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.

Существует 31 неэквивалентных кубических форм от восьми переменных [3]. В [4] приведена классификация форм четвёртой степени от восьми переменных, которые можно достроить до бент-функций [4], всего таких форм 536.

В таблице приведены результаты для кубических форм от восьми переменных. Во втором столбце представлена однородная кубическая форма, в третьем указано, можно ли достроить её до бент-функции, в четвёртом столбце — число k, показывающее, с помощью скольких форм четвёртой степени можно достроить кубические формы в том случае, если они достраиваются.

№	Однородная кубическая форма	Бент-функция	k
f_1	123	Достраивается	60
f_2	123+145	Достраивается	58
f_3	123+456	Не достраивается	–
f_4	124+135+236	Достраивается	38
f_5	123+124+135+236+456	Не достраивается	–
f_6	123+145+167	Достраивается	53
f_7	123+246+357	Достраивается	25
f_8	123+145+167+246	Достраивается	44
f_9	123+145+246+357	Не достраивается	–
f_{10}	123+124+135+236+456+167	Достраивается	42
f_{11}	123+145+167+246+357	Не достраивается	–
f_{12}	123+476+568	Не достраивается	–
f_{13}	123+145+167+568	Достраивается	17
f_{14}	123+246+357+568	Достраивается	24
f_{15}	123+246+357+128+138	Не достраивается	–
f_{16}	123+145+167+357+568	Не достраивается	–
f_{17}	123+145+478+568	Достраивается	46
f_{18}	123+124+135+236+456+167+258	Не достраивается	–
f_{19}	123+124+135+236+456+178	Не достраивается	–
f_{20}	123+145+246+357+568	Достраивается	12
f_{21}	123+145+246+467+578	Достраивается	11
f_{22}	123+145+357+478+568	Достраивается	43
f_{23}	123+246+357+478+568	Не достраивается	–
f_{24}	123+246+357+148+178+258	Не достраивается	–
f_{25}	123+145+167+246+357+568	Не достраивается	–
f_{26}	123+145+167+246+238+258+348	Не достраивается	–
f_{27}	123+145+167+258+268+378+468	Достраивается	34
f_{28}	123+145+246+357+238+678	Достраивается	29
f_{29}	123+145+246+357+478+568	Не достраивается	–
f_{30}	123+124+135+236+456+167+258+378	Не достраивается	–
f_{31}	123+156+246+256+147+157+357+348+258+458	Не достраивается	–

Теорема 2. Функции f_1, f_2, f_4, f_6, f_8 от восьми переменных можно дополнить до бент-функций с помощью добавления булевых функций второй степени от восьми переменных; остальные функции $f_3, f_5, f_7, f_9, f_{10}, \ldots, f_{31}$ нельзя дополнить до бент-функций таким образом.

Теорема 3. Функции $f_1, f_2, f_4, f_6, f_7, f_8, f_{10}, f_{13}, f_{14}, f_{17}, f_{20}, f_{21}, f_{22}, f_{27}, f_{28}$ от восьми переменных можно дополнить до бент-функций с помощью добавления слагаемых второй и четвёртой степеней от восьми переменных; остальные функции $f_3, f_5, f_9, f_{11}, f_{12}, f_{15}, f_{16}, f_{18}, f_{19}, f_{23}, f_{24}, f_{25}, f_{26}, f_{29}, f_{30}, f_{31}$ нельзя дополнить до бент-функций таким способом.

ЛИТЕРАТУРА

1. *Tokareva N.* Bent Functions: Results and Applications to Cryptography. Acad. Press. Elsevier, 2015.
2. *Tokareva N.* Algebraic Normal Form of a Bent Function: Properties and Restrictions. IACR Cryptology ePrint Archive. https://eprint.iacr.org/2018/1160.
3. *Черемушкин А. В.* Методы аффинной и линейной классификации булевых функций // Труды по дискретной математике. М.: Физматлит, 2001. Т. 4. С. 273–314.
4. *Langevin P.* Classification of Boolean Quartics Forms in Eight Variables. http://langevin.univ-tln.fr/project/quartics/quartics.html.

УДК 519.7 DOI 10.17223/2226308X/12/16

ИЗОМЕТРИЧНЫЕ ОТОБРАЖЕНИЯ МНОЖЕСТВА ВСЕХ БУЛЕВЫХ ФУНКЦИЙ В СЕБЯ, СОХРАНЯЮЩИЕ САМОДУАЛЬНОСТЬ И ОТНОШЕНИЕ РЭЛЕЯ[1]

А. В. Куценко

Изучаются изометричные отображения множества всех булевых функций от n переменных в себя. Получено полное описание изометричных отображений, сохраняющих самодуальность функций. Доказано, что каждое такое отображение сохраняет также антисамодуальность. Найдены все изометричные отображения, определяющие взаимно-однозначные соответствия между множествами самодуальных и антисамодуальных бент-функций. Получены все изометричные отображения, сохраняющие отношение Рэлея каждой булевой функции. Следствием данных результатов является полное описание всех изометричных отображений, сохраняющих максимальную нелинейность и расстояние Хэмминга между каждой бент-функцией и дуальной к ней.

Ключевые слова: *булева функция, изометричное отображение, самодуальная бент-функция, отношение Рэлея.*

Булевой функцией от n переменных называется любое отображение $f : \mathbb{F}_2^n \to \mathbb{F}_2$. *Скалярным произведением* $\langle x, y\rangle$ двух векторов $x = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_2^n$, $y = (y_1, y_2, \ldots, y_n) \in \mathbb{F}_2^n$ называется значение $\bigoplus\limits_{i=1}^{n} x_i y_i$. *Весом Хэмминга* $\mathrm{wt}(x)$ вектора $x \in \mathbb{F}_2^n$ называется количество единиц в нём. *Расстояние Хэмминга* $\mathrm{dist}(f, g)$ между булевыми функциями f, g от n переменных — число двоичных векторов длины n, на которых эти функции принимают различные значения. Через $\mathcal{O}_n$ обознается ортогональная группа $\mathcal{O}_n = \left\{L \in GL(n, 2) : LL^T = I_n\right\}$, где L^T — операция транспонирования L; I_n — единичная матрица порядка n над полем $\mathbb{F}_2$ [1]. *Преобразованием Уолша — Адамара* булевой функции f от n переменных называется целочисленная функция $W_f : \mathbb{F}_2^n \to \mathbb{Z}$, заданная равенством $W_f(y) = \sum\limits_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus \langle x, y\rangle}$, $y \in \mathbb{F}_2^n$.

Булева функция f от чётного числа переменных n называется *бент-функцией*, если $|W_f(y)| = 2^{n/2}$ для каждого $y \in \mathbb{F}_2^n$ [2]. Для множества бент-функций от n переменных используется обозначение $\mathcal{B}_n$. Для каждой $f \in \mathcal{B}_n$ однозначным образом определяется *дуальная* к ней бент-функция $\widetilde{f} \in \mathcal{B}_n$, значения которой находятся из соответствия $W_f(y) = (-1)^{\widetilde{f}(y)} 2^{n/2}$ для каждого $y \in \mathbb{F}_2^n$. Бент-функция f называется *самодуальной*

[1]Исследование выполнено при финансовой поддержке РФФИ (проекты №18-07-01394 и 18-31-00374).