А. Б. Ш и ш к о в, **А. В. З я з и н** (Москва, МИРЭА(ТУ)). **Об индексе многочлена, представляющего бент-функцию над простым полем нечетной характеристики.**

Интерес к булевым функциям, находящимся на наибольшем расстоянии, с точки зрения метрики Хэмминга, от класса аффинных функций, появился у специалистов по теории кодирования и криптографии в 70ые годы прошлого века. Для таких функций О. С. Ротхауз [1] ввел термин «бент-функция». Впоследствии обобщение этого понятия было произведено для функций над кольцами вычетов [2], непростыми полями [3] и произвольными конечными абелевыми группами [4, 5].

Несмотря на то, что в последнее время появилось достаточно большое количество работ, посвященных характеризации бент-функций, описанию некоторых классов бент-функций и их обобщений, задача полного описания этого класса функций даже в булевом случае остается нерешенной. Этим объясняется повышенное внимание к описанию всевозможных свойств бент-функций над различными алгебраическими структурами.

В этой работе мы введем понятие бент-функции над простым полем нечетной характеристики и опишем свойства некоторых представлений таких отображений. Введем необходимые обозначения. Пусть $P = Z_p$ — простое поле характеристики p. Пусть $F : P^n \to P$ — функция от n переменных над полем P. Коэффициенты Уолша–Адамара для функции F определим следующим образом:

$$C_\alpha^F = 1/p^n \sum_{x \in P^n} (\xi)^{F(x) - <x,\alpha>}$$

Здесь $< x, \alpha >= x_1a_1 + x_2a_2 + \cdots + x_na_n \bmod p$, $x = (x_1, \mathrm{E}, x_n)$, $\alpha = (a_1, \mathrm{E}, a_n) \in P^n$, ξ — примитивный корень из единицы степени p. Справедливы соотношения:

$$\xi^{F(x)} = \sum_{\alpha \in P^n} C_\alpha^F \xi^{<x,\alpha>}, \ \sum_{\alpha \in P^n} |C_\alpha^F|^2 = 1.$$

F — бент-функция, если для всех $\alpha \in P^n$

$$|C_\alpha^F| = p^{-n/2}.$$

При выборе фиксированного базиса поля $Q = GF(p^n)$ над полем P, функция F однозначно задается многочленом $\Phi(x)$ из кольца $Q[x]$ степени не выше $p^n - 1$.

Индекс нелинейности $\operatorname{ind}\Phi(x)$ *многочлена* $\Phi(x)$ *— максимальный индекс нелинейности его мономов*;

Индекс нелинейности монома ax^t — целочисленная сумма разрядов p-ичного разложения числа t:

$$t = t_0 + t_1p + \cdots + t_{n-1}p^{n-1} \Rightarrow \operatorname{ind} ax^t = t_0 + t_1 + \ldots + t_{n-1}.$$

Основным результатом работы является:

Теорема. *Если $\Phi(x)$ — многочлен, представляющий бент-функцию от n переменных над полем P, то* $\operatorname{ind}\Phi(x) \leqslant (p-1)(]n/2[+1) - 1$.

Работа выполнена при поддержке гранта Президента РФ НШ 4.2008.10

СПИСОК ЛИТЕРАТУРЫ

1. *Rothaus O. S.* On bent functions. — J. Comb. Theory, 1976, v. 20, p. 300–305.
2. *Kumar P. V.*, *Scholtz R. A.*, *Welch L. R.* Generalized Bent Functions and Their Properties. — J. Comb. Theory, 1985, Ser. A 40(1), p. 90–107.
3. *Амбросимов А. С.* Свойства бент-функций q-значной логики над конечными полями. — Дискретн. матем., 1994, т. 6, в. 3, с. 50–60

4. *Солодовников В. И.* Бент-функции из конечной абелевой группы в конечную абелеву группу. — Дискретн. матем., 2002, т. 14, в. 1, с. 99–113
5. *Логачев О. А.*, *Сальников А. А.*, *Ященко В. В.* Бент-функции на конечной абелевой группе. — Дискретн. матем., 1997, т. 9, в. 4, с. 3–20