

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

DOI 10.17223/20710410/6/1

УДК 519.7

СВОЙСТВА БЕНТ-ФУНКЦИЙ, НАХОДЯЩИХСЯ НА МИНИМАЛЬНОМ РАССТОЯНИИ ДРУГ ОТ ДРУГА¹

Н. А. Коломеец, А. В. Павлов

*Новосибирский государственный университет, г. Новосибирск, Россия***E-mail:** nkolomeec@gmail.com, apavlov.nsk@gmail.com

В работе получено минимальное расстояние Хэмминга в классе бент-функций от n переменных, равное $2^{n/2}$. Доказано, что бент-функции находятся на минимальном расстоянии тогда и только тогда, когда они различаются на линейном многообразии и обе функции на нем аффинны. Описан алгоритм построения всех бент-функций на минимальном расстоянии от заданной бент-функции. Приведены экспериментальные данные для бент-функций от малого числа переменных.

Ключевые слова: бент-функция, CDMA, OFDM.

Введение

Данная работа посвящена исследованию метрических характеристик класса бент-функций. Бент-функции — это булевы функции от четного числа переменных, максимально удаленные от класса аффинных функций. Впервые бент-функции были введены еще в 60-х годах XX века О. Ротхаузом, и до сих пор интерес к ним не ослабевает. Причиной этого служат как многочисленные теоретические и практические приложения, так и множество открытых вопросов, с ними связанных (см. подробнее в [1]).

Задача исследования метрических свойств бент-функций возникает в теории кодирования и находит свое применение в системах коллективного доступа [2], таких, как стандарты CDMA — Code Division Multiple Access (множественный доступ с кодовым разделением каналов) и OFDM — Orthogonal Frequency Division Multiplexing (ортогональное частотное мультиплексирование). Данные стандарты используют бент-функции для построения кодов постоянной амплитуды (constant-amplitude codes), что позволяет предельно снизить коэффициент отношения пиковой и средней мощностей сигнала (PARP — peak-to-average power ratio). Такие коды состоят из векторов значений бент-функций. Таким образом, являются актуальными задачи построения таких кодов с различными кодовыми расстояниями, что непосредственно связано с исследованием метрической структуры класса бент-функций.

Данная работа имеет следующую структуру. В п. 1 показывается, что минимальное расстояние в классе бент-функций равно $2^{n/2}$, и бент-функции, находящиеся на этом расстоянии друг от друга, должны отличаться на линейном многообразии, причем обе функции должны быть на нем аффинны. Заметим, что этим результатам

¹Работа выполнена при финансовой поддержке гранта Президента РФ для молодых российских ученых (грант МК-1250.2009.1) и РФФИ (проект № 08-01-00671).

предшествовали исследования В. В. Яценко [3] и К. Карле [4] построения различных бент-функций по заданной бент-функции. В п. 2 предлагаются простые способы построения бент-функций на минимальном расстоянии от заданной бент-функции. В п. 3 приводятся примеры бент-функций, для которых существуют бент-функции на минимальном расстоянии. В п. 4 используется аффинная классификация бент-функций для исследования существования бент-функций на минимальном расстоянии для бент-функций от малого количества переменных. В п. 5 приводятся алгоритм построения всех бент-функций на минимальном расстоянии от заданной бент-функции, а также экспериментальные данные для бент-функций от малого числа переменных.

Приведем известные определения и факты, имеющие отношения к бент-функциям.

Под расстоянием между булевыми функциями f и g мы подразумеваем расстояние Хэмминга, обозначим его как $\text{dist}(f, g)$. Через E^n будем обозначать n -мерный куб, через $\mathcal{F}_n$ — множество булевых функций от n переменных.

Определение 1. Множество $L \subseteq E^n$ называется *линейным многообразием* в E^n , если $L = x_0 \oplus U$, где x_0 — элемент из E^n , а U — подпространство в E^n .

Определение 2. Преобразование $W_f : E^n \rightarrow \mathbb{C}$ следующего вида называется *преобразованием Уолша — Адамара* функции f :

$$W_f(w) = \sum_{x \in E^n} (-1)^{f(x) \oplus \langle w, x \rangle}.$$

Число $W_f(w)$ называется *коэффициентом Уолша — Адамара* в точке w (или просто коэффициентом Уолша).

Известно, что две различные функции не могут иметь одинаковые коэффициенты Уолша. Также справедливо равенство Парсеваля: пусть $f \in \mathcal{F}_n$. Тогда имеет место следующее равенство:

$$\sum_{w \in E^n} W_f^2(w) = 2^{2n}.$$

Имеет место формула свертки: пусть $f, g \in \mathcal{F}_n$, тогда

$$W_{f \oplus g}(w) = \frac{1}{2^n} \sum_{x \in E^n} W_f(x) W_g(x \oplus w).$$

Определение 3 (альтернативное определение бент-функций). Булева функция f от четного числа переменных называется *бент-функцией*, если все ее коэффициенты Уолша равны $\pm 2^{n/2}$.

Класс бент-функций от n переменных будем обозначать как $\mathfrak{B}_n$, а минимальное расстояние между функциями из него — как $d(\mathfrak{B}_n)$.

Определение 4. Пусть f — бент-функция от n переменных. Определим *дуальную функцию* $\tilde{f}(w)$, исходя из равенства

$$(-1)^{\tilde{f}(w)} \cdot 2^{n/2} = W_f(w).$$

Стоит заметить, что дуальная к бент-функции функция также является бент-функцией.

Так как расстояние Хэмминга берется между бент-функциями, то здесь и далее будем считать, что n (так будет обозначаться количество переменных функции) является четным натуральным числом.

1. Критерий расположения бент-функций на минимальном расстоянии

Получим минимальное расстояние между бент-функциями и описание всех бент-функций на минимальном расстоянии от заданной бент-функции.

Обозначим через $D(f, g)$ множество значений аргументов, на которых функции f и g от n переменных отличаются. Будем говорить, что $D(f, g)$ — это *множество разностей* функций f и g . Заметим, что $|D(f, g)| = \text{dist}(f, g)$. Через $I_D(x)$ мы будем обозначать индикатор множества D , то есть булеву функцию, которая принимает значение 1 на всех элементах из D , и только на них. Через $\text{rank } D$ обозначим размерность линейной оболочки векторов из D .

Определение 5. Булева функция f от n переменных *аффинна на множестве* $D \subseteq E^n$, если для некоторых $w_0 \in E^n$, $c \in E$ и для любого $x \in D$ выполняется тождество $f(x) = \langle w_0, x \rangle \oplus c$.

Для удобства введем следующее обозначение:

$$a_{f,g}(w) = \sum_{x \in D(f,g)} (-1)^{f(x) \oplus \langle w, x \rangle}.$$

Утверждение 1. Для любого $w \in E^n$ справедливо $|a_{f,g}(w)| \leq |D(f, g)|$, причем равенство достигается тогда и только тогда, когда функция $f(x) \oplus \langle w, x \rangle$ является константой на $D(f, g)$.

Утверждение 2. Пусть $f, g \in \mathcal{F}_n$. Тогда для любого w из E^n выполняется

$$W_f(w) - W_g(w) = 2a_{f,g}(w).$$

Доказательство. Запишем коэффициенты Уолша функций f и g следующим образом:

$$\begin{aligned} W_f(w) &= \sum_{x \in D(f,g)} (-1)^{f(x) \oplus \langle w, x \rangle} + \sum_{x \in E^n \setminus D(f,g)} (-1)^{f(x) \oplus \langle w, x \rangle}, \\ W_g(w) &= \sum_{x \in D(f,g)} (-1)^{g(x) \oplus \langle w, x \rangle} + \sum_{x \in E^n \setminus D(f,g)} (-1)^{g(x) \oplus \langle w, x \rangle}. \end{aligned}$$

Отсюда разность этих коэффициентов равна

$$W_f(w) - W_g(w) = \sum_{x \in D(f,g)} (-1)^{f(x) \oplus \langle w, x \rangle} - \sum_{x \in D(f,g)} (-1)^{g(x) \oplus \langle w, x \rangle} = 2a_{f,g}(w). \blacksquare$$

Имеет место следующая нижняя оценка минимального расстояния.

Лемма 1 (о расстоянии). Для всех четных n выполняется неравенство

$$d(\mathfrak{B}_n) \geq 2^{n/2}.$$

Доказательство. Предположим, что существуют различные $f, g \in \mathfrak{B}_n$, такие, что $\text{dist}(f, g) < 2^{n/2}$. Из предыдущего утверждения имеем: $W_f(w) - W_g(w) = 2a_{f,g}(w)$ для любого w из E^n . Так как f и g — бент-функции, то все их коэффициенты Уолша — Адамара по модулю равны $2^{n/2}$, следовательно,

$$a_{f,g}(w) \in \{0, 2^{n/2}, -2^{n/2}\}.$$

По утверждению 1 $|a_{f,g}(w)| \leq |D(f, g)| < 2^{n/2}$ для всех $w \in E^n$. Получается, что $a_{f,g}(w) = 0$, следовательно, $W_f(w) = W_g(w)$ для любого w .

Но коэффициенты Уолша однозначно определяют функцию, поэтому $f = g$. Получаем противоречие с тем, что f и g различны. $\blacksquare$

Следующие леммы потребуются для доказательства основной теоремы, следствием которой будет описание всех бент-функций на минимальном расстоянии от заданной бент-функции.

Лемма 2. Пусть $f, g \in \mathfrak{B}_n$. Тогда $|D(f, g)| = |D(\tilde{f}, \tilde{g})|$.

Доказательство. Воспользуемся формулой свертки:

$$W_{f \oplus g}(w) = \frac{1}{2^n} \sum_{x \in E^n} W_f(x) W_g(x \oplus w),$$

отсюда

$$W_{f \oplus g}(0) = \frac{1}{2^n} \sum_{x \in E^n} W_f(x) W_g(x) = \sum_{x \in E^n} (-1)^{\tilde{f}(x) \oplus \tilde{g}(x)} = W_{\tilde{f} \oplus \tilde{g}}(0).$$

Осталось заметить, что

$$W_{f \oplus g}(0) = 2^n - 2|D(f, g)|,$$

откуда и следует утверждение леммы. ■

Следствие 1. Пусть $f, g \in \mathfrak{B}_n$. Тогда $\text{dist}(f, g) = d$, если и только если существует ровно d векторов $w \in E^n$, таких, что $W_f(w) \neq W_g(w)$.

Лемма 3. Пусть $D \subseteq E^n$, $|D| = 2^k$, $\text{rank } D = k + 1$ и для любых $x, y \in D$ выполняется $x \oplus y \notin D$. Тогда D — линейное многообразие.

Доказательство. Пусть $\langle D \rangle$ — линейная оболочка D , $U = \langle D \rangle \setminus D$, $x_0 \in D$. Покажем, что $U = x_0 \oplus D$. Очевидно включение $x_0 \oplus D \subseteq U$. Также верно

$$|U| = |\langle D \rangle| - |D| = 2^{k+1} - 2^k = 2^k = |D| = |x_0 \oplus D|.$$

Следовательно, $U = x_0 \oplus D$.

Теперь покажем, что U — подпространство E^n . Множество U непусто, следовательно, достаточно показать только его замкнутость относительно $\oplus$.

Пусть $x, y \in U$, тогда $x = x_0 \oplus x', y = x_0 \oplus y', x', y' \in D$. Имеем

$$x \oplus y = (x_0 \oplus x') \oplus (x_0 \oplus y') = x' \oplus y' \in U,$$

так как по условию леммы для любых $x', y' \in D$ справедливо $x' \oplus y' \in U$.

Таким образом, U — подпространство E^n . И следовательно, D — линейное многообразие. ■

Лемма 4. Любая аффинная функция, заданная на линейном многообразии и не являющаяся константой, уравновешена (принимает значения 1 и 0 одинаковое количество раз).

Доказательство. Пусть f — аффинная функция, заданная на линейном многообразии U , и f — не константа. По определению линейного многообразия $U = x_0 \oplus L$ для некоторого подпространства L и вектора x_0 . Рассмотрим функцию $f'(x) = f(x \oplus x_0) \oplus f(x_0)$, определенную на подпространстве L . Очевидно, что f' линейна на L . Также легко понять, что f уравновешена на U тогда и только тогда, когда f' уравновешена на L (сдвиг множества является взаимнооднозначным отображением, а прибавление к функции константы сохраняет свойство уравновешенности), поэтому нам достаточно доказать утверждение леммы для функции f' .

Рассмотрим множества $L_0 = \{x \in L \mid f'(x) = 0\}$ и $L_1 = \{x \in L \mid f'(x) = 1\}$. Покажем, что множества L_0 и L_1 равноможны.

Функция f' — не константа на L , так как f — не константа на U . Поэтому выберем элемент y_0 из L_1 . Тогда для любого $x \in L_0$

$$f'(x \oplus y_0) = f'(x) \oplus f'(y_0) = 0 \oplus 1 = 1.$$

Значит, $y_0 \oplus L_0 \subseteq L_1$. Отсюда $|L_0| \leq |L_1|$ в силу взаимнооднозначности сдвига множества на y_0 . Но для любого $y \in L_1$

$$f'(y \oplus y_0) = f'(y) \oplus f'(y_0) = 1 \oplus 1 = 0.$$

Следовательно, $y_0 \oplus L_1 \subseteq L_0$ и $|L_1| \leq |L_0|$. Таким образом, $|L_0| = |L_1|$. А это и означает уравнищенность функции f' . ■

Следующая теорема дает необходимые и достаточные условия принадлежности функции на расстоянии $2^{n/2}$ от заданной бент-функции к классу бент-функций.

Теорема 1 (критерий расположения бент-функций на минимальном расстоянии). Пусть $f, g \in \mathcal{F}_n$, $f \in \mathfrak{B}_n$, $\text{dist}(f, g) = 2^{n/2}$. Тогда $g \in \mathfrak{B}_n$, если и только если $D(f, g)$ — линейное многообразие и функция f аффинна на $D(f, g)$.

Доказательство. Необходимость. Пусть $f, g \in \mathfrak{B}_n$, $|D(f, g)| = 2^{n/2}$. Покажем, что $D(f, g)$ — линейное многообразие и f аффинна на $D(f, g)$. Введем обозначения для следующих множеств:

$$W_{=0} = \{w \in E^n \mid a_{f,g}(w) = 0\},$$

$$W_{\neq 0} = \{w \in E^n \mid a_{f,g}(w) \neq 0\}.$$

По утверждению 2

$$W_f(w) - W_g(w) = 2a_{f,g}(w).$$

Так как $f, g \in \mathfrak{B}_n$, то $a_{f,g}(w) \in \{0, 2^{n/2}, -2^{n/2}\}$. Согласно следствию 1, $|W_{\neq 0}| = |D(f, g)|$.

По утверждению 1 $|a_{f,g}(w_0)| = |D(f, g)| = 2^{n/2} \iff \forall x \in D(f, g) \ f(x) = \langle w_0, x \rangle \oplus c$ для подходящей константы c . То есть аффинность мы доказали.

Таким образом, все $w \in W_{\neq 0}$ являются решениями одной из следующих систем:

$$\langle b, w \rangle = \langle b, w_0 \rangle, \quad b \in D(f, g),$$

$$\langle b, w \rangle = \langle b, w_0 \rangle \oplus 1, \quad b \in D(f, g).$$

Обозначив $w \oplus w_0$ за x , получаем равносильные системы уравнений:

$$\langle b, x \rangle = 0, \quad b \in D(f, g), \tag{1}$$

$$\langle b, x \rangle = 1, \quad b \in D(f, g). \tag{2}$$

Видно, что решения систем не пересекаются.

Теперь оценим $|W_{\neq 0}|$, исходя из того, что обе системы разрешимы:

$$2^{n/2} = |W_{\neq 0}| \leq 2 \cdot 2^{n - \text{rank } D(f, g)} = 2^{n - \text{rank } D(f, g) + 1}$$

(первая система всегда имеет $2^{n - \text{rank } D(f, g)}$ решений, а вторая либо имеет столько же решений, либо вообще не имеет). Отсюда

$$\text{rank } D(f, g) \leq n/2 + 1.$$

Но, исходя из мощности множества $D(f, g)$, получаем

$$\text{rank } D(f, g) \in \{n/2, n/2 + 1\}.$$

Рассмотрим два случая.

Случай 1: $\text{rank } D(f, g) = n/2$. Очевидно, в этом случае $D(f, g)$ является подпространством.

Случай 2: $\text{rank } D(f, g) = n/2 + 1$. В этом случае обе системы должны иметь решение, поэтому у второй системы должно существовать частное решение, т. е. существует $t_0 \in E^n$, такое, что $\langle t_0, b \rangle = 1$ для всех $b \in D(f, g)$.

Если существуют $x, y \in D(f, g)$, такие, что $x \oplus y \in D(f, g)$, то вторая система будет противоречива. Действительно, с одной стороны,

$$\langle t_0, x \rangle = 1, \langle t_0, y \rangle = 1 \implies \langle t_0, x \oplus y \rangle = 0,$$

с другой стороны, $\langle t_0, x \oplus y \rangle = 1$. Следовательно, выполняется условие леммы 3 для множества $D(f, g)$. Таким образом, $D(f, g)$ — линейное многообразие. Необходимость доказана.

Достаточность. Пусть $D(f, g)$ — линейное многообразие и f аффинна на $D(f, g)$. Для начала покажем, что

$$a_{f,g}(w) \in \{0, 2^{n/2}, -2^{n/2}\}.$$

Так как f аффинна на $D(f, g)$, то функция $h_w(x) = f(x) \oplus \langle w, x \rangle$ будет также аффинной на $D(f, g)$. Если $h_w(x)$ не является константой на $D(f, g)$, то по лемме 4 функция h_w уравновешена на $D(f, g)$. Поэтому

$$a_{f,g}(w) = \sum_{x \in D(f,g)} (-1)^{h_w(x)} = 0.$$

Если же $h_w(x)$ — константа на $D(f, g)$, то $|a_{f,g}(w)| = |D(f, g)| = 2^{n/2}$ по утверждению 1. Следовательно, $a_{f,g}(w) \in \{0, 2^{n/2}, -2^{n/2}\}$.

Осталось доказать, что $g \in \mathfrak{B}_n$. Имеем

$$W_g(w) = W_f(w) - 2a_{f,g}(w).$$

Следовательно,

$$W_g(w) \in \{2^{n/2}, -2^{n/2}, 3 \cdot 2^{n/2}, -3 \cdot 2^{n/2}\}.$$

Отсюда

$$\min_{w \in E^n} |W_g(w)| \geq 2^{n/2},$$

поэтому из равенства Парсеваля следует, что $|W_g(w)| = 2^{n/2}$ для любого w . Получаем, что $g \in \mathfrak{B}_n$. Достаточность доказана. ■

Следствие 2 (минимальное расстояние в классе $\mathfrak{B}_n$). Справедливо $d(\mathfrak{B}_n) = 2^{n/2}$.

Доказательство. Как известно, $f(x) = x_1 x_2 \oplus \dots \oplus x_{n-1} x_n$ является бент-функцией. Пусть

$$D = \{(y_1, 0, \dots, y_{n/2}, 0) \mid y_i \in E\};$$

очевидно, что

$$D \subseteq E^n,$$

$$|D| = 2^{n/2},$$

$$\forall x \in D \quad f(x) = 0.$$

Пусть $g(x) = f(x) \oplus I_D(x)$. Понятно, что $D(f, g) = D$. Тогда по теореме 1 $g \in \mathfrak{B}_n$, т.е. $f, g \in \mathfrak{B}_n$, $\text{dist}(f, g) = 2^{n/2}$. А из леммы 1 мы знаем, что $d(\mathfrak{B}_n) \geq 2^{n/2}$. Следовательно, $d(\mathfrak{B}_n) = 2^{n/2}$. ■

Пусть $L_{\text{all}}(f)$ — всевозможные линейные многообразия размерности $n/2$, на которых f аффинна. Теперь можно более компактно описать бент-функции на минимальном расстоянии от заданной бент-функции.

Следствие 3 (общий вид функций на минимальном расстоянии). Пусть $f \in \mathfrak{B}_n$. Тогда существует $g \in \mathfrak{B}_n$ на минимальном расстоянии от f , если и только если множество $L_{\text{all}}(f)$ непусто, причем $g(x) = f(x) \oplus I_L(x)$, где $L \in L_{\text{all}}(f)$.

Следствие 4. Бент-функция от n переменных не может быть аффинна на линейных многообразиях размерности больше чем $n/2$.

Доказательство. Предположим, что для бент-функции f и линейного многообразия L утверждение неверно. Введем $g(x) = f(x) \oplus I_L(x)$ и $h_w(x) = f(x) \oplus \langle w, x \rangle$. Далее приводим рассуждения, аналогичные доказательству достаточности теоремы 1: так как f аффинна на L , то и h_w аффинна на L . Если размерность $D(f, g)$ больше чем $n/2$, то для всех элементов w , таких, что h_w константа (т.е. $a_{f,g}(w) \neq 0$) $|a_{f,g}(w)| > 2^{n/2}$, а для w , при которых h_w не константа, $a_{f,g}(w) = 0$ в силу уравновешенности функции h_w на L (лемма 4). Тогда из $W_g(w) = W_f(w) - 2a_{f,g}(w)$ следует

$$\min_{w \in E^n} |W_g(w)| \geq 2^{n/2},$$

но у различных функций все коэффициенты Уолша совпадать не могут. Таким образом, существует w_0 , для которого $a_{f,g}(w_0) \neq 0$ и, следовательно, $|W_g(w_0)| > 2^{n/2}$, что противоречит равенству Парсеваля. ■

Следствие 5. Пусть $D(f, g) = x_0 \oplus L$, L — подпространство и $f(x) = \langle w_0, x \rangle \oplus c$ для всех $x \in D(f, g)$ и некоторых w_0 и c . Тогда коэффициенты Уолша функций f и g отличаются только на элементах множества $w_0 \oplus L^\perp$.

Доказательство. В доказательстве необходимости теоремы 1 показано, что $W_{\neq 0} = w_0 \oplus U$, где U — множество решений следующих систем уравнений:

$$\langle b, x \rangle = 0, \quad b \in D(f, g),$$

$$\langle b, x \rangle = 1, \quad b \in D(f, g).$$

Так как $D(f, g)$ — линейное многообразие, то эти системы эквивалентны следующим системам:

$$\begin{cases} \langle b, x_0 \rangle = 0, \\ \langle b, x \rangle = 0, \quad b \in L \end{cases} \quad \text{и} \quad \begin{cases} \langle b, x_0 \rangle = 1, \\ \langle b, x \rangle = 0, \quad b \in L. \end{cases}$$

А эти системы, в свою очередь, эквивалентны одной системе

$$\langle b, x \rangle = 0, \quad b \in L.$$

Следовательно, $U = L^\perp$ и $W_{\neq 0} = w_0 \oplus L^\perp$. ■

Замечание. Результатам, полученным в теореме 1 и следствиях, предшествовали следующие исследования: В.В. Яценко [3] и К. Карле [4] рассматривали задачу построения различных бент-функций по имеющейся бент-функции путем прибавления индикатора линейного многообразия. Как показывает следствие 3, эта задача тесно

связана с задачей построения бент-функций на минимальном расстоянии от заданной бент-функции. В работе В. В. Яценко предлагалось к бент-функции прибавлять индикатор линейного многообразия, на котором она аффинна. К. Карле рассматривал индикаторы линейных многообразий произвольной размерности. В своей работе он предложил необходимые и достаточные условия на бент-функцию, при которых прибавление индикатора линейного многообразия к ней дает в результате бент-функцию.

Таким образом, достаточность в теореме 1 следует из результатов В. В. Яценко и К. Карле.

2. Индикаторы линейных многообразий и координатные подпространства

В связи с полученным описанием бент-функций на минимальном расстоянии от заданной бент-функции интересно рассмотреть, что из себя представляют индикаторы линейных многообразий размерности $n/2$.

Рассмотрим $I_U(x)$, где U — подпространство.

Пусть $a_1, a_2, \dots, a_{n/2}$ — базис $U^\perp$. Исходя из $U^{\perp\perp} = U$, имеем

$$x \in U \iff \forall i \in \{1, \dots, n/2\} \langle a_i, x \rangle = 0.$$

Отсюда получаем формулу для индикатора:

$$I_U(x) = (\langle a_1, x \rangle \oplus 1) \cdot (\langle a_2, x \rangle \oplus 1) \cdot \dots \cdot (\langle a_{n/2}, x \rangle \oplus 1).$$

Таким образом, индикатор подпространства размерности $n/2$ является конъюнкцией $n/2$ сомножителей, каждый из которых — отрицание скалярного произведения вектора переменных и базисного вектора $U^\perp$.

Рассмотрим $I_L(x)$, где L — линейное многообразие.

Пусть $x_0 \in L$, $U = x_0 \oplus L$. Очевидно, что U — подпространство. Тогда

$$I_L(x) = I_U(x_0 \oplus x).$$

Утверждение 3. Пусть U — линейное многообразие размерности $n/2$. Тогда $\deg(I_U) = n/2$.

Следствие 6. Если бент-функции находятся на минимальном расстоянии друг от друга, то хотя бы одна из них имеет алгебраическую степень $n/2$.

В общем случае задача нахождения подпространств, на которых f аффинна, достаточно сложна и не решается методом «пристального взгляда». Но если полином Жегалкина функции f содержит мало слагаемых, то часто существуют координатные подпространства (подпространства, базисом которых являются векторы веса 1 из E^n), на которых f аффинна. Рассмотрим алгоритм построения бент-функции, находящейся на минимальном расстоянии от данной, с использованием координатных подпространств.

Алгоритм 1

Вход: $f(x)$ — исходная бент-функция.

Выход: $g(x)$ — бент-функция на минимальном расстоянии от функции $f(x)$.

- 1) Фиксируем значения любых $n/2$ переменных так, чтобы функция от оставшихся $n/2$ переменных стала аффинной.
- 2) Если первый шаг завершился успешно, то получаем индикатор многообразия в следующем виде:

$$I_L(x) = (x_{i_1} \oplus x_{i_1}^0 \oplus 1) \cdot (x_{i_2} \oplus x_{i_2}^0 \oplus 1) \cdot \dots \cdot (x_{i_{n/2}} \oplus x_{i_{n/2}}^0 \oplus 1),$$

где x_{i_j} — переменные, которые мы зафиксировали на первом шаге алгоритма; $x_{i_j}^0$ — значения зафиксированных переменных.

Таким образом, если мы фиксировали переменную x_i значением 0, то в индикатор многообразия войдет отрицание этой переменной, если же мы фиксировали значением 1, то в индикатор войдет сама переменная.

3) Получаем

$$g(x) = f(x) \oplus I_L(x).$$

Пример 1. Пусть

$$f(x) = x_1x_2 \oplus x_3x_4 \oplus \dots \oplus x_{n-1}x_n.$$

1) Фиксируем все переменные с чётными номерами значением 1. Получаем следующую функцию:

$$f(x_1, 1, x_3, 1, \dots, x_{n-1}, 1) = x_1 \oplus x_3 \oplus \dots \oplus x_{n-1}.$$

Видно, что получилась аффинная функция.

2) Индикатор будет выглядеть следующим образом:

$$I_L(x) = x_2x_4 \dots x_n.$$

3) Получаем следующую выходную функцию:

$$g(x) = x_1x_2 \oplus x_3x_4 \oplus \dots \oplus x_{n-1}x_n \oplus x_2x_4 \dots x_n.$$

3. Известные подклассы бент-функций с точки зрения существования функций на минимальном расстоянии

Рассматривается существование бент-функций на минимальном расстоянии для бент-функций из известных подклассов класса $\mathfrak{B}_n$.

3.1. Класс Мэйорана — Мак-Фарланда

Класс Мэйорана — Мак-Фарланда обозначается как $\mathcal{M}$. В этом классе содержатся бент-функции следующего вида:

$$f(x, y) = \langle x, \pi(y) \rangle \oplus \psi(y), \quad (3)$$

где $x, y \in E^{n/2}$, $\psi \in \mathcal{F}_{n/2}$, π — подстановка на $E^{n/2}$.

Более подробно об этой конструкции можно узнать в [5].

Покажем, что для любой функции из класса $\mathcal{M}$ существует бент-функция на минимальном расстоянии: достаточно воспользоваться алгоритмом 1.

1) Фиксируем значение y : пусть $y = y_0$. Тогда

$$f(x, y_0) = \langle x, \pi(y_0) \rangle \oplus \psi(y_0).$$

Понятно, что это аффинная функция.

2) Получаем индикатор, в который входят только переменные из y .

3) Получаем бент-функцию в классе $\mathcal{M}$ на минимальном расстоянии от исходной.

Класс $\mathcal{M}$ является простым и достаточно богатым.

$$|\mathcal{M}_n| = 2^{n/2!} \cdot 2^{2^{n/2}}. \quad (4)$$

Известно (см. описание бент-функций в виде линейного разветвления в [6]), что если бент-функция имеет вид $f(x, y) = \langle x, \pi(y) \rangle \oplus \psi(y)$, где $x, y \in E^{n/2}$, $\psi \in \mathcal{F}_{n/2}$, то отображение π взаимнооднозначно и, следовательно, функция $f(x)$ принадлежит классу $\mathcal{M}_n$.

Мощность класса $\mathcal{M}_n$ часто используется как нижняя оценка мощности класса $\mathfrak{B}_n$. Если рассматривать функции, аффинно эквивалентные функциям из $\mathcal{M}_n$, то идею Мэйорана — Мак-Фарланда можно трактовать следующим образом:

- 1) Берем подпространство U размерности $n/2$ в E^n .
- 2) Разбиваем E^n на смежные классы относительно U .
- 3) На каждом смежном классе U строим аффинную функцию.

Также следует отметить, что бент-функции, аффинно эквивалентные функциям из класса Мэйорана — Мак-Фарланда, не являются всеми бент-функциями, имеющими непустое L_{all} . Пример такой бент-функции будет приведен в п. 4.

3.2. Partial Spreads

Класс бент-функций Partial Spreads обозначается как $\mathcal{PS}$. Он состоит из двух подклассов $\mathcal{PS}^-$, $\mathcal{PS}^+$, определяемых следующим образом.

$\mathcal{PS}^-$. Пусть

- 1) L_i — подпространства в E^n , $i \in \{1, 2, \dots, 2^{n/2-1}\}$;
- 2) размерность L_i равна $n/2$;
- 3) $L_i \cap L_j = \{0\} \forall i \neq j$.

Тогда функции вида

$$f(x) = \bigoplus_{i=1}^{2^{n/2-1}} I_{L_i}(x) \quad (5)$$

принадлежат $\mathcal{PS}^-$.

$\mathcal{PS}^+$. Пусть

- 1) L_i — подпространства в E^n , $i \in \{1, 2, \dots, 2^{n/2-1} + 1\}$;
- 2) размерность L_i равна $n/2$;
- 3) $L_i \cap L_j = \{0\} \forall i \neq j$.

Тогда функции вида

$$f(x) = \bigoplus_{i=1}^{2^{n/2-1}+1} I_{L_i}(x) \quad (6)$$

принадлежат $\mathcal{PS}^+$.

Класс $\mathcal{PS}$ впервые был описан Дж. Диллоном в [7].

С точки зрения существования бент-функций на минимальном расстоянии больший интерес представляет класс $\mathcal{PS}^+$ (для функций из $\mathcal{PS}^-$ это сложный вопрос). Нетрудно убедиться, что все функции из класса $\mathcal{PS}^+$ имеют непустые множества L_{all} : для всех подпространств L_i из определения функций в этом классе выполняется

$$\forall x \in L_i \setminus \{0\} \quad f(x) = 1,$$

потому что пространства пересекаются только по нулевому элементу. Кроме того,

$$f(0) = 1,$$

так как 0 лежит во всех пространствах, а количество пространств нечетно. Следовательно,

$$\forall x \in L_i \quad f(x) = 1.$$

Таким образом, $L_i \in L_{\text{all}}(f)$ для всех i , причем функции вида

$$g(x) = f(x) \oplus I_{L_i}(x)$$

будут принадлежать $\mathcal{PS}^-$, и порождающими пространствами для них будут все подпространства для f , кроме L_i .

4. Аффинная эквивалентность бент-функций и минимальное расстояние

Рассмотрим известные факты об аффинной классификации бент-функций и взаимосвязь этих фактов с расстоянием между бент-функциями.

Определение 6. Булевы функции f и g от n переменных называются *аффинно эквивалентными*, если существует невырожденная матрица A размера $n \times n$, вектор b длины n и аффинная функция l от n переменных, такие, что $g(x) = f(A \cdot x \oplus b) \oplus l(x)$ для любого x .

Рассмотрим известные факты об аффинной классификации бент-функций.

Утверждение 4 [8]. Все бент-функции степени 2 аффинно эквивалентны функции $f(x) = x_1x_2 \oplus x_3x_4 \oplus \dots \oplus x_{n-1}x_n$.

Утверждение 5 [9] и др. Каждая бент-функция от 6 переменных аффинно эквивалентна одной из следующих функций:

- 1) $f_1^6 = x_1x_2 \oplus x_3x_4 \oplus x_5x_6$;
- 2) $f_2^6 = x_1x_2x_3 \oplus x_1x_4 \oplus x_2x_5 \oplus x_3x_6$;
- 3) $f_3^6 = x_1x_2x_3 \oplus x_2x_4x_5 \oplus x_1x_2 \oplus x_1x_4 \oplus x_2x_6 \oplus x_3x_5 \oplus x_4x_5$;
- 4) $f_4^6 = x_1x_2x_3 \oplus x_2x_4x_5 \oplus x_3x_4x_6 \oplus x_1x_4 \oplus x_2x_6 \oplus x_3x_4 \oplus x_3x_5 \oplus x_3x_6 \oplus x_4x_5 \oplus x_4x_6$.

Утверждение 6 [10]. Каждая бент-функция от 8 переменных степени не больше 3 аффинно эквивалентна одной из следующих функций:

- 1) $f_1^8 = x_1x_2 \oplus x_3x_4 \oplus x_5x_6 \oplus x_7x_8$;
- 2) $f_2^8 = x_1x_2x_3 \oplus x_1x_4 \oplus x_2x_5 \oplus x_3x_6 \oplus x_7x_8$;
- 3) $f_3^8 = x_1x_2x_3 \oplus x_2x_4x_5 \oplus x_3x_4 \oplus x_2x_6 \oplus x_1x_7 \oplus x_5x_8$;
- 4) $f_4^8 = x_1x_2x_3 \oplus x_2x_4x_5 \oplus x_1x_3 \oplus x_1x_5 \oplus x_2x_6 \oplus x_3x_4 \oplus x_7x_8$;
- 5) $f_5^8 = x_1x_2x_3 \oplus x_2x_4x_5 \oplus x_3x_4x_6 \oplus x_3x_5 \oplus x_2x_6 \oplus x_2x_5 \oplus x_1x_7 \oplus x_4x_8$;
- 6) $f_6^8 = x_1x_2x_3 \oplus x_2x_4x_5 \oplus x_3x_4x_6 \oplus x_3x_5 \oplus x_1x_3 \oplus x_1x_4 \oplus x_2x_7 \oplus x_6x_8$;
- 7) $f_7^8 = x_1x_2x_3 \oplus x_2x_4x_5 \oplus x_3x_4x_6 \oplus x_3x_5 \oplus x_2x_6 \oplus x_2x_5 \oplus x_1x_2 \oplus x_1x_3 \oplus x_1x_4 \oplus x_7x_8$;
- 8) $f_8^8 = x_1x_2x_3 \oplus x_2x_4x_5 \oplus x_3x_4x_6 \oplus x_3x_5 \oplus x_1x_6 \oplus x_2x_7 \oplus x_4x_8$;
- 9) $f_9^8 = x_1x_2x_7 \oplus x_3x_4x_7 \oplus x_5x_6x_7 \oplus x_1x_4 \oplus x_3x_6 \oplus x_2x_5 \oplus x_4x_5 \oplus x_7x_8$;
- 10) $f_{10}^8 = x_1x_2x_3 \oplus x_2x_4x_5 \oplus x_3x_4x_6 \oplus x_1x_4x_7 \oplus x_3x_5 \oplus x_2x_7 \oplus x_1x_5 \oplus x_1x_6 \oplus x_4x_8$.

Рассмотрим связь расстояний между бент-функциями и аффинной эквивалентностью.

Так как класс $\mathfrak{B}_n$ замкнут относительно отрицания функции, то из формулы $d(\mathfrak{B}_n) = 2^{n/2}$ следует

Утверждение 7. Наибольшее расстояние в классе $\mathfrak{B}_n$, не равное 2^n , равно $2^n - 2^{n/2}$.

Определение 7 (спектр расстояний для функции). Пусть $f \in \mathfrak{B}_n$. Тогда вектор r из $\mathbb{Z}^{2^n}$ называется *спектром расстояний* для бент-функции f , если i -я компонента вектора r равна количеству бент-функций на расстоянии i от функции f .

Утверждение 8. Спектры расстояний для аффинно эквивалентных бент-функций одинаковы.

Доказательство. Имеют место следующие равенства:

$$\text{dist}(f(x), g(x)) = \text{dist}(f(A \cdot x \oplus b), g(A \cdot x \oplus b)), \det(A) \neq 0;$$

$$\forall h \in \mathcal{F}_n \quad \text{dist}(f, g) = \text{dist}(f \oplus h, g \oplus h).$$

Так как класс бент-функций замкнут относительно аффинного преобразования переменных и относительно прибавления любой аффинной функции, то из этих равенств очевидным образом следует утверждение. ■

Следовательно, чтобы получить всевозможные спектры расстояний для бент-функций, достаточно найти спектры расстояний для одной бент-функции из каждого класса аффинной эквивалентности.

Утверждение 9. Любая бент-функция степени 2 имеет непустое $L_{\text{all}}(f)$.

Доказательство. Из утверждения 4 известно, что все бент-функции степени 2 аффинно эквивалентны функции $f(x) = x_1 \cdot x_2 \oplus x_3 \cdot x_4 \oplus \dots \oplus x_{n-1} \cdot x_n$. А для этой функции условие теоремы выполнено. ■

Утверждение 10. Все функции из класса $\mathfrak{B}_6$ имеют непустое L_{all} .

Доказательство. Применяем алгоритм 1 к аффинно неэквивалентным бент-функциям от 6 переменных:

- 1) $f_1^6(x_1, 0, x_3, 0, x_5, 0) = 0;$
- 2) $f_2^6(0, 0, 0, x_4, x_5, x_6) = 0;$
- 3) $f_3^6(0, 0, x_3, x_4, 0, x_6) = 0;$
- 4) $f_4^6(x_1, 0, 0, 0, x_5, x_6) = 0,$

то есть первый шаг алгоритма для каждой функции завершился успешно. Отсюда следует утверждение теоремы. ■

Утверждение 11. Все бент-функции от 8 переменных степени не больше 3 имеют непустое L_{all} .

Доказательство. Применяем алгоритм 1 к аффинно неэквивалентным бент-функциям от 8 переменных степени не больше 3:

- 1) $f_1^8(0, x_2, 0, x_4, 0, x_6, 0, x_8) = 0;$
- 2) $f_2^8(0, 0, 0, x_4, x_5, x_6, 0, x_8) = 0;$
- 3) $f_3^8(0, 0, x_3, 0, 0, x_6, x_7, x_8) = 0;$
- 4) $f_4^8(0, 0, 0, x_4, x_5, x_6, 0, x_8) = 0;$
- 5) $f_5^8(0, 0, 0, 0, x_5, x_6, x_7, x_8) = 0;$
- 6) $f_6^8(0, 0, 0, x_4, x_5, 0, x_7, x_8) = 0;$
- 7) $f_7^8(0, 0, 0, x_4, x_5, x_6, 0, x_8) = 0;$
- 8) $f_8^8(0, 0, 0, 0, x_5, x_6, x_7, x_8) = 0;$
- 9) $f_9^8(x_1, 0, 0, 0, x_5, x_6, 0, x_8) = 0;$
- 10) $f_{10}^8(0, 0, 0, 0, x_5, x_6, x_7, x_8) = 0,$

то есть первый шаг алгоритма для каждой функции завершился успешно. Отсюда следует утверждение теоремы. ■

Утверждение 12. Пусть $f \in \mathfrak{B}_n$. Тогда f аффинно эквивалентна функции из класса Мэйорана — Мак-Фарланда тогда и только тогда, когда существует $L \in L_{\text{all}}(f)$, такое, что $x_0 \oplus L \in L_{\text{all}}(f)$ для всех $x_0 \in E^n$.

Доказательство. Необходимость. Пусть f представлена в виде

$$f(x, y) = \langle x, h(y) \rangle \oplus g(y), \quad x, y \in E^{n/2}.$$

Тогда зададим L следующим образом:

$$L = \{(x, 0) \mid x \in E^{n/2}\}.$$

Очевидно, что данное L удовлетворяет условию утверждения.

Достаточность. Пусть существует линейное многообразие L , удовлетворяющее заданному условию. Понятно, что невырожденным аффинным преобразованием мы можем привести функцию f к виду

$$f'(x, y) = \langle x, h(y) \rangle \oplus g(y), \quad x, y \in E^{n/2}.$$

Из критерия Ященко о представлении бент-функции в виде линейного разветвления (см. [6]) следует, что $h(y)$ взаимнооднозначно и f' принадлежит классу $\mathcal{M}_n$. ■

Утверждение 13. В классе $\mathfrak{B}_8$ существуют бент-функции с непустым L_{all} , аффинно неэквивалентные функциям из класса Мэйорана — Мак-Фарланда.

Пример 2. Бент-функция от 8 переменных с непустым L_{all} , аффинно неэквивалентная функциям из класса Мэйорана — Мак-Фарланда:

$$\begin{aligned} f(x) = & x_1x_2x_5x_8 \oplus x_1x_2x_6x_8 \oplus x_1x_4x_5x_8 \oplus x_1x_4x_6x_8 \oplus x_1x_5x_6x_8 \oplus x_2x_4x_5x_8 \oplus x_2x_4x_6x_8 \oplus \\ & x_3x_4x_5x_8 \oplus x_4x_5x_6x_8 \oplus x_1x_2x_3 \oplus x_1x_2x_5 \oplus x_1x_2x_6 \oplus x_1x_2x_8 \oplus x_1x_4x_5 \oplus x_1x_4x_6 \oplus x_1x_4x_8 \oplus \\ & x_1x_5x_6 \oplus x_1x_5x_8 \oplus x_1x_6x_8 \oplus x_2x_4x_5 \oplus x_2x_4x_6 \oplus x_2x_4x_8 \oplus x_2x_5x_8 \oplus x_2x_6x_8 \oplus x_3x_4x_5 \oplus x_3x_4x_8 \oplus \\ & x_3x_5x_8 \oplus x_4x_5x_6 \oplus x_4x_6x_8 \oplus x_5x_6x_8 \oplus x_1x_2 \oplus x_1x_5 \oplus x_1x_6 \oplus x_1x_8 \oplus x_2x_4 \oplus x_2x_6 \oplus x_2x_8 \oplus \\ & x_3x_4 \oplus x_3x_5 \oplus x_3x_6 \oplus x_3x_8 \oplus x_4x_6 \oplus x_5x_6 \oplus x_6x_8 \oplus x_7x_8 \oplus x_1 \oplus x_2 \oplus x_3 \oplus x_6. \end{aligned}$$

С помощью программы, реализующей алгоритм 2 из п. 5, было показано, что у данной функции имеются линейные многообразия размерности 4, на которых она аффинна, но при этом ни для одного из них не выполняется условие утверждения 12.

5. Алгоритм перебора бент-функций, находящихся на минимальном расстоянии от заданной бент-функции

Из теоремы 1 следует, что для того чтобы перебрать все бент-функции, находящиеся на минимальном расстоянии от заданной бент-функции, достаточно перебрать все многообразия размерности $n/2$, на которых заданная бент-функция аффинна.

Базис подпространства размерности $n/2$ задаётся $n/2$ строками матрицы ступенчатого вида, состоящей из нулей и единиц, такой, что

- 1) каждая из последующих строк заканчивается меньшим количеством подряд идущих нулей, чем предыдущая строка;
- 2) под каждой ведущей единицей (первая единица в строке) в столбце стоят нули;
- 3) остальные элементы произвольны.

Приведём пример такой матрицы и бент-функций, находящихся на минимальном расстоянии друг от друга.

Пример 3. Пусть дана бент-функция от шести переменных:

$$f_1(x) = x_1x_2x_3 \oplus x_1x_4 \oplus x_2x_5 \oplus x_3x_6.$$

Для построения бент-функции, находящейся на минимальном расстоянии от данной, нужно найти такое многообразие $L = x_0 \oplus U$, что f_1 будет аффинна на этом многообразии. На компьютере с помощью алгоритма, который приведен ниже, были построены

все базисы подпространств U и все x_0 , такие, что f_1 аффинна на $L = x_0 \oplus U$. Приведем пример таких x_0 и U . Пусть

$$A_U = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \text{ — базисная матрица подпространства } U;$$

$x_0 = (0 \ 1 \ 0 \ 0 \ 0 \ 0)$. Тогда базисная матрица ортогонального подпространства

$$A_{U^\perp} = (a_{ij}) = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 \end{pmatrix}.$$

Теперь построим индикатор, являющийся конъюнкцией $n/2$ сомножителей, где i -й сомножитель получен из i -й строки матрицы $A_{U^\perp}$ таким образом:

$$(a_{i1}x_1 \oplus a_{i2}x_2 \oplus \dots \oplus a_{in}x_n \oplus 1).$$

Отсюда следует $I_L(x) = I_U(x \oplus x_0) = I_U(x_1, x_2 \oplus 1, x_3, x_4, x_5, x_6) = (x_6 \oplus 1)(x_2 \oplus 1 \oplus 1)(x_1 \oplus x_3 \oplus x_4 \oplus 1) = x_1x_2x_6 \oplus x_2x_3x_6 \oplus x_2x_4x_6 \oplus x_2x_6 \oplus x_1x_2 \oplus x_2x_3 \oplus x_2x_4 \oplus x_2$. Отсюда получаем вторую бент-функцию $f_2(x) = f_1(x) \oplus I_L(x) = x_1x_2x_3 \oplus x_1x_4 \oplus x_2x_5 \oplus x_3x_6 \oplus x_1x_2x_6 \oplus x_2x_3x_6 \oplus x_2x_4x_6 \oplus x_2x_6 \oplus x_1x_2 \oplus x_2x_3 \oplus x_2x_4 \oplus x_2$, которая находится на минимальном расстоянии $2^{n/2} = 8$ от функции f_1 .

Следующий алгоритм нам потребуется для нахождения всех бент-функций, находящихся на минимальном расстоянии от заданной бент-функции, но мы приведем его в общем виде для произвольной булевой функции.

Алгоритм 2 (поиск всех многообразий размерности $n/2$, на которых функция аффинна).

- 1) На вход алгоритма подается булева функция $f(x)$ (в нашем случае это бент-функция).
- 2) Далее для всех x_0 из E^n получаем новую функцию: $g(x) = f_{x_0}(x) = f(x \oplus x_0)$.
- 3) После этого $g(x)$ нормируется: $g(x) = g(x) \oplus g(0)$.

Таким образом, мы перешли от поиска многообразий, на которых заданная функция аффинна, к поиску подпространств, на которых заданная функция линейна. Для каждой такой функции $g(x)$ будем рекуррентно строить все базисные матрицы размера $n/2 \times n$.

- 4) Пусть A_1 — матрица, содержащая одну строку.
- 5) Допустим, что построена матрица A_{i-1} размера $s - 1 \times n$, где $s - 1 < n/2$, и нужно построить матрицу A_i размера $s \times n$. Для этого добавим ещё один вектор в базис. Перебираем все векторы v в лексикографическом порядке² и приписываем их к матрице A_{i-1} , так, чтобы получившаяся матрица A_i удовлетворяла условиям 1–3 на с. 17. Для каждого вектора v , претендующего стать базисным, проверяются два условия:

а) $g(x \oplus v) = g(x) \oplus g(v)$;

б) вектор x_0 лексикографически предшествует вектору $v \oplus x \oplus x_0$, где x пробегает множество всех ранее добавленных в подпространство векторов.

Если хотя бы одно условие не выполняется, вектор v отбрасывается. Таким образом, сразу отсекается большое количество ненужных векторов. Если ни один из векторов не подошел, значит, это тупиковая ветка рекурсии.

²Заметим, что в реализации удобнее нумеровать компоненты векторов справа налево.

Трудоёмкость данного алгоритма в самом худшем случае (если на вход алгоритма подать линейную функцию) не превышает $T = O(n/2 \cdot P_{n/2} \cdot 2^{n/2})$, где $n/2$ — количество операций, необходимое для построения одного подпространства; $P_{n/2} = \frac{(2^n - 1)(2^{n-1} - 1) \dots (2^{n/2+1} - 1)}{(2^{n/2} - 1)(2^{n/2-1} - 1) \dots (2^1 - 1)}$ — количество подпространств размерности $n/2$; $2^{n/2}$ — количество операций, затрачиваемых на проверку условий. Но на практике данный алгоритм работает значительно быстрее.

Приведем экспериментальные данные. В таблице показаны бент-функции (по утверждению 8 достаточно рассматривать представителей различных классов аффинной эквивалентности), количество многообразий, на которых данная бент-функция аффинна, и время работы программы в секундах (на процессоре с тактовой частотой 2,4 ГГц).

n	Бент-функция	$ L_{\text{all}} $	Время
4	$x_1x_2 \oplus x_3x_4$	60	0
6	$x_1x_2x_3 \oplus x_2x_4x_5 \oplus x_3x_4x_6 \oplus x_1x_4 \oplus x_2x_6 \oplus x_3x_4 \oplus x_3x_5 \oplus x_3x_6 \oplus x_4x_5 \oplus x_4x_6$	376	0,001
6	$x_1x_2x_3 \oplus x_2x_4x_5 \oplus x_1x_2 \oplus x_1x_4 \oplus x_2x_6 \oplus x_3x_5 \oplus x_4x_5$	440	0,001
6	$x_1x_2x_3 \oplus x_1x_4 \oplus x_2x_5 \oplus x_3x_6$	568	0,001
6	$x_1x_2 \oplus x_3x_4 \oplus x_5x_6$	1080	0,002
8	$x_1x_2x_3 \oplus x_2x_4x_5 \oplus x_3x_4x_6 \oplus x_1x_4x_7 \oplus x_3x_5 \oplus x_2x_7 \oplus x_1x_5 \oplus x_1x_6 \oplus x_4x_8$	1392	0,035
8	$x_1x_2x_3 \oplus x_2x_4x_5 \oplus x_3x_4x_6 \oplus x_3x_5 \oplus x_2x_6 \oplus x_2x_5 \oplus x_1x_7 \oplus x_4x_8$	2928	0,035
8	$x_1x_2x_3 \oplus x_2x_4x_5 \oplus x_3x_4x_6 \oplus x_3x_5 \oplus x_1x_3 \oplus x_1x_4 \oplus x_2x_7 \oplus x_6x_8$	2928	0,035
8	$x_1x_2x_3 \oplus x_2x_4x_5 \oplus x_3x_4x_6 \oplus x_3x_5 \oplus x_2x_6 \oplus x_2x_5 \oplus x_1x_2 \oplus x_1x_3 \oplus x_1x_4 \oplus x_7x_8$	2928	0,036
8	$x_1x_2x_3 \oplus x_2x_4x_5 \oplus x_3x_4x_6 \oplus x_3x_5 \oplus x_1x_6 \oplus x_2x_7 \oplus x_4x_8$	2928	0,034
8	$x_1x_2x_7 \oplus x_3x_4x_7 \oplus x_5x_6x_7 \oplus x_1x_4 \oplus x_3x_6 \oplus x_2x_5 \oplus x_4x_5 \oplus x_7x_8$	4464	0,036
8	$x_1x_2x_3 \oplus x_2x_4x_5 \oplus x_3x_4 \oplus x_2x_6 \oplus x_1x_7 \oplus x_5x_8$	6000	0,037
8	$x_1x_2x_3 \oplus x_2x_4x_5 \oplus x_1x_3 \oplus x_1x_5 \oplus x_2x_6 \oplus x_3x_4 \oplus x_7x_8$	6000	0,037
8	$x_1x_2x_3 \oplus x_1x_4 \oplus x_2x_5 \oplus x_3x_6 \oplus x_7x_8$	12144	0,045
8	$x_1x_2 \oplus x_3x_4 \oplus x_5x_6 \oplus x_7x_8$	36720	0,070
10	$x_1x_2 \oplus x_3x_4 \oplus x_5x_6 \oplus x_7x_8 \oplus x_9x_{10}$	2424520	8,543

ЛИТЕРАТУРА

1. Токарева Н. Н. Бент-функции: результаты и приложения. Обзор работ // Прикладная дискретная математика. 2009. № 3. С. 15–37.
2. Paterson K. G. Sequences For OFDM and Multi-code CDMA: two problems in algebraic Coding Theory // Sequences and their applications. Seta 2001. Second Int. Conference (Bergen, Norway, May 13–17, 2001). Proc. Berlin: Springer, 2002. P. 46–71.
3. Логачев О. А., Сальников А. А., Яценко В. В. Булевы функции в теории кодирования и криптологии. М.: МЦНМО, 2004. 470 с.
4. Carlet C. Boolean Functions for Cryptography and Error Correcting Codes // Chapter of the monograph «Boolean Methods and Models», Cambridge Univ.

- Press / eds. P. Hammer, Y. Crama, to appear. Prelim. version is available at www-rocq.inria.fr/secret/Claude.Carlet/chap-fcts-Bool.pdf.
5. *McFarland R. L.* A family of difference sets in non-cyclic groups // J. Combin. Theory. Ser. A. 1973. V. 15. No. 1. P. 1–10.
 6. *Яценко В. В.* О критерии распространения для булевых функций и о бент-функциях // Пробл. передачи информации. 1997. Т. 33. Вып. 1. С. 75–86.
 7. *Dillon J. F.* Elementary Hadamard Difference sets // Ph. D. Thesis. Univ. of Maryland, 1974.
 8. *Dillon J. F.* A survey of bent functions // The NSA Technical J. 1972. Special Issue. P. 191–215.
 9. *Rothaus O.* On bent functions // J. Combin. Theory. Ser. A. 1976. V. 20. No. 3. P. 300–305.
 10. *Braeken A.* Cryptographic properties of Boolean functions and S-boxes // Ph. D. Thesis, Katholieke Univ. Leuven, 2006.