2014 Теоретические основы прикладной дискретной математики № 3(25)

DOI 10.17223/20710410/25/3

УДК 519.7

ВЕРХНЯЯ ОЦЕНКА ЧИСЛА БЕНТ-ФУНКЦИЙ НА РАССТОЯНИИ 2^k ОТ ПРОИЗВОЛЬНОЙ БЕНТ-ФУНКЦИИ ОТ $2k$ ПЕРЕМЕННЫХ

Н. А. Коломеец

Институт математики им. С. Л. Соболева СО РАН, г. Новосибирск, Россия

E-mail: nkolomeec@gmail.com

Получена точная верхняя оценка числа бент-функций на расстоянии 2^k от произвольной бент-функции от $2k$ переменных. Установлено, что она достигается только для квадратичных бент-функций. Введено понятие полной аффинной расщепляемости булевой функции. Доказано, что полностью аффинно расщепляемыми могут быть только аффинные и квадратичные функции.

Ключевые слова: *булевы функции, бент-функции, квадратичные бент-функции.*

Введение

Рассматриваются метрические свойства класса бент-функций, а именно число бент-функций на минимальном возможном расстоянии от произвольной бент-функции. Бент-функции — булевы функции от чётного числа переменных, наиболее удалённые от множества всех аффинных функций. Они предложены О. Ротхаусом в 1966 г. в работе [1]. Бент-функции имеют приложения в криптографии, теории кодирования, комбинаторике, алгебре, теории символьных последовательностей (см., например, обзор [2]).

В работе [3] доказан критерий расположения двух бент-функций на минимальном возможном расстоянии друг от друга. В [4] построены все бент-функции на минимальном расстоянии от квадратичной бент-функции и подсчитано число таких бент-функций. В [5] получены возможные расстояния между двумя бент-функциями от $2k$ переменных, принадлежащие интервалу от 2^k до $2^{k+1} - 1$ (от минимального до удвоенного минимального). Заметим, что гипотеза о том, что любую булеву функцию степени не больше k можно представить как сумму двух бент-функций от $2k$ переменных, высказанная Н. Н. Токаревой в работе [6], также связана с метрическими свойствами класса бент-функций.

Работа построена следующим образом: в п. 1 вводятся необходимые определения; в п. 2 приводится обзор свойств булевых функций, связанных с аффинностью на подпространстве; в п. 3 вводится понятие полностью аффинно расщепляемой булевой функции. Доказывается, что полностью аффинно расщепляемыми являются только аффинные и квадратичные булевы функции. Отметим, что в работе [7] рассмотрен частный случай полной аффинной расщепляемости, а именно доказано, что только аффинные и квадратичные булевы функции от n переменных являются полностью аффинно расщепляемыми порядка $\lceil n/2 \rceil$. В п. 4 доказывается точная верхняя оценка числа бент-функций на расстоянии 2^k от бент-функции от $2k$ переменных. Данная оценка достигается только для полностью аффинно расщепляемых бент-функций, т. е. только для квадратичных бент-функций.

1. Определения

Введём необходимые определения. Функция вида $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$ называется *булевой функцией* от n переменных; $x = (x_1, \ldots, x_n) \in \mathbb{Z}_2^n$ — *двоичным вектором* длины n.

Через $\mathcal{F}_n$ обозначим множество всех булевых функций от n переменных. *Расстоянием* между двумя булевыми функциями $f, g \in \mathcal{F}_n$ называется число векторов из $\mathbb{Z}_2^n$, на которых значения функций различаются.

Для $x, y \in \mathbb{Z}_2^n$ определим $x \oplus y = (x_1 \oplus y_1, \ldots, x_n \oplus y_n)$, где $\oplus$ — сложение по модулю 2. Введём аналог скалярного произведения векторов x и y:

$$\langle x, y \rangle = x_1 y_1 \oplus x_2 y_2 \oplus \ldots \oplus x_n y_n,$$

где $x_i y_i$ — умножение по модулю 2.

Весом $\mathrm{wt}(f)$ булевой функции $f \in \mathcal{F}_n$ называется число векторов из $\mathbb{Z}_2^n$, на которых она принимает значение 1.

Подфункцией $f_{i_1,\ldots,i_k}^{b_1,\ldots,b_k}$ функции f, где $0 \leqslant k \leqslant n$; $1 \leqslant i_1 < i_2 < \ldots < i_k \leqslant n$ и $b_1, \ldots, b_k \in \mathbb{Z}_2$, называется функция из $\mathcal{F}_{n-k}$, полученная из f подстановкой вместо $x_{i_1}, \ldots, x_{i_k}$ констант $b_1, \ldots, b_k$.

Ограничением булевой функции $f \in \mathcal{F}_n$ на множество $S \subseteq \mathbb{Z}_2^n$ называется функция $f|_S : S \to \mathbb{Z}_2$, такая, что $f|_S(x) = f(x)$ для всех $x \in S$.

Булева функция $f \in \mathcal{F}_n$ называется *уравновешенной* (или *сбалансированной*), если $\mathrm{wt}(f) = 2^{n-1}$. Уравновешенность также обобщают на ограничения булевых функций: функция f называется *уравновешенной на множестве* $D \subseteq \mathbb{Z}_2^n$, $|D|$ чётна, если она принимает значение 1 ровно на половине элементов множества D.

Представление булевой функции $f \in \mathcal{F}_n$ в виде

$$f(x_1, \ldots, x_n) = a_0 \oplus \bigoplus_{k=1}^{n} \bigoplus_{1 \leqslant i_1 < i_2 < \ldots < i_k \leqslant n} a_{i_1 \ldots i_k} x_{i_1} \ldots x_{i_k}, \text{ где } a_0, a_{i_1 \ldots i_k} \in \mathbb{Z}_2,$$

называется *алгебраической нормальной формой* (*АНФ*) или *полиномом Жегалкина*; $x_{i_1} \ldots x_{i_k}$ — *мономом степени* k; $a_{i_1 \ldots i_k}, a_0$ — *коэффициентами* при мономах. *Степенью* $\deg f$ функции f называется длина монома наибольшей степени с ненулевым коэффициентом (или $-\infty$, если все коэффициенты нулевые). Известно, что любая булева функция может быть представлена в виде АНФ, причём единственным способом.

Производной $D_\alpha f$ функции $f \in \mathcal{F}_n$ *по направлению* $\alpha \in \mathbb{Z}_2^n$ называется функция $f(x) \oplus f(x \oplus \alpha)$. Заметим, что если $\deg f > 0$, то $\deg D_\alpha f < \deg f$ для любого $\alpha \in \mathbb{Z}_2^n$.

Непустое множество $L \subseteq \mathbb{Z}_2^n$ называется *линейным подпространством* $\mathbb{Z}_2^n$, если для любых $a, b \in L$ верно, что $a \oplus b \in L$. Обозначим через $s \oplus D$, где $s \in \mathbb{Z}_2^n$ и $D \subseteq \mathbb{Z}_2^n$, *сдвиг* множества D, а именно $s \oplus D = \{s \oplus x : x \in D\}$. Множество $U \subseteq \mathbb{Z}_2^n$ называется *аффинным подпространством* $\mathbb{Z}_2^n$ (или просто *подпространством*), если оно является сдвигом некоторого линейного подпространства. *Размерностью* аффинного подпространства называется размерность соответствующего линейного подпространства. Размерность обозначается через $\dim U$. Отметим, что линейное подпространство также является аффинным подпространством. Далее в тексте будем часто опускать слово «аффинное», т. е. будем называть аффинное подпространство просто подпространством. Будем говорить, что L является подпространством U, если L и U являются подпространствами $\mathbb{Z}_2^n$ и $L \subseteq U$.

Аффинной булевой функцией от n переменных называется булева функция, степень которой не превосходит 1, или, другими словами, функция вида

$$\ell_{a,c}(x) = \langle a, x \rangle \oplus c \text{ для некоторых } a \in \mathbb{Z}_2^n, c \in \mathbb{Z}_2.$$

Через $\mathcal{A}_n$ обозначается множество всех аффинных булевых функций от n переменных.

Преобразованием Уолша — Адамара булевой функции $f \in \mathcal{F}_n$ называется функция $W_f : \mathbb{Z}_2^n \to \mathbb{Z}$, заданная равенством

$$W_f(y) = \sum_{x \in \mathbb{Z}_2^n} (-1)^{f(x) \oplus \langle x, y \rangle},$$

числа $W_f(y)$ называются *коэффициентами Уолша — Адамара*. Эти коэффициенты однозначно определяют функцию f. Для них справедливо *равенство Парсеваля*:

$$\sum_{y \in \mathbb{Z}_2^n} W_f^2(y) = 2^{2n}.$$

Для произвольной булевой функции $f \in \mathcal{F}_n$, линейного подпространства $L \subseteq \mathbb{Z}_2^n$ и $a, b \in \mathbb{Z}_2^n$ справедлива следующая формула:

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

Бент-функцией называется булева функция от $2k$ переменных, все коэффициенты Уолша — Адамара которой по модулю равны 2^k. Множество всех бент-функций от $2k$ переменных обозначается через $\mathfrak{B}_{2k}$. Заметим, что для бент-функции $f \in \mathfrak{B}_{2k}$ справедливо

$$\mathrm{wt}(f),\ \mathrm{dist}(f, \ell_{y,c}) \in \{2^{2k-1} \pm 2^{k-1}\} \text{ для любых } y \in \mathbb{Z}_2^{2k}, c \in \mathbb{Z}_2.$$

С бент-функцией f связывают *дуальную* функцию $\tilde{f}$, определяемую равенством

$$(-1)^{\tilde{f}(y)} = \frac{1}{2^k} W_f(y) \text{ для всех } y \in \mathbb{Z}_2^{2k}.$$

Функция $\tilde{f}$ тоже является бент-функцией. Для бент-функции f формула (1) имеет более простой вид:

$$\sum_{x \in a \oplus L} (-1)^{f(x) \oplus \langle b, x \rangle} = 2^{\dim L - k} (-1)^{\langle a, b \rangle} \sum_{y \in b \oplus L^\perp} (-1)^{\tilde{f}(y) \oplus \langle a, y \rangle}, \tag{2}$$

где L — линейное подпространство $\mathbb{Z}_2^{2k}$; $a, b \in \mathbb{Z}_2^{2k}$.

Булевы функции $f, g \in \mathcal{F}_n$ называются *аффинно эквивалентными*, если существует невырожденная двоичная матрица A размера $n \times n$, вектор $b \in \mathbb{Z}_2^n$ и аффинная функция $\ell \in \mathcal{A}_n$, такие, что

$$f(x) = g(xA \oplus b) \oplus \ell(x) \text{ для всех } x \in \mathbb{Z}_2^n.$$

Булева функция называется *квадратичной*, если её степень равна 2. Для квадратичных функций справедлива *теорема Диксона*: любую квадратичную булеву функцию $f \in \mathcal{F}_n$ можно привести преобразованием вида $f(xA)$, где A — невырожденная двоичная матрица размера $n \times n$, к виду

$$x_1 x_2 \oplus x_3 x_4 \oplus \ldots \oplus x_{2t-1} x_{2t} \oplus \ell(x), \text{ где } \ell \in \mathcal{A}_n \text{ и } 1 \leqslant t \leqslant n/2.$$

Таким образом, любая квадратичная булева функция из $\mathcal{F}_n$ аффинно эквивалентна функции $g_t(x_1, \ldots, x_n) = x_1 x_2 \oplus x_3 x_4 \oplus \ldots \oplus x_{2t-1} x_{2t}$ для некоторого t, $1 \leqslant t \leqslant n/2$.

Определение 1. Булева функция $f \in \mathcal{F}_n$ *аффинна на подпространстве* L, если $f|_L = \ell_{a,c}|_L$, где $a \in \mathbb{Z}_2^n, c \in \mathbb{Z}_2$. Далее будем обозначать это как $f|_L(x) = \langle a, x \rangle \oplus c$.

В случае если $f|_L = c$, $c \in \mathbb{Z}_2$, будем говорить, что f *постоянна* на L.

Через Ind_D, $D \subseteq \mathbb{Z}_2^n$, обозначим булеву функцию от n переменных, принимающую значение 1 на всех элементах множества D (и только на них). Для бент-функции $f \in \mathfrak{B}_{2k}$ справедлива следующая конструкция. Пусть L — подпространство $\mathbb{Z}_2^{2k}$ размерности k и f аффинна на L. Тогда

$$f \oplus Ind_L \tag{3}$$

тоже является бент-функцией. Данная конструкция предложена К. Карле в работе [8].

Для $f, g \in \mathfrak{B}_{2k}$, $f \neq g$, справедливо $\operatorname{dist}(f, g) \geqslant 2^k$. В работе [3] доказан критерий расположения двух бент-функций на расстоянии 2^k.

Утверждение 1 [3]. Пусть $f \in \mathfrak{B}_{2k}$. Тогда все бент-функции на расстоянии 2^k от f имеют вид $f \oplus Ind_L$, где L — подпространство размерности k и f аффинна на L.

Более подробную информацию о бент-функциях можно найти в [9, 10].

2. Аффинность булевых функций на подпространстве

Рассмотрим существующие понятия, связанные с аффинностью булевой функции на подпространстве.

Гранью $\mathbb{Z}_2^n$ называется множество вида $\Gamma^{b_1,\ldots,b_k}_{i_1,\ldots,i_k} = \{x \in \mathbb{Z}_2^n : x_{i_1} = b_1, \ldots, x_{i_k} = b_k\}$, где $1 \leqslant i_1 < i_2 < \ldots < i_k \leqslant n$; $b_1, \ldots, b_k \in \mathbb{Z}_2$. Отметим, что грань является подпространством $\mathbb{Z}_2^n$.

Определение 2. Функция $f \in \mathcal{F}_n$ называется *k-аффинной*, если она аффинна на грани размерности $n - k$.

Уровнем аффинности f называется минимальное возможное k, такое, что f является k-аффинной. Эти определения ввели О. А. Логачёв, А. А. Сальников и В. В. Ященко в работе [11]. Аффинные функции обладают нулевым уровнем аффинности (и только они). Уровень аффинности не может превышать $n - 1$. В [12] доказано, что уровнем аффинности $n - 1$ обладают исключительно квадратичные функции, АНФ которых содержит все мономы степени 2. М. Л. Буряков в [13] доказал, что задача нахождения уровня аффиности булевой функции $f \in \mathcal{F}_n$, число мономов в АНФ которой не превосходит cn, где c — некоторая константа, является NP-трудной.

Обобщённым уровнем аффинности f называется минимальное возможное k, такое, что f аффинна на подпространстве размерности $n - k$. О. А. Логачёв в работе [14] доказал, что для почти всех булевых функций от n переменных обобщённый уровень аффинности лежит в интервале $[n - \log_2 n, n - \log_2 n + 1]$.

Определение 3. Функция $f \in \mathcal{F}_n$ называется *k-нормальной* (*k-слабо нормальной*), если она постоянна (аффинна) на некотором подпространстве размерности k.

Определение 4. Функция $f \in \mathcal{F}_n$ называется *нормальной* (*слабо нормальной*), если она $\lceil n/2 \rceil$-нормальна ($\lceil n/2 \rceil$-слабо нормальна).

Через $\lceil a \rceil$ обозначена целая часть сверху числа $a \in \mathbb{R}$.

Понятие нормальности предложено Х. Доббертином в работе [15], а затем обобщено П. Шарпин в [16]. Х. Доббертин ввёл его для функций от чётного числа переменных. Данное определение тесно связано с классом бент-функций. На тот момент вопрос о существовании бент-функций, не являющихся нормальными, оставался открытым. А. Канто, М. Даум, Х. Доббертин и Г. Леандр в [17] нашли примеры бент-функций от 10 переменных, которые не являются нормальными, и бент-функций от 14 переменных, которые не являются слабо нормальными. Авторы предложили также конструкцию, позволяющую по произвольной не нормальной (не слабо нормальной) бент-

функции от $2k$ переменных построить не нормальную (не слабо нормальную) бент-функцию от $2k+2$ переменных.

Определение 5. Булева функция $f \in \mathcal{F}_n$ задана в виде *линейного разветвления*, если существуют $k \in \mathbb{N}$, $1 \leqslant k \leqslant n$, функции $\Phi : \mathbb{Z}_2^{n-k} \to \mathbb{Z}_2^k$ и $\varphi \in \mathcal{F}_{n-k}$, такие, что

$$f(x, y) = \langle x, \Phi(y) \rangle \oplus \varphi(y)$$

для всех $x \in \mathbb{Z}_2^k$, $y \in \mathbb{Z}_2^{n-k}$.

Подробную информацию об этом представлении можно найти в [9]; см. также работу В. В. Ященко [18] о характеризации бент-функций в виде линейного разветвления.

3. Полностью аффинно расщепляемые булевы функции

Определение 6. Функция $f \in \mathcal{F}_n$ является *аффинно расщепляемой* по подпространству L, если функция f аффинна на каждом сдвиге L.

Определение 7. Функция $f \in \mathcal{F}_n$ называется *полностью аффинно расщепляемой* порядка k, $2 \leqslant k \leqslant n$, если она аффинна на некотором подпространстве $\mathbb{Z}_2^n$ размерности k и аффинно расщепляема по всем подпространствам размерности k, на которых она аффинна.

Порядки $k = 0$ и 1 рассматривать не имеет смысла, поскольку тогда бы все булевы функции удовлетворяли определению.

Тривиально доказывается следующее утверждение.

Утверждение 2. Пусть $f, g \in \mathcal{F}_n$ — аффинно эквивалентные булевы функции. Тогда f является полностью аффинно расщепляемой порядка k тогда и только тогда, когда g является полностью аффинно расщепляемой порядка k.

Все аффинные и квадратичные булевы функции обладают следующим свойством.

Утверждение 3. Пусть $f \in \mathcal{F}_n$ — аффинная или квадратичная. Тогда если f аффинна на подпространстве $L \subseteq \mathbb{Z}_2^n$, то f аффинна на каждом сдвиге L.

Доказательство. Пусть $a \in \mathbb{Z}_2^n$. Функция f аффинна на $a \oplus L$ тогда и только тогда, когда $f(x \oplus a)$ аффинна на L. Отметим, что $f(x \oplus a) = f(x) \oplus D_a f(x)$, при этом из условия утверждения следует, что $\deg D_a f \leqslant 1$. Следовательно, f аффинна на L тогда и только тогда, когда f аффинна на $a \oplus L$. ■

Докажем вспомогательные леммы об аффинности функции на подпространстве.

Лемма 1. Пусть $f \in \mathcal{F}_n$ аффинна на подпространстве $L \subseteq \mathbb{Z}_2^n$ ненулевой размерности. Тогда для некоторого подпространства $U \subset L$ и $a \in L$, таких, что $L = U \cup (a \oplus U)$, функция f постоянна и на U, и на $a \oplus U$.

Доказательство. Без ограничения общности можно считать, что L — линейное подпространство $\mathbb{Z}_2^n$. Тогда для любого $w \in \mathbb{Z}_2^n$ решением системы уравнений $\langle w, x \rangle = 0$, $x \in L$, является либо всё множество L, либо его подпространство размерности $\dim L - 1$. Лемма доказана. ■

Лемма 2. Пусть $f \in \mathcal{F}_n$, L — подпространство $\mathbb{Z}_2^n$ и f постоянна на L. Тогда f аффинна на подпространстве $L \cup (a \oplus L)$, $a \in \mathbb{Z}_2^n$, тогда и только тогда, когда f постоянна на $a \oplus L$.

Доказательство. Без ограничения общности можно считать, что L — линейное подпространство $\mathbb{Z}_2^n$.

Необходимость. Если f постоянна на $L \cup (a \oplus L)$, то утверждение очевидно. Пусть $f|_{L \cup (a \oplus L)}(x) = \langle w, x \rangle \oplus c$, $w \in \mathbb{Z}_2^n$, $c \in \mathbb{Z}_2$. Тогда $f|_{a \oplus L}(x) = \langle w, x \rangle \oplus c = f|_L(a \oplus x) \oplus \langle w, a \rangle$.

Достаточность. Пусть $f|_L = c_1$ и $f|_{a\oplus L} = c_2$, $c_1, c_2 \in \mathbb{Z}_2$. Если $c_1 = c_2$, то утверждение очевидно. Пусть $c_1 \neq c_2$, т. е. $c_2 = c_1 \oplus 1$. Рассмотрим $L^\perp$. Для некоторого $w \in L^\perp$ верно, что $\langle w, a\rangle = 1$, поскольку если $\langle w, a\rangle = 0$ для всех $w \in L^\perp$, то $a \in L^{\perp\perp} = L$, но $a \notin L$. Следовательно, $\langle w, x\rangle|_L = 0$ и $\langle w, x\rangle|_{a\oplus L} = 1$, отсюда $f|_{L\cup(a\oplus L)}(x) = \langle w, x\rangle \oplus c_1$. ■

Утверждение 4. Если булева функция является полностью аффинно расщепляемой порядка k, то она также полностью аффинно расщепляема порядка t для всех $2 \leqslant t \leqslant k$.

Для доказательства утверждения 4 достаточно воспользоваться следующей леммой.

Лемма 3. Пусть $f \in \mathcal{F}_n$ является полностью аффинно расщепляемой порядка k. Тогда если f аффинна на некотором линейном подпространстве U размерности $t < k$, то существует линейное подпространство L размерности k, такое, что $U \subseteq L$ и f аффинна на L.

Доказательство. Воспользуемся индукцией по размерности U. База индукции $\dim U = 0$ очевидно следует из условия леммы.

Предположим, что для всех линейных подпространств размерности t, $t \leqslant k-1$, утверждение леммы верно. Докажем, что оно верно и для U размерности $t+1$.

Представим U как $U' \cup (a \oplus U')$, где U' — подпространство U размерности t, $a \in U$. Тогда по предположению индукции существует L размерности k, $U' \subseteq L$ и f аффинна на L. Без ограничения общности можно считать, что $f|_L = 0$, поскольку прибавление аффинной функции не влияет на наличие или отсутствие аффинности. Тогда по лемме 2 верно, что $f|_{a\oplus U'} = c$, где $c \in \mathbb{Z}_2$. Поскольку по условию леммы f аффинна на $a \oplus L$, то по лемме 1 существует подпространство $a \oplus T$ размерности $k-1$, такое, что $a \oplus U' \subseteq a \oplus T \subset a \oplus L$ и $f|_{a\oplus T} = c$. А так как $f|_T = 0$, то по лемме 2 функция f аффинна на линейном подпространстве $T \cup (a \oplus T)$ размерности k, которое содержит U. ■

Далее докажем, что полностью аффинно расщепляемыми порядка 2 могут быть только аффинные и квадратичные булевы функции.

Лемма 4. Пусть $f \in \mathcal{F}_n$, $n > 2$, и $L = \{a, b, c, d\}$ — подпространство $\mathbb{Z}_2^n$ размерности 2. Тогда f аффинна на L тогда и только тогда, когда $f(a) \oplus f(b) \oplus f(c) \oplus f(d) = 0$.

Доказательство леммы очевидно.

Лемма 5. Пусть $f \in \mathcal{F}_n$, $n > 2$. Тогда существует подпространство размерности 2, на котором f аффинна.

Доказательство. Докажем, что f аффинна на некотором подпространстве размерности 2 при $n = 3$. Из этого будет следовать справедливость леммы, поскольку любая булева функция от большего числа переменных имеет подфункцию от трёх переменных.

В алгебраической нормальной форме f могут присутствовать четыре монома степеней 2 и 3: $x_1x_2x_3$, x_1x_2, x_1x_3 и x_2x_3. Рассмотрим два случая.

С л у ч а й 1. Моном $x_1x_2x_3$ не присутствует. Имеем два подслучая.

1) Не все мономы степени 2 присутствуют в АНФ. Тогда, очевидно, у присутствующих мономов есть общая переменная x_i, $1 \leqslant i \leqslant 3$. Следовательно, f_i^0 — аффинная.
2) Мономы x_1x_2, x_1x_3 и x_2x_3 присутствуют в АНФ. Заметим, что $x_1x_2 \oplus x_1x_3 \oplus \oplus x_2x_3 = x_1(x_2 \oplus x_3) \oplus x_2x_3$, поэтому f аффинна на подпространстве $D = \{(x_1, x_2, x_3) : x_2 \oplus x_3 = 1, x_1, x_2, x_3 \in \mathbb{Z}_2\}$ размерности 2.

С л у ч а й 2. Моном $x_1x_2x_3$ присутствует. Также имеем два подслучая.

1) В АНФ нет мономов степени 2. Тогда, очевидно, f_1^0 — аффинная.
2) В АНФ есть моном степени 2; без ограничения общности положим, что там присутствует x_1x_2. Тогда f_3^1 аффинна, поскольку у неё $x_1x_2x_3$ и x_1x_2 сократятся, а мономы x_1x_3 и x_2x_3 содержат x_3.

Лемма доказана. ■

Лемма 5 следует также из того, что уровнем аффинности $n-1$ обладают только квадратичные функции, АНФ которых содержит все мономы степени 2 (М. Л. Буряков, О. А. Логачёв, [12]).

Лемма 6. Пусть $f \in \mathcal{F}_n$ является полностью аффинно расщепляемой порядка 2. Тогда f либо аффинная, либо квадратичная.

Доказательство. Воспользуемся индукцией по числу переменных. Очевидно, что любая булева функция от двух и меньше переменных является либо аффинной, либо квадратичной. Предположим, что если $g \in \mathcal{F}_k$, $k < n$, является полностью аффинно расщепляемой порядка 2, то $\deg g \leqslant 2$. Докажем, что $\deg f \leqslant 2$.

Рассмотрим линейное подпространство

$$L = \{(\mathbf{0}, 0, 0), (\mathbf{0}, 0, 1), (\mathbf{0}, 1, 0), (\mathbf{0}, 1, 1)\} \subseteq \mathbb{Z}_2^n.$$

Тогда все сдвиги L можно представить следующим образом:

$$\{(\mathbf{x}, 0, 0), (\mathbf{x}, 0, 1), (\mathbf{x}, 1, 0), (\mathbf{x}, 1, 1)\},\ \mathbf{x} \in \mathbb{Z}_2^{n-2}.$$

Поскольку f является полностью аффинно расщепляемой порядка 2, то она либо аффинна на всех сдвигах L, либо не аффинна ни на одном из сдвигов. Поэтому по лемме 4 для некоторой константы $c \in \mathbb{Z}_2$ верно

$$\forall \mathbf{x} \in \mathbb{Z}_2^{n-2}\ (f(\mathbf{x}, 0, 0) \oplus f(\mathbf{x}, 0, 1) \oplus f(\mathbf{x}, 1, 0) \oplus f(\mathbf{x}, 1, 1) = c).$$

Разложим f по последним двум переменным:

$$\begin{gathered} f(\mathbf{x}, y, z) = (y \oplus 1)(z \oplus 1) f(\mathbf{x}, 0, 0) \oplus (y \oplus 1) z f(\mathbf{x}, 0, 1) \oplus y(z \oplus 1) f(\mathbf{x}, 1, 0) \oplus yz f(\mathbf{x}, 1, 1) = \\ = (f(\mathbf{x}, 0, 0) \oplus f(\mathbf{x}, 0, 1) \oplus f(\mathbf{x}, 1, 0) \oplus f(\mathbf{x}, 1, 1)) yz \oplus \\ \oplus (f(\mathbf{x}, 0, 0) \oplus f(\mathbf{x}, 1, 0)) y \oplus (f(\mathbf{x}, 0, 0) \oplus f(\mathbf{x}, 0, 1)) z \oplus f(\mathbf{x}, 0, 0). \end{gathered}$$

Пусть $f'(\mathbf{x}, y) = f(\mathbf{x}, y, 0)$ и $f''(\mathbf{x}, y) = f(\mathbf{x}, 0, y)$, т. е. это подфункции f, и $\alpha = (\mathbf{0}, 1) \in \in \mathbb{Z}_2^{n-1}$. Тогда

$$f(\mathbf{x}, y, z) = c \cdot yz \oplus y D_\alpha f'(x) \oplus z D_\alpha f''(x) \oplus f(\mathbf{x}, 0, 0). \tag{4}$$

Пусть h — любая из функций f', f'' или $f(\mathbf{x}, 0, 0)$. Если h от трёх и более переменных, то по лемме 5 она аффинна на некотором подпространстве размерности 2, при этом h — подфункция f, следовательно, она, как и f, является полностью аффинно расщепляемой порядка 2. Таким образом, по предположению индукции $\deg h \leqslant 2$.

Отсюда $\deg f(\mathbf{x}, 0, 0) \leqslant 2$, а $\deg D_\alpha f', \deg D_\alpha f'' \leqslant 1$. Исходя из равенства (4), получаем, что $\deg f \leqslant 2$. ■

Лемма 7. Бент-функция $f \in \mathfrak{B}_{2k}$ не может быть аффинна на подпространстве размерности больше k.

Доказательство. Пусть $f|_L(x) = \langle w, x\rangle \oplus c$, L — подпространство размерности $k+1$. Тогда бент-функция $f'(x) = f(x) \oplus \langle w, x\rangle \oplus c$ равна 0 на L. Так как размерность L больше k, существуют два различных подпространства U и $a \oplus U$, содержащиеся в L. Тогда $g = f' \oplus Ind_U \oplus Ind_{a\oplus U}$ тоже является бент-функцией по конструкции (3), при этом $\mathrm{wt}(g) = \mathrm{wt}(f') + 2^{k+1}$. Приходим к противоречию, поскольку вес бент-функции равен $2^{2k-1} \pm 2^{k-1}$. ■

Данную лемму также можно найти в [8].

Теорема 1. Пусть $f \in \mathcal{F}_n$. Справедливы следующие утверждения.

(i) Функция f является полностью аффинно расщепляемой порядка k, $2 \leqslant k \leqslant \lceil n/2 \rceil$, тогда и только тогда, когда f либо аффинная, либо квадратичная.

(ii) Функция f является полностью аффинно расщепляемой порядка k, $\lceil n/2 \rceil \leqslant k < n$, и не является полностью аффинно расщепляемой порядка $k+1$ тогда и только тогда, когда f аффинно эквивалентна функции

$$g_{n-k}(x_1, \ldots, x_n) = x_1x_2 \oplus x_3x_4 \oplus \ldots \oplus x_{2n-2k-1}x_{2n-2k}.$$

Доказательство. Заметим, что если f является полностью аффинно расщепляемой порядка k, то она либо аффинная, либо квадратичная: это следует из утверждения 4 и леммы 6.

Так как для аффинных и квадратичных булевых функций имеет место утверждение 3, для доказательства полной аффинной расщепляемости функции достаточно доказать существование подпространства соответствующей размерности, на котором функция аффинна.

Если f является аффинной, доказательство теоремы тривиально.

По теореме Диксона любая квадратичная функция аффинно эквивалентна функции $g_t(x_1, \ldots, x_n) = x_1x_2 \oplus x_3x_4 \oplus \ldots \oplus x_{2t-1}x_{2t}$ для некоторого t, $1 \leqslant t \leqslant n/2$. Таким образом, g_t аффинна на грани $x_2 = x_4 = \ldots = x_{2t} = 0$ размерности $n-t$, т. е. пункт (i) доказан. Для доказательства пункта (ii) достаточно воспользоваться тем, что функция $h(x_1, \ldots, x_{2n-2k}) = x_1x_2 \oplus x_3x_4 \oplus \ldots \oplus x_{2n-2k-1}x_{2n-2k}$ от $2n-2k$ переменных является бент-функцией и по лемме 7 не может быть аффинна на подпространстве размерности большей, чем $n-k$: тогда функция g не может быть аффинна на подпространстве размерности большей, чем $n-k+(n-(2n-2k)) = k$. ■

Таким образом, среди бент-функций полностью аффинно расщепляемыми являются только квадратичные бент-функции.

Отметим, что в работе [7] рассматривался частный случай полной аффинной расщепляемости. В ней доказано, что булева функция от n переменных является полностью аффинно расщепляемой порядка $\lceil n/2 \rceil$ тогда и только тогда, когда она либо аффинная, либо квадратичная.

4. Верхняя оценка числа бент-функций на расстоянии 2^k от произвольной бент-функции из $\mathfrak{B}_{2k}$

Докажем точную верхнюю оценку числа бент-функций на расстоянии 2^k от произвольной бент-функции $f \in \mathfrak{B}_{2k}$. Напомним, что число бент-функций на расстоянии 2^k от f равно числу подпространств $\mathbb{Z}_2^{2k}$ размерности k, на которых f аффинна (утверждение 1).

Поскольку любое подпространство размерности k, $k > 0$, можно представить как $L \cup (a \oplus L)$, где L — подпространство $\mathbb{Z}_2^n$ размерности $k-1$, следующее утверждение

даёт условие, при котором можно увеличить на 1 размерность подпространства, на котором булева функция аффинна.

Утверждение 5. Пусть $f \in \mathcal{F}_n$, L — подпространство $\mathbb{Z}_2^n$ и $f|_L(x) = \langle w, x\rangle \oplus c$ для некоторых $w \in \mathbb{Z}_2^n$ и $c \in \mathbb{Z}_2$. Тогда f аффинна на подпространстве $L \cup (a \oplus L)$, $a \in \mathbb{Z}_2^n$, тогда и только тогда, когда $f|_{a\oplus L}(x) = \langle w, x\rangle \oplus c'$ для некоторого $c' \in \mathbb{Z}_2$.

Доказательство. Рассмотрим функцию $f'(x) = f(x) \oplus \langle w, x\rangle \oplus c$. Очевидно, что $f'|_L = 0$. Следовательно, по лемме 2 функция f' аффинна на $L \cup (a \oplus L)$ тогда и только тогда, когда $f'|_{a\oplus L} = c'$ для некоторого $c' \in \mathbb{Z}_2$. ■

Далее оценим число способов, которыми можно, используя утверждение 5, увеличить на 1 размерность подпространства, на котором бент-функция аффинна. Для этого потребуется следующее понятие. Пусть $f \in \mathcal{F}_n$, $S \subseteq \mathbb{Z}_2^n$. *Неполным преобразованием Уолша* функции $f|_S$ называется отображение

$$W_{f_S}(y) = \sum_{x\in S} (-1)^{f(x)\oplus\langle y,x\rangle},\ y \in \mathbb{Z}_2^n.$$

Приведём аналог равенства Парсеваля для неполного преобразования Уолша:

$$\sum_{y\in\mathbb{Z}_2^n} W_{f_S}^2(y) = \sum_{y\in\mathbb{Z}_2^n}\sum_{u\in S}\sum_{v\in S} (-1)^{f(u)\oplus f(v)\oplus\langle u\oplus v,y\rangle} =$$
$$= \sum_{u\in S}\sum_{v\in S}(-1)^{f(u)\oplus f(v)} \sum_{y\in\mathbb{Z}_2^n}(-1)^{\langle u\oplus v,y\rangle} = \sum_{u\in S}(-1)^{f(u)\oplus f(u)}2^n = 2^n|S|.$$

Более подробную информацию о неполном преобразовании Уолша можно найти в монографии О. А. Логачёва, А. А. Сальникова, С. В. Смышляева, В. В. Ященко [9].

Лемма 8. Пусть f — бент-функция от $2k$ переменных, L — линейное подпространство $\mathbb{Z}_2^{2k}$ размерности t, $t \leqslant k$ и $a_1 \oplus L, \ldots, a_n \oplus L$ — различные сдвиги L. Пусть для некоторого $w \in \mathbb{Z}_2^{2k}$ верно, что

$$f|_{a_i\oplus L}(x) = \langle w, x\rangle \oplus c_i,\ c_i \in \mathbb{Z}_2 \ \text{ для всех } \ i = 1, \ldots, n.$$

Тогда $n \leqslant 2^{2k-2t}$. При этом в случае $n = 2^{2k-2t}$ функция $f(x) \oplus \langle w, x\rangle$ уравновешена на каждом $a \oplus L$, где $a \notin (a_1 \oplus L) \cup \ldots \cup (a_n \oplus L)$.

Доказательство. Известно, что для произвольных бент-функции f, линейного подпространства L и $a, w \in \mathbb{Z}_2^{2k}$ справедлива формула (см. (2) при $b = w$)

$$\sum_{x\in a\oplus L}(-1)^{f(x)\oplus\langle w,x\rangle} = 2^{\dim L-k}(-1)^{\langle a,w\rangle}\sum_{y\in w\oplus L^\perp}(-1)^{\tilde{f}(y)\oplus\langle a,y\rangle}. \tag{5}$$

Пусть $S = w \oplus L^\perp$. Рассмотрим неполное преобразование Уолша функции $\tilde{f}|_S$: $W_{\tilde{f}_S}(u) = \sum\limits_{y\in S}(-1)^{\tilde{f}(y)\oplus\langle u,y\rangle}$, $u \in \mathbb{Z}_2^{2k}$. Тогда, согласно равенству (5),

$$W_{\tilde{f}_S}(u) = 2^{k-t}(-1)^{\langle u,w\rangle}\sum_{x\in u\oplus L}(-1)^{f(x)\oplus\langle w,x\rangle}. \tag{6}$$

Пусть $V = (a_1 \oplus L) \cup \ldots \cup (a_n \oplus L)$. Из равенства (6) и условия леммы следует, что для всех $u \in V$ справедливо $|W_{\tilde{f}_S}(u)| = 2^{k-t}2^t = 2^k$. Так как для частичного преобразования Уолша функции $\tilde{f}|_S$ справедлив аналог равенства Парсеваля, а $|S| = 2^{2k-t}$ и $|V| = n2^t$, то

$$\sum_{u\in\mathbb{Z}_2^{2k}} W_{\tilde{f}_S}^2(u) = \sum_{u\in V} W_{\tilde{f}_S}^2(u) + \sum_{u\notin V} W_{\tilde{f}_S}^2(u) = n2^t2^{2k} + \sum_{u\notin V} W_{\tilde{f}_S}^2(u) = 2^{2k}2^{2k-t}.$$

Следовательно, $n \leqslant 2^{2k-2t}$. Если же $n = 2^{2k-2t}$, то $W_{\tilde{f}_S}(u) = 0$ при $u \notin V$. Отсюда по равенству (6) получаем, что $\sum\limits_{x \in u \oplus L} (-1)^{f(x) \oplus \langle w, x \rangle} = 0$ для $u \notin V$. ■

Сформулируем случай $n = 2^{2k-2t}$ из предыдущей леммы отдельно.

Утверждение 6. Пусть бент-функция $f \in \mathfrak{B}_{2k}$ постоянна на 2^{2k-2t} различных сдвигах подпространства $L \subseteq \mathbb{Z}_2^{2k}$ размерности t, $1 \leqslant t \leqslant k$. Тогда на всех других сдвигах L бент-функция f является уравновешенной.

Данный случай является обобщением утверждения, доказанного К. Карле.

Утверждение 7 [8]. Пусть бент-функция $f \in \mathfrak{B}_{2k}$ постоянна на некотором подпространстве L размерности k. Тогда f уравновешена на каждом сдвиге L, отличном от самого L.

Таким образом, утверждение 6 эквивалентно утверждению 7 в случае $t = k$. Используя идею утверждения 7, Х. Доббертин в работе [15] предложил конструкцию, порождающую нормальные бент-функции.

Докажем, что аффинное подпространство, на котором аффинна полностью аффинно расщепляемая бент-функция, можно «достроить» максимальным для бент-функции числом способов.

Лемма 9. Пусть $f \in \mathfrak{B}_{2k}$ и для некоторого линейного подпространства $L \subseteq \mathbb{Z}_2^{2k}$ размерности t, $t \leqslant k$, бент-функция f аффинна на каждом сдвиге L. Тогда $f(x) \oplus \langle w, x \rangle$ является константой ровно на 2^{2k-2t} различных сдвигах L для любого $w \in \mathbb{Z}_2^{2k}$.

Доказательство. Обозначим через S_w множество сдвигов L, на которых $f(x) \oplus \oplus \langle w, x \rangle$ является константой. Заметим, что если $f|_{a \oplus L}(x) = \langle w, x \rangle \oplus c$, то для любого $w' \in w \oplus L^{\perp}$ верно, что $f|_L(x) = \langle w', x \rangle \oplus \langle w \oplus w', a \rangle \oplus c$. Таким образом, $S_w = S_{w \oplus u}$ для $u \in L^{\perp}$. Поскольку f аффинна на каждом сдвиге L, а число различных сдвигов равно 2^{2k-t}, то должно быть справедливо

$$\frac{1}{2^{2k-t}} \sum_{w \in \mathbb{Z}_2^{2k}} |S_w| \geqslant 2^{2k-t},$$

при этом по лемме 8 $|S_w| \leqslant 2^{2k-2t}$. Следовательно, неравенство справедливо, только если $|S_w| = 2^{2k-2t}$ для всех $w \in \mathbb{Z}_2^{2k}$. ■

Докажем основную теорему.

Теорема 2. Пусть f — бент-функция от $2k$ переменных. Тогда число бент-функций на расстоянии 2^k от f не превосходит $2^k(2^1 + 1) \cdot \ldots \cdot (2^k + 1)$. При этом данная оценка достигается, только если f — квадратичная.

Доказательство. Обозначим через h произвольную квадратичную бент-функцию от $2k$ переменных. Определим следующее множество:

$$D^t(f) = \{a \oplus L : L \text{ — линейное подпространство } \mathbb{Z}_2^{2k} \text{ размерности } t, \\ a \in \mathbb{Z}_2^{2k} \text{ и } f \text{ аффинна на } a \oplus L\},\ 0 \leqslant t \leqslant k.$$

По утверждению 1 число бент-функций на расстоянии 2^k от f равно $|D^k(f)|$. Докажем, что $|D^k(f)| \leqslant |D^k(h)|$.

Воспользуемся индукцией по t, $0 \leqslant t \leqslant k$, и покажем, что $|D^t(f)| \leqslant |D^t(h)|$.

База индукции $t = 0$: очевидно, что $|D^0(f)| = |D^0(h)| = 2^{2k}$.

Пусть для $t < k$ верно, что $|D^t(f)| \leqslant |D^t(h)|$. Докажем, что $|D^{t+1}(f)| \leqslant |D^{t+1}(h)|$. Пусть $N_f(L) = \{U \in D^{t+1}(f) : L \subset U\}$, где $L \in D^t(f)$. Отметим, что любое $U \in N_f(L)$ имеет вид $U = L \cup (a \oplus L)$ для некоторого $a \in \mathbb{Z}_2^{2k}$. Тогда

$$|D^{t+1}(f)| = \frac{1}{2(2^{t+1}-1)} \sum_{L \in D^t(f)} |N_f(L)|,$$

поскольку в подпространстве U содержится ровно $2(2^{t+1}-1)$ различных подпространств размерности t. По утверждению 5 и леммам 8 и 9 для любых $L \in D^t(f)$ и $L' \in D^t(h)$ справделиво $|N_f(L)| \leqslant |N_h(L')| = 2^{2k-2t} - 1$. Отсюда $|D^{t+1}(f)| \leqslant |D^{t+1}(h)|$.

Таким образом, $|D^k(f)| \leqslant |D^k(h)|$. Поскольку $|N_h(L')| = 2^{2k-2\dim L'} - 1$, то

$$|D^k(h)| = 2^{2k} \prod_{t=0}^{k-1} \frac{2^{2k-2t}-1}{2(2^{t+1}-1)} = 2^k \prod_{t=1}^{k} \frac{2^{2t}-1}{2^t-1} = 2^k(2^1+1)\cdot\ldots\cdot(2^k+1).$$

Отметим, что значение $|D^k(h)|$ было подсчитано ранее в работе [4].

Докажем, что оценка достигается только на квадратичных бент-функциях. Пусть f не является квадратичной (из этого автоматически следует, что $k > 2$). Тогда по теореме 1 она не является полностью аффинно расщепляемой порядка k, т. е. f аффинна на подпространстве L размерности k и не аффинна на некотором его сдвиге (если f не аффинна ни на одном подпространстве размерности k, то $|D^k(f)| = 0$).

Без ограничения общности можем полагать, что L — линейное подпространство и $f|_L = 0$ (этого можно добиться за счёт преобразований вида $f(x \oplus a) \oplus \langle w, x\rangle \oplus c$). Из утверждения 6 следует, что на всех сдвигах L, отличных от L, функция f уравновешена.

Пусть L' — линейное подпространство L размерности $k-1$. Очевидно, что $f|_{L'} = 0$. Пусть $N_f(L') > 1$, т. е. функция f аффинна на $L' \cup (a \oplus L')$ для некоторого $a \notin L$. Тогда из леммы 2 следует, что $f|_{a \oplus L'} = c$ для некоторого $c \in \mathbb{Z}_2$. Но в силу уравновешенности f на $a \oplus L$ получаем, что $f|_{(a\oplus L)\setminus(a\oplus L')} = c \oplus 1$, и по лемме 2 функция f аффинна на $a \oplus L$.

Заметим, что если L' и L'' — различные линейные подпространства L размерности $k-1$, то f не может быть аффинна одновременно на $L' \cup (a \oplus L')$ и на $L'' \cup (a \oplus L'')$ в силу уравновешенности f на $a \oplus L$. Число различных L' равно $2^k - 1$. Число различных сдвигов L, не равных L, тоже равно $2^k - 1$. Поэтому если $N_f(L') > 1$ для всех L', то f аффинна на всех сдвигах L. Следовательно, $N_f(L') = 1$ для какого-то L', в то время как $N_h(U) = 3$ для любого $U \in D^{k-1}(h)$. ■

Заключение

Рассмотрим тривиальную верхнюю оценку числа бент-функций на расстоянии 2^k от произвольной бент-функции из $\mathfrak{B}_{2k}$.

Утверждение 8. Пусть $f \in \mathfrak{B}_{2k}$. Тогда число бент-функций на расстоянии 2^k от f не больше чем

$$2^k \frac{(2^{2k}-1)\cdot\ldots\cdot(2^{k+1}-1)}{(2^k-1)\cdot\ldots\cdot(2^1-1)}.$$

Это число аффинных подпространств $\mathbb{Z}_2^{2k}$ размерности k. Его можно оценить как

$$2^{k^2+k} < 2^k \frac{(2^{2k}-1)\cdot\ldots\cdot(2^{k+1}-1)}{(2^k-1)\cdot\ldots\cdot(2^1-1)} < 2^{k^2+2k}.$$

Таким образом, доказанная верхняя оценка близка к квадратному корню из тривиальной оценки.

ЛИТЕРАТУРА

1. *Rothaus O.* On bent functions // J. Combin. Theory. Ser. A. 1976. V. 20. No. 3. P. 300–305.
2. *Токарева Н. Н.* Бент-функции: результаты и приложения. Обзор работ // Прикладная дискретная математика. 2009. № 1. С. 15–37.
3. *Коломеец Н. А., Павлов А. В.* Свойство бент-функций, находящихся на минимальном расстоянии друг от друга // Прикладная дискретная математика. 2009. № 4. С. 5–20.
4. *Коломеец Н. А.* Перечисление бент-функций на минимальном расстоянии от квадратичной бент-функции // Дискретный анализ и исследование операций. 2012. Т. 19. № 1. С. 41–58.
5. *Потапов В. Н.* Спектр мощностей компонент корреляционно-иммунных функций, бент-функций, совершенных раскрасок и кодов // Проблемы передачи информации. 2012. Т. 48. № 1. С. 54–63.
6. *Tokareva N.* On the number of bent functions from iterative constructions: lower bounds and hypothesis // Adv. Math. Commun. 2011. V. 5. No. 4. P. 609–621.
7. *Коломеец Н. А.* Пороговое свойство квадратичных булевых функций // Дискретный анализ и исследование операций. 2014. Т. 21. № 2. С. 52–58.
8. *Carlet C.* Two new classes of bent functions // EUROCRYPT'93. LNCS. 1994. V. 765. P. 77–101.
9. *Логачёв О. А., Сальников А. А., Смышляев С. В., Ященко В. В.* Булевы функции в теории кодирования и криптологии. 2-е изд. М.: МЦНМО, 2012.
10. *Токарева Н. Н.* Нелинейные булевы функции: бент-функции и их обобщения. Saarbrucken: LAP LAMBERT Academic Publishing, 2011.
11. *Логачёв О. А., Сальников А. А., Ященко В. В.* Комбинирующие k-аффинные функции // Труды конф. «Математика и безопасность информационных технологий», Москва, 23–24 октября 2003 г. М.: МЦНМО, 2004. С. 176–178.
12. *Буряков М. Л., Логачёв О. А.* Об уровне аффинности булевых функций // Дискретная математика. 2005. Т. 17. № 4. С. 98–107.
13. *Буряков М. Л. О связи уровня аффинности с криптографическими параметрами булевых функций* // Дискретная математика. 2008. Т. 20. № 2. С. 3–14.
14. *Логачёв О. А.* О значениях уровня аффинности для почти всех булевых функций // Прикладная дискретная математика. 2010. № 3. С. 17–21.
15. *Dobbertin H.* Construction of bent functions and balanced Boolean functions with high nonlinearity // Fast Software Encryption Int. Workshop (Leuven, Belgium, December 14–16, 1994). LNCS. 1994. V. 1008. P. 61–74.
16. *Charpin P.* Normal Boolean functions // J. Complexity. 2004. V. 20. P. 245–265.
17. *Canteaut A., Daum M., Dobbertin H., and Leander G.* Finding nonnormal bent functions // Discrete Appl. Math. 2006. V. 154. No. 2. P. 202–218.
18. *Ященко В. В.* О критерии распространения для булевых функций и о бент-функциях // Проблемы передачи информации. 1997. Т. 33. № 1. С. 75–86.