4. *Буров Д. А.* О существовании нелинейных инвариантов специального вида для раундовых преобразований XSL-алгоритмов // Дискретная математика. 2021. Т. 33. № 2. С. 31–45.
5. *Nyberg K.* Differentially uniform mappings for cryptography // LNCS. 1994. V. 765. P. 245–265.
6. *Carlet C.* Open questions on nonlinearity and on APN functions // LNCS. 2015. V. 9061. P. 83–107.
7. *Kolomeec N. and Bykov D.* On the Image of an Affine Subspace under the Inverse Function within a Finite Field. arXiv preprint arXiv:2206.14980. `https://arxiv.org/abs/2206.14980`. 2022.
8. *Коломеец Н. А., Быков Д. А.* Об инвариантных подпространствах функций, аффинно эквивалентных обращению элементов конечного поля // Прикладная дискретная математика. Приложение. 2022. № 15. С. 5–8.
9. *Charpin P.* Normal Boolean functions // J. Complexity. 2004. V. 20. No. 2–3. P. 245–265.
10. *Городилова А. А.* Характеризация почти совершенно нелинейных функций через подфункции // Дискретная математика. 2015. Т. 27. № 3. С. 3–16.
11. *Canteaut A., Carlet C., Charpin P., and Fontaine C.* On cryptographic properties of the cosets of R(1, m) // IEEE Trans. Inform. Theory. 2001. V. 47. P. 1494–1513.
12. *Carlet C. and Feukoua S.* Three parameters of Boolean functions related to their constancy on affine spaces // Adv. Math. Commun. 2020. V. 14. No. 4. P. 651–676.

УДК 519.7 DOI 10.17223/2226308X/16/7

МАТРИЦЫ ГРАМА БЕНТ-ФУНКЦИЙ И СВОЙСТВА ПОДФУНКЦИЙ КВАДРАТИЧНЫХ САМОДУАЛЬНЫХ БЕНТ-ФУНКЦИЙ[1]

А. В. Куценко

Булева фунция от чётного числа переменных n называется бент-функцией, если она имеет спектр Уолша — Адамара, состоящий из чисел $\pm 2^{n/2}$. Бент-функция называется самодуальной, если она совпадает со своей дуальной бент-функцией. Ранее автором было сформулировано достаточное условие того, что подфункции от $n-2$ переменных самодуальной бент-функции от n переменных, полученные фиксацией первых двух переменных, являются бент-функциями. В настоящей работе доказано, что для квадратичных самодуальных бент-функций данное условие при $n \geqslant 6$ не является необходимым. Введено понятие «матрица Грама бент-функции», установлен общий вид матрицы Грама бент-функции и дуальной к ней функции. Доказано, что если матрица Грама бент-функции от n переменной является необратимой, её подфункции от $n-2$ переменных, полученные фиксацией первых двух переменных, являются бент-функциями. Установлено, что в этом случае подфункции дуальной к ней функции также являются бент-функциями.

Ключевые слова: *самодуальная бент-функция, подфункция, матрица Грама, квадратичная бент-функция, конкатенация бент-функций.*

Через $\mathbb{F}_2^n$ обозначим линейное пространство всех двоичных векторов длины n над полем $\mathbb{F}_2$. *Булевой функцией* от n переменных называется отображение вида $\mathbb{F}_2^n \to \mathbb{F}_2$. Множество всех булевых функций от n переменных обозначается через $\mathcal{F}_n$. *Характеристическим вектором* (характеристической последовательностью) булевой функ-

[1]Работа выполнена в рамках госзадания ИМ СО РАН (проект № FWNF-2022-0018).

ции $f \in \mathcal{F}_n$ называется вектор

$$F \equiv (-1)^f = \left((-1)^{f(0)}, (-1)^{f(1)}, \ldots, (-1)^{f(2^n-1)}\right) \in \{\pm 1\}^{2^n},$$

где $(f(0), f(1), \ldots, f(2^n-1)) \in \mathbb{F}_2^{2^n}$ — вектор значений функции f. Каждая булева функция от n переменных может быть единственным образом представлена в виде многочлена над полем $\mathbb{F}_2$:

$$f(x_1, x_2, \ldots, x_n) = \bigoplus_{i_1, i_2, \ldots i_n \in \mathbb{F}_2} a_{i_1 i_2 \ldots i_n} x_1^{i_1} x_2^{i_2} \cdot \ldots \cdot x_n^{i_n}.$$

Здесь $a_z \in \mathbb{F}_2$ для всех $z \in \mathbb{F}_2^n$ (с соглашением $0^0 = 1$). Данное представление называется *многочленом Жегалкина* булевой функции f. Степенью $\deg(f)$ функции f называется максимальная из степеней слагаемых, входящих в многочлен Жегалкина с ненулевыми коэффициентами. Если $\deg(f) = 2$, функция называется *квадратичной*.

Для каждой пары $x, y \in \mathbb{F}_2^n$ через $\langle x, y \rangle$ обозначим значение $\bigoplus_{i=1}^{n} x_i y_i$. *Преобразованием Уолша — Адамара* булевой функции f от n переменных называется целочисленная функция $W_f : \mathbb{F}_2^n \to \mathbb{Z}$, заданная равенством

$$W_f(y) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus \langle x, y \rangle}, \quad y \in \mathbb{F}_2^n.$$

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

Изучению данного подкласса бент-функций посвящено множество работ. В частности, в [2–4] исследован вопрос аффинной классификации самодуальных бент-функций от $n \leqslant 8$ переменных, а также квадратичных самодуальных бент-функций относительно преобразований, сохраняющих (анти-)самодуальность. Конструкции самодуальных бент-функций представлены в работах [5–7]. Обзор известных метрических свойств приведён в [8].

Известно, что все подфункции от $n-2$ переменных бент-функции от n переменных имеют одинаковые спектры Уолша — Адамара [9]. Следовательно, либо все подфункции являются бент-функциями, либо $W_f(y) \in \left\{0, \pm 2^{(n+2)/2}\right\}$ для каждого $y \in \mathbb{F}_2^n$ (то есть все подфункции — почти бент-функции), либо их спектры Уолша — Адамара состоят из чисел 0, $\pm 2^{(n-2)/2}$, $\pm 2^{n/2}$.

Далее для булевой функции f от n переменных через (f_0, f_1, f_2, f_3) будем обозначать разложение её вектора значений на четыре подвектора, являющихся векторами значений её подфункций от $n-2$ переменных, полученных фиксацией первых двух переменных. Случай, когда данные подфункции являются бент-функциями, ведёт, в свою очередь, к итеративной конструкции бент-функции, вектор значений которой есть (f_0, f_1, f_2, f_3). В [10] найдены необходимые и достаточные условия, накладываемые на подфункции f_i, $i = 0, \ldots, 3$. В работах [11, 12] данные подфункции рассмотрены для случая, когда f является самодуальной бент-функцией.

1. Линейная независимость характеристических векторов подфункций квадратичной самодуальной бент-функции

В работе [12] доказано:

Теорема 1 [12]. Если характеристические векторы подфункций f_0, f_1, f_2, f_3 самодуальной бент-функции f линейно зависимы, то данные подфункции являются бент-функциями.

Этот результат описывает достаточное условие того, что все подфункции самодуальной бент-функции, полученные фиксацией первых двух переменных, являются бент-функциями. При этом для случая $n = 4$ данное условие также является необходимым. Хорошо известно, что все (самодуальные) бент-функции от 4 переменных являются квадратичными, что позволило обозначить следующий вопрос: является ли линейная зависимость характеристических векторов необходимым условием для *квадратичных* самодуальных функций?

Ответ на данный вопрос даёт следующее

Утверждение 1. Для каждого чётного $n \geqslant 6$ существуют квадратичные самодуальные бент-функции от n переменных, подфункции которых образуют линейно независимые множества характеристических векторов.

Таким образом, обращение теоремы 1 не имеет места при $n \geqslant 6$ и для квадратичных самодуальных бент-функций, то есть линейная зависимость характеристических векторов не является необходимым условием и, как и в случае без ограничения на степень, обеспечивает лишь достаточное условие того, что подфункции f_0, f_1, f_2, f_3 являются бент-функциями.

2. Матрица Грама произвольной бент-функции

Пусть $f \in \mathcal{B}_n$. *Матрицей Грама* $\mathrm{Gram}(f) = \left(g_{ij}\right)$ функции f назовём квадратную матрицу размера 4×4, элементами которой являются числа

$$g_{ij} = \sum_{x \in \mathbb{F}_2^{n-2}} (-1)^{f_i(x) \oplus f_j(x)}, \quad i, j = 0, 1, 2, 3,$$

которые являются скалярными произведениями характеристических векторов её подфункций.

Общий вид матриц Грама бент-функции и дуальной к ней описывает следующая

Теорема 2. Матрицы Грама бент-функции f от n переменных и дуальной к ней функции $\widetilde{f}$ имеют вид

$$\mathrm{Gram}(f) = \begin{pmatrix} 2^{n-2} & b & c & -a \\ b & 2^{n-2} & a & -c \\ c & a & 2^{n-2} & -b \\ -a & -c & -b & 2^{n-2} \end{pmatrix}, \quad \mathrm{Gram}\left(\widetilde{f}\right) = \begin{pmatrix} 2^{n-2} & c & b & -a \\ c & 2^{n-2} & a & -b \\ b & a & 2^{n-2} & -c \\ -a & -b & -c & 2^{n-2} \end{pmatrix}$$

для некоторых целых чисел a, b, c, таких, что

$$-2^{n-2} + |b + c| \leqslant a \leqslant 2^{n-2} - |b - c|.$$

Определители данных матриц совпадают, в частности, для f определитель имеет вид

$$\mathrm{Gramian}(f) = \left(2^{n-2} - a + b - c\right)\left(2^{n-2} - a - b + c\right)\left(2^{n-2} + a - b - c\right)\left(2^{n-2} + a + b + c\right).$$

Теорема 1 в терминах матриц Грама означает, что если матрица Грама самодуальной бент-функции являтся необратимой, то подфункции f_0, f_1, f_2, f_3 являются бент-функциями. Другими словами, для самодуальных бент-функций равенство $\mathrm{Gramian}(f) = 0$ влечёт тот факт, что указанные подфункции являются бент-функциями. Данный результат можно обобщить так:

Теорема 3. Если характеристические векторы подфункций f_0, f_1, f_2, f_3 бент-функции f линейно зависимы, то данные подфункции являются бент-функциями. Бент-функциями являются также подфункции дуальной функции $\widetilde{f}$.

Таким образом, данное утверждение позволяет получить достаточное условие того, что подфункции рассматриваемой бент-функции также являются бент-функциями и, кроме того, отображение дуальности сохраняет их максимальную нелинейность.

ЛИТЕРАТУРА

1. *Rothaus O.* On bent functions // J. Combin. Theory. Ser. A. 1976. V. 20. No. 3. P. 300–305.
2. *Carlet C., Danielsen L. E., Parker M. G., and Solé P.* Self-dual bent functions // Int. J. Inform. Coding Theory. 2010. V. 1. P. 384–399.
3. *Hou X.-D.* Classification of self dual quadratic bent functions // Des. Codes Cryptogr. 2012. V. 63. No. 2. P. 183–198.
4. *Feulner T., Sok L., Solé P., and Wassermann A.* Towards the classification of self-dual bent functions in eight variables // Des. Codes Cryptogr. 2013. V. 68. No. 1. P. 395–406.
5. *Luo G., Cao X., and Mesnager S.* Several new classes of self-dual bent functions derived from involutions // Cryptogr. Commun. 2019. V. 11. No. 6. P. 1261–1273.
6. *Li Y., Kan H., Mesnager S., et al.* Generic constructions of (Boolean and vectorial) bent functions and their consequences // IEEE Trans. Inform. Theory. 2022. V. 68. No. 4. P. 2735–2751.
7. *Su S. and Guo X.* A further study on the construction methods of bent functions and self-dual bent functions based on Rothaus's bent function // Des. Codes Cryptogr. 2023. V. 91. No. 4. P. 1559–1580.
8. *Kutsenko A. V. and Tokareva N. N.* Metrical properties of the set of bent functions in view of duality // Прикладная дискретная математика. 2020. № 49. С. 18–34.
9. *Canteaut A. and Charpin P.* Decomposing bent functions // IEEE Trans. Inf. Theory. 2003. V. 49. No. 8. P. 2004–2019.
10. *Preneel B., Van Leekwijck W., Van Linden L., et al.* Propagation characteristics of Boolean functions // LNCS. 1990. V. 473. P. 161–173.
11. *Kutsenko A.* Metrical properties of self-dual bent functions // Des. Codes Cryptogr. 2020. V. 88. No. 1. P. 201–222.
12. *Куценко А. В.* Свойства подфункций самодуальных бент-функций // Прикладная дискретная математика. Приложение. 2022. № 15. С. 26–30.

УДК 519.7 DOI 10.17223/2226308X/16/8

ПОСТРОЕНИЕ ПОДСТАНОВКИ НА $\mathbb{F}_2^n$ НА ОСНОВЕ ОДНОЙ БУЛЕВОЙ ФУНКЦИИ

И. А. Панкратова, А. А. Медведев

Приведены некоторые необходимые условия того, что векторная булева функция, координаты которой получены из одной булевой функции с помощью перестановок переменных, является подстановкой.

Ключевые слова: *подстановки, векторные булевы функции.*