веряем её на дифференциальную равномерность. Если S дифференциально 4-равномерная, то она может являться $(n-1)$-подфункцией некоторой взаимно однозначной APN-функции. Необходимо проверить, существует ли сбалансированная булева функция f, такая, что взаимно однозначная функция $H = S \cup f$ является APN-функцией. Заметим, что требуется проверить $2^{2^{n-1}}$ булевых функций, поскольку на каждую пару одинаковых значений 2-в-1 функции S приходится пара $\{0,1\}$ из значений булевой функции f.

Обозначим через $nf(S)$ число булевых функций f, таких, что $H = S \cup f$ является взаимно однозначной APN-функцией. Получена следующая нижняя оценка для данной величины:

Теорема 2. Пусть S — векторная функция из $\mathcal{T}_n$, построенная с помощью допустимой последовательности. Тогда если $nf(S) \neq 0$, то $nf(S) \geqslant 2^n$.

С помощью компьютерных вычислений проверено, что данная оценка является точной при $n = 3, 5$, а также при $n = 6$ для всех $(n-1)$-подфункций APN-функции Диллона.

ЛИТЕРАТУРА

1. *Nyberg K.* Differentily uniform mappings for cryptography // Eurocrypt 1993. LNCS. 1994. V. 765. P. 55–64.
2. *Глухов М. М.* О приближении дискретных функций линейными функциями // Математические вопросы криптографии. 2016. Т. 7. № 4. С. 29–50.
3. *Blondeau C. and Nyberg K.* Perfect nonlinear functions and cryptography // Fields and Their Appl. 2015. V. 32. P. 120–147.
4. *Тужилин М. Э.* Почти совершенные нелинейные функции // Прикладная дискретная математика. 2009. № 3(5). С. 14–20.
5. *Pott A.* Almost perfect and planar functions // Des. Codes Cryptography. 2016. No. 78(1). P. 141–195.
6. *Carlet C.* Open questions on nonlinearity and on APN functions // LNCS. 2015. V. 9061. P. 83–107.
7. *McQuistan M. T., Wolfe A. J., Browning K. A., and Dillon J. F.* An apn permutation in dimension six // Amer. Math. Soc. 2010. No. 518. P. 33–42.
8. *Idrisova V. A.* On an algorithm generating 2-to-1 APN functionsand its applications to "the big APN problem" // Cryptography and Communications. 2018. Published online.
9. *Идрисова В. А.* О построении APN-функций специального вида и их связи с взаимно однозначными APN-функциями // Прикладная дискретная математика. Приложение. 2017. № 10. С. 36–38.

УДК 519.7 DOI 10.17223/2226308X/11/12

О НЕКОТОРЫХ СВОЙСТВАХ КОНСТРУКЦИИ БЕНТ-ФУНКЦИЙ С ПОМОЩЬЮ ПОДПРОСТРАНСТВ ПРОИЗВОЛЬНОЙ РАЗМЕРНОСТИ[1]

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 порож-

[1]Работа поддержана грантом РФФИ, проект № 17-41-543364.

дающей бент-функции. Предложены необходимые и достаточные условия увеличения и уменьшения на 1 размерности подпространства L, при которых порождаемая функция тоже будет бент-функцией. Доказано, что если функция $f(x_1, \ldots, x_{2k}) \oplus x_{2k+1}x_{2k+2} \oplus \mathrm{Ind}_U$ является бент-функцией для некоторого аффинного подпространства U, то и $f \oplus \mathrm{Ind}_L$ является бент-функцией для некоторого L размерности $\dim U - 1$ или $\dim U - 2$. Приведён пример бент-функции от 10 переменных, по которой конструкция порождает бент-функции только при $\dim L \in \{9, 10\}$.

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

Бент-функции — булевы функции от чётного числа переменных, обладающие максимально возможной нелинейностью. Они представляют интерес в первую очередь для криптографии. Понятие бент-функции предложено О. Ротхаусом [1]. Подробную информацию об этом классе булевых функций можно найти в [2, 3].

Введем 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.

В работе исследуются свойства конструкции бент-функций по заданной бент-функции $f \in \mathcal{B}_{2k}$ и аффинному подпространству $L \subseteq \mathbb{F}_2^{2k}$, порождающей бент-функции вида $f \oplus \mathrm{Ind}_L$. Необходимое и достаточное условие принадлежности $f \oplus \mathrm{Ind}_L$ множеству бент-функций $\mathcal{B}_{2k}$ доказано К. Карле [4]. Заметим, что при $\dim L < k$ функция $f \oplus \mathrm{Ind}_L$ не может являться бент-функцией, а при $\dim L \geqslant 2k - 1$ конструкция тривиальна и порождает бент-функцию вне зависимости от выбранной бент-функции f и аффинного подпространства L.

Пусть $f \in \mathcal{B}_{2k}$ и для некоторого аффинного подпространства $L \subseteq \mathbb{F}_2^{2k}$ справедливо $f \oplus \mathrm{Ind}_L \in \mathcal{B}_{2k}$. Рассмотрим случаи, в которых можно построить бент-функцию по надпространству или подпространству L.

Теорема 1. Пусть $f \in \mathcal{B}_{2k}$ и $f \oplus \mathrm{Ind}_L \in \mathcal{B}_{2k}$, где $L \subseteq \mathbb{F}_{2k}$ — аффинное подпространство. Пусть $a \in \mathbb{F}_2^{2k}$. Тогда $f \oplus \mathrm{Ind}_{L\cup(a\oplus L)} \in \mathcal{B}_{2k}$ если и только если $f \oplus \mathrm{Ind}_{a\oplus L} \in \mathcal{B}_{2k}$.

Отметим, что в одну сторону утверждение теоремы легко следует, например, из критерия, доказанного в [4].

Следствие 1. Пусть $f \in \mathcal{B}_{2k}$ и $f \oplus \mathrm{Ind}_L \in \mathcal{B}_{2k}$, где $L \subseteq \mathbb{F}_{2k}$ — аффинное подпространство размерности $2k - 2$. Тогда $f \oplus \mathrm{Ind}_{a\oplus L} \in \mathcal{B}_{2k}$ при любом $a \in \mathbb{F}_{2k}$.

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

$$L_a = \{x \in L : \langle a, x\rangle = 0\}.$$

Тогда $f \oplus \mathrm{Ind}_{L_a} \in \mathcal{B}_{2k}$, если и только если для всех $y \in \mathbb{F}_2^{2k}$ справедливо

$$|\sum_{x\in L}(-1)^{f(x)\oplus\langle x,y\rangle}| = |\sum_{x\in L}(-1)^{f(x)\oplus\langle x,y\oplus a\rangle}|.$$

Замечание 1. При $\dim L = k+1$ всегда найдётся такое a, при котором $\dim L_a = k$ и выполнено равенство из условия теоремы 2.

Отметим, что у некоторых бент-функций существуют подпространства, которые нельзя «расширить» согласно теореме 1 и «сузить» согласно теореме 2. Например, такие подпространства есть у мономиальных бент-функций Касами от 8 переменных с показателем 57.

Заметим также, что по некоторым бент-функциям рассматриваемая конструкция порождает бент-функции только в тривиальных случаях.

Утверждение 1. Существует бент-функция $f \in \mathcal{B}_{10}$, для которой $f \oplus \mathrm{Ind}_L \notin \mathcal{B}_{10}$ для любого аффинного подпространства $L \subseteq \mathbb{F}_2^{10}$ размерности меньшей чем 9.

Утверждение 1 справедливо для функции, найденной в [5].

Известно, что если $f \in \mathcal{B}_{2k}$, то и $f(x_1, \ldots, x_{2k}) \oplus x_{2k+1}x_{2k+2} \in \mathcal{B}_{2k+2}$. Более того, в [6] доказано, что для $f \in \mathcal{B}_{2k}$ существует аффинное подпространство $L \subseteq \mathbb{F}_2^{2k}$ размерности k, такое, что $f \oplus \mathrm{Ind}_L \in \mathcal{B}_{2k}$, если и только если существует аффинное подпространство $U \subseteq \mathbb{F}_2^{2k+2}$ размерности $k+1$, такое, что $f(x_1, \ldots, x_{2k}) \oplus x_{2k+1}x_{2k+2} \oplus \mathrm{Ind}_U \in \mathcal{B}_{2k+2}$. Обобщим этот результат на подпространства произвольной размерности.

Лемма 1. Пусть $f \in \mathcal{B}_{2k}$ и $f \oplus \mathrm{Ind}_L \in \mathcal{B}_{2k}$ для некоторого аффинного подпространства $L \subseteq \mathbb{F}_2^{2k}$. Тогда для бент-функции $g(x_1, \ldots, x_{2k+2}) = f(x_1, \ldots, x_{2k}) \oplus x_{2k+1}x_{2k+2}$ справедливы следующие свойства:

1) $g(x) \oplus \mathrm{Ind}_{L'} \in \mathcal{B}_{2k+2}$, где $L' = \{(x', a, 0) : x' \in L, a \in \mathbb{F}_2\}$, т. е. $\dim L' = \dim L + 1$;
2) $g(x) \oplus \mathrm{Ind}_{L''} \in \mathcal{B}_{2k+2}$, где $L'' = \{(x', a, b) : x' \in L, a, b \in \mathbb{F}_2\}$, т. е. $\dim L'' = \dim L + 2$.

Теорема 3. Пусть для бент-функции $g(x_1, \ldots, x_{2k+2}) = f(x_1, \ldots, x_{2k}) \oplus x_{2k+1}x_{2k+2}$ верно $g \oplus \mathrm{Ind}_U \in \mathcal{B}_{2k+2}$, где $U \subseteq \mathbb{F}_2^{2k+2}$ — аффинное подпространство. Тогда существует аффинное подпространство $L \subseteq \mathbb{F}_2^{2k}$ размерности $\dim U - 1$ или $\dim U - 2$, для которого верно $f \oplus \mathrm{Ind}_L \in \mathcal{B}_{2k}$.

Следствие 2. Пусть для $f \in \mathcal{B}_{2k}$ и любого аффинного подпространства $L \subseteq \mathbb{F}_2^{2k}$, такого, что $\dim L \in \{k, k+1, \ldots, k+t-1\}$, $t \in \mathbb{N}$, справедливо $f \oplus \mathrm{Ind}_L \notin \mathcal{B}_{2k}$. Тогда для бент-функции

$$g(x_1, \ldots, x_{2k+2n}) = f(x_1, \ldots, x_{2k}) \oplus x_{2k+1}x_{2k+2} \oplus \ldots \oplus x_{2k+2n-1}x_{2k+2n}, \quad n \in \mathbb{N},$$

и любого аффинного подпространства $L' \subseteq \mathbb{F}_2^{2k+2n}$, такого, что $\dim L' \in \{k+n, k+n+1, \ldots, k+n+t-1\}$, справедливо $g \oplus \mathrm{Ind}_{L'} \notin \mathcal{B}_{2k+2n}$.

Следствие 3. Существует бент-функция f от $2k$ переменных, $2k \geqslant 10$, такая, что для любого аффинного подпространства $L \subseteq \mathbb{F}_2^{2k}$, $\dim L \leqslant k+3$, справедливо $f \oplus \mathrm{Ind}_L \notin \mathcal{B}_{2k}$.

ЛИТЕРАТУРА

1. *Rothaus O.* On bent functions // J. Combin. Theory. Ser. A. 1976. V. 20. No. 3. P. 300–305.
2. *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.
3. *Tokareva N. N.* Bent Functions, Results and Applications to Cryptography. Acad. Press. Elsevier, 2015.
4. *Carlet C.* Two new classes of bent functions // LNCS. 1994. V. 765. P. 77–101.
5. *Leander G. and McGuire G.* Construction of bent functions from near-bent functions // J. Combin. Theory. Ser. A. 2009. V. 116. No. 4. P. 960–970.
6. *Canteaut A., Daum M., Dobbertin H., and Leander G.* Finding nonnormal bent functions // Discr. Appl. Math. V. 154. No. 2. P. 202–218.