О свойствах максимально нелинейных булевых функций от нечетного числа переменных

О. А. Логачев, С. Н. Федоров, В. В. Ященко

***Аннотация*—Булевы функции, являющиеся максимально нелинейными, то есть максимально удаленные в метрике Хэмминга от аффинных булевых функций, широко используются, например, при построении шифров, так как повышают их стойкость к некоторым методам криптоанализа. Класс максимально нелинейных булевых функций от *нечетного* числа переменных в настоящее время изучен довольно слабо. До сих пор отсутствуют какие-либо содержательные необходимые и достаточные условия принадлежности функции к этому классу. Исследования алгебраических, спектральных и комбинаторных свойств таких функций далеки от каких бы то ни было системных обобщений. В то же время в случае *четного* числа переменных ситуация гораздо более благоприятная. Исследования класса соответствующих булевых функций, называемых бент-функциями, весьма результативны. В частности, существует спектральная характеризация этого класса, известны собственно значение нелинейности и методы построения таких функций. Задача получения подобных знаний при нечетном числе переменных является несомненно важной для возможных приложений теории булевых функций.**

Данная работа имеет целью в некотором смысле восстановить равновесие и частично восполняет указанный пробел. Она посвящена разработке математического аппарата, необходимого для исследования данной задачи в геометрической интерпретации. Кроме того, в ней получены новые свойства спектральных коэффициентов, ряд свойств бент-функций переносится на случай нечетного числа переменных.

***Ключевые слова*—булева функция, максимально нелинейная булева функция, коэффициенты Уолша—Адамара, нелинейность, амплитуда, гиперсфера**

I. Введение

Булевы функции имеют многочисленные приложения, в том числе в теории кодирования и криптографии (см. монографию [1]). При этом функции с максимальным значением нелинейности — т. е. наиболее удаленные от аффинных в смысле расстояния Хэмминга — представляют особый интерес, так как обладают требуемыми во многих приложениях свойствами. В частности, поскольку некоторые методы криптоанализа, такие как линейный или дифференциальный, тем эффективнее, чем лучше используемые функции аппроксимируются аффинными, максимально нелинейные булевы функции крайне важны с точки зрения задачи построения шифров, стойких против данных методов.

Статья получена 20.11.2022.

Олег Алексеевич Логачев, институт проблем информатики Федерального исследовательского центра «Информатика и управление» Российской академии наук (email: ollog@inbox.ru).

Сергей Николаевич Федоров (email: s.n.feodorov@yandex.ru).

Валерий Владимирович Ященко, центр проблем информационной безопасности факультета ВМК МГУ имени М. В. Ломоносова (email: valery.yashchenko@yandex.ru).

При четном числе переменных такие функции в 1976 г. были названы бент-функциями [2], и с тех пор в большом количестве работ были доказаны разнообразные свойства бент-функций (см. обзорную монографию [3]). Нелинейность таких функций вычисляется легко, класс бент-функций имеет простую спектральную характеризацию (т. е. описывается заданием значений коэффициентов Уолша—Адамара), а также может быть определен через условие на производную функций. Для булевых функций от нечетного числа переменных ситуация совершенно иная. Известны значения максимальной нелинейности для числа переменных $n = 3, 5, 7$ (см. [4]). Известны также двусторонние неравенства для этого параметра (см. [5]) для $n \geqslant 9$. При этом неизвестна точная верхняя грань для нелинейности булевых функций при нечетных n, нет критериальных характеризаций максимально нелинейных функций в этом случае. Отсутствуют содержательно глубокие результаты, описывающие спектральные, алгебраические и комбинаторные свойства этих функций.

В настоящей статье ряд свойств бент-функций переносится на интересующий нас случай нечетного числа переменных. Для этого, в частности, используется «геометрический» подход, предложенный в [6]. Этот подход позволяет более эффективно оценивать некоторые параметры максимально нелинейных функций и получать новые методы нахождения таких функций. Отметим, что, говоря о нелинейности булевой функции, мы активно используем введенное в [7] понятие амплитуды булевой функции, которое связано с нелинейностью очень простым соотношением (см. (1) ниже), но при этом более удобно в наших рассуждениях.

II. Необходимые понятия и обозначения

Предварительно приведем нужные для дальнейшего элементы работ [6], [8], в которых разрабатывался геометрический подход к исследованию метрических свойств булевых функций.

Зафиксируем естественное упорядочение на пространстве двоичных векторов $V_n = \{0,1\}^n$ с операцией $\oplus$ покомпонентного сложения по модулю 2 и «скалярным произведением» $\langle \cdot, \cdot \rangle$: $\langle u, v \rangle = \bigoplus_{i=1}^{n} u_i v_i$. Рассмотрим множество $\mathcal{F}_n = \{f : V_n \to \{0,1\}\}$ всех булевых функций от n переменных, а также $W_f(u) = \sum_{x \in V_n} (-1)^{f(x) \oplus \langle u, x \rangle}$, $u \in V_n$, — коэффициенты Уолша—Адамара функции $f \in \mathcal{F}_n$. Множество $\mathcal{F}_n$ с помощью биекции $f \leftrightarrow W_f$ размещается на гиперсфере S^{m-1}, $m = 2^n$, в евклидовом пространстве $\mathbb{R}^m$:

$$S^{m-1} = \{X \in \mathbb{R}^m : \sum_{u \in V_n} X^2(u) = m^2 = 2^{2n}\},$$

где $X(u)$ — координаты вектора X, занумерованные элементами V_n. Последнее дает возможность называть точки X *псевдобулевыми функциями*. Мы далее будем говорить, что булева функция *соответствует* точке на гиперсфере, имея в виду данную биекцию. Более того, для краткости изложения точки гиперсферы будем отождествлять с соответствующими им булевыми функциями и говорить о «булевых функциях, лежащих на гиперсфере». Гиперсфера разбивается на 2^n (вообще говоря, пересекающихся) *сегментов* $C(\varphi) \subset S^{m-1}$, пронумерованных функциями $\varphi \in \mathcal{F}_n$:

$$C(\varphi) = \{X \in S^{m-1} : \forall u \in V_n \;\; X(u) = (-1)^{\varphi(u)}|X(u)|\}.$$

Также будем писать $f \in C(\varphi)$, имея в виду $W_f \in C(\varphi)$.

У каждого сегмента $C(\varphi)$ есть 2^n вершин $X_{\alpha,\varphi}$, $\alpha \in V_n$, — точек пересечения гиперсферы с осями координат:

$$X_{\alpha,\varphi}(u) = \begin{cases} (-1)^{\varphi(\alpha)} \cdot 2^n, & \text{если } u = \alpha, \\ 0 & \text{в противном случае.} \end{cases}$$

Вершина $X_{\alpha,\varphi}$ является образом аффинной функции $\langle \alpha, u\rangle \oplus \varphi(\alpha)$ при биекции $f \leftrightarrow W_f$.

Нелинейностью $\mathrm{nl_E}\, X$ точки $X \in S^{m-1}$ мы называем минимальное евклидово расстояние $\rho(X, X_{\alpha,\varphi})$ от точки X до точек $X_{\alpha,\varphi}$ по всем α и φ. В работе [8] доказано, что значение нелинейности всегда достигается в том же сегменте, в котором находится сама точка:

$$\mathrm{nl_E}\, X = \min_{\alpha \in V_n} \rho(X, X_{\alpha,\varphi}), \quad \text{если } X \in C(\varphi).$$

Там же показано, что понятие максимальной нелинейности точки сферы согласуется с максимальной нелинейностью булевой функции, соответствующей данной точке (если таковая существует).

В каждом сегменте $C(\varphi)$ выделяется его *полюс* — «центральная» точка:

$$\mathrm{pole}_\varphi(u) = (-1)^{\varphi(u)} \cdot 2^{\frac{n}{2}} \quad \text{по всем } u \in V_n.$$

Полюс соответствует некоторой булевой функции тогда и только тогда, когда φ — бент-функция (а n, соответственно, — четное число) [6].

Кривизной $\mathrm{curv}\, X$ произвольной точки (псевдобулевой функции) $X \in S^{m-1}$ назовем следующую величину:

$$\mathrm{curv}\, X = \sum_{u \in V_n} |X(u)|.$$

Все точки сегмента $C(\varphi)$ с кривизной d расположены на пересечении гиперсферы с гиперплоскостью, задаваемой уравнением $\sum_{u \in V_n} (-1)^{\varphi(u)} X(u) = d$. Если рассмотреть множество $M\Gamma_d = \{X \in \mathbb{R}^m : \sum_{i=1}^m |X_i| = d\}$, то при $d \leqslant 2^{n+\frac{n}{2}}$ пересечение $M\Gamma_d \cap S^{m-1}$ совпадает с множеством псевдобулевых функций (точек) кривизны d, а, в частности, при $d = 2^{n+\frac{n}{2}}$ — с множеством из 2^n полюсов сегментов.

III. Амплитуда булевой функции

Докажем два вспомогательных утверждения, представляющих самостоятельных интерес. Напомним еще некоторые понятия и обозначения из работ [6], [7], а также введем новые. Пусть $f, g \in \mathcal{F}_n$.

- $\mathrm{ampl}\, f = \max\limits_{u \in V_n} |W_f(u)|$ — *амплитуда* булевой функции f, известно, что
$$\mathrm{ampl}\, f + 2\,\mathrm{nl}\, f = 2^n; \tag{1}$$
- $\mathrm{dist}(f, g) = \big|\{u \in V_n : f(u) \neq g(u)\}\big|$ — *расстояние Хэмминга* между f и g;
- $\delta_z(x) = \begin{cases} 1, & \text{если } x = z, \\ 0 & \text{в противном случае;} \end{cases}$
- $g = \widetilde{f} \Leftrightarrow f \in C(g)$, т. е. $\widetilde{f}$ — номер сегмента, в котором лежит f;
- $\min^W f = \min\limits_{u \in V_n} |W_f(u)|$;
- $\mathcal{F}_n^0 = \{f \in \mathcal{F}_n : \min^W f = 0\}$, в работе [6] эти функции названы *граничными* (для сегментов), а функции из $\mathcal{F}_n \setminus \mathcal{F}_n^0$ — *внутренними* (для сегментов).

Замечание 1. В работе [6] множество $C(g) \setminus \mathcal{F}_n^0$, т. е. множество внутренних функций сегмента $C(g)$, названо *секцией* и рассмотрена проблема пустоты секций: для каких g выполнено $C(g) \subset \mathcal{F}_n^0$?

В частности, для сегментов $C(g)$ с номером — внутренней функцией g получены следующие результаты:

1) если $C(g) \setminus \mathcal{F}_n^0 \neq \varnothing$, тогда в этом сегменте $C(g)$ находится внутренняя функция, являющаяся номером того сегмента, в котором лежит g, в наших обозначениях имеем $\widetilde{g} \in C(g) \setminus \mathcal{F}_n^0$, и, кроме того,
$$\max_{f \in C(g)} \mathrm{curv}\, f = \mathrm{curv}\, \widetilde{g} = \mathrm{curv}\, g = \max_{f \in C(\widetilde{g})} \mathrm{curv}\, f,$$
при этом $\widetilde{\widetilde{g}} = g$ и для каждой $h \in \big(C(g) \cup C(\widetilde{g})\big) \setminus \big(\mathcal{F}_n^0 \cup \{g, \widetilde{g}\}\big)$ выполнено $C(h) \subset \mathcal{F}_n^0$;
2) если $C(g) \subset \mathcal{F}_n^0$, то $\widetilde{g} \in \mathcal{F}_n^0$, при этом для всех $h \in C(\widetilde{g}) \setminus \mathcal{F}_n^0$ выполнено $C(h) \subset \mathcal{F}_n^0$.

Лемма 1. *Для любой функции $f \in \mathcal{F}_n^0$ при нечетном n выполнено неравенство* $\mathrm{ampl}\, f \geqslant 2^{\frac{n+1}{2}}$.

Доказательство. Пусть $f \in \mathcal{F}_n^0$. Зафиксируем $u_0 \in V_n$, при котором $W_f(u_0) = 0$, и рассмотрим функцию $f'(x) = f(x) \oplus \langle u_0, x\rangle$. Очевидно, что f' уравновешена ($W_{f'}(u_0) = 0$) и $\mathrm{ampl}\, f = \mathrm{ampl}\, f'$. В соответствии с известным для уравновешенных функций от нечетного числа переменных результатом (см., например, [3, с. 63]) в терминах амплитуды имеем $\mathrm{ampl}\, f = \mathrm{ampl}\, f' \geqslant 2^{\frac{n+1}{2}}$. □

Лемма 2. *Для любой функции $f \in \mathcal{F}_n$ при нечетном n выполнены следующие соотношения:*

1) $\mathrm{dist}(f, \mathcal{F}_n^0) = \min\limits_{g \in \mathcal{F}_n^0} \mathrm{dist}(f, g) = \frac{1}{2}\min^W f$,
2) $\mathrm{ampl}\, f + \min^W f \geqslant 2^{\frac{n+1}{2}}$.

Доказательство. При $\min^W f = 0$ соотношения очевидно вытекают из леммы 1. Пусть теперь $\min^W f \geqslant 2$. В работе [6] показано: при условии $f,\ f \oplus \delta_z \in C(\widetilde{f})$, — что справедливо при $\min^W f \geqslant 2$, — выполняется равенство

$$|W_{f \oplus \delta_z}(u)| = |W_f(u)| - 2 \cdot (-1)^{\widetilde{f}(u) \oplus f(z) \oplus \langle u, z\rangle}. \tag{2}$$

Для каждого $u \in V_n$ найдется такой $z_1 \in V_n$, что $|W_{f \oplus \delta_{z_1}}(u)| = |W_f(u)| - 2$. Действительно, пусть это не так: для некоторого u_0 при всех z верно $\widetilde{f}(u_0) \oplus f(z) \oplus \langle u_0, z\rangle = 1$. Тогда $f(z) = \langle u_0, z\rangle \oplus \widetilde{f}(u_0) \oplus 1$, т. е. f — аффинная функция. Но это противоречит условию $\min^W f \geqslant 2$.

Находя далее таким же образом z_i, $2 \leqslant i \leqslant t = \frac{1}{2}\min^W f$, последовательно для тех u, на которых дости-

гается минимум $|W_{f\oplus\delta_{z_{i-1}}}|$, мы придем к функции со свойством

$$\min^W(f\oplus\bigoplus_{i=1}^{t}\delta_{z_i})=\min^W f-2t=0.$$

Таким образом, $f\oplus\bigoplus_{i=1}^{t}\delta_{z_i}\in\mathcal{F}_n^0$ и, очевидно, за меньшее, чем t, число таких элементарных изменений функции f достигнуть множества $\mathcal{F}_n^0$ невозможно. Поскольку при каждом элементарном изменении мы отдаляемся от f на расстояние 1 по Хэммингу, первое утверждение доказано.

При описанных преобразованиях на каждом шаге значение любого коэффициента Уолша—Адамара, согласно (2), меняется на $+2$ или -2, поэтому справедливы неравенства

$$\operatorname{ampl} f-2t\leqslant\operatorname{ampl}(f\oplus\bigoplus_{i=1}^{t}\delta_{z_i})\leqslant\operatorname{ampl} f+2t.$$

Поскольку $\operatorname{ampl}(f\oplus\bigoplus_{i=1}^{t}\delta_{z_i})\geqslant 2^{\frac{n+1}{2}}$ в силу леммы 1, получаем $\operatorname{ampl} f+\min^W f\geqslant 2^{\frac{n+1}{2}}$. □

Для удобства дальнейших рассуждений объединим в одно утверждение известные свойства множества булевых функций с «небольшой» амплитудой.

Теорема 1. *Множество* $\mathcal{F}_n^+=\{f\in\mathcal{F}_n:\operatorname{ampl} f<2^{\frac{n+1}{2}}\}$

1) *G-инвариантно, где $G=GA(n,2)\ltimes\mathcal{A}_n$ — расширение полной аффинной группы с помощью аддитивной группы $\mathcal{A}_n$ аффинных функций,*
2) *содержит все максимально нелинейные функции,*
3) *состоит только из внутренних функций, причем для любой функции $f\in\mathcal{F}_n^+$ при нечетном n выполнено неравенство* $\operatorname{ampl} f\geqslant 2^{\frac{n+1}{2}}-\min^W f$.
4) *обладает тем свойством, что для любой функции $g\in\mathcal{F}_n^+$, такой, что $C(g)\setminus\mathcal{F}_n^0\neq\varnothing$, функция $\widetilde{g}$ лежит в $C(g)\setminus\mathcal{F}_n^0$ и*

$$\operatorname{curv}\widetilde{g}=\max_{f\in C(g)}\operatorname{curv} f=\max_{f\in C(\widetilde{g})}\operatorname{curv} f=\operatorname{curv} g.$$

При этом $\widetilde{\widetilde{g}}=g$ и для всех $h\in\big(C(g)\cup C(\widetilde{g})\big)\setminus\big(\mathcal{F}_n^0\cup\{g,\widetilde{g}\}\big)$ выполнено $C(h)\subset\mathcal{F}_n^0$.

Доказательство. 1) Очевидно, поскольку $\operatorname{ampl} f$ является G-инвариантом (подробнее об этом см. [7]).

2) Свойство максимальной нелинейности эквивалентно обладанию минимальной амплитудой, при этом существуют булевы функции с амплитудой, меньшей, чем $2^{\frac{n+1}{2}}$ (для четных n это бент-функции, о построении таких примеров в нечетном случае см. [7]).

3) Вытекает из лемм 1 и 2.

4) Следует из результатов, изложенных в замечании 1, с применением пункта 3. □

Следствие 1. 1) *Для любой максимально нелинейной функции g, такой, что $C(g)\setminus\mathcal{F}_n^0\neq\varnothing$, функция $\widetilde{g}\in C(g)\setminus\mathcal{F}_n^0$ и*

$$\operatorname{curv}\widetilde{g}=\max_{f\in C(g)}\operatorname{curv} f=\max_{f\in C(\widetilde{g})}\operatorname{curv} f=\operatorname{curv} g.$$

При этом $\widetilde{\widetilde{g}}=g$ и для всех $h\in\big(C(g)\cup C(\widetilde{g})\big)\setminus\big(\mathcal{F}_n^0\cup\{g,\widetilde{g}\}\big)$ выполнено $C(h)\subset\mathcal{F}_n^0$.

2) *Для любой максимально нелинейной функции f выполнено неравенство*

$$\min^W f\geqslant 2^{\frac{n+1}{2}}-a_n,\quad\text{где } a_n=\min_{f\in\mathcal{F}_n}\operatorname{ampl} f.$$

IV. Оценка минимальной амплитуды

Рассмотрим теперь поведение при растущем нечетном n последовательности

$$\Theta_n=\frac{a_n}{2^{n/2}},\quad\text{где } a_n=\min_{f\in\mathcal{F}_n}\operatorname{ampl} f.$$

Теорема 2. *Последовательность Θ_n, n нечетно, обладает следующими свойствами:*

1) *Θ_n не возрастает, $\Theta_n\leqslant\Theta_k$ при любых $k\geqslant 1$, $n\geqslant k+2$;*
2) *$\Theta_n>1$ для всех n;*
3) *$\Theta_n=\sqrt{2}$ при $1\leqslant n\leqslant 7$ и $\Theta_n<\sqrt{2}$ при $n\geqslant 9$.*

Доказательство. 1) Рассмотрим следующую булеву функцию от n переменных:

$$g(x_1,\ldots,x_n)=\varphi(x_1,\ldots,x_{n-k})\oplus\psi(x_{n-k+1},\ldots,x_n),$$

где $\varphi\in\mathcal{F}_{n-k}$ — бент-функция, а $\psi\in\mathcal{F}_k$ — максимально нелинейная функция (т. е. имеющая минимальную амплитуду в $\mathcal{F}_k$). Тогда $\operatorname{ampl} g=2^{\frac{n-k}{2}}\operatorname{ampl}\psi=2^{\frac{n}{2}}\frac{\operatorname{ampl}\psi}{2^{k/2}}=2^{\frac{n}{2}}\Theta_k$. Поэтому $\Theta_k=\frac{\operatorname{ampl} g}{2^{n/2}}\geqslant\Theta_n$.

2) Достаточно заметить, что для любой функции $f\in\mathcal{F}_n$ выполнено неравенство $\operatorname{ampl} f\geqslant 2^{\frac{n}{2}}$, а в случае нечетного n неравенство, очевидно, строгое.

3) Из опубликованных результатов о максимальной нелинейности булевых функций от 5, 7, 9, 15 переменных (обзор публикаций приведен в [1, с. 292]) легко получить, что

$$\Theta_5=\Theta_7=\sqrt{2},\quad\Theta_9\leqslant\frac{7}{8}\sqrt{2},\quad\Theta_{15}\leqslant\frac{27}{32}\sqrt{2}.$$

Остается применить первое утверждение теоремы. □

Таким образом, по теореме Вейерштрасса об ограниченной монотонной последовательности, последовательность Θ_n (n нечетно) при $n\to\infty$ имеет предел, совпадающий с её точной нижней гранью.

V. Приближение максимально нелинейных функций

Введем в рассмотрение более общее понятие, чем «максимально нелинейная булева функция».

Определение 1. Для любого множества $M\subset\mathcal{F}_n$ через $O(M)$ обозначим следующее множество функций:

$$O(M)=\{f\in\mathcal{F}_n:\operatorname{dist}(f,M)=\max_{\varphi\in\mathcal{F}_n}\operatorname{dist}(\varphi,M)\}.$$

Функции из множества $O(M)$ максимально удалены от множества M, или, на языке теории кодирования, являются «глубокими дырами» для множества M (см., например, [1, гл. 5, 6]). Множество максимально нелинейных булевых функций — это в точности $O(\mathcal{A}_n)$, где, напомним, $\mathcal{A}_n$ — множество всех аффинных булевых функций от n переменных. Величина $r_M=\max_{\varphi\in\mathcal{F}_n}\operatorname{dist}(\varphi,M)$ называется *радиусом покрытия* множества M. Практически очевидно следующее утверждение.

Лемма 3. *Если $M_1\subset M_2\subset\mathcal{F}_n$, то $r_{M_1}\geqslant r_{M_2}$.*

Определение 2. Два множества $M_1,M_2\subset\mathcal{F}_n$ называются взаимно дуальными, если $O(M_1)=M_2$ и $O(M_2)=M_1$.

Очевидно, что при этом $r_{M_1}=r_{M_2}=\operatorname{dist}(M_1,M_2)$. Следуя монографии Токаревой [3], через $\operatorname{Aut} M$ обозначим группу автоморфизмов множества M, то есть группу

изометрических (сохраняющих хэммингово расстояние) преобразований пространства $\mathcal{F}_n$, оставляющих на месте множество M. Как показано в [3], при четных n множества аффинных функций $\mathcal{A}_n$ и бент-функций $\mathcal{B}_n$ взаимно дуальны и, как следствие,

$$\operatorname{Aut}\mathcal{A}_n = \operatorname{Aut}\mathcal{B}_n.$$

Замечание 2. В настоящее время неизвестно других пар взаимно дуальных множеств функций, кроме $\mathcal{A}_n$ и $\mathcal{B}_n$.

Равенство $\operatorname{Aut} M_1 = \operatorname{Aut} M_2$ для взаимно дуальных функций справедливо и в общем случае как следствие из следующего утверждения.

Лемма 4. *Для любого множества $M \subset \mathcal{F}_n$ справедливо включение* $\operatorname{Aut} M \leqslant \operatorname{Aut} O(M)$.

Доказательство. Возьмем произвольные $f \in O(M)$, $\Psi \in \operatorname{Aut} M$. Справедлива цепочка равенств

$$r_M = \operatorname{dist}(f, M) = \operatorname{dist}\big(\Psi(f), \Psi(M)\big) = \operatorname{dist}\big(\Psi(f), M\big).$$

Поэтому $\Psi(f) \in O(M)$, и таким образом получаем $\operatorname{Aut} M \leqslant \operatorname{Aut} O(M)$. □

Для полноты изложения приведем еще одно свойство максимально нелинейных функций, которое рассматривалось в [7]: любая максимально нелинейная функция $f \in \mathcal{F}_n$ является *локально максимально нелинейной* (в пределах хэммингова шара радиуса 1) в том смысле, что для нее выполнено условие $\operatorname{ampl} f \leqslant \min_{z \in V_n} \operatorname{ampl}(f \oplus \delta_z)$. Локальная максимальная нелинейность естественным образом исследуется с помощью упомянутого выше равенства (2), а также рассмотрения различных вариантов значений функции $\widetilde{f}(u) \oplus f(z) \oplus \langle u, z\rangle$ в зависимости от принадлежности $u \in V_n$ к множествам

$$M_f^1 = \{u \in V_n : |W_f(u)| = \operatorname{ampl} f\},$$
$$M_f^2 = \{u \in V_n : |W_f(u)| = \operatorname{ampl} f - 2\}.$$

При этом очевидно следующее утверждение.

Лемма 5. *Функция $f \in \mathcal{F}_n$ является локально максимально нелинейной тогда и только тогда, когда верно одно из следующих условий:*

1) *для любого $z \in V_n$ найдется такое $u_z \in M_f^1$, что выполнено равенство $\widetilde{f}(u_z) \oplus f(z) \oplus \langle u_z, z\rangle = 1$;*
2) *если для некоторого $z_0 \in V_n$ и всех $u \in M_f^1$ выполнено равенство $\widetilde{f}(u) \oplus f(z_0) \oplus \langle u, z_0\rangle = 0$, то найдется такое $u_0 \in M_f^2$, что справедливо равенство $\widetilde{f}(u_0) \oplus f(z_0) \oplus \langle u_0, z_0\rangle = 1$.*

VI. Заключение

В серии статей, к которой относится и настоящая, предложен «геометрический» подход к решению проблемы поиска и изучения максимально нелинейных функций от нечетного числа переменных. Этот подход представляется продуктивным в силу возможности посмотреть на задачу в другом ракурсе и привлечь дополнительный инструментарий.

При изучении вопроса о максимальной нелинейности рассмотрение булевых функций как точек на гиперсфере дает возможность локализовать максимально нелинейные функции и тем самым наметить путь к оценке их параметров и собственно нахождению таких функций. В данной статье приведены лишь некоторые результаты в этом направлении. Как представляется, дальнейшее развитие этих идей приведет к решению многих вопросов, связанных с поставленной задачей описания класса максимально нелинейных булевых функций от нечетного числа переменных.

Библиография

[1] Булевы функции в теории кодирования и криптологии / О. А. Логачев, А. А. Сальников, С. В. Смышляев, В. В. Ященко. — Москва : ЛЕНАНД, 2015.

[2] Rothaus O. S. On “bent” functions // Journal of Combinatorial Theory, Series A. — 1976. — Vol. 20, no. 3. — P. 300–305.

[3] Токарева Н. Н. Нелинейные булевы функции: бент-функции и их обобщения. — Saarbrücken (Germany) : Lambert Academic Publishing, 2011.

[4] Mykkeltveit J. J. The covering radius of the $(128, 8)$ Reed—Muller code is 56 // IEEE Transactions on Information Theory. — 1980. — Vol. IT-26, no. 3. — P. 359–362.

[5] Brualdi R. A., Litsyn S., Pless V. Covering radius // Handbook of Coding Theory, Volume 1 / Ed. by V. Pless, W. C. Huffman. — Amsterdam; New York : Elsevier Science, 1998. — P. 755–826.

[6] Логачев О. А., Федоров С. Н., Ященко В. В. Булевы функции как точки на гиперсфере в евклидовом пространстве // Дискретная математика. — 2018. — Т. 30, № 1. — С. 39–55.

[7] Логачев О. А., Федоров С. Н., Ященко В. В. О некоторых инвариантах действия расширения $GA(n, 2)$ на множестве булевых функций // Дискретная математика. — 2021. — Т. 33, № 2. — С. 66–85.

[8] Логачев О. А., Федоров С. Н., Ященко В. В. Псевдобулевы функции со значениями на гиперсфере // International Journal of Open Information Technologies. — 2022. — Т. 10, № 4. — С. 10–14.

On properties of maximally nonlinear functions of odd number of variables

Oleg A. Logachev, Sergei N. Fedorov, Valeriy V. Yashchenko

***Abstract*—Boolean functions that are maximally nonlinear, that is, having maximal Hamming distance from the set of affine Boolean functions, are widely used, for example, in the construction of ciphers, since they increase their security against certain cryptanalysis methods. By now, the class of maximally nonlinear Boolean functions of an *odd* number of variables is not sufficiently studied. There are still no meaningful necessary and sufficient conditions for a function to belong to this class. Studies of algebraic, spectral and combinatorial properties of such functions are far from any systematic generalizations. At the same time, in the case of an *even* number of variables, the situation is much more favorable. Studies of the class of corresponding Boolean functions, called bent functions, are very effective. In particular, there is a spectral characterization of this class, the actual value of nonlinearity and methods for constructing such functions are known. The task of obtaining similar knowledge for an odd number of variables is undoubtedly important for possible applications of the Boolean function theory.**

This work aims, in a sense, to restore balance and partially fills this gap. It is devoted to the development of the mathematical apparatus needed for the study of this problem in geometric interpretation. In addition, new properties of spectral coefficients are obtained in it, a number of properties of bent functions are transferred to the case of an odd number of variables.

***Keywords*—Boolean function, maximally nonlinear Boolean function, Walsh—Hadamard transform, nonlinearity, amplitude, hypersphere**

References

[1] Logachev O. A., Salnikov A. A., Yashchenko V. V. Boolean functions in coding theory and cryptography. Providence (Rhode Island, USA) : American Mathematical Society, 2011.

[2] Rothaus O. S. On “bent” functions // Journal of Combinatorial Theory, Series A. 1976. Vol. 20, no. 3. P. 300–305.

[3] Tokareva N. N. Bent functions : Results and applications to cryptography. Amsterdam : Academic Press, 2015.

[4] Mykkeltveit J. J. The covering radius of the (128, 8) Reed—Muller code is 56 // IEEE Transactions on Information Theory. 1980. Vol. IT-26, no. 3. P. 359–362.

[5] Brualdi R. A., Litsyn S., Pless V. Covering radius // Handbook of Coding Theory, Volume 1 / Ed. by V. Pless, W. C. Huffman. Amsterdam; New York : Elsevier Science, 1998. P. 755–826.

[6] Logachev O. A., Fedorov S. N., Yashchenko V. V. Boolean functions as points on the hypersphere in the Euclidean space // Discrete Mathematics and Applications. 2019. Vol. 29, no. 2. P. 89–101.

[7] Logachev O. A., Fedorov S. N., Yashchenko V. V. On some invariants under the action of an extension of $GA(n, 2)$ on the set of Boolean functions // Discrete Mathematics and Applications. 2022. Vol. 32, no. 3. P. 177–192.

[8] Logachev O. A., Fedorov S. N., Yashchenko V. V. Pseudo-Boolean functions valued on hypershere // International Journal of Open Information Technologies. 2022. Vol. 10, no. 4. P. 10–14. [in Russian].