кратные производные булевых функций Касами высоких порядков. Сформулируем и докажем теорему, которая является основой для получения результата о кратных производных булевых функций Касами.

Теорема 2. *Пусть $f(\beta) = \mathrm{tr}(\lambda\beta^k)$ — булева функция от n переменных, где n чётное, $n \geqslant 8$, $\lambda \in GF^*(2^n)$, $k = 2^{2d} - 2^d + 1$, $3 \leqslant d < n/2$, и пусть натуральное число m равно $d-2$ при $d > n/3$ и $d-1$ при $d \leqslant n/3$. Тогда для произвольных линейно независимых над $GF(2)$ элементов $a_1, \ldots, a_m$ из $GF^*(2^n)$ производная $D_{a_1} \ldots D_{a_m} f$ не равна нулю тождественно.*

Доказательство. Разобьём доказательство на три этапа. На первом этапе получим представление производной $D_{a_1} \ldots D_{a_m} f$, удобное для анализа, на втором найдём достаточное условие того, что производная не равна нулю тождественно, а на третьем покажем, что это условие выполнено.

Этап 1. Так как $a_1, \ldots, a_m$ не равны нулю и попарно различны, производная по направлению $a_1, \ldots, a_m$ равна

$$D_{a_1} \ldots D_{a_m} f(\beta) = f(\beta) + \sum_{1 \leqslant i \leqslant m} f(\beta + a_i) + \sum_{1 \leqslant i < j \leqslant m} f(\beta + a_i + a_j)$$
$$+ \sum_{1 \leqslant i < j < l \leqslant m} f(\beta + a_i + a_j + a_l) + \ldots + f(\beta + a_1 + \ldots + a_m)$$
$$= \mathrm{tr}\Big(\lambda(\beta^k + \sum_{1 \leqslant i \leqslant m} (\beta + a_i)^k + \sum_{1 \leqslant i < j \leqslant m} (\beta + a_i + a_j)^k + \ldots + (\beta + a_1 + \ldots + a_m)^k)\Big)$$

в силу линейности следа. Пользуясь формулой бинома Ньютона в полях характеристики 2 и тем, что $C_k^\ell \equiv 1 (\mathrm{mod}\ 2)$ только при $\ell \preceq k$, получаем

$$D_{a_1} \ldots D_{a_m} f(\beta) = \sum_{\ell \preceq k} \mathrm{tr}(q_\ell \beta^\ell), \tag{1}$$

где

$$q_\ell = \lambda\Big(\sum_{1 \leqslant i \leqslant m} a_i^{k-\ell} + \sum_{1 \leqslant i < j \leqslant m} (a_i + a_j)^{k-\ell} + \ldots + (a_1 + \ldots + a_m)^{k-\ell} \Big).$$

В выражении (1) остаётся сумма только по ℓ таким, что $\ell \prec k$, так как в случае $\ell = k$ слагаемое β^k встречается чётное число раз, а следовательно, по модулю два сокращается. Заметим также, что если $k - \ell = 2^{r_1} + \ldots + 2^{r_p}$ для некоторых $r_1, \ldots, r_p$, т. е. $\mathrm{wt}(k-\ell) = p$, то из леммы 5(i) следует, что $q_\ell = 0$ для всех $p < m$.

Определим множество $I = \{\ell \mid \ell \prec k,\ \mathrm{wt}(k-\ell) \geqslant m\}$. Тогда, используя два последних замечания, можем переписать выражение (1) в виде

$$D_{a_1} \ldots D_{a_m} f(\beta) = \mathrm{tr}\Big(\sum_{\ell \in I} q_\ell \beta^\ell\Big) = Q(\beta) = \sum_{\ell \in I} \mathrm{tr}(q_\ell \beta^\ell).$$

Разделим множество I на части, каждая из которых состоит из представителей одного циклотомического класса по модулю $2^n - 1$. Пусть J — подмножество I, состоящее из наименьших представителей циклотомических классов по модулю $2^n - 1$. Тогда $Q(\beta) = \mathrm{tr}\Big(\sum\limits_{j \in J} \sum\limits_{i \in C'(j)} q_i \beta^i\Big)$, где $C'(j) = I \cap C(j)$.

Используя свойство (b) циклотомического класса, получим удобный для анализа вид рассматриваемой производной:

$$Q(\beta) = \mathrm{tr}\Big(\sum_{j \in J} q'_j \beta^j\Big) = \sum_{j \in J} \mathrm{tr}(q'_j \beta^j), \tag{2}$$

где q'_j зависит от $a_1, \ldots,\ a_m,\ \lambda,\ C(j)$.

Этап 2. В выражении (2) множество J выбрано так, что $Q \equiv 0$ тогда и только тогда, когда для всех $j \in J$ выполняется $\mathrm{tr}(q'_j \beta^j) \equiv 0$. Заметим, что для любого $j \in J$ такого, что $|C(j)| = n$, функция $\mathrm{tr}(q'_j \beta^j)$ не может тождественно равняться константе, если $q'_j \neq 0$.

Таким образом, чтобы рассматриваемая производная не равнялась нулю тождественно, достаточно показать, что существует $j_0 \in J,\ j_0 > 0$, такой, что $|C(j_0)| = n$ и $q'_{j_0} \neq 0$.

Для этого представим $k = 2^{2d} - 2^d + 1$ в виде

$$k = 2^{2d-1} + 2^{2d-2} + 2^{2d-3} + \ldots + 2^d + 1$$

и выберем $j_0 = 2^{2d-m-1} + 2^{2d-m-2} + \ldots + 2^d + 1$. По выбору j_0 имеем $j_0 \prec k$ и $\mathrm{wt}(k - j_0) = m$, а значит, $j_0 \in I$. Следовательно, $j_0 \in C'(j_0)$.

Рассмотрим два случая и покажем, что в каждом из них элемент j_0 является единственным в $C'(j_0)$.

Случай 1: $d > n/3$. Тогда $m = d-2$. По лемме 3 для $s = m+1$ имеем $|C(j_0)| = n$. Из леммы 2 для $s = m+1$ следует, что $I \cap (C(j_0) \setminus \{j_0\}) = \varnothing$,

поскольку $I \subseteq S(k)$, а $C(j_0) \setminus \{j_0\} = M(j_0)$, если $|C(j_0)| = n$. Другими словами, $C'(j_0)$ содержит единственный элемент j_0. Отсюда $j_0 \in J$.

Случай 2: $d \leqslant n/3$. Тогда $m = d-1$, т. е. $j_0 = 2^d+1$. Тогда $|C(j_0)| = n$ по лемме 4 и при $d \leqslant n/3$ множество $C'(j_0)$ содержит единственный элемент j_0 и $j_0 \in J$ (рассуждения аналогичны случаю 1).

Таким образом, $C'(j_0) = \{j_0\}$ в обоих случаях, а значит, $q'_{j_0} = q_{j_0}$. Распишем коэффициент q'_{j_0}, подставляя $k-j_0 = 2^{2d-1}+2^{2d-2}+\ldots+2^{2d-m}$:

$$q'_{j_0} = \lambda\Big(\sum_{1\leqslant i\leqslant m} a_i^{2^{2d-1}+2^{2d-2}+\ldots+2^{2d-m}} + \sum_{1\leqslant i<j\leqslant m} (a_i+a_j)^{2^{2d-1}+2^{2d-2}+\ldots+2^{2d-m}} + \ldots + (a_1+\ldots+a_m)^{2^{2d-1}+2^{2d-2}+\ldots+2^{2d-m}}\Big).$$

Используя лемму 5(ii), преобразуем коэффициент q'_{j_0} следующим образом:

$$\begin{aligned} q'_{j_0} &= \lambda \sum_{\pi\in S_m} a_1^{2^{2d-1\pi}} a_2^{2^{2d-2\pi}} \ldots a_m^{2^{2d-m\pi}} \\ &= \lambda \sum_{\pi\in S_m} \big(a_1^{2^{m-1\pi}} a_2^{2^{m-2\pi}} \ldots a_m^{2^{m-m\pi}}\big)^{2^{2d-m}} \\ &= \lambda\Big(\sum_{\pi\in S_m} a_1^{2^{m-1\pi}} a_2^{2^{m-2\pi}} \ldots a_m^{2^{m-m\pi}}\Big)^{2^{2d-m}}. \end{aligned}$$

Окончательно получаем

$$q'_{j_0} = \lambda\Big(\sum_{\pi\in S_m} a_1^{2^{m-1\pi}} a_2^{2^{m-2\pi}} \ldots a_m^{2^{m-m\pi}}\Big)^{2^{2d-m}}. \tag{3}$$

Заметим, что любая степень ненулевого элемента поля $GF(2^n)$ есть ненулевой элемент. Следовательно, для доказательства теоремы осталось показать, что в выражении (3) сумма в скобках не равна нулю.

Этап 3. По лемме 6 справедливо равенство

$$\begin{aligned} \sum_{\pi\in S_m} a_1^{2^{m-1\pi}} a_2^{2^{m-2\pi}} \ldots a_m^{2^{m-m\pi}} &= (a_1+\ldots+a_m) \\ \times \prod_{1\leqslant i_1<\ldots<i_{m-1}\leqslant m} (a_{i_1}+\ldots+a_{i_{m-1}}) \ldots & \prod_{1\leqslant i_1<i_2\leqslant m} (a_{i_1}+a_{i_2}) \prod_{1\leqslant i\leqslant m} a_i. \end{aligned}$$

Поскольку в условии теоремы элементы поля $a_1, \ldots, a_m$ полагаются линейно независимыми над $GF(2)$, произведение всевозможных сумм

этих элементов есть ненулевой элемент. Следовательно, коэффициент q'_{j_0} не равен нулю, и поэтому рассматриваемая производная не равна нулю тождественно. Теорема 2 доказана.

Используя теорему 2, докажем основной результат работы о кратных производных булевых функций Касами.

Теорема 3. *Пусть f — произвольная булева функция Касами от n переменных, где n чётное, $n \geqslant 8$, и $\deg(f) = t$. Тогда справедливы следующие утверждения*:

(i) *при $4 \leqslant t \leqslant (n+3)/3$ производная $D_{a_1} \dots D_{a_{t-2}} f$ не равна нулю тождественно для произвольных линейно независимых над $GF(2)$ элементов $a_1, \dots, a_{t-2} \in GF(2^n)$*;

(ii) *при $(n+3)/3 < t \leqslant n/2$ производная $D_{a_1} \dots D_{a_{t-3}} f$ не равна нулю тождественно для произвольных линейно независимых над $GF(2)$ элементов $a_1, \dots, a_{t-3} \in GF(2^n)$*.

Доказательство. По определению функция Касами выглядит следующим образом: $f(\beta) = \mathrm{tr}(\lambda\beta^k)$, где $\lambda \in GF^*(2^n)$, $k = 2^{2d} - 2^d + 1$ для $0 < d < n$ и $\mathrm{НОД}(d, n) = 1$.

Рассмотрим вначале случай $0 < d < n/2$. По утверждению 1 степень функции f при этом равна $d+1$. Получаем, что число d лежит в интервале $3 \leqslant d \leqslant n/3$ при $4 \leqslant t \leqslant (n+3)/3$ и в интервале $n/3 < d < n/2$ при $(n+3)/3 < t \leqslant n/2$. Следовательно, попадаем в условия теоремы 2, и число m равно $t-2$ и $t-3$ соответственно для случаев (i) и (ii).

Рассмотрим случай $n/2 < d < n$. Так как по условию $\mathrm{НОД}(d, n) = 1$, имеем $\mathrm{НОД}(n-d, n) = 1$. Таким образом, для каждого $n/2 < d < n$ существует $d' = n - d$ такой, что $0 < d' < n/2$ и $\mathrm{НОД}(d', n) = 1$. Также по лемме 1 $[k] = 2^r k'$ для $r = n - 2d'$ и $k' = 2^{2d'} - 2^{d'} + 1$ (заметим, что $\beta^k = \beta^{[k]}$ для любого элемента поля β).

Проведём цепочку преобразований:

$$\mathrm{tr}(\lambda\beta^{2^r k'}) \;=\; \mathrm{tr}(\lambda'^{2^r}\beta^{2^r k'}) \;=\; \mathrm{tr}((\lambda'\beta^{k'})^{2^r}) \;=\; \mathrm{tr}(\lambda'\beta^{k'}),$$

где $\lambda = \lambda'^{2^r}$ (это представление справедливо ввиду теоремы об автоморфизмах [1], утверждающей, что множество автоморфизмов поля $GF(2^n)$ является циклической мультипликативной группой порядка n с порождающим элементом $\varphi : \beta \to \beta^2$).

Таким образом, вновь получаем случай $0 < d < n/2$, для которого доказательство уже разобрано. Теорема 3 доказана.

6. Существенная зависимость булевых функций Касами

В данном разделе сформулирован и доказан основной результат работы, заключающийся в установлении нового свойства алгебраической нормальной формы булевой функции Касами, а именно, её существенной зависимости от произведений достаточно большого числа переменных.

Введём следующее понятие.

Определение 2. Булеву функцию от n переменных назовём *k-существенно зависимой*, если для любого набора попарно различных индексов $i_1, \ldots, i_k$, где $0 < k \leqslant n$, в АНФ функции существует слагаемое $y_{j_1} \ldots y_{j_m}$ такое, что $\{i_1, \ldots, i_k\} \subseteq \{j_1, \ldots, j_m\}$. Наибольшее число k, для которого функция k-существенно зависима, назовём *порядком* существенной зависимости функции.

Другими словами, функция называется *k-существенно зависимой*, если для любого произведения из k различных переменных в АНФ функции существует слагаемое, содержащее это произведение.

Пример 1. Функция $f(y_1, y_2, y_3, y_4) = 1 \oplus y_1y_2 \oplus y_1y_3y_4 \oplus y_2y_3y_4$ является 2-существенно зависимой, но не является 3-существенно зависимой.

Обозначим через e_i вектор из $\mathbb{Z}_2^n$ такой, что $e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$, где единица стоит на месте с номером i. Пусть f — произвольная булева функция от n переменных. Нетрудно убедиться, что если производная $D_{e_{i_1}} \ldots D_{e_{i_k}} f$ не равна нулю тождественно для каждого набора индексов $i_1, \ldots, i_k$ из множества $\{1, \ldots, n\}$, то функция f k-существенно зависима.

Теорема 4. *Пусть f — произвольная булева функция Касами от n переменных, где n чётное, $n \geqslant 8$. Тогда справедливы следующие утверждения*:

(i) *при* $\deg(f) = 4$ *функция f является 2-существенно зависимой*;

(i) *при* $\deg(f) = t$, *где* $4 \leqslant t \leqslant (n+3)/3$, *функция f является $(t-2)$-существенно зависимой*;

(ii) *при* $\deg(f) = t$, *где* $(n+3)/3 < t \leqslant n/2$, *функция f является $(t-3)$-существенно зависимой*.

Доказательство. Напомним, что между элементами $GF(2^n)$ и $\mathbb{Z}_2^n$ существует взаимно однозначное соответствие, а именно, элементу β из $GF(2^n)$, представленному в виде многочлена $\beta(x) = \beta_1 + \beta_2 x + \ldots + \beta_n x^{n-1}$, однозначно соответствует вектор $\beta = (\beta_1, \ldots, \beta_n) \in \mathbb{Z}_2^n$.

Используя последнее равенство получаем, что утверждения (i), (ii) и (iii) являются прямыми следствиями теорем 1 и 3, где в качестве эле-

ментов $a_1, \ldots, a_{t-2}$ выбираем линейно независимые над $GF(2)$ элементы $e_{i_1}, \ldots, e_{i_{t-2}}$. Теорема 4 доказана.

Замечание 1. По результатам исследования функций Касами от малого числа переменных можно заметить, что в общем случае максимально возможный порядок существенной зависимости функций Касами степени t равен $t-2$ (минимальный порядок равен $t-3$ в силу теоремы 4), поскольку можно привести пример функции, которая уже не обладает свойством $(t-1)$-существенной зависимости.

Пример 2. Пусть $n = 12$, поле $GF(2^n)$ построено с помощью неприводимого многочлена $x^{12} + x^3 + 1$. Рассмотрим $d = 5,\ k = 2^{2d} - 2^d + 1 = 993,\ \lambda = x + 1$. Тогда бент-функция Касами $f(\beta) = \mathrm{tr}(\lambda\beta^k)$ $(\deg(f) = 6)$ является 4-существенно зависимой, но не является 5-существенно зависимой.

Замечание 2. Приведённые рассуждения для булевых функций Касами верны, в частности, и для бент-функций Касами.

Выражаю благодарность научному руководителю Н. Н. Токаревой, а также Д. О. Ревину и А. А. Бутурлакину за полезные обсуждения работы.

ЛИТЕРАТУРА

1. **Логачев О. А., Сальников А. А., Ященко В. В.** Булевы функции в теории кодирования и криптологии. — М.: Московский центр непрерывного математического образования, 2004. — 470 с.
2. **Токарева Н. Н.** Нелинейные булевы функции: бент-функции и их обобщения. — Saarbrücken: LAP LAMBERT Acad. Publ., 2011. — 180 с. (ISBN: 978–3–8433–0904–2)
3. **Canteaut A., Daum M., Dobbertin H., Leander G.** Finding non-normal bent functions // Discrete Appl. Math. — 2006. — Vol. 154. — P. 202–218.
4. **Carlet C.** Boolean functions for cryptography and error correcting codes // Boolean methods and models. — Cambridge: Cambridge Univ. Press, to appear.
`www-rocq.inria.fr/secret/Claude.Carlet/chap-fcts-Bool.pdf`.
5. **Dillon J. F., Dobbertin H.** New cyclic difference sets with Singer parameters // Finite Fields Their Appl. — 2004. — Vol. 10. — P. 342–389.
6. **Langevin P., Leander G.** Monomial bent function and Stickelberger's theorem // Finite Fields Their Appl. — 2008. — Vol. 14. — P. 727—742.
7. **Langevin P., Leander G., McGuire G.** Kasami bent function are not equivalent to their duals // Finite Fields Appl. — 2008. — Vol. 461. — P. 187–197.

8. Sharma D., Gangopadhyay S. On Kasami bent function // Cryptology ePrint Archive, Report 2008/426. — 10 p. `http://eprint.iacr.org`

Фролова Анастасия Александровна,
e-mail: frolova.anast@gmail.com

Статья поступила
26 декабря 2011 г.

Переработанный вариант —
18 июня 2012 г.