Транзитивные дифференцируемые функции составляют долю $1/p^n$ в множестве биективных дифференцируемых функций. По модулю p^2 все биективные, а соответственно и транзитивные дифференцируемые функции являются полиномиальными вследствие формул для числа биективных и транзитивных полиномиальных функций, приведённых в [2]. Однако производная дифференцируемой функции зависит от $n - 1$ первых координат x и при подъёме модуля в общем случае производная по большему модулю не зависит от производных по меньшему модулю, в то время как производная полиномиальной функции зависит только от первой координаты и при подъёме модуля не изменяется. Таким образом, по модулю p^n , $n > 2$, число транзитивных дифференцируемых функций больше, чем число транзитивных полиномиальных функций. Однако ещё не известно представлений для дифференцируемых функций, позволяющих эффективно вычислять их. Таким образом, появляется задача поиска таких представлений для функций класса D_n . Если такие представления будут найдены, то дифференцируемые функции могут быть использованы для генерации последовательностей элементов из $\mathbb{Z}_{p^n}$ по формуле (1).

ЛИТЕРАТУРА

1. Анашкин В. С. Равномерно распределённые последовательности целых p -адических чисел // Дискретная математика. 2002. № 14:4. С. 3–64.
2. Ларин М. В. Транзитивные полиномиальные преобразования колец вычетов // Дискретная математика. 2002. № 14:2. С. 20–32.

УДК 519.7

ВЕРХНЯЯ ОЦЕНКА ЧИСЛА БЕНТ-ФУНКЦИЙ НА РАССТОЯНИИ 2^k ОТ ПРОИЗВОЛЬНОЙ БЕНТ-ФУНКЦИИ ОТ $2k$ ПЕРЕМЕННЫХ¹

Н. А. Коломеец

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

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

Функция $f : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2$ называется *булевой функцией* от n переменных. Булева функция называется *аффинной*, если степень её алгебраической нормальной формы не превосходит 1, и *квадратичной*, если степень равна 2. Заметим, что любая аффинная функция от n переменных представима в виде $f(x) = \langle a, x \rangle \oplus c$, где $a \in \mathbb{Z}_2^n$; $c \in \mathbb{Z}_2$; $\langle a, x \rangle = a_1x_1 \oplus \dots \oplus a_nx_n$. *Расстояние* между двумя булевыми функциями от n переменных — расстояние Хэмминга между векторами их значений. *Бент-функция* — булева функция от чётного числа переменных, находящаяся на максимально возможном расстоянии от множества всех аффинных функций. Подробнее о бент-функциях можно узнать в работах [1, 2]. Множество $s \oplus D = \{s \oplus x : x \in D\}$ называется *сдвигом* множества $D \subseteq \mathbb{Z}_2^n$, $s \in \mathbb{Z}_2^n$. *Аффинное подпространство* $\mathbb{Z}_2^n$ — сдвиг некоторого линейного подпространства $\mathbb{Z}_2^n$. *Размерностью* аффинного подпространства называется размер-

¹Работа поддержана грантом НШ-1939.2014.1 Президента России для ведущих научных школ.

ность соответствующего линейного подпространства. Для краткости будем называть аффинное подпространство просто *подпространством*.

Булева функция f от n переменных *аффинна на подпространстве* $L \subseteq \mathbb{Z}_2^n$, если для некоторых $a \in \mathbb{Z}_2^n$ и $c \in \mathbb{Z}_2$ верно, что $f(x) = \langle a, x \rangle \oplus c$ для всех $x \in L$. Булева функция f называется *аффинно расщепляемой по подпространству* L , если она аффинна на всех сдвигах L . Аффинность булевых функций на подпространствах рассматривали М. Л. Буряков, О. А. Логачев, А. А. Сальников, С. В. Смышляев, В. В. Яценко [1, 3, 4], а также применительно к бент-функциям Х. Доббертин, К. Карле и П. Шарпин [5–7].

Введём следующее понятие.

Определение 1. Булева функция f от n переменных называется *полностью аффинно расщепляемой* порядка k , $2 \leq k \leq n$, если она аффинна хотя бы на одном подпространстве $\mathbb{Z}_2^n$ размерности k и аффинно расщепляема по всем подпространствам размерности k , на которых она аффинна.

Приведём примеры полностью аффинно расщепляемых функций.

Утверждение 1. Справедливы следующие утверждения:

(i) Любая квадратичная функция от n переменных является полностью аффинно расщепляемой порядка k при $2 \leq k \leq \lceil n/2 \rceil$.

(ii) Функция $g(x_1, \dots, x_n) = x_1x_2 \oplus x_3x_4 \oplus \dots \oplus x_{2n-2k-1}x_{2n-2k}$, где $\lceil n/2 \rceil \leq k < n$, является полностью аффинно расщепляемой порядка k .

(iii) Булева функция является полностью аффинно расщепляемой любого возможного порядка тогда и только тогда, когда она аффинная.

В работе [8] установлено, что все полностью аффинно расщепляемые функции порядка $\lceil n/2 \rceil$ являются аффинными или квадратичными (n — число переменных). В данной работе мы обобщаем этот результат.

Теорема 1. Пусть f — булева функция от n переменных и f полностью аффинно расщепляемая порядка k , $2 \leq k < n$. Тогда

(i) f либо аффинная, либо квадратичная;

(ii) если $k \geq \lceil n/2 \rceil$ и f не является полностью аффинно расщепляемой порядка $k+1$, то f аффинно эквивалентна функции $g(x_1, \dots, x_n) = x_1x_2 \oplus x_3x_4 \oplus \dots \oplus x_{2n-2k-1}x_{2n-2k}$.

Напомним, что две булевы функции f и g от n переменных называются *аффинно эквивалентными*, если существует невырожденная двоичная матрица A размера $n \times n$, вектор $b \in \mathbb{Z}_2^n$ и аффинная функция ℓ от n переменных, такие, что $f(x) = g(Ax \oplus b) \oplus \ell(x)$ для всех $x \in \mathbb{Z}_2^n$.

Известно [5], что если f — бент-функция от $2k$ переменных, L — подпространство $\mathbb{Z}_2^{2k}$ размерности k и f аффинна на L , то $f \oplus \text{Ind}_L$ также является бент-функцией, где Ind_L — характеристическая функция множества L . В работе [9] доказано, что все бент-функции на расстоянии 2^k от бент-функции f можно построить таким способом. Заметим также, что 2^k является минимальным возможным расстоянием между двумя бент-функциями от $2k$ переменных. Таким образом, подпространства размерности k , на которых бент-функция аффинна, представляют особый интерес.

В данной работе получена верхняя оценка числа бент-функций на расстоянии 2^k от произвольной бент-функции.

Теорема 2. Пусть f — произвольная бент-функция от $2k$ переменных. Тогда существует не более чем $2^k(2^1 + 1) \cdot \dots \cdot (2^k + 1)$ бент-функций на расстоянии 2^k от f . При этом оценка достигается, если и только если f — квадратичная бент-функция.

Достижимость оценки только на квадратичных бент-функциях следует из теоремы 1.

ЛИТЕРАТУРА

1. *Логачев О. А., Сальников А. А., Смышляев С. В., Яценко В. В.* Булевы функции в теории кодирования и криптологии. 2-е изд. М.: МЦНМО, 2012.
2. *Токарева Н. Н.* Нелинейные булевы функции: бент-функции и их обобщения. Saarbrücken: LAP LAMBERT Academic Publishing, 2011.
3. *Буряков М. Л.* Алгебраические, комбинаторные и криптографические свойства параметров аффинных ограничений булевых функций: дис. ... канд. физ.-мат. наук. М., 2007.
4. *Логачев О. А.* О значениях уровня аффинности для почти всех булевых функций // Прикладная дискретная математика. 2010. № 3. С. 17–21.
5. *Carlet C.* Two new classes of bent functions // EUROCRYPT'93. LNCS. 1994. V. 765. P. 77–101.
6. *Charpin P.* Normal Boolean functions // J. Complexity. 2004. V. 20. P. 245–265.
7. *Dobbertin H.* Construction of bent functions and balanced Boolean functions with high nonlinearity // LNCS. 1994. V. 1008. P. 61–74.
8. *Коломеец Н. А.* Об аффинности булевых функций на подпространствах и их сдвигах // Прикладная дискретная математика. Приложение. 2013. № 6. С. 15–16.
9. *Коломеец Н. А., Павлов А. В.* Свойство бент-функций, находящихся на минимальном расстоянии друг от друга // Прикладная дискретная математика. 2009. № 4. С. 5–20.

УДК 519.7

ОЦЕНКИ НЕЛИНЕЙНОСТИ ВЕКТОРНЫХ БУЛЕВЫХ ФУНКЦИЙ СПЕЦИАЛЬНОГО ВИДА

Е. П. Корсакова

Получена верхняя оценка нелинейности векторных булевых функций, построенных из аффинных булевых функций. Построен пример функций, на которых оценка достижима. Получена нижняя оценка числа векторных функций с фиксированной нелинейностью, построенных из уравновешенных булевых функций.

Ключевые слова: векторная булева функция, нелинейность, аффинная функция, уравновешенность.

Векторные булевы функции, используемые в криптографических приложениях, должны обладать рядом специальных свойств для обеспечения стойкости к известным видам криптоанализа и иметь относительно простую структуру [1–3]. Задачи совмещения различных свойств функции, а также оценки числа функций с выделенными свойствами являются сложными. Данная работа посвящена изучению нелинейности векторных булевых функций при относительно простом способе их построения и совмещению свойств нелинейности и уравновешенности.

Булевой функцией от n переменных называется функция, действующая из $\mathbb{Z}_2^n$ в $\mathbb{Z}_2$. Каждая булева функция однозначно задается своей *алгебраической нормальной формой* (АНФ), т. е. представляется в виде $f(x) = \left(\bigoplus_{k=1}^n \bigoplus_{i_1, \dots, i_k} a_{i_1, \dots, i_k} x_{i_1} \cdot \dots \cdot x_{i_k} \right) \oplus a_0$, где $\{i_1, \dots, i_k\} \subseteq \{1, \dots, n\}$ и $a_{i_1, \dots, i_k}, a_0 \in \mathbb{Z}_2$. *Степенью* $\deg f$ булевой функции f называется число переменных в самом длинном слагаемом её АНФ. Булева функция называется *аффинной*, если её степень не превосходит 1. Множество всех аффинных