Псевдобулевы функции со значениями на гиперсфере

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

***Аннотация*—Вещественнозначные функции от n булевых переменных (псевдобулевы функции) при фиксации некоторого упорядочения на области их определения могут быть отождествлены с векторами в евклидовом пространстве $\mathbb{R}^{2^n}$ размерности 2^n. С точки зрения теории булевых функций особый интерес представляют целозначные псевдобулевы функции, которые являются результатом применения преобразования Уолша—Адамара к булевым функциям, поскольку спектр Уолша—Адамара булевой функции однозначно характеризует ее. При представлении таких псевдобулевых функций точками евклидова пространства все они оказываются расположенными на (2^n-1)-мерной сфере радиуса 2^n.**

Ранее уже исследовалось отображение множества булевых функций от n переменных на гиперсферу в пространстве $\mathbb{R}^{2^n}$. Настоящая статья представляет попытку распространить полученные в этом контексте результаты на подмножество псевдобулевых функций, соответствующих точкам на данной гиперсфере. В частности, рассматриваются новые понятия кривизны и нелинейности применительно к таким псевдобулевым функциям, устанавливается соотношение между ними и выражение кривизны через метрические параметры описываемого геометрического представления псевдобулевых функций.

Одной из целей этого исследования является выработка подхода к оценке максимальной нелинейности булевых функций от нечетного числа переменных.

***Ключевые слова*—Гиперсфера, евклидово пространство, кривизна, нелинейность, псевдобулева функция, хэммингово расстояние**

I. Введение

В приложениях теории булевых функций большую роль играют числовые параметры, которые позволяют оценить «качество» и пригодность функции в той или иной сфере ее возможного применения. В частности, в криптографических приложениях немаловажное значение имеет нелинейность булевой функции — ее «непохожесть» на аффинные функции, которые легко обращаются и поэтому неприменимы в некоторых ситуациях. В том случае, когда количество переменных, от которых зависит функция, четно, наилучшие в этом смысле булевы функции вполне охарактеризованы: это так называемые бент-функции. Но при нечетном числе переменных вопрос об описании класса максимально нелинейных булевых функций и о значении максимальной нелинейности остается до сих пор открытым.

Крайне эффективным инструментом при исследовании свойств булевых функций является преобразование Уолша—Адамара — дискретное преобразование Фурье экспоненты булевой функции. Коэффициенты Уолша—Адамара задают целозначную функцию от тех же переменных, от которых зависела исходная булева функция, причем эта новая функция однозначно определяет исходную. Таким образом, каждой n-местной булевой функции (взаимно однозначно) соответствует некоторая псевдобулева функция, то есть вещественнозначная функция от n булевых переменных. Если зафиксировать некоторый порядок на области определения этих функций — множестве двоичных векторов мощности 2^n, — каждой псевдобулевой функции можно однозначно сопоставить точку (вектор) в вещественном линейном пространстве размерности 2^n. Отождествляя псевдобулевы функции с элементами евклидова пространства $\mathbb{R}^{2^n}$, мы можем реализовать геометрический подход к исследованию псевдобулевых функций с использованием понятий расстояния, скалярного произведения и т. д.

Поскольку нас интересуют псевдобулевы функции, соответствующие булевым по описанному выше принципу, мы знаем (благодаря известным соотношениям ортогональности для коэффициентов Уолша—Адамара), что их представляют точки евклидова пространства, расположенные на гиперсфере радиуса 2^n в пространстве $\mathbb{R}^{2^n}$. В работе [1] исследовалось такое отображение множества булевых функций на гиперсферу.

В настоящей статье предлагается рассматривать не только точки, представляющие булевы функции (точнее, спектр Уолша—Адамара этих функций), а все точки гиперсферы и соответствующие им псевдобулевы функции. При этом описываемый подход, реализуя в некоторым смысле метод расширения модели, как ожидается, даст дополнительные возможности для изучения свойств булевых функций и их параметров и, в частности, поможет в оценке максимальной нелинейности булевых функций от нечетного числа переменных.

Следуя этой идее, мы вводим новые понятия кривизны и нелинейности применительно к рассматриваемым псевдобулевым функциям — по аналогии с уже изучавшимися одноименными понятиями для булевых функций и, соответственно, для их преобразований Уолша—Адамара. С помощью геометрического подхода без особого труда удается выразить кривизну функции через определенные метрические характеристики, а также оценить снизу нелинейность булевой функции через ее кривизну.

Статья получена 18.03.2022.

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

Сергей Николаевич Федоров, центр проблем информационной безопасности ВМК МГУ имени М. В. Ломоносова (email: s.n.feodorov@yandex.ru).

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

II. Общие определения

Пусть $V_n = \mathbb{F}_2^n$ — n-мерное векторное пространство над полем $\mathbb{F}_2$, называемое *пространством Хэмминга*, с операцией $\oplus$ покомпонентного сложения по модулю 2 и *метрикой (расстоянием) Хэмминга*

$$\operatorname{dist}(u, v) = \operatorname{wt}(u \oplus v), \quad u, v \in V_n,$$

где $\operatorname{wt}(\cdot)$ — *вес Хэмминга* вектора — число его ненулевых компонент. Вектор из V_n, все компоненты которого нулевые, обозначим через 0^n.

Множество всех булевых функций от n переменных $\mathcal{F}_n = \{f : V_n \to \mathbb{F}_2\}$ тоже является пространством Хэмминга размерности $m = 2^n$ (и на нем определены метрика и вес Хэмминга) при представлении каждой функции вектором своих значений, записанных в некотором фиксированном порядке.

Рассмотрим обобщение понятия булевой функции. Компоненты (координаты) векторов евклидова пространства $\mathbb{R}^m$ занумеруем векторами из V_n, расположенными в лексикографическом порядке. Сопоставим произвольному вектору X из $\mathbb{R}^m$ функцию из V_n в $\mathbb{R}$, которая номер u координаты вектора X отображает в вещественное значение соответствующей компоненты $X(u)$ этого вектора. Другими словами, устанавливается естественное взаимно однозначное соответствие множеств $\mathbb{R}^m$ и $\operatorname{Fun}(V_n, \mathbb{R})$ сопоставлением каждой функции вектора ее значений. Функции из $\operatorname{Fun}(V_n, \mathbb{R})$ называются *псевдобулевыми*.

Скалярное произведение (X, Y) векторов $X, Y \in \mathbb{R}^m$ и (евклидово) *расстояние* $\rho(X, Y)$ между ними имеют стандартный вид:

$$(X, Y) = \sum_{u \in V_n} X(u)Y(u),$$

$$\rho(X, Y) = \sqrt{\sum_{u \in V_n} \big(X(u) - Y(u)\big)^2}.$$

Соответственно, те же понятия можно перенести и на псевдобулевы функции. Вообще, далее мы не будем делать различия между псевдобулевой функцией и точкой в $\mathbb{R}^m$.

На множестве булевых функций определено *преобразование Уолша—Адамара* (или коротко — *Уолша*)

$$W_f(u) = \sum_{x \in V_n} (-1)^{f(x) \oplus \langle u, x \rangle}, \quad u \in V_n,$$

для $f \in \mathcal{F}_n$, где $\langle u, x \rangle = u_1x_1 \oplus \ldots \oplus u_nx_n$. *Коэффициенты Уолша* $W_f(u)$, $u \in V_n$, задают целочисленную псевдобулеву функцию W_f, удовлетворяющую следующим *соотношениям ортогональности*:

$$\sum_{u \in V_n} W_f(u)W_f(u \oplus v) = \begin{cases} 0, & \text{если } v \neq 0^n, \\ 2^{2n}, & \text{если } v = 0^n. \end{cases}$$

III. Отображение функций на гиперсферу

В работе [1] для изучения метрических и спектральных свойств булевых функций множество $\mathcal{F}_n$ с помощью биекции $f \leftrightarrow W_f$ размещалось на гиперсфере S^{m-1} радиуса $m = 2^n$ в пространстве $\mathbb{R}^m$:

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

где $X(u)$, как уже отмечалось, рассматривается как координата вектора X с номером u или как значение соответствующей псевдобулевой функции.

Координатными гиперплоскостями сфера S^{m-1} разбивается на 2^n *сегментов* $C(g) \subset S^{m-1}$, пронумерованных булевыми функциями $g \in \mathcal{F}_n$:

$$C(g) = \big\{X \in S^{m-1} : X(u) = (-1)^{g(u)}|X(u)|,\ u \in V_n\big\}.$$

Подчеркнем, что в работе [1] использовалось понятие *секции* $S(g)$ гиперсферы S^{m-1}, состоящей из всех векторов сегмента $C(g)$ без нулевых координат (секция — сегмент без границы). Таким образом, различные секции не пересекаются, и каждый сегмент $C(g)$ является — в терминологии [1] — объединением своих *внутренних точек* (то есть точек секции $S(g)$) и *граничных точек*.

В [1] рассматривались некоторые характеристики точек $W_f \in C(g)$, связанные с приложениями булевых функций в теории кодирования и криптографии (обзор этих приложений см. в [2]). Рассмотрим эти характеристики для произвольных точек гиперсферы (не только для точек вида W_f при некоторой $f \in \mathcal{F}_n$). У каждого сегмента $C(g)$, $g \in \mathcal{F}_n$, есть 2^n *вершин* — точек пересечения гиперсферы с осями координат. Множество вершин сегмента $C(g)$ будем обозначать через

$$\mathcal{A}_{n,g} = \{X_{\alpha,g} : \alpha \in V_n\}, \quad \text{где}$$

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

Множество $\mathcal{A}_n = \bigcup_{g \in \mathcal{F}_n} \mathcal{A}_{n,g}$ является образом множества аффинных булевых функций при биекции $f \mapsto W_f$.

Нелинейностью $\operatorname{nl} X$ точки $X \in S^{m-1}$ (и соответствующей псевдобулевой функции) назовем — по аналогии с булевыми функциями — минимальное расстояние от X до $\mathcal{A}_n$:

$$\operatorname{nl} X = \min_{Y \in \mathcal{A}_n} \rho(X, Y).$$

Для булевых функций вместо евклидова расстояния в определении нелинейности берется расстояние Хэмминга до множества аффинных функций. Однако эта разница не влияет на результат сравнения нелинейностей различных булевых функций, представленных точками гиперсферы, поскольку справедливо следующее утверждение.

Лемма 1. *Для любых функций $f, f' \in \mathcal{F}_n$ справедливо соотношение*

$$\operatorname{dist}(f, f') = \frac{1}{4m}\rho^2(W_f, W_{f'}).$$

Доказательство. Пусть $h = f \oplus f'$. Как известно,

$$W_h(0^n) = \frac{1}{2^n} \sum_{u \in V_n} W_f(u)W_{f'}(u) = \frac{1}{2^n}(W_f, W_{f'}).$$

С другой стороны,

$$W_h(0^n) = 2^n - 2\operatorname{wt}(h) = 2^n - 2\operatorname{dist}(f, f').$$

Таким образом,

$$(W_f, W_{f'}) = 2^{2n} - 2^{n+1}\operatorname{dist}(f, f'). \tag{1}$$

Для любых $X, Y \in S^{m-1}$ справедлива следующая цепочка равенств:

$$\rho^2(X,Y) = \sum_{u\in V_n} (X(u)-Y(u))^2 = \\ = \sum_{u\in V_n} X^2(u) - 2\sum_{u\in V_n} X(u)Y(u) + \sum_{u\in V_n} Y^2(u) = \\ = 2^{2n+1} - 2(X,Y). \quad (2)$$

Сравнивая равенства (1) и (2) при $X = W_f$, $Y = W_{f'}$, получаем утверждение леммы. □

Лемма 1 позволяет при решении задач минимизации и максимизации хэммингова расстояния в $\mathcal{F}_n$ переходить к евклидову расстоянию между соответствующими точками гиперсферы и использовать геометрические соображения в евклидовом пространстве. Таким образом, в частности, максимальная удаленность от множества аффинных функций (максимальная нелинейность) булевой функции f равносильна тому, что нелинейность соответствующей псевдобулевой функции W_f максимальна среди всех $W_{f'}$, $f' \in \mathcal{F}_n$.

Псевдобулеву функцию $X \in S^{m-1}$ назовем *максимально нелинейной*, если выполнено соотношение

$$\operatorname{nl} X = \max_{Z\in S^{m-1}} \operatorname{nl} Z = \max_{Z\in S^{m-1}} \min_{Y\in\mathcal{A}_n} \rho(Z,Y).$$

В каждом сегменте $C(g)$ выделяется *полюс* — его «центральная» точка с координатами

$$\operatorname{pole}_g(u) = (-1)^{g(u)}2^{n/2}, \quad u \in V_n.$$

Полюс соответствует некоторой булевой функции тогда и только тогда, когда n четно, а g — бент-функция [1]. При этом функция, соответствующая полюсу, также является бент-функцией $\tilde{g}$, дуальной к функции g (подробнее о бент-функциях см. [2], [3]).

В работе [1] для булевых функций был рассмотрен параметр, названный кривизной: $\operatorname{curv} f = \sum_{u\in V_n} |W_f(u)|$ для $f \in \mathcal{F}_n$. Этот параметр характеризует, в частности, близость функции W_f к полюсу сегмента, к которому она относится. Распространим это понятие: для произвольной точки X на гиперсфере S^{m-1} — и соответствующей псевдобулевой функции — назовем ее *кривизной* величину

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

Очевидно, что для произвольного сегмента $C(g)$ и $X \in C(g)$ выполнены неравенства

$$2^n \leqslant \operatorname{curv} X \leqslant 2^{n+\frac{n}{2}}, \quad (3)$$

причем максимум достигается на полюсах, а минимум — на вершинах секций, то есть на множестве $\mathcal{A}_n$ (при этом, если говорить об образе множества булевых функций на сфере, то максимум достигается в случае бент-функций, а минимум — в случае аффинных функций).

IV. Основные результаты

Предварительно докажем одно вспомогательное утверждение для нелинейности псевдобулевых функций.

Лемма 2. *Для любого сегмента $C(g) \subset S^{m-1}$ и любой псевдобулевой функции $X \in C(g)$ выполнено*

$$\operatorname{nl} X = \min_{Y\in\mathcal{A}_n} \rho(X,Y) = \min_{Y\in\mathcal{A}_{n,g}} \rho(X,Y).$$

Доказательство. Для произвольного $\alpha \in V_n$ рассмотрим двумерную плоскость, натянутую на три точки X, $X_{\alpha,g}$, $X_{\alpha,g\oplus 1}$. Точки $X_{\alpha,g}$, $X_{\alpha,g\oplus 1}$ по определению лежат на одном диаметре сферы. Соответственно, сечение гиперсферы двумерной плоскостью, проходящей через данные три точки, дает окружность, описывающую треугольник $\triangle X X_{\alpha,g} X_{\alpha,g\oplus 1}$ так, что он опирается на диаметр этой окружности (см. рис. 1).

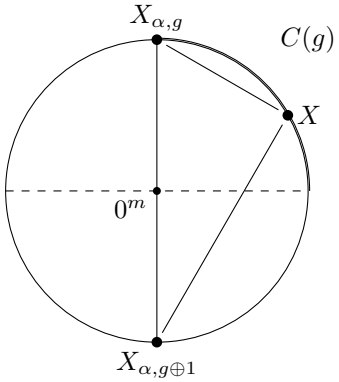

Рис. 1. Сечение гиперсферы двумерной плоскостью.

Таким образом, треугольник $\triangle X X_{\alpha,g} X_{\alpha,g\oplus 1}$ — прямоугольный, и так как X лежит в сегменте $C(g)$ и, значит, на четверти окружности, смежной с $X_{\alpha,g}$, то

$$\rho(X, X_{\alpha,g}) \leqslant \rho(X, X_{\alpha,g\oplus 1})$$

для любого вектора $\alpha \in V_n$. Остается только заметить, что $\mathcal{A}_n = \{X_{\alpha,g} : \alpha \in V_n\} \cup \{X_{\alpha,g\oplus 1} : \alpha \in V_n\}$. □

Рассмотрим теперь взаимные расстояния между псевдобулевыми функциями, расположенными в одном сегменте гиперсферы.

Теорема 1. *Для любой функции $g \in \mathcal{F}_n$ и произвольной пары псевдобулевых функций $X, Y \in C(g)$ выполнено равенство*

$$\sum_{u\in V_n} |X(u)|\cdot|Y(u)| = 2^{2n} - \frac{1}{2}\rho^2(X,Y).$$

Если, кроме того, $X = W_f$, $Y = W_{f'}$ для некоторых булевых функций $f, f' \in \mathcal{F}_n$, то имеет место равенство

$$\sum_{u\in V_n} |W_f(u)|\cdot|W_{f'}(u)| = 2^{2n} - 2^{n+1}\operatorname{dist}(f,f').$$

Доказательство. По условию знаки соответствующих координат X и Y не могут быть противоположными, поэтому из (2) получаем

$$\rho^2(X,Y) = 2^{2n+1} - 2\sum_{u\in V_n} |X(u)|\cdot|Y(u)|.$$

Аналогично, из (1) получается

$$2^n - 2\operatorname{dist}(f,f') = \frac{1}{2^n}\sum_{u\in V_n} |W_f(u)|\cdot|W_{f'}(u)|.$$

□

Подставляя в теореме 1 $Y = \operatorname{pole}_g$, приходим к следующему утверждению.

Следствие 1. *Для любой булевой функции $g \in \mathcal{F}_n$ и для любой псевдобулевой функции $X \in C(g)$ выполнено равенство*

$$\operatorname{curv} X = 2^{n+\frac{n}{2}} - \frac{1}{2^{1+\frac{n}{2}}}\rho^2(X, \operatorname{pole}_g).$$

Тем самым в сегменте $C(g)$ псевдобулева функция pole_g и только она находится на евклидовом расстоянии $\sqrt{2^{1+\frac{n}{2}}(2^{n+\frac{n}{2}} - d)}$ от всех псевдобулевых функций из $C(g)$, имеющих кривизну d.

С учетом неравенств (3) очевидно следующее утверждение.

Следствие 2. *Псевдобулевы функции pole_g при g, пробегающем $\mathcal{F}_n$, и только они являются максимально нелинейными с расстоянием от множества $\mathcal{A}_n$, равным $\sqrt{2^{1+\frac{n}{2}}(2^{n+\frac{n}{2}} - 2^n)}$.*

Для булевых функций аналогично следствию 1 получаем еще одно утверждение.

Следствие 3. *Пусть n четно, $g \in \mathcal{F}_n$ — бент-функция, а значит, $\operatorname{pole}_g = W_{\tilde{g}}$, где $\tilde{g}$ — дуальная к g бент-функция. Тогда для любой такой булевой функции $f \in \mathcal{F}_n$, что $W_f \in C(g)$, выполнено равенство*

$$\operatorname{curv} f = 2^{n+\frac{n}{2}} - 2^{1+\frac{n}{2}} \operatorname{dist}(f, \tilde{g}).$$

Тем самым бент-функции и только они находятся на хэмминговом расстоянии $\frac{1}{2^{1+\frac{n}{2}}}(2^{n+\frac{n}{2}} - d)$ от любой функции f из $\mathcal{F}_n$ с $W_f \in C(g)$ и $\operatorname{curv} f = d$.

Для булевых функций, в отличие от псевдобулевых, при нечетном числе переменных величина максимальной нелинейности в общем случае неизвестна. Результаты следствий 1 и 2 позволяют получить оценку снизу для нелинейности любой булевой функции через ее кривизну.

Теорема 2. *Для любой булевой функции $f \in \mathcal{F}_n$ справедливо неравенство*

$$\operatorname{nl} f \geqslant \frac{1}{2^{\frac{n}{2}+1}}\left(\sqrt{2^{n+\frac{n}{2}} - 2^n} - \sqrt{2^{n+\frac{n}{2}} - \operatorname{curv} f}\right)^2.$$

Доказательство. Возьмем g так, чтобы $W_f \in C(g)$, и пусть $\operatorname{nl} f = \operatorname{dist}(f, h)$, где h — подходящая аффинная функция из $\mathcal{F}_n$ (ближайшая по Хэммингу к f), причем $W_h = X_{\alpha,g}$ для некоторого $\alpha \in V_n$. Рассмотрим треугольник с вершинами pole_g, W_f, $X_{\alpha,g}$. В соответствии со следствиями 1 и 2 имеем

$$\rho(\operatorname{pole}_g, X_{\alpha,g}) = \sqrt{2^{\frac{n}{2}+1}(2^{n+\frac{n}{2}} - 2^n)},$$
$$\rho(\operatorname{pole}_g, W_f) = \sqrt{2^{\frac{n}{2}+1}(2^{n+\frac{n}{2}} - \operatorname{curv} f)}.$$

Воспользуемся неравенством треугольника

$$\rho(W_f, X_{\alpha,g}) \geqslant \rho(\operatorname{pole}_g, X_{\alpha,g}) - \rho(\operatorname{pole}_g, W_f)$$

и получим по лемме 1

$$\operatorname{nl} f = \operatorname{dist}(f, h) = \frac{1}{2^{n+2}}\rho^2(W_f, X_{\alpha,g}) \geqslant$$
$$\geqslant \frac{1}{2^{n+2}}\left(\sqrt{2^{\frac{n}{2}+1}(2^{n+\frac{n}{2}} - 2^n)} - \sqrt{2^{\frac{n}{2}+1}(2^{n+\frac{n}{2}} - \operatorname{curv} f)}\right)^2.$$

□

V. Заключение

В результате применения геометрического подхода к исследованию свойств булевых функций удается получить нижнюю оценку нелинейности булевой функции от произвольного числа переменных через ее кривизну, являющуюся по сути спектральным (в смысле преобразования Уолша—Адамара) параметром булевой функции. Вообще, кривизна псевдобулевых функций — точек гиперсферы предоставляет, как кажется, удобный инструмент для оценки нелинейности булевых функций, поскольку, с одной стороны, характеризует близость точек к полюсам сегментов этой гиперсферы, которым в случае четного n только и могут соответствовать максимально нелинейные булевы функции, а с другой стороны, выражается очень простым образом через коэффициенты Уолша—Адамара. Поэтому есть основания полагать, что дальнейшее изучение свойств описанного геометрического представления булевых и псевдобулевых функций поможет получить близкие к реальному значению оценки максимальной нелинейности и определить условия, при которых у булевой функции нелинейность достаточно высока.

Библиография

[1] 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.

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

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

Pseudo-Boolean functions valued on hypershere

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

***Abstract*—Fixing some ordering on the domain of real-valued functions of n Boolean variables (*i. e.* pseudo-Boolean functions) we can identify these functions (or rather tables of their values) with vectors in the Euclidean space $\mathbb{R}^{2^n}$ of dimension 2^n. From a perspective of the Boolean function theory the integer-valued pseudo-Boolean functions are of special interest. It is due to the fact that the Walsh–Hadamard transform of a Boolean function gives the integer-valued pseudo-Boolean function that identically corresponds to the Boolean function. If we represent such pseudo-Boolean functions by points of Euclidean space then all of them appear to be placed on the (2^n-1)-dimensional sphere with radius 2^n.**

Previously the mapping of the n-variables Boolean function set on the Euclidean hypersphere in $\mathbb{R}^{2^n}$ was already studied. This paper represents an attempt to extend the results obtained in those settings to the subset of pseudo-Boolean functions corresponding to the points on the hypersphere. In particular, we consider new concepts of curvature and nonlinearity of such pseudo-Boolean functions. We set relations between them and express curvature value via some metric parameters related to the described geometric representation of the pseudo-Boolean functions.

One of the aims of this investigation is to work out an approach to bounding maximum nonlinearity of Boolean functions with odd number of variables.

***Keywords*—Curvature, Euclidean space, Hamming distance, hypersphere, nonlinearity, pseudo-Boolean function**

References

[1] 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.

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

[3] Tokareva N. N. Nonlinear Boolean functions : bent functions and their generalizations. Saarbrücken (Germany) : LAMBERT Academic Publishing, 2011 [in Russian].