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

ЛИТЕРАТУРА

1. *Логачев О. А., Сальников А. А., Смышляев С. В., Ященко 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. Saarbrucken: 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 $f(x) = \left(\bigoplus\limits_{k=1}^{n} \bigoplus\limits_{i_1,\ldots,i_k} a_{i_1,\ldots,i_k} x_{i_1} \cdot \ldots \cdot x_{i_k} \right) \oplus a_0$, где $\{i_1, \ldots, i_k\} \subseteq \{1, \ldots, n\}$ и $a_{i_1,\ldots,i_k},\ a_0 \in \mathbb{Z}_2$. *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

функций от n переменных обозначим через $\mathfrak{A}_n$. *Нелинейностью* булевой функции $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$ называется число $Nl(f) = \operatorname{dist}(f, \mathfrak{A}_n)$, где $\operatorname{dist}(\cdot,\cdot)$ — расстояние Хэмминга между булевыми функциями. *Векторной булевой функцией* называется функция вида $F : \mathbb{Z}_2^n \to \mathbb{Z}_2^m$. *Нелинейностью* векторной булевой функции $F : \mathbb{Z}_2^n \to \mathbb{Z}_2^m$, где $F = (f_1, f_2, \ldots, f_m)$, называется число $Nl(F) = \min\limits_{b \in \mathbb{Z}_2^{m*}} \operatorname{dist}\left(\bigoplus\limits_{i=1}^{n} b_i f_i, \mathfrak{A}_n\right)$.

Для нелинейности векторной булевой функции от n переменных имеется та же верхняя оценка, что и в случае обычной булевой функции: $Nl(F) \leqslant 2^{n-1} - 2^{n/2-1}$. При $m \geqslant n-1$ данная оценка была улучшена В. М. Сидельниковым [4].

Для класса векторных булевых функций, построенных из аффинных, найдена следующая оценка нелинейности.

Теорема 1. Пусть $F_1 = (f_{11}, \ldots, f_{1m})$ и $F_2 = (f_{21}, \ldots, f_{2m})$ — функции, действующие из $\mathbb{Z}_2^{n-1}$ в $\mathbb{Z}_2^m$, и f_{ij} — аффинные функции для всех $i = 1, 2$, $j \in \{1, \ldots, m\}$. Тогда для функции $F : \mathbb{Z}_2^n \to \mathbb{Z}_2^m$, определённой правилом $F(x, 0) = F_1(x)$, $F(x, 1) = F_2(x)$ для каждого $x \in \mathbb{Z}_2^{n-1}$, справедлива оценка $Nl(F) \leqslant 2^{n-2}$, причём при $m \leqslant n/2$ данная оценка достижима.

Пусть $(n-1, m)$-функция $F = (f_1, \ldots, f_m)$ с аффинными координатными функциями задаётся двоичной $(n \times m)$-матрицей $A(F) = (a_{ij})$, где a_{ij} получены из АНФ соответствующих функций $f_j(x_1, \ldots, x_{n-1}) = \bigoplus\limits_{i=1}^{n-1} a_{ij} x_i \oplus a_{nj}$. Тогда при $m \leqslant n/2$ оценка из теоремы 1 достижима на $(n-1, m)$-функциях с матрицами $A(F_1) = \begin{pmatrix} A \\ 0 \end{pmatrix}$, $A(F_2) = \begin{pmatrix} 0 \\ B \end{pmatrix}$, где A и B — $(m \times m)$-матрицы полного ранга.

Полученная в теореме 1 оценка нелинейности векторных булевых функций, построенных из аффинных булевых функций, слаба по сравнению с известными оценками, поскольку $\lim\limits_{n\to\infty} (2^{n-1} - 2^{(n-1)/2} - 2^{n-2}) = \infty$ и $\lim\limits_{n\to\infty} \dfrac{2^{n-1} - 2^{(n-1)/2}}{2^{n-2}} = 2$. То есть максимум нелинейности функций из описанного класса приблизительно в 2 раза меньше максимально возможного значения нелинейности. Это позволяет сделать вывод, что в данном классе нет функций с хорошими нелинейными свойствами.

Булева функция $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$ называется *уравновешенной*, если она принимает значения 0 и 1 одинаково часто. Рассмотрим множество векторных булевых функций $F : \mathbb{Z}_2^n \to \mathbb{Z}_2^n$, $F = (f_1, \ldots, f_n)$, для которых каждая f_i уравновешенная. Обозначим это множество Sb_n. Через $N(\ell, n)$ обозначим число векторных булевых функций от n переменных из класса Sb_n с нелинейностью равной ℓ. Для $N(\ell, n)$ имеет место следующая оценка.

Теорема 2. Если n и k удовлетворяют неравенству $k \leqslant 2^{n-2}/(n+2)$, то справедлива оценка

$$N(2k, n) \geqslant \binom{n}{2^n - 1} \binom{sn}{2^{n-1}} \binom{t}{2^{n-1} - sn}^n \frac{sn!}{(s!)^n},$$

где $s = \lceil k/2 \rceil$; $t = k - s$.

Приведём таблицу значений верхней границы оценки Сидельникова [4] для нелинейности (n, n)-функций при малых значениях n (табл. 1).

Для тех же значений n приведём таблицу нижних оценок числа (n, n)-функций с нелинейностью ℓ для подходящих параметров ℓ из теоремы 2 (табл. 2).

Таблица 1

n	5	6	7
Nl	12	26	56

Таблица 2

$\ell \setminus n$	5	6	7
2	2^{36}	2^{55}	2^{78}
4	–	2^{83}	2^{118}
6	–	–	2^{150}
$\geqslant 0$	2^{145}	2^{364}	2^{868}

Известно, что для нечётных n оценка Сидельникова точна на классе AB-функций, причём AB-функции существуют при всех нечётных n. Из табл. 2 видно, что оценка, полученная в теореме 2, применима только к значениям нелинейности, далёким от максимальных. Однако доказательство теоремы 2 конструктивно и может оказаться полезным, поскольку описывает метод построения функций с фиксированной нелинейностью.

ЛИТЕРАТУРА

1. *Логачев О. А., Сальников А. А., Смышляев С. В., Ященко В. В.* Булевы функции в теории кодирования и криптологии. 2-е изд. М.: МЦНМО, 2012. 584 с.
2. *Панкратова И. А.* Булевы функции в криптографии: учеб. пособие. Томск: Издательский Дом Томского государственного университета, 2014. 88 с.
3. *Carlet C.* Boolean functions for cryptography and error-correcting codes // Boolean Models and Methods in Mathematics, Computer Science, and Engeneering / eds. P. Hammer, Y. Crama. Cambridge Univ. Press, 2010. Ch. 8. P. 257–397. `www.math.univ-paris13.fr/~carlet/`
4. *Сидельников В. М.* О взаимной корреляции последовательностей // Проблемы кибернетики. 1971. Т. 24. С. 15–42.

УДК 510.53

ПРОБЛЕМА ДОСТИЖИМОСТИ В НЕПРЕРЫВНЫХ КУСОЧНО-АФФИННЫХ ОТОБРАЖЕНИЯХ ОКРУЖНОСТИ СТЕПЕНИ 2

А. Н. Курганский

На примере непрерывных кусочно-аффинных отображений окружности в себя степени два, для которых в работе доказывается алгоритмическая разрешимость проблемы достижимости из точки точки, обсуждаются некоторые алгоритмические аспекты моделирования дискретных систем непрерывными в контексте криптографического преобразования информации. Все такие кусочно-аффинные отображения топологически сопряжены с хаотическим отображением $E_2(x) = 2x \pmod 1 : \mathbb{R}/\mathbb{Z} \to \mathbb{R}/\mathbb{Z}$. Из доказательства основного результата работы следует, что любое другое непрерывное кусочно-аффинное отображение с рациональными коэффициентами и сопряжённое с E_2 показывает хаотическое поведение для некоторых рациональных чисел, что делает их интересными в задачах криптографического преобразования информации.