ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 27 МАТЕМАТИКИ Выпуск 1
2020

И. П. Баксова, Ю. В. Таранников (Москва, Лаб. ТВП, Московский Государственный Университет им. М. В. Ломоносова). **Об одной конструкции бент-функций.**

УДК 519.115.4

Резюме: Предложена новая конструкция бент-функций, обобщающая семейство бент-функций Майораны-Мак-Фарланда, в рамках которой получены оценки числа порождаемых бент-функций.

Ключевые слова: бент-функция, семейство Майораны-Мак-Фарланда, оценки.

Введение. Задачи описания общего вида бент-функций, зависящих от произвольного числа переменных $n \in \mathbb{N}$, и оценки их числа являются вичислительно сложными и в настоящее время остаются нерешенными. Так, например, число бент-функций от $n = 2, 4, 6, 8$ переменных составляет

$$8, \quad 896, \quad 5425430528 \simeq 2^{32,3}, \quad 2^9 \times 19388786966002806700348801024 0 \simeq 2^{106,29}$$

соответственно, а уже при $n \geqslant 10$ (с учетом такой скорости роста значения мощности) имеют место только очень грубые оценки [**?**].

Так, наибольшим по мощности считается семейство бент-функций Майораны-Мак-Фарланда [**?**], содержащее $2^{n/2}! \cdot 2^{2^{n/2}}$ функций. При этом при $n \to \infty$ справедлива асимптотическая эквивалентность

$$\log_2 \left(2^{n/2}! \cdot 2^{2^{n/2}}\right) \sim \frac{n}{2} \cdot 2^{n/2}.$$

Следует отметить, что добавление аффинно эквивалентных функций увеличивает мощность класса, но не влияет на асимптотику логарифма.

В настоящей работе предлагается новая конструкция бент-функций и делаются оценки числа порождаемых этой конструкцией бент-функций в зависимости от выбора вспомогательного параметра.

О п р е д е л е н и е 1. *Преобразованием Уолша* булевой функции $f\colon \mathbf{F}_2^n \to \mathbf{F}_2$ называется целочисленная функция $W_f(u) = \sum\limits_{x \in \mathbf{F}_2^n} (-1)^{f(x)+\langle u,x\rangle}$, где $\langle u, x\rangle = u_1x_1 + \cdots + u_nx_n$ — скалярное произведение векторов $u, x \in \mathbf{F}_2^n$.

Для каждого $u \in \mathbf{F}_2^n$ значение $W_f(u)$ называется *коэффициентом Уолша* или *спектральным коэффициентом.*

Множество $\{W_f(u),\ u \in \mathbf{F}_2^n\}$ всех 2^n коэффициентов Уолша называются *спектром* функции $f\colon \mathbf{F}_2^n \to \mathbf{F}_2$.

О п р е д е л е н и е 2. Булева функция называется *бент-функцией*, если ее коэффициенты Уолша на всех наборах равны $\pm 2^{n/2}$.

Бент-функции существуют для всех четных n. Бент-функция — это функция с максимально возможной нелинейностью $2^{n-1} - 2^{(n/2)-1}$ среди всех функций от n переменных для четного n.

О п р е д е л е н и е 3. Булева функция $f\colon \mathbf{F}_2^n \to \mathbf{F}_2$ называется *платовидной*, если ее коэффициенты Уолша принимают ровно три возможных значения: 0 и $\pm 2^c$ для некоторого $c \in \left[\frac{n}{2}, n\right]$.

1. Описание конструкции (К). Рассмотрим $\mathbf{F}_2^n$ — линейное n-мерное векторное пространство над $\mathbf{F}_2$, $n \in \mathbb{N}$.

Пусть далее $n = n_1 + n_2$, $n_1 \leqslant n_2$, где n_1 и n_2 — целые неотрицательные числа одной четности. Рассмотрим разложение n-местной булевой функции $f\colon \mathbf{F}_2^n \to \mathbf{F}_2$ по первым n_1 переменным:

$$f(x_1, \ldots, x_n) = \bigoplus_{(\sigma_1,\ldots,\sigma_{n_1}) \in \mathbf{F}_2^{n_1}} \left(\left(\prod_{i=1}^{n_1} (x_i \sim \sigma_i) \right) f(\sigma_1, \ldots, \sigma_{n_1}, x_{n_1+1}, \ldots, x_{n_1+n_2}) \right)$$
$$= \overline{x}_1 \cdot \ldots \cdot \overline{x}_{n_1-1} \overline{x}_{n_1} f_1(x) \oplus \overline{x}_1 \cdot \ldots \cdot \overline{x}_{n_1-1} x_{n_1} f_2(x)$$
$$\oplus\, \overline{x}_1 \cdot \ldots \cdot x_{n_1-1} \overline{x}_{n_1} f_3(x) \oplus x_1 \cdot \ldots \cdot x_{n_1-1} x_{n_1} f_{2^{n_1}}(x),$$

где $f_i = f\left(\alpha_1^{(i)}, \ldots, \alpha_{n_1}^{(i)}, x_{n_1+1}, \ldots, x_n\right)$, а $\left(\alpha_1^{(i)}, \ldots, \alpha_{n_1}^{(i)}\right)$ совпадает с i-м набором $(\sigma_1, \ldots, \sigma_{n_1})$ в упорядоченном в лексикографическом порядке множестве всех двоичных наборов длины n_1.

Пространство $\mathbf{F}_2^{n_2}$ от правых n_2 переменных разбиваем на 2^{n_1} классов смежности линейных подпространств размерности $n_2 - n_1$ каждый. Пусть C_i — i-й класс смежности в разбиении, $C_i \subseteq \mathbf{F}_2^{n_2}$. Класс C_i объявляется носителем спектра своей платовидной подфункции f_i.

Подфункция f_i задается следующим образом: к произвольной бент-функции g_i от $n_2 - n_1$ переменных добавим n_1 фиктивных переменных и осуществим аффинное преобразование спектра $\mathbf{F}_2^{n_2} \to \mathbf{F}_2^{n_2}$ так, чтобы носитель спектра функции g_i перешел в C_i (подробнее об аффинных преобразованиях носителя спектра см. §2 в [**?**]).

Теорема 1. *Конструкция К задает бент-функцию.*

Из указанного выше описания конструкции К вытекает следующий результат.

Теорема 2. *Пусть $n \in \mathbb{N}$ — четно. Тогда для произвольного $n_1 \leqslant \frac{n}{2}$ число L бент-функций от n переменных, порожденных конструкцией К, составляет*

$$L = \left(b_{n_2-n_1}\right)^{2^{n_1}} \cdot N_{n_2}^{n_2-n_1}, \tag{1}$$

где $n_2 = n - n_1$, $b_{n_2-n_1}$ — число бент-функций от $n_2 - n_1$ переменных, $N_{n_2}^{n_2-n_1}$ — число упорядоченных разбиений $\mathbf{F}_2^{n_2}$ на 2^{n_1} классов смежности линейных подпространств размерности $n_2 - n_1$.

Замечание 1. Семейство функций Майораны-Мак-Фарланда представляет собой частный случай конструкции К при $n_1 = n_2 = \frac{n}{2}$. Действительно, $b_0 = 2$, а $N_{n/2}^0 = 2^{n/2}!$ Отсюда

$$L = 2^{2^{n/2}} \cdot 2^{n/2}! \quad и \quad \log_2 L \sim \frac{n}{2} \cdot 2^{n/2}.$$

Величина $\frac{n}{2} \cdot 2^{n/2}$ является ориентиром для дальнейшего исследования: если при некотором параметре n_1 получится верхняя оценка на $\log_2 L$ асимптотически меньше, чем $\frac{n}{2} \cdot 2^{n/2}$, то этот случай можно считать неинтересным в силу малого числа порождаемых бент-функций.

Логарифмируя (1), получаем:

$$\log_2 L = 2^{n_1} \log_2 b_{n_2-n_1} + \log_2 N_{n_2}^{n_2-n_1}. \tag{2}$$

Теорема 3. *Пусть $n \in \mathbb{N}$. Тогда при произвольных $n_1, n_2\colon n_1 \leqslant n_2$, $n_1 + n_2 = n$ для числа $N_{n_2}^{n_2-n_1}$ упорядоченных разбиений $\mathbf{F}_2^{n_2}$ на 2^{n_1} классов смежности линейных подпространств размерности $n_2 - n_1$ справедливо неравенство*

$$\log_2 N_{n_2}^{n_2-n_1} < (n_1 + 1)(n_2 - n_1 + 1)\, 2^{n_1}. \tag{3}$$

Замечание 2. Из (3) следует, что если n_1 недостаточно близко к $\frac{n}{2}$, то $\log_2 N_{n_2}^{n_2-n_1} = o\left(\frac{n}{2}\cdot 2^{n/2}\right)$. Кроме того, если $n_1 \leqslant \frac{n}{2}-3$, то $\log_2 N_{n_2}^{n_2-n_1} < \frac{n}{2}\cdot 2^{n/2}$.

СПИСОК ЛИТЕРАТУРЫ

1. *Таранников Ю. В.* О значениях аффинного ранга носителя спектра платовидной функции. — Дискретн. матем., 2006, т. 18, в. 3, с. 120–137; Discrete Math. Appl., 2006, 16:4 p. 401–421.
2. *Логачёв О. А.*, *Сальников А. А.*, *Смышляев С. В.*, *Ященко В. В.* Булевы функции в теории кодирования и криптологии. М.: ЛЕНАНД, 2015.
3. *Токарева Н. Н.* Нелинейные булевы функции: бент-функции и их обощения. Издательство LAP LAMBERT Academic Publishing (Saarbrucken, Germany), 2011. ISBN: 978-3-8433-0904-2. 180 с.

UDC 519.115.4

Baksova I. P., ***Tarannikov Y. V.*** (Moscow, TVP Laboratory, Lomonosov Moscow State University)**. On some construction of bent functions**

Abstract: A new construction of bent functions generalizing the Majorana-McFarland class of bent functions is proposed. Estimates for the number of generated bent functions are obtained.

Keywords:bent function, Majorana-McFarland class, bounds.