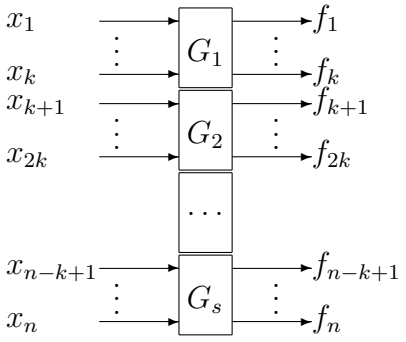

Рис. 1

$$M(F) = \begin{pmatrix} \overbrace{11\dots1}^{k} & 00\dots0 & \dots & 00\dots0 \\ \dots & \dots & \dots & \dots \\ 11\dots1 & 00\dots0 & \dots & 00\dots0 \\ 00\dots0 & 11\dots1 & \dots & 00\dots0 \\ \dots & \dots & \dots & \dots \\ 00\dots0 & 11\dots1 & \dots & 00\dots0 \\ \dots & \dots & \dots & \dots \\ 00\dots0 & 00\dots0 & \dots & 11\dots1 \\ \dots & \dots & \dots & \dots \\ 00\dots0 & 00\dots0 & \dots & 11\dots1 \end{pmatrix}.$$

Рис. 2

Видно, что $(M(F))^t = M(F)$ для всех $t \in \mathbb{N}$, поэтому

$$(i,j)\text{-}\exp M(F) = \begin{cases} 1, & \text{если } m_{ij} = 1, \\ \infty & \text{иначе,} \end{cases}$$

где $M(F) = (m_{ij})$. Для достижения перемешивающих свойств функции класса $P_{n,k}$ можно применять в качестве преобразований замены только в SP-сетях [2, с. 290], чередуя их с преобразованиями перестановки.

ЛИТЕРАТУРА

1. *Agibalov G. P.* Substitution block ciphers with functional keys // Прикладная дискретная математика. 2017. № 38. С. 57–65.
2. *Фомичев В. М.* Методы дискретной математики в криптологии. М.: Диалог-МИФИ, 2010. 424 с.
3. *Фомичев В. М.* Оценки экспонентов примитивных графов // Прикладная дискретная математика. 2011. № 2(12). С. 101–112.
4. *Фомичев В. М.* О характеристиках локально примитивных орграфов и матриц // Прикладная дискретная математика. Приложение. 2017. № 10. С. 96–99.
5. *Панкратова И. А.* Об обратимости векторных булевых функций // Прикладная дискретная математика. Приложение. 2015. № 8. С. 35–37.
6. *Pankratova I. A.* Construction of invertible vectorial Boolean functions with coordinates depending on given number of variables // Материалы Междунар. науч. конгресса по информатике: Информационные системы и технологии. Республика Беларусь, Минск, 24–27 окт. 2016. Минск: БГУ, 2016. С. 519–521.
7. *Кяжин С. Н., Фомичев В. М.* Локальная примитивность графов и неотрицательных матриц // Прикладная дискретная математика. 2014. № 3. С. 68–80.

УДК 519.7 DOI 10.17223/2226308X/12/14

О СВОЙСТВАХ БЕНТ-ФУНКЦИЙ, ПОСТРОЕННЫХ ПО НЕКОТОРОЙ БЕНТ-ФУНКЦИИ С ПОМОЩЬЮ ПОДПРОСТРАНСТВ

Н. А. Коломеец

Рассматриваются свойства конструкции $f \oplus \mathrm{Ind}_L$, где f — бент-функция от $2k$ переменных, а L — аффинное подпространство, при определённых условиях порождающей бент-функции. Доказано, что с помощью подпространств размерности $k+1$ конструкция порождает одинаковое число функций и по f, и по её дуальной

бент-функции. Приведён ряд экспериментальных результатов для бент-функций от 6 и 8 переменных, отражающих количество порождаемых конструкцией бент-функций, равенство и неравенство этого количества для бент-функции и её дуальной, а также отсутствие бент-функций при подпространствах некоторых размерностей. Усилена теорема 2018 г. о связи подпространств для бент-функций f и $f(x_1, \ldots, x_{2k}) \oplus x_{2k+1}x_{2k+2}$ в контексте рассматриваемой конструкции.

Ключевые слова: *булевы функции, бент-функции, подпространства, аффинность.*

Данная работа является продолжением исследований, начатых в [1]. Центральный объект исследований — *бент-функции* [2]. Это булевы функции от чётного числа переменных, обладающие максимальной возможной нелинейностью. В первую очередь они представляют интерес для криптографии. Подробную информацию об этом классе булевых функций можно найти в [3, 4].

Введём необходимые обозначения. Отображение вида $f : \mathbb{F}_2^n \to \mathbb{F}_2$ называется *булевой функцией* от n переменных. Пусть $\langle x, y\rangle = x_1y_1 \oplus \ldots \oplus x_ny_n$, где $x, y \in \mathbb{F}_2^n$. Обозначим через Ind_S характеристическую булеву функцию множества $S \subseteq \mathbb{F}_2^n$ и через $\mathcal{B}_{2k}$ — множество всех бент-функций от $2k$ переменных. Для любой бент-функции $f \in \mathcal{B}_{2k}$ существует дуальная к ней бент-функция $\widetilde{f} \in \mathcal{B}_{2k}$, определяемая знаками коэффициентов Уолша — Адамара функции f.

Как и в [1], в работе исследуются свойства конструкции бент-функций

$$f \oplus \mathrm{Ind}_L, \text{ где } f \in \mathcal{B}_{2k} \text{ и } L \subseteq \mathbb{F}_2^{2k} \text{ — аффинное подпространство.} \tag{1}$$

К. Карле [5] доказал критерий принадлежности $f \oplus \mathrm{Ind}_L$ множеству бент-функций $\mathcal{B}_{2k}$.

Обозначим через $C(f, m)$, где $f \in \mathcal{B}_{2k}$, множество всех бент-функций, порождаемых конструкцией (1) по функции f с помощью аффинных подпространств размерности m. Рассмотрим, как связаны мощности $C(f, m)$ и $C(\widetilde{f}, m)$. Во-первых, отметим, что при $m < k$ конструкция не может порождать бент-функции. Во-вторых, размерности $m = 2k$ и $2k - 1$ являются тривиальными, так как для подпространств таких размерностей конструкция порождает бент-функции при любой заданной начальной бент-функции, т. е.

$$|C(f, m)| = |C(\widetilde{f}, m)| \text{ при } m \in \{0, \ldots, k - 1, 2k - 1, 2k\}.$$

Таким образом, нетривиальными размерностями можно считать $m \in \{k, \ldots, 2k - 2\}$.

Из [5] известно взаимно-однозначное соответствие между функциями из $C(f, k)$ и $C(\widetilde{f}, k)$, таким образом, $|C(f, k)| = |C(\widetilde{f}, k)|$. Оказывается, аналогичное утверждение справедливо и для $m = k + 1$.

Теорема 1. Пусть $f \in \mathcal{B}_{2k}$. Тогда $|C(f, k + 1)| = |C(\widetilde{f}, k + 1)|$.

Приведём экспериментальные результаты с учётом известной аффинной классификации бент-функций. В табл. 1–4 для функции f указаны $|C(f, m)|$ и $|C(\widetilde{f}, m)|$ при $m \in \{k, \ldots, 2k - 2\}$ (или одно число, если эти мощности совпадают).

Для всех бент-функций из $\mathcal{B}_6$ количество функций в $C(\cdot, m)$ совпадает с $|C(f, m)|$ для некоторой f из табл. 1. Для всех бент-функций из $\mathcal{B}_8$ степени не выше 3 количество функций в $C(\cdot, m)$ совпадает с $|C(f, m)|$ для некоторой f из табл. 2. Начиная уже с 8 переменных, в $C(f, m)$ может не быть функций даже в нетривиальных случаях. Хорошо иллюстрируют это свойство мономиальные функции с показателем Касами (табл. 3).

Отметим, что для всех приведённых в табл. 1–3 функций $f \in \mathcal{B}_{2k}$ и всех m справедливо $|C(f,m)| = |C(\widetilde{f},m)|$. Напомним, что [5] и теорема 1 гарантируют это только при $m = k$ и $m = k+1$. Более того, в классе бент-функций Мэйорана — МакФарланда [6], начиная уже с 8 переменных, есть функции с $|C(f,6)| \neq |C(\widetilde{f},6)|$ (табл. 4).

Таблица 1

№ п/п	Функция f (6 переменных)	3	4
1	$x_1x_2 \oplus x_3x_4 \oplus x_5x_6$	1080	1260
2	$x_1x_2x_3 \oplus x_1x_4 \oplus x_2x_5 \oplus x_3x_6$	568	364
3	$x_1x_2x_3 \oplus x_2x_4x_5 \oplus x_1x_2 \oplus x_1x_4 \oplus x_2x_6 \oplus x_3x_5 \oplus x_4x_5$	440	140
4	$x_1x_2x_3 \oplus x_2x_4x_5 \oplus x_3x_4x_6 \oplus x_1x_4 \oplus x_2x_6 \oplus x_3x_4 \oplus x_3x_5 \oplus x_3x_6 \oplus x_4x_5 \oplus x_4x_6$	376	28

Таблица 2

№ п/п	Функция f (8 переменных)	4	5	6
1	$x_1x_2 \oplus x_3x_4 \oplus x_5x_6 \oplus x_7x_8$	36720	91800	21420
2	$x_1x_2x_3 \oplus x_1x_4 \oplus x_2x_5 \oplus x_3x_6 \oplus x_7x_8$	12144	16024	7084
3	$x_1x_2x_3 \oplus x_2x_4x_5 \oplus x_1x_7 \oplus x_2x_6 \oplus x_3x_4 \oplus x_5x_8$	6000	5272	3500
4	$x_1x_2x_3 \oplus x_2x_4x_5 \oplus x_1x_3 \oplus x_1x_5 \oplus x_2x_6 \oplus x_3x_4 \oplus x_7x_8$	6000	4760	3500
5	$x_1x_2x_7 \oplus x_3x_4x_7 \oplus x_5x_6x_7 \oplus x_1x_4 \oplus x_2x_5 \oplus x_3x_6 \oplus x_4x_5 \oplus x_7x_8$	4464	3096	2604
6	$x_1x_2x_3 \oplus x_2x_4x_5 \oplus x_3x_4x_6 \oplus x_1x_6 \oplus x_2x_7 \oplus x_3x_5 \oplus x_4x_8$	2928	1944	1708
7	$x_1x_2x_3 \oplus x_2x_4x_5 \oplus x_3x_4x_6 \oplus x_1x_7 \oplus x_2x_5 \oplus x_2x_6 \oplus x_3x_5 \oplus x_4x_8$	2928	1432	1708
8	$x_1x_2x_3 \oplus x_2x_4x_5 \oplus x_3x_4x_6 \oplus x_1x_3 \oplus x_1x_4 \oplus x_2x_7 \oplus x_3x_5 \oplus x_6x_8$	2928	1432	1708
9	$x_1x_2x_3 \oplus x_2x_4x_5 \oplus x_3x_4x_6 \oplus x_1x_2 \oplus x_1x_3 \oplus x_1x_4 \oplus x_2x_5 \oplus x_2x_6 \oplus \oplus x_3x_5 \oplus x_7x_8$	2928	1048	1708
10	$x_1x_2x_3 \oplus x_1x_4x_7 \oplus x_2x_4x_5 \oplus x_3x_4x_6 \oplus x_1x_5 \oplus x_1x_6 \oplus x_2x_7 \oplus x_3x_5 \oplus x_4x_8$	1392	792	812

Таблица 3

Функция f (8 переменных)	4	5	6
$\mathrm{tr}(\alpha x^{57})$, $x \in \mathbb{F}_{2^8}$, α — порождающий элемент $\mathbb{F}_{2^8}^*$	493	0	0

Таблица 4

Функция f (8 переменных)	4	5	6
$\langle x, \pi_1(y)\rangle \oplus \varphi_1(y)$, где $x, y \in \mathbb{F}_2^4$ и $\pi_1 = (9,10,4,3,5,7,11,13,12,14,2,15,1,6,8,0)$, $\varphi_1(y) = y_1y_2y_3 \oplus y_1y_3y_4 \oplus y_2y_3y_4 \oplus y_1y_3 \oplus y_2y_3 \oplus y_2y_4 \oplus y_1 \oplus y_3 \oplus y_4 \oplus 1$	1392	408	300/236

Усилим теорему 3 из [1]. Пусть $S \subseteq \mathbb{F}_2^{2k+2}$ и

$$\widehat{S} = \{x \in \mathbb{F}_2^{2k} : (x,a,b) \in S \text{ для некоторых } a,b \in \mathbb{F}_2\}, \quad F_{00}^{2k} = \{(x,0,0) : x \in \mathbb{F}_2^{2k}\}.$$

Теорема 2. Пусть для $g(x_1,\ldots,x_{2k+2}) = f(x_1,\ldots,x_{2k}) \oplus x_{2k+1}x_{2k+2} \in \mathcal{B}_{2k+2}$ верно $g \oplus \mathrm{Ind}_{a\oplus U} \in \mathcal{B}_{2k+2}$, где $U \subseteq \mathbb{F}_2^{2k+2}$ — линейное подпространство и $a \in \mathbb{F}_2^{2k+2}$. Тогда существует линейное подпространство $L \subseteq \mathbb{F}_2^{2k}$, такое, что

$$f \oplus \mathrm{Ind}_{b\oplus L} \in \mathcal{B}_{2k} \text{ для некоторого } b \in \mathbb{F}_2^{2k},$$

причём $\widehat{U \cap F_{00}^{2k}} \subseteq L \subseteq \widehat{U}$ и $\dim L < \dim U$.

Теорема 2 отличается от теоремы из [1] соотношением $\widehat{U \cap F_{00}^{2k}} \subseteq L \subseteq \widehat{U}$.

ЛИТЕРАТУРА

1. *Коломеец Н. А.* О некоторых свойствах конструкции бент-функций с помощью подпространств произвольной размерности // Прикладная дискретная математика. Приложение. 2018. № 11. С. 41–43.
2. *Rothaus O.* On bent functions // J. Combin. Theory. Ser. A. 1976. V. 20. No. 3. P. 300–305.
3. *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.
4. *Tokareva N. N.* Bent Functions, Results and Applications to Cryptography. Acad. Press. Elsevier, 2015.
5. *Carlet C.* Two new classes of bent functions // LNCS. 1994. V. 765. P. 77–101.
6. *McFarland R. L.* A family of difference sets in non-cyclic groups // J. Combin. Theory. Ser. A. 1973. V. 15. P. 1–10.

УДК 519.7 DOI 10.17223/2226308X/12/15

О КУБИЧЕСКОЙ ЧАСТИ АЛГЕБРАИЧЕСКОЙ НОРМАЛЬНОЙ ФОРМЫ ПРОИЗВОЛЬНОЙ БЕНТ-ФУНКЦИИ

Т. А. Кузьмина

Доказано, что кубическая часть бент-функции от n переменных не может быть произвольной при $n = 6, 8$.

Ключевые слова: *булева функция, бент-функция, линейная функция, квадратичная функция, кубическая функция, однородная функция.*

Булевы функции, максимально удалённые в метрике Хэмминга от множества всех аффинных функций, называются бент-функциями. Известно, что каждая булева функция может быть единственным образом представлена в её алгебраической нормальной форме (АНФ). Одна из проблем в области бент-функций: верно ли, что произвольная однородная булева функция степени k от n переменных (n чётное) является частью АНФ некоторой бент-функции от n переменных? Известно, что линейная часть в АНФ бент-функции может быть произвольной [1]. Доказано, что любая однородная квадратичная булева функция является квадратичной частью некоторой бент-функции [2].

В данной работе доказано, что при $n = 6, 8$ не каждую однородную кубическую булеву функцию можно достроить до бент-функции от n переменных. Для случая $n = 8$ лишь часть однородных кубических булевых функций может быть достроена до бент-функций от восьми переменных с помощью добавления однородных функций второй и/или четвёртой степеней.

Далее будем использовать индексные обозначения АНФ функции; например, 12+34 означает булеву функцию $x_1x_2 \oplus x_3x_4$.

Всего существует пять неэквивалентных кубических булевых форм от шести переменных [3], а именно: $123; 123+145; 123+456; 124+135+236; 123+124+135+236+456$.

Теорема 1. Для $n = 6$ функции $123; 123 + 145; 124 + 135 + 236$ можно дополнить до бент-функций с помощью добавления однородных квадратичных булевых функций от шести переменных; функции $123 + 456; 123 + 124 + 135 + 236 + 456$ нельзя дополнить до бент-функций от шести переменных.