Список литературы

1. Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А. Теория кодов, исправляющих ошибки. — М.: Связь, 1979. — 744 с.

2. Ben-Sasson E., Sudan M. Robust locally testable codes and products of codes // Random Structures & Algorithms. — 2006. — Vol. 28, no. 4. — P. 387–402.

3. Dinur I., Evra S., Livne R., Lubotzky A., Mozes S. Locally Testable Codes with constant rate, distance, and locality // ArXiv e-prints. — 2021. — https://arxiv.org/abs/2111.04808

4. Panteleev P. A., Kalachev G. V. Asymptotically good quantum and locally testable classical ldpc codes // ArXiv e-prints. — 2021. — https://arxiv.org/abs/2111.03654

5. Dinur I., Sudan M., Wigderson A. Robust local testability of tensor products of LDPC codes // Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques. — 2006. — P. 304–315.

6. Polishchuk A., Spielman D. Nearly linear size holographic proofs // 26th ACM Symp. on Theory of Computing. — 1994. — P. 194–203.

7. Leverrier A., Zémor G. Quantum Tanner codes // ArXiv e-prints. — 2022. — https://arxiv.org/abs/2202.13641

DOI: 10.20948/dms-2022-84

НОВЫЕ КОНСТРУКЦИИ И НИЖНЯЯ ОЦЕНКА ЧИСЛА САМОДУАЛЬНЫХ БЕНТ-ФУНКЦИЙ

А. В. Куценко (Новосибирск)

В данной работе рассматриваются бент-функции — максимально нелинейные булевы функции от чётного числа переменных. Они представляют большой интерес для теоретических исследований и имеют приложения в ряде областей, включая алгебру, теорию кодирования и криптографию. Данные математические объекты впервые изучались в 60-х годах XX века, понятие *бент-функции* было введено О. Ротхаусом позднее в работе [1]. Известно, что функции,

обладающие аналогичными свойствами, в тот же период времени исследовались отечественными учёными В. А. Елисеевым и О. П. Степченковым [2].

Через $\mathbb{F}_2^n$ обозначим линейное пространство всех двоичных векторов длины n над полем $\mathbb{F}_2$. Для каждой пары $x, y \in \mathbb{F}_2^n$ через $\langle x, y\rangle$ обозначим значение $\bigoplus\limits_{i=1}^{n} x_i y_i$, где операция $\oplus$ есть *сложение по модулю* 2. *Булевой функцией* от n переменных называется отображение вида $\mathbb{F}_2^n \to \mathbb{F}_2$. *Преобразованием Уолша — Адамара* булевой функции f от n переменных называется целочисленная функция $W_f : \mathbb{F}_2^n \to \mathbb{Z}$, заданная равенством $W_f(y) = \sum\limits_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus \langle x, y\rangle}$, где $y \in \mathbb{F}_2^n$.

Булева функция f от чётного числа переменных n называется *бент-функцией*, если $|W_f(y)| = 2^{n/2}$ для каждого $y \in \mathbb{F}_2^n$. Для множества бент-функций от n переменных используется обозначение $\mathcal{B}_n$. Для каждой бент-функции f из соотношения $W_f(y) = (-1)^{\widetilde{f}(y)} 2^{n/2}$, $y \in \mathbb{F}_2^n$ однозначным образом определяется *дуальная* к ней булева функция $\widetilde{f}$. Дуальная функция также является бент-функцией. Бент-функция f называется *самодуальной*, если $f = \widetilde{f}$. Множество самодуальных бент-функций от n переменных обозначается через $\mathcal{SB}_n^+$. Подробную информацию о классе бент-функций, включая известные результаты, а также открытые проблемы, можно найти в монографии [3].

Отметим, что характеристические векторы самодуальных бент-функций являются собственными векторами матрицы Сильвестра — Адамара, имеющей приложения в комбинаторике, теории сигналов и квантовых вычислениях. Описание класса самодуальных бент-функций является открытой проблемой, исследованию которой посвящён ряд работ. В частности, в работе [4] получен ряд конструкций, а также приведена аффинная классификация самодуальных бент-функций от малого числа переменных относительно преобразования, сохраняющего самодуальность. В статье [5] приведена классификация всех квадратичных самодуальных бент-функций. Аффинную классификацию квадратичных и кубических самодуальных бент-функций от 8 переменных можно найти в работе [6]. В работах [7, 8] представлены новые конструкции самодуальных бент-функций.

В настоящей работе предложены новые конструкции, а также получена новая итеративная нижняя оценка числа самодуальных

бент-функций. Описание данных конструкций приводится через их векторы значений, формируемые с помощью конкатенации векторов знчений бент-функций от $n-4$ переменных. Пусть h — бент-функция от $n-4$ переменных, f — самодуальная и g — антисамодуальная бент-функции от $n-4$ переменных. Далее приведём описание конструкций, используя конкатенацию векторов значений функций h, f, g:

- конструкция **K1**: вектор значений функции имеет вид

$$\big(h, g, g\oplus 1, h, \widetilde{h}, f, f\oplus 1, \widetilde{h}, \widetilde{h}, f\oplus 1, f, \widetilde{h}, h\oplus 1, g, g\oplus 1, h\oplus 1\big).$$

  Можно показать, что все подфункции от $n-2$ переменных, полученные фиксацией первых двух координат, являются бент-функциями;
- конструкция **K2**: вектор значений функции имеет вид

$$\big(h, g, \widetilde{h}, f, g\oplus 1, h, f\oplus 1, \widetilde{h}, \widetilde{h}, f\oplus 1, h\oplus 1, g, f, \widetilde{h}, g\oplus 1, h\oplus 1\big).$$

  Все подфункции от $n-2$ переменных, полученные фиксацией первых двух координат, являются бент-функциями тогда и только тогда, когда $h\oplus\widetilde{h}\oplus f\oplus g=0$. Таким образом, данная конструкция позволяет построить функции не представимые в виде конкатенации четырёх бент-функций от $n-2$ переменных;
- конструкция **K3**: вектор значений функции имеет вид

$$\big(h, h\oplus 1, \widetilde{h}, \widetilde{h}, h, h, \widetilde{h}\oplus 1, \widetilde{h}, \widetilde{h}, \widetilde{h}, h\oplus 1, h, \widetilde{h}\oplus 1, \widetilde{h}, h\oplus 1, h\oplus 1\big).$$

  Как и в конструкции **K1**, можно показать, что все подфункции от $n-2$ переменных, полученные фиксацией первых двух координат, являются бент-функциями.

Утверждение. *Конструкции **K1**, **K2** и **K3** описывают векторы значений самодуальных бент-функций от n переменных.*

Данные конструкции позволяют построить непересекающиеся множества самодуальных бент-функций. Анализ данных множеств, а также их пересечений с множествами функций, порождаемых ранее известными итеративными конструкциями, позволяет получить новую итеративную нижнюю оценку числа самодуальных бент-функций.

Теорема. *Число самодуальных бент-функций от $n\geqslant 6$ переменных не меньше, чем*

$$|\mathcal{B}_{n-2}|+\left|\mathcal{SB}^{+}_{n-2}\right|^2+|\mathcal{B}_{n-4}|\left(2\left|\mathcal{SB}^{+}_{n-4}\right|^2+1\right)-2\left|\mathcal{SB}^{+}_{n-4}\right|.$$

Таким образом, предыдущая известная итеративная нижняя оценка изменяется на слагаемое, соответствующее самодуальным бент-функциям от $n-4$ переменных.

Работа выполнена в рамках государственного задания ИМ СО РАН (проект № FWNF-2022-0018).

Список литературы

1. Rothaus O. On bent functions // J. Combin. Theory. Ser. A. — 1976. — V. 11, no. 5. — P. 300–305.

2. Кузьмин А. С., Марков В. Т., Нечаев А. А., Шишкин В. А., Шишков А. Б. Бент-функции и гипербент-функции над полем из 2^l элементов // Пробл. передачи информации. — 2008. — Т. 44, вып. 1. — С. 15–37.

3. Tokareva N. Bent Functions: Results and Applications to Cryptography. — London: Acad. Press, 2015.

4. Carlet C., Danielsen L. E., Parker M. G., Solé P. Self dual bent functions // Int. J. Inform. Coding Theory. — 2010. — V. 1 — P. 384–399.

5. Hou X.-D. Classification of self dual quadratic bent functions // Des. Codes Cryptogr. — 2012. — V. 62, no. 2. — P. 183–198.

6. Feulner T., Sok L., Solé P., Wassermann A. Towards the classification of self-dual bent functions in eight variables // Des. Codes Cryptogr. — 2013. — V. 68, no. 1. — P. 395–406.

7. Luo G., Cao X., Mesnager S. Several new classes of self-dual bent functions derived from involutions // Cryptogr. Commun. — 2019. — V. 11, no. 6. — P. 1261–1273.

8. Li Y., Kan H., Mesnager S., Peng J., How Tan C., Zheng L. Generic Constructions of (Boolean and Vectorial) Bent Functions and Their Consequences // IEEE Trans. Inform. Theory. — 2022. — V. 68, no. 4. — P. 2735–2751.

DOI: 10.20948/dms-2022-85

ПОСТРОЕНИЕ ДУАЛЬНОГО АГ-КОДА МАЛОЙ РАЗМЕРНОСТИ В ЭЛЛИПТИЧЕСКОМ СЛУЧАЕ

Е. С. Малыгина (Калининград)

Пусть $F/\mathbb{F}_p$ — функциональное поле, определенное над конечным полем $\mathbb{F}_p$, где p — простое число. Будем считать, что поле F задается