УДК 512.62

НЕКОТОРЫЕ СВОЙСТВА q-ИЧНЫХ БЕНТ-ФУНКЦИЙ

В. А. Шишкин

Рассматриваются свойства бент-функций над полями характеристики 2. Расширен спектр значений параметров, при которых можно указать точные значения весовой структуры q-ичной бент-функции. Показано также, что если весовая структура q-ичной функции имеет специальный вид, то значение периода данной функции делится на определённую величину.

Ключевые слова: *бент-функция, период функции, уравнения в конечных полях.*

Пусть P — конечное поле мощности $q = 2^l$, $l \geqslant 1$, и Q — расширение степени n поля P. Будем рассматривать функции вида $F : Q \to P$. Пусть θ — примитивный элемент поля Q. Периодом функции F будем называть период последовательности $u(i) = F(\theta^i)$, $i \in \mathbb{N}_0$ [1]. Через $N_a(F)$ будем обозначать число решений в поле Q уравнения $F(x) = a$, $a \in P$. Набор чисел $\{N_a(F) : a \in P\}$ будем называть весовой структурой отображения F.

Существует несколько подходов к обобщению понятия бент-функции на случай q-ичных отображений [2]. Мы пользуемся определением q-ичной бент-функции, впервые предложенным в работе [3].

В [4] получен ряд результатов, характеризующих период и весовую структуру q-ичных бент-функций.

Теорема 1 [4]. Пусть $n > 2$ и функция F является бент-функцией. Тогда

$$N_a(f) = q^{n-1} + n_a q^{n/2-1},$$

где n_a принимает целые нечётные значения в интервале $[-(q-1), q-1]$.

Утверждение 1 [4]. Если $n > 2$ и F есть бент-функция, то её период t удовлетворяет неравенству $t \geqslant q^{n/2} - 1$.

Легко показать, что приведённые результаты справедливы и при $n = 2$.

В [4] также продемонстрировано, что при ряде значений параметров оказывается возможным указать точные значения весовой структуры бент-функции. В данной работе приводятся результаты дальнейших исследований в этом направлении.

Заметим, что если период t бент-функции удовлетворяет неравенству $t < q^n - 1$, то, ввиду утверждения 1, значение t делится либо на $q^{n/2} - 1$, либо на $q^{n/2} + 1$.

Теорема 2. Пусть период бент-функции F удовлетворяет неравенству $t < q^n - 1$ и $F(0) = c$. Тогда

1. Если период $F(x)$ делится на $q^{n/2} + 1$, то

$$\forall a \in P \backslash \{c\} \quad \left(N_a(F) = q^{n-1} - q^{n/2-1}\right),$$
$$N_c(F) = q^{n-1} + (q-1)q^{n/2-1}.$$

2. Если период $F(x)$ делится на $q^{n/2} - 1$, то

$$\forall a \in P \backslash \{c\} \quad \left(N_a(F) = q^{n-1} + q^{n/2-1}\right),$$
$$N_c(F) = q^{n-1} - (q-1)q^{n/2-1}.$$

Имеет место следующее утверждение, которое представляет в некотором роде обратный результат.

Утверждение 2. Пусть $\varepsilon \in \{-1, 1\}$ и весовая структура функции F для некоторого $c \in P$ описывается значениями

$$\forall a \in P \backslash \{c\} \quad \left(N_a(F) = q^{n-1} + \varepsilon q^{n/2-1}\right),$$
$$N_c(F) = q^{n-1} - \varepsilon(q-1)q^{n/2-1}.$$

Тогда значение периода функции F делится на величину $q^{n/2} - \varepsilon$.

Представленные утверждения позволяют в ряде случаев указать точные значения весовой структуры q-ичных бент-функций. Однако, как показывает следующее утверждение, область действия данных результатов существенно ограничена.

Утверждение 3. Пусть H — множество всех гомоморфизмов из группы $(Q, +)$ в группу $(P, +)$. Множество функций $\{F + h : h \in H\}$ содержит не более одной функции, период которой строго меньше $q^n - 1$.

Таким образом, среди бент-функций вида $F + h$ (где h — гомоморфизм соответствующих групп) не более одной функции может иметь период, значение которого удовлетворяет условиям теоремы 2.

ЛИТЕРАТУРА

1. *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 // Проблемы передачи информации. 2008. Т. 44. Вып. 1. С. 15–37.
2. *Токарева Н. Н.* Обобщения бент-функций. Обзор работ // Дискретн. анализ и исслед. операций. 2010. Т. 17. Вып. 1. С. 34–64.
3. *Солодовников В. И.* Бент-функции из конечной абелевой группы // Дискретная математика. 2002. Т. 14. Вып. 1. С. 99–113.
4. *Кузьмин А. С., Нечаев А. А., Шишкин В. А.* Бент- и гипербент-функции над конечным полем // Труды по дискретной математике. 2007. Т. 10. С. 86–111.

УДК 621.391: 519.728

О СРАВНЕНИИ НЕДООПРЕДЁЛЕННЫХ АЛФАВИТОВ[1]

Л. А. Шоломов

Представлены несколько подходов к сравнению недоопределённых алфавитов по силе и доказана их эквивалентность. Установлено, что введённые соотношения по силе полиномиально проверяемы.

Ключевые слова: *недоопределённый алфавит, равносильные алфавиты, энтропия недоопределённых данных, сложность по Колмогорову.*

Задан конечный алфавит $A_0 = \{a_i : i \in M\}$ *основных* символов. Каждому непустому $T \subseteq M$ соответствует *недоопределённый символ* a_T, *доопределением* которого считается всякий основной символ a_i, $i \in T$. Выделена система $\mathcal{T} \subseteq 2^M$ некоторых подмножеств $T \subseteq M$ и с ней связан *недоопредёленный алфавит* $A = \{a_T : T \in \mathcal{T}\}$.

Пусть помимо A_0 и A заданы основной алфавит $B_0 = \{b_j : j \in L\}$, недоопределённый алфавит $B = \{b_U : U \in \mathcal{U} \subseteq 2^L\}$ и соответствие $R_{AB} \subseteq A \times B$, указывающее,

[1]Работа поддержана ОНИТ РАН по программе фундаментальных исследований.