ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ
Июль–сентябрь 2021. Т. 28, № 3. С. 49–64

УДК 519.8+518.25 DOI 10.33048/daio.2021.28.705

О НЕЛИНЕЙНОСТИ БУЛЕВЫХ ФУНКЦИЙ, ПОСТРОЕННЫХ ОБОБЩЁННОЙ КОНСТРУКЦИЕЙ ДОББЕРТИНА

И. А. Сутормин

Институт математики им. С. Л. Соболева,
пр. Акад. Коптюга, 4 630090 Новосибирск, Россия
E-mail: ivan.sutormin@gmail.com

Аннотация. Предложено обобщение конструкции, описанной Доббертином в 1995 г., для сбалансированных булевых функций, обладающих высокой нелинейностью. Исследован спектр Уолша — Адамара предложенных функций. Доказана точная верхняя оценка на спектральный радиус (нижняя оценка нелинейности), и показан способ построения сбалансированной функции от $2n$ переменных со спектральным радиусом, равным $2^n + 2^k R$, при помощи сбалансированной функции от $n - k$ переменных со спектральным радиусом, равным R. Библиогр. 20.

Ключевые слова: булева функция, бент-функция, нелинейность, сбалансированность, спектральный радиус.

Введение

В различных криптографических алгоритмах часто используются булевы функции. Нелинейность — одно из основных для них свойств. Она показывает, насколько хорошо функцию можно приблизить некоторой аффинной функцией, работать с которой значительно проще. Шифр может стать уязвимым к линейному криптоанализу при низкой нелинейности даже одной его части. Примером криптографического алгоритма, скомпрометированного своими компонентами с низкой нелинейностью, может послужить старый стандарт шифрования США — DES. Описание линейного криптоанализа для этого шифра можно найти в [1].

В случае чётного числа переменных n известна максимальная возможная для булевой функции нелинейность: $N_f = 2^{n-1} - 2^{\frac{n}{2}-1}$. Она

Исследование выполнено в рамках государственного задания ИМ СО РАН (проект № 0314–2019–0017) при финансовой поддержке Российского фонда фундаментальных исследований (проект № 20–31–70043) и лаборатории криптографии «JetBrains Research».

достигается на функциях, называемых бент-функциями. Они были впервые описаны О. Ротхаусом [2] в 1976 г. В СССР в 1960-е гг. В. Елисеев и О. Степченков также занимались изучением этого класса функций. Подробную информацию о бент-функциях и других криптографических функциях можно найти в монографиях [3–7].

В практических целях также часто требуется, чтобы функция была сбалансированной — принимала значения 0 и 1 одинаково часто. Идеально было бы использовать сбалансированную функцию с максимальной возможной нелинейностью, но бент-функции не сбалансированы. Для максимального значения нелинейности сбалансированных функций существует асимптотическая оценка [8], но точное значение неизвестно. Наилучшие нижние оценки этого значения получены как следствие конкретных конструкций сбалансированных функций [9–14].

Одна из таких конструкций, предложенная в 1995 г. Доббертином [15], основана на модификации нормальных бент-функций — функций от $2n$ переменных, постоянных на некотором аффинном подпространстве L размерности n. Спектральный радиус R_f — один из возможных параметров, через который можно выразить нелинейность функции: $N_f = 2^{n-1} - \frac{R_f}{2}$, именно его для этой конструкции удобно оценивать. Суть конструкции заключается в замене значений бент-функции на подпространстве L значениями сбалансированной функции θ от n переменных. У сбалансированной функции Θ, имеющей конструкцию Доббертина, спектральный радиус равен $R_\Theta = 2^n + R_\theta$, а нелинейность равна $N_\Theta = 2^{2n-1} - 2^{n-1} - \frac{R_\theta}{2}$. Также в [15] была сформулирована не опровергнутая до сих пор гипотеза о несуществовании сбалансированных функций с нелинейностью выше, чем можно получить при помощи этой конструкции. Простая структура конструкции Доббертина позволяет модифицировать её для получения новых конструкций функций с хорошими криптографическими свойствами. Пример такого обобщения конструкции на случай векторных булевых функций можно найти в [16].

Данная работа посвящена новому обобщению конструкции Доббертина. Для этого используется класс бент-функций с близкими к нормальности свойствами. Функции, принадлежащие этому классу, постоянны на некотором подпространстве размерности 2^{n-k} и на $2^{2k}-1$ его сдвигах, $0 \leqslant k \leqslant n-2$. С их помощью в работе построено обобщение конструкции Доббертина. Результатом работы является оценка спектрального радиуса для полученной сбалансированной функции Θ от $2n$ переменных:

$$R_\Theta \leqslant 2^n + \sum_{y \in I_0 \cup I_1} R_{\theta_y},$$

где θ_y — набор 2^{2k} произвольных сбалансированных функций от $n-k$ переменных, требуемых для конструкции. Доказано, что неравенство

в этой оценке достигается при «неудачном» выборе θ_y, найден набор функций для которого оценка спектрального радиуса принимает вид

$$R_\Theta = 2^n + 2^k R_\theta,$$

где θ — произвольная сбалансированная функция от $n-k$ переменных, по которой определяются все θ_y. К сожалению, наилучший результат в данной оценке достигается при $k=0$, т. е. в случае, описанном Доббертином.

1. Определения

Введём необходимые определения и обозначения. Обозначим через $\mathbb{F}_2^n$ векторное пространство размерности n над полем из двух элементов $\mathbb{F}_2$. Далее при работе с элементами $\mathbb{F}_2^n$ знаком $+$ будем обозначать покомпонентное сложение по модулю 2. Нулевой вектор будет обозначаться $\mathbf{0}$. Для двух двоичных векторов x, y введём обозначение $\langle x, y\rangle = x_1y_1 + \cdots + x_ny_n$. Функция из $\mathbb{F}_2^n$ в $\mathbb{F}_2$ называется *булевой функцией*. *Расстоянием Хэмминга* между двумя булевыми функциями называется количество аргументов, на которых их значения отличаются. Расстояние Хэмминга от функции до класса функций — минимальное из расстояний Хэмминга от неё до одного из представителей этого класса. *Аффинная функция* — функция вида $\langle a, x\rangle + c$, где $a \in \mathbb{F}_2^n$, $c \in \mathbb{F}_2$. Функция называется *сбалансированной*, если она принимает значения 0 и 1 одинаково часто.

Преобразование Уолша — Адамара $W_f\colon \mathbb{F}_2^n \to \mathbb{Z}$ для булевой функции $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$ определяется следующим образом:

$$W_f(a) = \sum_{x\in\mathbb{F}_2^n} (-1)^{f(x)+\langle x,a\rangle}.$$

Спектральным радиусом булевой функции f называется

$$R_f = \max_{a\in\mathbb{F}_2^n} |W_f(a)|.$$

Нелинейностью — расстояние Хэмминга от функции f до класса аффинных функций, она равна

$$N_f = 2^{n-1} - \frac{R_f}{2}.$$

Бент-функции — функции от n переменных, все коэффициенты Уолша — Адамара которых равны $\pm 2^{n/2}$. Они существуют только при чётном n. На бент-функциях достигается максимальная возможная нелинейность. Функция $\widetilde{f}$, заданная равенством

$$W_f(y) = 2^{\frac{n}{2}}(-1)^{\widetilde{f}(y)},$$

называется *дуальной* к бент-функции f. Известно, что такая функция также будет являться бент-функцией.

Булевы функции f и g от n переменных *аффинно эквивалентны*, если для всех x выполнено $g(x) = f(Ax+b)$, где A — невырожденная двоичная матрица размера $n \times n$, а b — двоичный вектор размерности n. Известно, что аффинная эквивалентность сохраняет нелинейность и сбалансированность булевых функций. Непустое множество $M \subseteq \mathbb{F}_2^n$ называется *линейным подпространством*, если для любых $x, y \in M$ выполнено $x + y \in M$. Сдвиги элементов $x \in M$ на постоянную $a \in \mathbb{F}_2^n$ — всевозможные суммы вида $a + x$ — образуют *аффинное подпространство* той же размерности.

Булева функция от $2n$ переменных называется *нормальной*, если она постоянна на некотором аффинном подпространстве L размерности n. Известно (см. [15]), что любая такая бент-функция аффинно эквивалентна функции $f\colon \mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{F}_2$, постоянной на $L = \{(x, \mathbf{0}) \mid x \in \mathbb{F}_2^n\}$ и равной некоторой сбалансированной $f_y\colon \mathbb{F}_2^n \to \mathbb{F}_2$ на $\{(x, y) \mid x \in \mathbb{F}_2^n\}$, где $y \in \mathbb{F}_2^n$, $y \neq \mathbf{0}$.

2. Конструкция Доббертина

Идея конструкции Доббертина для высоконелинейных сбалансированных функций заключается в замене значений нормальной бент-функции f от $2n$ переменных на всём подпространстве L значениями некоторой сбалансированной функции $\theta\colon \mathbb{F}_2^n \to \mathbb{F}_2$. Результатом такой замены будет

$$\Theta(x, y) = \begin{cases} \theta(x), & \text{если } y = \mathbf{0}, \\ f(x, y) & \text{иначе.} \end{cases}$$

Получившаяся функция сбалансирована, а её коэффициенты Уолша — Адамара вычисляются по формуле

$$W_\Theta(a, b) = \begin{cases} 0, & \text{если } a = \mathbf{0}, \\ W_f(a, b) + W_\theta(a) & \text{иначе.} \end{cases}$$

Спектральный радиус функции Θ выражается через спектральный радиус θ:

$$R_\Theta = 2^n + R_\theta.$$

Это позволяет оценить минимальный возможный спектральный радиус сбалансированной функции от $2n$ переменных через спектральный радиус сбалансированной функции от n переменных:

$$RB(2n) \leqslant 2^n + RB(n).$$

Здесь $RB(n) = \min\{R_f \mid f\colon \mathbb{F}_2^n \to \mathbb{F}_2,\ f - \text{сбалансированная}\}$. В [15] также была сформулирована не опровергнутая до сих пор гипотеза о несуществовании сбалансированных функций с нелинейностью выше, чем можно получить при помощи этой конструкции.

3. Обобщение конструкции Доббертина

Мы рассматриваем обобщение конструкции Доббертина, использующее функции с близкими к нормальности свойствами, а именно бент-функции от $2n$ переменных, принимающие постоянное значение на 2^{2k} сдвигах некоторого подпространства L размерности $n-k$, здесь $0 \leqslant k \leqslant n-2$. Так как аффинная эквивалентность сохраняет нелинейность и сбалансированность, можем без ограничения общности рассматривать такую бент-функцию в виде $f\colon \mathbb{F}_2^{n-k} \times \mathbb{F}_2^{n+k} \to \mathbb{F}_2$, для которого существуют подмножества $I_0, I_1 \subset \mathbb{F}_2^{n+k}$ мощностей $|I_0| = 2^{2k-1} + 2^{k-1}$, $|I_1| = 2^{2k-1} - 2^{k-1}$, для которых справедливо

$$f(x,y) = \begin{cases} 0 & \text{при } y \in I_0, \\ 1 & \text{при } y \in I_1. \end{cases} \tag{1}$$

Из [18, теорема 2.2] и [17, утверждение 7] известно, что тогда f сбалансирована при любом фиксированном $y \notin I_0 \cup I_1$. Отметим, что равенство $||I_0| - |I_1|| = 2^k$ легко следует из максимальной нелинейности бент-функций, а при прибавлении к такой функции тождественной единицы получим бент-функцию, равную единице на $2^{2k-1} + 2^{k-1}$ сдвигах L и нулю на $2^{2k-1} - 2^{k-1}$ сдвигах. Все приведённые далее утверждения для функций вида (1) верны и для их отрицания.

Представление (1) напрямую связано с конструкцией вида $\widetilde{f} + \mathrm{Ind}_{L^\perp}$ [17–19].

В [20] описано представление бент-функций в виде линейного разветвления:

$$f(x,y) = \langle \Phi(y), x \rangle + \psi(y).$$

Необходимым условием для того, чтобы f была бент-функцией, является следующее условие на функцию $\Phi\colon \mathbb{F}_2^{n+k} \to \mathbb{F}_2^{n-k}$:

$$|\Phi^{-1}(\alpha)| = 2^{2k} \quad \text{для любого } \alpha \in \mathbb{F}_2^{n-k},$$

т. е. f должна быть постоянна ровно на 2^{2k} различных сдвигах $L = \{(x, \mathbf{0}) \mid x \in \mathbb{F}_2^{n-k}\}$. Любая такая функция имеет вид (1).

Используя бент-функцию $f(x,y)$, имеющую представление (1), и набор из 2^{2k} произвольных сбалансированных функций $\theta_y\colon \mathbb{F}_2^{n-k} \to \mathbb{F}_2$, можно построить сбалансированную функцию $\Theta\colon \mathbb{F}_2^{n-k} \times \mathbb{F}_2^{n+k} \to \mathbb{F}_2$,

имеющую конструкцию, подобную конструкции высоконелинейных сбалансированных функций Доббертина:

$$\Theta(x,y)=\begin{cases}\theta_y(x) & \text{при } y\in I_0\cup I_1,\\ f(x,y) & \text{иначе.}\end{cases}$$

Несложно заметить, что при $k=0$ описанная конструкция полностью совпадает с конструкцией Доббертина.

4. Свойства спектра Уолша — Адамара используемых бент-функций

Установим несколько полезных свойств спектра Уолша — Адамара функций вида (1).

Лемма 1. *Пусть f — функция вида* (1). *Тогда для любого $b\in\mathbb{F}_2^{n+k}$ выполнено*

$$W_f(\mathbf{0},b)=2^{n-k}\Big(\sum_{y\in I_0}(-1)^{\langle b,y\rangle}-\sum_{y\in I_1}(-1)^{\langle b,y\rangle}\Big).$$

Доказательство.

$$W_f(\mathbf{0},b)=\sum_{x\in\mathbb{F}_2^{n-k}}\sum_{y\in\mathbb{F}_2^{n+k}}(-1)^{f(x,y)+\langle b,y\rangle}$$

$$=\sum_{y\in\mathbb{F}_2^{n+k}}(-1)^{\langle b,y\rangle}\Big(\sum_{x\in\mathbb{F}_2^{n-k}}(-1)^{f(x,y)}\Big)$$

$$=\sum_{y\in I_0}(-1)^{\langle b,y\rangle}\Big(\sum_{x\in\mathbb{F}_2^{n-k}}(-1)^{f(x,y)}\Big)+\sum_{y\in I_1}(-1)^{\langle b,y\rangle}\Big(\sum_{x\in\mathbb{F}_2^{n-k}}(-1)^{f(x,y)}\Big)$$

$$+\sum_{y\notin I_0\cup I_1}(-1)^{\langle b,y\rangle}\Big(\sum_{x\in\mathbb{F}_2^{n-k}}(-1)^{f(x,y)}\Big)=\sum_{y\in I_0}(-1)^{\langle b,y\rangle}\cdot 2^{n-k}$$

$$-\sum_{y\in I_1}(-1)^{\langle b,y\rangle}\cdot 2^{n-k}+\sum_{y\notin I_0\cup I_1}(-1)^{\langle b,y\rangle}\Big(\sum_{x\in\mathbb{F}_2^{n-k}}(-1)^{f(x,y)}\Big).$$

Так как f сбалансирована при $y\notin I_0\cup I_1$, сумма $\sum\limits_x(-1)^{f(x,y)}$ в последнем слагаемом равна 0 для любого y. Лемма 1 доказана.

В общем случае поиск подходящих подмножеств I_0 и I_1, для которых f — бент-функция, может быть очень сложной задачей, поэтому интересным следствием леммы 1 является необходимый признак их выбора.

Следствие 1. *Для того чтобы функция вида* (1) *являлась бент-функцией, необходимо, чтобы для подмножеств* I_0 *и* I_1 *и любого* $b \in \mathbb{F}_2^{n+k}$ *было выполнено*

$$\left| \sum_{y \in I_0} (-1)^{\langle b, y_i \rangle} - \sum_{y \in I_1} (-1)^{\langle b, y_i \rangle} \right| = 2^k.$$

Лемма 2. *Пусть* f *— функция вида* (1). *Тогда для любых* $a \in \mathbb{F}_2^{n-k}$, $a \neq \mathbf{0}$, *и* $b \in \mathbb{F}_2^{n+k}$ *имеет место равенство*

$$W_f(a,b) = \sum_{x \in \mathbb{F}_2^{n-k}} \sum_{y \notin I_0 \cup I_1} (-1)^{f(x,y)+\langle a,x \rangle + \langle b,y \rangle}.$$

Доказательство.

$$W_f(a,b) = \sum_{x \in \mathbb{F}_2^{n-k}} \sum_{y \in I_0} (-1)^{f(x,y)+\langle a,x \rangle + \langle b,y \rangle}$$
$$+ \sum_{x \in \mathbb{F}_2^{n-k}} \sum_{y \in I_1} (-1)^{f(x,y)+\langle a,x \rangle + \langle b,y \rangle} + \sum_{x \in \mathbb{F}_2^{n-k}} \sum_{y \notin I_0 \cup I_1} (-1)^{f(x,y)+\langle a,x \rangle + \langle b,y \rangle}.$$

Преобразуя

$$\sum_{x \in \mathbb{F}_2^{n-k}} \sum_{y \in I_0} (-1)^{f(x,y)+\langle a,x \rangle + \langle b,y \rangle}$$
$$= \sum_{x \in \mathbb{F}_2^{n-k}} \sum_{y \in I_0} (-1)^{\langle a,x \rangle + \langle b,y \rangle} = \Big(\sum_{x \in \mathbb{F}_2^{n-k}} (-1)^{\langle a,x \rangle} \Big) \Big(\sum_{y \in I_0} (-1)^{\langle b,y \rangle} \Big),$$

получаем множитель $\sum\limits_{x \in \mathbb{F}_2^{n-k}} (-1)^{\langle a,x \rangle}$, равный 0. Аналогично можно показать, что

$$\sum_{x \in \mathbb{F}_2^{n-k}} \sum_{y \in I_1} (-1)^{f(x,y)+\langle a,x \rangle + \langle b,y \rangle} = 0.$$

Лемма 2 доказана.

Лемма 3. *Пусть* f *— функция вида* (1). *Тогда для любого* $a \in \mathbb{F}_2^{n-k}$, $a \neq \mathbf{0}$, *произведение* $W_f(a,b)W_f(\mathbf{0},b)$ *при различных значениях* $b \in \mathbb{F}_2^{n+k}$ *принимает как значение* 2^{2n}, *так и значение* -2^{2n}.

Доказательство. Воспользовавшись леммами 1 и 2, преобразуем сумму:

$$
\begin{aligned}
&2^{k-n}\sum_{b\in\mathbb{F}_2^{n+k}} W_f(a,b)\cdot W_f(\mathbf{0},b)\\
&=\sum_{b\in\mathbb{F}_2^{n+k}}\Bigg(\sum_{x\in\mathbb{F}_2^{n-k}}\sum_{y\notin I_0\cup I_1}(-1)^{f(x,y)+\langle a,x\rangle+\langle b,y\rangle}\Bigg)\Bigg(\sum_{z\in I_0}(-1)^{\langle b,z\rangle}-\sum_{z\in I_1}(-1)^{\langle b,z\rangle}\Bigg)\\
&\quad=\sum_{b\in\mathbb{F}_2^{n+k}}\Bigg(\sum_{x\in\mathbb{F}_2^{n-k}}\sum_{y\notin I_0\cup I_1}(-1)^{f(x,y)+\langle a,x\rangle+\langle b,y\rangle}\Bigg)\Bigg(\sum_{z\in I_0\cup I_1}(-1)^{f(x,z)+\langle b,z\rangle}\Bigg)\\
&\qquad=\sum_{b\in\mathbb{F}_2^{n+k}}\sum_{x\in\mathbb{F}_2^{n-k}}\sum_{y\notin I_0\cup I_1}\sum_{z\in I_0\cup I_1}(-1)^{f(x,y)+f(x,z)+\langle a,x\rangle+\langle b,y+z\rangle}\\
&\qquad=\sum_{x\in\mathbb{F}_2^{n-k}}\sum_{y\notin I_0\cup I_1}\sum_{z\in I_0\cup I_1}(-1)^{f(x,y)+f(x,z)+\langle a,x\rangle}\Bigg(\sum_{b\in\mathbb{F}_2^{n+k}}(-1)^{\langle b,y+z\rangle}\Bigg).
\end{aligned}
$$

Заметим, что $\sum\limits_{b\in\mathbb{F}_2^{n+k}}(-1)^{\langle b,y+z\rangle}=0$, так как $y\neq z$. Следовательно, сумма $\sum\limits_{b}W_f(a,b)W_f(\mathbf{0},b)$ равна 0, что возможно, только если произведения $W_f(a,b)W_f(\mathbf{0},b)$ меняют знак при изменении b. Лемма 3 доказана.

5. Свойства спектра Уолша — Адамара полученных сбалансированных функций

Теорема 1. *Функция, имеющая предложенную конструкцию, является сбалансированной функцией, и её коэффициенты Уолша — Адамара вычисляются по формуле*

$$
W_\Theta(a,b)=\begin{cases}W_f(a,b)+\sum\limits_{y\in I_0\cup I_1}(-1)^{\langle b,y\rangle}W_{\theta_y}(a), & \text{если } a\neq\mathbf{0},\\ 0 & \text{иначе.}\end{cases}
$$

Доказательство. Сбалансированность функции очевидна. Преобразуем её выражение для спектра Уолша — Адамара:

$$
\begin{aligned}
&W_\Theta(a,b)=\sum_{x\in\mathbb{F}_2^{n-k}}\sum_{y\in\mathbb{F}_2^{n+k}}(-1)^{\Theta(x,y)+\langle a,x\rangle+\langle b,y\rangle}\\
&=\sum_{y\in I_0\cup I_1}\sum_{x\in\mathbb{F}_2^{n-k}}(-1)^{\theta_y(x)+\langle a,x\rangle+\langle b,y\rangle}+\sum_{y\notin I_0\cup I_1}\sum_{x\in\mathbb{F}_2^{n-k}}(-1)^{f(x,y)+\langle a,x\rangle+\langle b,y\rangle}.
\end{aligned}
$$

Прибавим и отнимем $\sum\limits_{y\in I_0\cup I_1}\sum\limits_{x\in\mathbb{F}_2^{n-k}}(-1)^{f(x,y)+\langle a,x\rangle+\langle b,y\rangle}$ от последнего выражения. Тогда оно примет вид

$$\sum_{y\in I_0\cup I_1}(-1)^{\langle b,y\rangle}W_{\theta_y}(a)+W_f(a,b)$$
$$-\sum_{x\in\mathbb{F}_2^{n-k}}(-1)^{\langle a,x\rangle}\Big(\sum_{y\in I_0}(-1)^{\langle b,y\rangle}-\sum_{y\in I_1}(-1)^{\langle b,y\rangle}\Big).$$

Так как $\sum\limits_{x\in\mathbb{F}_2^{n-k}}(-1)^{\langle a,x\rangle}=0$ при $a\neq\mathbf{0}$ и $W_{\theta_y}(\mathbf{0})=0$, то

$$W_\Theta(a,b)=\begin{cases}W_f(a,b)+\sum\limits_{y\in I_0\cup I_1}(-1)^{\langle b,y\rangle}W_{\theta_y}(a), & \text{если } a\neq\mathbf{0},\\ W_f(\mathbf{0},b)-2^{n-k}\Big(\sum\limits_{y\in I_0}(-1)^{\langle a,x\rangle+\langle b,y\rangle}\\ \qquad\qquad -\sum\limits_{y\in I_1}(-1)^{\langle a,x\rangle+\langle b,y\rangle}\Big) & \text{иначе.}\end{cases}$$

По лемме 1

$$W_f(\mathbf{0},b)=2^{n-k}\Big(\sum_{y\in I_0}(-1)^{\langle a,x\rangle+\langle b,y\rangle}-\sum_{y\in I_1}(-1)^{\langle a,x\rangle+\langle b,y\rangle}\Big).$$

Следовательно, $W_\Theta(\mathbf{0},b)=0$. Теорема 1 доказана.

6. Оценки спектрального радиуса

Нас интересуют функции с высокой нелинейностью, а значит, с как можно более низким спектральным радиусом. Для функции, полученной при помощи конструкции Доббертина, $R_\Theta=2^n+R_\theta$. Из теоремы 1 вытекает следующее утверждение о спектральном радиусе функции, имеющей предложенную конструкцию.

Следствие 2. *Для спектрального радиуса Θ верна оценка*

$$R_\Theta\leqslant 2^n+\sum_{y\in I_0\cup I_1}R_{\theta_y};$$

при этом всегда можно выбрать θ_y, при которых оценка достигается.

Доказательство. Преобразуя выражение для коэффициентов Уолша — Адамара из теоремы 1, можно получить оценку

$$R_\Theta = \max_{a,b}\left|W_f(a,b) + \sum_{y\in I_0\cup I_1}(-1)^{\langle b,y\rangle}W_{\theta_y}(a)\right| \leqslant \max_{a,b}|W_f(a,b)| + \sum_{y\in I_0\cup I_1}\max_a|W_{\theta_i}(a)| = 2^n + \sum_{y\in I_0\cup I_1}R_{\theta_y}.$$

Так как f — бент-функция, все её коэффициенты Уолша — Адамара равны $\pm 2^n$. Зафиксируем некоторую сбалансированную функцию θ. Выберем $a = \widetilde{a}$, для которого $|W_\theta(\widetilde{a})| = \max_a(|W_\theta(a)|) = R_\theta$. Тогда, положив все θ_y равными θ, получим

$$W_\Theta(\widetilde{a},\mathbf{0}) = W_f(\widetilde{a},\mathbf{0}) + \sum_{y\in I_0\cup I_1}W_\theta(\widetilde{a}) = W_\theta(\widetilde{a}) + 2^{2k}W_\theta(\widetilde{a}),$$

а взяв все $\theta_y = \theta + 1$, аналогично получим $W_\Theta(\widetilde{a},\mathbf{0}) = W_\theta(\widetilde{a}) - 2^{2k}W_\theta(\widetilde{a})$. Независимо от знаков $W_\theta(\widetilde{a})$ и $W_\Theta(\widetilde{a},\mathbf{0})$ в одном из этих случаев знаки перед коэффициентами одинаковы и в неравенстве

$$R_\Theta \leqslant 2^n + \sum_{y\in I_0\cup I_1}R_{\theta_y}$$

достигается равенство. Следствие 2 доказано.

Возникает вопрос: можно ли более «удачным» выбором θ_y гарантировать спектральный радиус меньше, чем в худшем случае?

Теорема 2. *Пусть θ — сбалансированная функция от $n-k$ переменных, $\theta_y = \theta$ при $y \in I_0$ и $\theta_y = \theta \oplus 1$ при $y \in I_1$. Тогда $R_\Theta = 2^n + 2^k R_\theta$.*

Доказательство. Для такого выбора функций преобразуем коэффициенты Уолша — Адамара при $a \neq \mathbf{0}$:

$$W_\Theta(a,b) = W_f(a,b) + \sum_{y\in I_0}(-1)^{\langle b,y\rangle}W_\theta(a) + \sum_{y\in I_1}(-1)^{\langle b,y\rangle}(-W_\theta(a)) = W_f(a,b) + W_\theta(a)\Big(\sum_{y\in I_0}(-1)^{\langle b,y\rangle} - \sum_{y\in I_1}(-1)^{\langle b,y\rangle}\Big).$$

Тогда согласно лемме 1

$$W_\Theta(a,b) = W_f(a,b) + W_\theta(a)\cdot 2^{k-n}W_f(\mathbf{0},b).$$

По лемме 3 произведение $W_f(a,b)W_f(\mathbf{0},b)$ для фиксированного $a \neq \mathbf{0}$ меняет знак при изменении значений b. Следовательно, для каждого ненулевого a существует b, для которого $W_f(a,b)$ и $W_f(\mathbf{0},b)$ имеют как

одинаковые, так и разные знаки. Тогда вне зависимости от $W_\theta(a)$ спектральный радиус Θ равен

$$R_\Theta = \max_{a,b}\left|W_f(a,b) + \sum_{y\in I_0}(-1)^{\langle b,y\rangle}W_\theta(a) + \sum_{y\in I_1}(-1)^{\langle b,y\rangle}(-W_\theta(a))\right|$$
$$= \max_{a\neq\mathbf{0},b}|W_f(a,b) + W_\theta(a)\cdot 2^{k-n}W_f(0,b)| = 2^n + \max_{a\neq\mathbf{0}}|W_\theta(a)|\cdot 2^k.$$

Кроме того, $W_\theta(\mathbf{0}) = 0$, значит, максимум на нём достигаться не может, и спектральный радиус равен

$$R_\Theta = 2^n + 2^k\cdot R_\theta.$$

Теорема 2 доказана.

В работе [8] доказано, что

$$\lim_{m\to\infty}\frac{RB(m)}{2^{\frac{m}{2}}} = 1.$$

Взяв в качестве θ функцию с $R_\theta \approx 2^{\frac{n-k}{2}}$, получим, что спектральный радиус функции Θ из теоремы 2 выражается следующим образом:

$$R_\Theta \approx 2^n + 2^k\cdot 2^{\frac{n-k}{2}} = 2^n + 2^{\frac{n+k}{2}}.$$

Видно, что наилучший результат достигается при $k = 0$, т. е. в случае, описанном Доббертином.

Заключение

В работе построено обобщение конструкции Доббертина при помощи класса бент-функций с близкими к нормальности свойствами. Также были доказаны некоторые свойства спектра Уолша — Адамара для функций, принадлежащих этому классу, и найдена точная нижняя оценка их нелинейности. Однако максимальная возможная нелинейность для построенных таким образом функций остаётся неизвестной.

ЛИТЕРАТУРА

1. **Matsui M.** Linear cryptanalysis method for DES cipher // Advances in Cryptology — EUROCRYPT'93. Proc. Workshop Theory Appl. Cryptogr. Techniques (Lofthus, Norway, May 23–27, 1993). Heidelberg: Springer, 1994. P. 386–397. (Lect. Notes Comput. Sci.; Vol. 765).
2. **Rothaus O.** On «bent» functions // J. Comb. Theory, Ser. A. 1976. Vol. 20, No. 3. P. 300–305.
3. **Tokareva N. N.** Bent functions: Results and applications to cryptography. Amsterdam: Acad. Press, 2015. 220 p.
4. **Mesnager S.** Binary bent functions: Fundamentals and results. Heidelberg: Springer, 2016. 540 p.

5. **Carlet C.** Boolean functions for cryptography and error-correcting codes // Boolean Models and Methods in Mathematics, Computer Science, and Engineering. New York: Camb. Univ. Press, 2010. P. 257–397.
6. **Cusick T., Stanica P.** Cryptographic Boolean functions and applications. Amsterdam: Acad. Press, 2009. 248 p.
7. **Логачёв О. А., Сальников А. А., Смышляев С. В., Ященко В. В.** Булевы функции в теории кодирования и криптологии. М.: МЦНМО, 2012. 584 с.
8. **Schmidt K.** Asymptotically optimal Boolean functions // J. Comb. Theory, Ser. A. 2019. Vol. 164. P. 50–59.
9. **Seberry J., Zhang X., Zheng Y.** Nonlinearly balanced Boolean functions and their propagation characteristics // Advances in Cryptology — Crypto'93. Proc. 13th Annu. Int. Cryptology Conf. (Santa Barbara, CA, USA, Aug. 22–26, 1993). Heidelberg: Springer, 1994. P. 49–60. (Lect. Notes Comput. Sci.; Vol. 773).
10. **Carlet C.** On bent and highly nonlinear balanced/resilient functions and their algebraic immunities // Applied Algebra, Algebraic Algorithms and Error-Correcting Codes. Proc. 16th Int. Symp. (Las Vegas, NV, USA, Feb. 20–24, 2006). Heidelberg: Springer, 2006. P. 1–28. (Lect. Notes Comput. Sci.; Vol. 3857).
11. **Wang Q., Tan C. H.** Properties of a family of cryptographic Boolean functions // Sequences and Their Applications — SETA 2014. Proc. 8th Int. Conf. (Melbourne, Australia, Nov. 24–28, 2014). Cham: Springer, 2014. P. 34–46. (Lect. Notes Comput. Sci.; Vol. 8865).
12. **Tang D., Maitra S.** Construction of n-variable ($n \equiv 2 \mod 4$) balanced Boolean functions with maximum absolute value in autocorrelation spectra $< 2^{\frac{n}{2}}$ // IEEE Trans. Inf. Theory. 2018. Vol. 64, No. 1. P. 393–402.
13. **Kavut S., Maitra S., Tang D.** Construction and search of balanced Boolean functions on even number of variables towards excellent autocorrelation profile // Des. Codes Cryptogr. 2019. Vol. 87, No. 3. P. 261–276.
14. **Patterson N. J., Wiedemann D. H.** The covering radius of the $(2^{15}, 16)$ Reed–Muller code is at least 16276 // IEEE Trans. Inf. Theory. 1983. Vol. 29, No. 3. P. 354–356.
15. **Dobbertin H.** Construction of bent functions and balanced Boolean functions with high nonlinearity // Fast Software Encryption. Proc. 2nd Int. Workshop (Leuven, Belgium, Dec. 14–16, 1994). Heidelberg: Springer, 1995. P. 61–74. (Lect. Notes Comput. Sci.; Vol. 1008).
16. **Fomin D.** New classes of 8-bit permutations based on a butterfly structure // Math. Asp. Cryptogr. 2019. Vol. 10, No. 2. P. 169–180.
17. **Kolomeec N.** The graph of minimal distances of bent functions and its properties // Des. Codes Cryptogr. 2017. Vol. 85, No. 3. P. 395–410.
18. **Kolomeec N.** On properties of a bent function secondary construction // Abs. 5th Int. Workshop Boolean Functions and Their Applications (Loen, Norway, Sept. 15–17, 2020). P. 23–26. Available at `https://boolean.w.uib.no/files/2020/09/BFA_2020_abstracts_numbered.pdf` (accessed Apr. 28, 2021).

19. Carlet C. Two new classes of bent functions // Advances in Cryptology — EUROCRYPT'93. Proc. Workshop Theory Appl. Cryptogr. Techniques (Lofthus, Norway, May 23–27, 1993). Heidelberg: Springer, 1994. P. 77–101. (Lect. Notes Comput. Sci.; Vol. 765).

20. Ященко В. В. О критерии распространения для булевых функций и о бент-функциях // Пробл. передачи информации. 1997. Т. 33, вып. 1. С. 75–86.

Сутормин Иван Александрович

Статья поступила
1 декабря 2020 г.
После доработки —
12 марта 2021 г.
Принята к публикации
15 марта 2021 г.

DISKRETNYI ANALIZ I ISSLEDOVANIE OPERATSII
/DISCRETE ANALYSIS AND OPERATIONS RESEARCH/
July–September 2021. Vol. 28, No. 3. P. 49–64

UDC 519.8+518.25 DOI 10.33048/daio.2021.28.705

ON NONLINEARITY OF BOOLEAN FUNCTIONS GENERATED BY THE GENERALIZED DOBBERTIN CONSTRUCTION

I. A. Sutormin

Sobolev Institute of Mathematics,
4 Acad. Koptyug Avenue, 630090 Novosibirsk, Russia
E-mail: ivan.sutormin@gmail.com

Abstract. We propose a generalization of Dobbertin's 1995 construction for balanced highly nonlinear Boolean functions. The Walsh–Hadamard spectrum of the proposed functions is studied. An exact upper bound for the spectral radius (lower bound for nonlinearity) is achieved. We also introduce a method for constructing a balanced function of $2n$ variables and spectral radius $2^n + 2^k R$ using a balanced function of $n - k$ variables and spectral radius R. Bibliogr. 20.

Keywords: boolean function, bent function, nonlinearity, balancedness, spectral radius.

REFERENCES

1. **M. Matsui,** Linear cryptanalysis method for DES cipher, in *Advances in Cryptology — EUROCRYPT'93* (Proc. Workshop Theory Appl. Cryptogr. Techniques, Lofthus, Norway, May 23–27, 1993) (Springer, Heidelberg, 1994), pp. 386–397 (Lect. Notes Comput. Sci., Vol. 765).
2. **O. Rothaus,** On «bent» functions, *J. Comb. Theory, Ser. A*, **20** (3), 300–305 (1976).
3. **N. N. Tokareva,** *Bent Functions: Results and Applications to Cryptography* (Acad. Press, Amsterdam, 2015).
4. **S. Mesnager,** *Binary Bent Functions: Fundamentals and Results* (Springer, Heidelberg, 2016).
5. **C. Carlet,** Boolean functions for cryptography and error-correcting codes, in *Boolean Models and Methods in Mathematics, Computer Science, and Engineering* (Camb. Univ. Press, New York, 2010), pp. 257–397.

This research is carried out within the framework of the state contract of the Sobolev Institute of Mathematics (Project 0314–2019–0017), supported by the Russian Foundation for Basic Research (Project 20–31–70043) and Laboratory of Cryptography "JetBrains Research".

English version: Journal of Applied and Industrial Mathematics **15** (3) (2021).

6. **T. Cusick** and **P. Stanica,** *Cryptographic Boolean Functions and Applications* (Acad. Press, Amsterdam, 2009).
7. **O. A. Logachyov, A. A. Sal'nikov, S. V. Smyshlyaev,** and **V. V. Yashchenko,** *Boolean Functions in Coding Theory and Cryptology* (MTsNMO, Moscow, 2012) [Russian].
8. **K. Schmidt,** Asymptotically optimal Boolean functions, *J. Comb. Theory, Ser. A*, **164**, 50–59 (2019).
9. **J. Seberry, X. Zhang,** and **Y. Zheng,** Nonlinearly balanced Boolean functions and their propagation characteristics, in *Advances in Cryptology — Crypto'93* (Proc. 13th Annu. Int. Cryptology Conf., Santa Barbara, CA, USA, Aug. 22–26, 1993) (Springer, Heidelberg, 1994), pp. 49–60 (Lect. Notes Comput. Sci., Vol. 773).
10. **C. Carlet,** On bent and highly nonlinear balanced/resilient functions and their algebraic immunities, in *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes* (Proc. 16th Int. Symp., Las Vegas, NV, USA, Feb. 20–24, 2006) (Springer, Heidelberg, 2006), pp. 1–28 (Lect. Notes Comput. Sci., Vol. 3857).
11. **Q. Wang** and **C. H. Tan,** Properties of a family of cryptographic Boolean functions, in *Sequences and Their Applications — SETA 2014* (Proc. 8th Int. Conf., Melbourne, Australia, Nov. 24–28, 2014) (Springer, Cham, 2014), pp. 34–46 (Lect. Notes Comput. Sci., Vol. 8865).
12. **D. Tang** and **S. Maitra,** Construction of n-variable ($n \equiv 2 \mod 4$) balanced Boolean functions with maximum absolute value in autocorrelation spectra $< 2^{\frac{n}{2}}$, *IEEE Trans. Inf. Theory* **64** (1), 393–402 (2018).
13. **S. Kavut, S. Maitra,** and **D. Tang,** Construction and search of balanced Boolean functions on even number of variables towards excellent autocorrelation profile, *Des. Codes Cryptogr.* **87** (3), 261–276 (2019).
14. **N. J. Patterson** and **D. H. Wiedemann,** The covering radius of the $(2^{15}, 16)$ Reed–Muller code is at least 16276, *IEEE Trans. Inf. Theory* **29** (3), 354–356 (1983).
15. **H. Dobbertin,** Construction of bent functions and balanced Boolean functions with high nonlinearity, in *Fast Software Encryption* (Proc. 2nd Int. Workshop, Leuven, Belgium, Dec. 14–16, 1994) (Springer, Heidelberg, 1995), pp. 61–74 (Lect. Notes Comput. Sci., Vol. 1008).
16. **D. Fomin,** New classes of 8-bit permutations based on a butterfly structure, *Math. Asp. Cryptogr.* **10** (2), 169–180 (2019).
17. **N. Kolomeec,** The graph of minimal distances of bent functions and its properties, *Des. Codes Cryptogr.* **85** (3), 395–410 (2017).
18. **N. Kolomeec,** On properties of a bent function secondary construction, *Abs. 5th Int. Workshop Boolean Functions and Their Applications, Loen, Norway, Sept. 15–17, 2020*, pp. 23–26. Available at `boolean.w.uib.no/files/2020/09/BFA_2020_abstracts_numbered.pdf` (accessed Apr. 28, 2021).

19. C. Carlet, Two new classes of bent functions, in *Advances in Cryptology — EUROCRYPT'93* (Proc. Workshop Theory Appl. Cryptogr. Techniques, Lofthus, Norway, May 23–27, 1993) (Springer, Heidelberg, 1994), pp. 77–101 (Lect. Notes Comput. Sci., Vol. 765).

20. V. V. Yashchenko, On the propagation criterion for Boolean functions and on bent functions, *Probl. Peredachi Inf.* **33** (1), 62–71 (1997) [Russian] [*Probl. Inf. Transm.* **33** (1), 75–86 (1997)].

Ivan A. Sutormin

Received December 1, 2020
Revised March 12, 2021
Accepted March 15, 2021